TABLA DE CONTENIDO PROCESO JCE-CCC-LPI-2024-0001
ESPECIFICACIÓN DE NÚMERO DE PÁGINA-FOLIO

3. DOCUMENTACIÓN TÉCNICA DEL CONSORCIO

índice original de la carpeta No. 2 ..... 2- 3 de 843

Plantilla (MATRIZ) enviada por la JCE “ELEGIBILIDAD” ..... 4- 7 de 843

Propuesta Técnica Consorcio “CÉDULA 4.0 RD” ..... 9-167 de 843

Cronograma ..... 168 de 843

Matriz de cumplimiento del pliego de condiciones Punto a Punto ..... 169-300 de 843

10 muestras de las tarjetas de Policarbonato ..... 301-302 de 843

Diseño de la CIE y de la CI..... 303-304 de 843

Presentación del Equipo del Fabricante de las Impresoras, el PKI y Mobile ID. ..... 305-309 de 843

Curriculum del Líder del Proyecto ..... 310-315 de 843

Curriculum del personal técnico certificado en tecnología de impresión de tarjetas de identidad localmente ..... 322-332 de 843

Curriculum del personal técnico en campo ..... 333-357 de 843

Acreditación de las Experiencias del consorcio – Consolidado de las Experiencias ..... 358-359 de 843

Experiencias Obligatorias ..... 360-405 de 843

Experiencias en proyecto de suministro de impresoras de documentos de identidad en policarbonato ....

Experiencias en proyecto de suministro de tarjetas de identidad electrónicas de policarbonato .....

Experiencias proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos .....

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica. .....

Experiencias Opcionales ..... 406-416 de 843

Experiencia en Identidades Móviles (Mobile ID).....

Experiencia de haber operado un proyecto de impresión de soluciones de identificación a nivel de gobierno .....

Experiencia en República Dominicana en proyectos de mantenimiento de tecnología en gobierno con al menos cinco (5) años de experiencia. .....

4. DOCUMENTACIÓN TÉCNICA DEL CONSORCIO – DOCUMENTACIÓN DE SOPORTE

Carta de Certificación de Propiedad y Manufactura de Impresoras, PKI y Mobile ID ..... 417-426 de 843

Declaración Jurada de no utilización de Materiales patentados en la Tarjeta de Policarbonato Con Chip Sin Contacto ..... 427-429 de 843

Ficha Técnica del Chip Sin Contacto ..... 430-436 de 843
Ficha Técnica del MiddleWare ..... 437-422 de 843
Certificaciones del Fabricante de las Tarjetas ..... 443 de 843
ISO INTERGRAF Nivel Gobierno .....444-449 de 843
ISO 27001:2022 .....449-454 de 843
ISO 14001:2015 .....455-460 de 843
ISO 9001-2015 .....461-466 de 843
Common Criteria EAL4+/ ISO 15408 (Características del Sistema Operativo y la Tarjeta) .....467-486 de 843
Common Criteria EAL5+ o Superior (Características del chip sin contacto) .....467-516 de 843
ISO 14443-1 .....517-544 de 843
ISO 14443-2 .....545-624 de 843
Prueba ISO de Durabilidad de la Tarjeta .....625-699 de 843
Carta Jurada de realización de Prueba ISO de Durabilidad de la Tarjeta .....700-705 de 843
Prueba ISO 18745-1 Resistencia .....706-739 de 843
Carta Jurada de realización de Prueba ISO 18745-1 Resistencia .....740-745 de 843
Certificaciones del Fabricante de las Impresoras, PKI y Mobile ID .....746 de 843
ISO 18013 iOS .....747-766 de 843
ISO 18013 Android .....767- 843 de 843
Carta Jurada de Certificación CMMI DEV5 .....794-802 de 843
EAL4+ .....811-816 de 843
ISO 30107-3 .....803-810 de 843
Brochures ..... 817 de 843
Brochures de las Impresoras .....818-820 de 843
Brochures Mobile ID.....821-823 de 843
Brochures Mobile la PKI .....824-827 de 843
Brochures de los Periféricos .....828-843 de 843

PROPUESTA TÉCNICA – DOCUMENTACIÓN ADMINISTRATIVA

CONSORCIO “CÉDULA 4.0 RD”

---

2 CARPETA

Documentación y Propuesta Técnica del Consorcio “CÉDULA 4.0 RD”

TABLA DE CONTENIDO PROCESO JCE-CCC-LPI-2024-0001

3. DOCUMENTACIÓN TÉCNICA DEL CONSORCIO

Plantilla (MATRIZ) enviada por la JCE .....

Propuesta Técnica Consorcio "CÉDULA 4.0 RD" 1

Matriz de cumplimiento del pliego de condiciones Punto a Punto 2

10 muestras de las tarjetas de Policarbonato 3

Diseño de la CIE y de la CI..... 4

Presentación del Equipo del Fabricante de las Impresoras, el PKI y Mobile ID. 5

Curriculum del Líder del Proyecto .....

Curriculum del personal técnico certificado en tecnología de impresión de tarjetas de identidad localmente .....

Curriculum del personal técnico en campo .....

Acreditación de las Experiencias del consorcio – Consolidado de las Experiencias 6

Experiencias Obligatorias ..... A

Experiencias en proyecto de suministro de impresoras de documentos de identidad en policarbonato .....

Experiencias en proyecto de suministro de tarjetas de identidad electrónicas de policarbonato .

Experiencias proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos .....

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica.....

Experiencias Opcionales ..... B

Experiencia en Identidades Móviles (Mobile ID).....

Experiencia de haber operado un proyecto de impresión de soluciones de identificación a nivel de gobierno .....

Experiencia en República Dominicana en proyectos de mantenimiento de tecnología en gobierno con al menos cinco (5) años de experiencia. .....

4. DOCUMENTACIÓN TÉCNICA DEL CONSORCIO – DOCUMENTACIÓN DE SOPORTE

Carta de Certificación de Propiedad y Manufactura de Impresoras, PKI y Mobile ID 7

Declaración Jurada de no utilización de Materiales patentados en la Tarjeta de Policarbonato Con Chip Sin Contacto 8

Ficha Técnica del Chip Sin Contacto 9

Ficha Técnica del MiddleWare 10

Certificaciones del Fabricante de las Tarjetas 11
ISO INTERGRAF Nivel Gobierno .....
ISO 27001:2022 .....
ISO 14001:2015 .....
ISO 9001-2015 .....
Common Criteria EAL4+/ ISO 15408 (Características del Sistema Operativo y la Tarjeta) .....
Common Criteria EAL5+ o Superior (Características del chip sin contacto) .....
ISO 14443-1 .....
ISO 14443-2 .....
Prueba ISO de Durabilidad de la Tarjeta .....
Carta Jurada de realización de Prueba ISO de Durabilidad de la Tarjeta .....
Prueba ISO 18745-1 Resistencia .....
Carta Jurada de realización de Prueba ISO 18745-1 Resistencia .....
Certificaciones del Fabricante de las Impresoras, PKI y Mobile ID 12
ISO 18013 iOS .....
ISO 18013 Android .....
Carta Jurada de Certificación CMMI DEV5 .....
EAL4+ .....
ISO 30107-3 .....
Brochures 13
Brochures de las Impresoras .....
Brochures Mobile ID .....
Brochures Mobile la PKI.....
Brochures de las Tarjetas.....
Brochures de los Periféricos .....

Plantilla (MATRIZ) enviada por la JCE – "ELEGIBILIDAD".

JCE-CCC-LPI-2024-0001

Se debe de rellenar el apartado cumple y no cumple, con la pagina del oferente donde lo cumple, así como comentarios adicionales si procede

Número		Cumple/No Cumple	Página del oferente	Comentarios
1	**REQUERIMIENTOS GENERALES**			
1.1	Deberán formalizar su inscripción (CON CARÁCTER OBLIGATORIO) mediante el llenado y presentación del Formulario FL-01 (Inscripción de Oferente), el cual se encuentra anexo al presente Pliego de Condiciones, y se podrá retirar en las oficinas del Comité de Compras y Contrataciones o descargarse de la página web de la Junta Central Electoral o del Portal Transaccional de la Dirección General de Contrataciones Públicas. El plazo para inscripción o registro de oferentes vence a las 4 horas de la tarde (4:00 P.M.) del día 17 de mayo del 2024. Capítulo VIII del Pliego. **(Repetido 4.4 de Credenciales y Propuestas).**	Si	CARPETA 1 SECCIÓN 2 -No.19.	Suministrado
1.2	El consorcio debe licitar como una sola entidad. Por lo tanto, los miembros del consorcio deben elegir al líder del consorcio para que lo represente. Numeral 5.4.1 del Pliego	Si	CARPETA 1 SECCIÓN 2 -No.20.	Se ha establecido en el Acuerdo Bajo Firma Privada la Representación del Consorcio por parte de Copy Solutions International S.A.
1.3	Ningún oferente (de tarjetas, de impresoras, de cédula digital, de ABIS) podrá presentar más de una Oferta para el Proyecto. Un oferente que licite individualmente o como miembro de un consorcio no tendrá derecho a presentar otra oferta ni individualmente ni como miembro de ningún Consorcio. Esta restricción no se aplica a los proveedores de materiales o equipos tales como equipos de infraestructura, dispositivos o consumibles. PARA ACREDITAR LA ELEGILIBILIDAD, EL OFERENTE DEBERÁ HACER UNA CARTA JURADA ASEGURANDO QUE SUS MIEMBROS SOLO PARTICIPA EN UN CONSORCIO EN ESTA LICITACIÓN. Numeral 5.4.1 del Pliego	Si	CARPETA 1 SECCIÓN 2 -No.25.	Suministrado
1.4	Al presentar su oferta mediante el Formulario FL-02 (Anexo 2), el oferente acepta el contenido del presente pliego y sus modificaciones posteriores incluyendo las respuestas a las preguntas durante el proceso de licitación. Numeral 5.4.1 del Pliego. **(Repetido 4.5 de Credenciales y Propuestas).**	Si	CARPETA 1 SECCIÓN 2 -No.21.	Entendemos, Aceptamos y Cumplimos.
1.5	El oferente deberá presentar cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee línea de crédito que pueda solventar al menos el monto de USD$2,000,000.00 (o su equivalente en pesos o euros). Se sugiere que al menos uno (1) de los miembros que componen el grupo del consorcio cumpla con este requisito. Numeral 5.4.1 del Pliego. **(Repetido 1.16 y 2.15 de Credenciales y Propuestas).**	Si	CARPETA 1 SECCIÓN 1 -No.16. CARPETA 4 SECCIÓN 5 - NO. 30	Suministrado
1.6	El oferente deberá presentar los Estados Financieros de los últimos tres (3) períodos fiscales, certificados por un Contador Público Autorizado, avalado con copia del IR-2 de esos últimos tres (3) períodos fiscales, incluyendo la entrega certificada con el soporte correspondiente y/o el código de envío electrónico recibido. Numeral 5.4.1 del Pliego. **(Repetido 1.11 y 2.14 de Credenciales y Propuestas).**	Si	CARPETA 1 SECCIÓN 1 -No.09. CARPETA 3 SECCIÓN 1 -No.08 SECCIÓN 2 -No.12 SECCIÓN 3 -No.18 SECCIÓN 4 -No.23. CARPETA 4 SECCIÓN 5 - NO. 30	Se aportan los Estados Financieros Auditados de todos y cada uno de los miembros del Consorcio como documentación de soporte no requerida en el pliego de condiciones para las empresas extranjeras.
1.7	Las hojas financieras auditadas deben presentarse según la plantilla facilitada (Anexo 8). Numeral 5.4.1 del Pliego. **(Repetido 1.11 y 2.14 de Credenciales y Propuestas).**	Si	CARPETA 1 SECCIÓN 1 -No.11. CARPETA 3 SECCIÓN 1 -No.08 SECCIÓN 2 -No.12 SECCIÓN 3 -No.18 SECCIÓN 4 -No.23. CARPETA 4 SECCIÓN 5 - NO. 30	Suministrado
1.8	El plazo de validez de las ofertas será de ciento cincuenta (150) días a partir de la fecha límite. Numeral 5.4.1 del pliego	Si	CARPETA 1 SECCIÓN 2 -No.21.	Suministrado
1.9	El oferente deberá proporcionar un mínimo de diez (10) muestras originales de las tarjetas junto con la propuesta técnica. Las muestras deben ser capaces de representar la personalización de las cédulas electrónicas y los detalles de las características de seguridad que el proveedor propone, y éstas deben explicarse claramente. Junto con las muestras, el proveedor deberá presentar informes de pruebas independientes de acuerdo con la norma ISO 18745. Las tarjetas preimpresas a entregar pueden ser genéricas; sin embargo, es fundamental que demuestren, ya sea de manera individual o sumando características, todas y cada una de las especificaciones requeridas en el pliego de condiciones. En total las terjetas a entregar deberán evidenciar las especificaciones técnicas solicitadas. Sólo es necesario presentar documentos de laboratorio externo que acrediten que el oferente cumple con la norma ISO 18745 para cualquiera de sus productos fabricados. No específico para las muestras. Numeral 5.4.1 del Pliego. **(Repetido 1.17 y 2.16 de Credenciales y Propuestas).**	Si	SOBRE DE SEGURIDAD NO.1 - Entrega de Muestra de las Tarjetas de PC.	Suministrado
1.10	Solvencia (Activo total / Pasivo total) del Consorcio debe ser mayor que >1. PARA ACREDITAR LA ELIGIBILIDAD , EL OFERENTE DEBERÁ REALIZAR UNA CARTA JURADA DICIENDO QUE SU SOLVENCIA ES MAYOR QUE UNO, ADJUNTANDO LOS ESTADOS FINANCIEROS DEL CONSORCIO Y RESALTANDO DE DONDE SE OBTIENEN LOS VALORES PARA REALIZAR DICHO CÁLCULO.	Si	CARPETA 1 SECCIÓN 2 -No.26.	Suministrado

1.11	Consorcio debe facturar (de media en los últimos 3 años) en su conjunto, al menos la totalidad del presupuesto de su propuesta total. PARA ACREDITAR EL REQUISITO, EL OFERENTE DEBE DE PRESENTAR CARTA JURADA ASEGURANDO QUE SU FACTURACION ES AL MENOS , LA TOTALIDAD DEL PRESUPUESTO DE SU OFERTA QUE SERÁ COMPROBADA EN EL SOBRE B.	Si	CARPETA 1 SECCIÓN 2 -No.27.	Suministrado
1.12	**Máximo** tiempo de implementación: 26 semanas.	Si	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
1.13	Impresora pesa menos de 80kg.	Si	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
1.14	Impresora modular.	Si	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
1.15	Que el proponente esté legalmente autorizado para realizar sus actividades comerciales en el país.	Si	CARPETA 1 SECCIÓN 1 -No.05 CARPETA 3 SECCIÓN 1 -No. 07 SECCIÓN 2 -No. 11 SECCIÓN 3 -No. 17 SECCIÓN 4 -No. 22 CARPETA 4 SECCIÓN 5 - No.29	Suministrado
1.16	Que el oferente demuestre que tiene capacidad y experiencia para la entrega a tiempo y en las condiciones establecidas.	Si	CARPETA 2 SECCIÓN 3 -No.6.	Suministrado
1.17	Que cuenta con la estabilidad financiera suficiente para ejecutar satisfactoriamente la eventual adjudicación. De las empresas nacionales, se evaluarán los estados financieros auditados de los últimos tres (3) períodos fiscales y el **formulario IR-2** con sus respectivos anexos para determinar los Índices Financieros mínimos correspondientes. Para las empresas extranjeras, no se requiere los Estados Financieros, éstas deben presentar la plantilla financiera (Anexo 8) en dólares estadounidenses (USD), tiene que presentar copia certificada del equivalente físico o electrónico al formulario IR-2 de la DGII, o su equivalente, de los últimos 3 periodos fiscales.	Si	CARPETA 1 SECCIÓN 1 -No.09, No. 10 y No. 11.	Suministrado
1.18	La experiencia del Mobile ID debe ser de alguna empresa del consorcio. PARA ACREDITAR LA ELIGIBILIDAD , EL OFERENTE DEBERÁ REALIZAR UNA CARTA JURADA DICIENDO CUAL DE SUS MIEMBROS TIENE UNA EXPERIENCIA EN CEDULA DIGITAL (MOBILE ID). Se aceptarán contratos de empresas miembros de un mismo grupo económico, siempre que se pueda demostrar que se trata de accionistas en común.	Si	CARPETA 1 SECCIÓN 2 -No.28.	Suministrado
2	**REQUERIMIENTOS DEL PROVEEDOR**			
2.1	Contar con la acreditación de la fábrica de pasaporte del certificado INTERGRAF ISO 14298:2013 o superior, a nivel gobierno en vigencia del fabricante de la tarjeta. Numeral 5.4.1 del Pliego.	Seleccionar	CARPETA 2 SECCIÓN 4 -No.11.	Suministrado
2.2	Tener el certificado ISO 27001 en vigencia del fabricante de la tarjeta. Numeral 5.4.1 del Pliego.	Seleccionar	CARPETA 2 SECCIÓN 4 -No.11.	Suministrado
2.3	Tener el certificado ISO 14001 en vigencia del fabricante de la tarjeta. Numeral 5.4.1 del Pliego.	Seleccionar	CARPETA 2 SECCIÓN 4 -No.11.	Suministrado
2.4	Tener el certificado ISO 9001 en vigencia del fabricante de la tarjeta. Numeral 5.4.1 del Pliego.	Seleccionar	CARPETA 2 SECCIÓN 4 -No.11.	Suministrado
2.5	Tener el certificado ISO 50001 en vigencia, al menos una empresa del consorcio. Especificaciones Técnicas Generales del Pliego, págs. 14 y 15	Seleccionar	CARPETA 2 SECCIÓN 4 -No.11.	Se entrega ISO 14001 En sustitución
2.6	Tener el certificado CWA 15374:2018 En vigencia . Observacion del Grupo 4 respuestas 22: Con la presentación del certificado del fabricante de tarjeta de ISO14298 a nivel gubernamental no se hace necesario la presentación del certificado CWA15374. Quien aporte dicho certificado debe estar dentro del consorcio. Con la presentación del certificado del fabricante de tarjeta de ISO14298 (2.1 arriba)a nivel gubernamental no se hace necesario la presentación del certificado CWA15374. Quien aporte dicho certificado debe estar dentro del consorcio. Con la presentación del certificado del fabricante de tarjeta de ISO14298 a nivel gubernamental no se hace necesario la presentación del certificado CWA15374. Quien aporte dicho certificado debe estar dentro del consorcio. Especificaciones Técnicas Generales del Pliego, pág. 14	Seleccionar	CARPETA 2 SECCIÓN 4 -No.11.	Se entrega ISO 14298 En sustitución
2.7	ISO 15408: PKI Compatible con ICAO para establecer un SOD activado en los datos del chip. Especificaciones Técnicas Generales del Pliego, págs. 14 y 15	Seleccionar	CARPETA 2 SECCIÓN 4 -No.11.	Suministrado
2.8	ISO / IEC 14443 Tarjetas de identificación de circuito integrado sin contacto. ITEM I, numeral I .3 del Pliego, pág. 16	Seleccionar	CARPETA 2 SECCIÓN 4 -No.11.	Suministrado
3	**OTROS REQUERIMIENTOS TECNICOS**			
3.1	Cronograma de trabajo: El oferente deberá presentar un plan de trabajo detallado que cubra las tres (3) etapas del proyecto. (ver numeral 1.27.2).	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.2	Etapa 1: Implantación y puesta en marcha del proyecto En esta etapa, que durará máximo veintiséis (26) semanas a partir de la firma del contrato.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.3	Etapa 2: Durará máximo 12 meses a partir de la finalización de la etapa 1	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado

3.4	Etapa 3: Durará 12 meses a partir de la finalización de la etapa 2	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.5	Etapa 1: Entregar el diseño de seguridad de las tarjetas a las cuatro (4) semanas después de la firma de contrato. (ver numeral 1.27.3).	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.6	Etapa 1: 2,000 tarjetas de policarbonato genéricas con chip para pruebas a las dieciséis (16) semanas.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.7	Etapa 1: Instalar la PKI y la CA, así como realizar la ceremonia de llaves a las dieciséis (16) semanas.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.8	Etapa 1: Entrega de 300,000 tarjetas de policarbonato a las veintidós (22) semanas después de la firma de contrato.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.9	Etapa 1: Suministrar dos impresoras de policarbonato a las dieciséis (16) semanas.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.10	Etapa 1: Instalación de la CA y la PKI, así como realizar la ceremonia de entrega de llaves a las dieciséis (16) semanas.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.11	Etapa 1: Realizar las pruebas piloto de la solución digital de la tarjeta CD (Mobile ID) antes de veintiséis (26) semanas, incluyendo el desarrollo de una app para la JCE.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.12	Etapa 1: Ayudar a los técnicos de la JCE a ladaptar la SDK de la impresora al sistema de la JCE. Realizar pruebas unitarias de integraciób, de pre-producción de las impresoras, las tarjetas.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.13	Etapa 1: Capacitación al personal de la JCE de la operación y mantenimiento del equipo de impresión, PKI y solución digital.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.14	Etapa 2: Suministro de inventario de tarjetas 500,000 tarjetas de Policarbonato a las 26 semanas después de la firma de contrato. 1,200,000 tarjetas de Policarbonato a las 30 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 34 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 38 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 42 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 46 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 50 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 54 semanas después de la firma de contrato.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado
3.15	Etapa 2: Ver 1.27.4 Adquisición e instalación de los equipos de impresión y puesta en marcha en las sedes de la República Dominicana y en el exterior. Las fechas de las entregas y cantidades de dichos equipos serán acordados con el proveedor adjudicado y la JCE. Puesta en marcha del mantenimiento de las impresoras en periodo de garantía. Para ello, el proveedor deberá de disponer de mínimo de dos (2| técnicos certificados en tecnología de impresión de tarjetas de identidad, y mínimo un total de diez (10) técnicos para soporte nacional de servicio para reparación de equipos en sitio durante el periodo de garantía. Para el exterior, el proveedor durante tiempo de garantía de las impresoras, deberá reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa), la JCE enviará las impresoras defectuosas a estos lugares según aplique.	Seleccionar	CARPETA 2 SECCIÓN 3 -No.1.	Suministrado

DOCUMENTACIÓN Y PROPUESTA TÉCNICA DEL CONSORCIO

Propuesta Técnica Consorcio CÉDULA 4.0 RD

PROPUESTA TÉCNICA
CONSORCIO “CEDULA 4.0 RD”

PARA EL PROCESO DESTINADO A LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA NUEVA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI) DE REF.: JCE-CCC-LPI-2024-0001.

Junta Central Electoral
Garantía de Identidad y Democracia

Cliente: Junta Central Electoral

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

Contenido

RESUMEN EJECUTIVO 7
PRESENTACIÓN DEL CONSORCIO 8
ALCANCE GEOGRÁFICO DE LA INFRAESTRUCTURA DE SERVICIOS QUE OPERARÁ EL FABRICANTE DE LA IMPRESORA 9
BENEFICIOS INMEDIATOS PARA LA JUNTA CENTRAL ELECTORAL (JCE) CON LA IMPLEMENTACIÓN DE LA SOLUCIÓN DEL CONSORCIO CÉDULA 4.0 RD 11
CREDENCIALES DE MIEMBROS DEL CONSORCIO CEDULA 4.0 RD 13
VISIÓN DEL PROYECTO, SUGERENCIAS Y RECOMENDACIONES 14
ESPECIFICACIONES TÉCNICAS GENERALES 18
EQUIPAMIENTO PARA LA EMISIÓN DE CÉDULAS 19
INFRAESTRUCTURA PKI – CA 19
CAPACITACIÓN PARA PERSONAL DE LA JCE 19
SEGURIDAD Y PROTECCIÓN DE DATOS 19
ÍTEM I - ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS 21
1. ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS 22
1.1 INTRODUCCIÓN 22
1.1.1 DISEÑO Y PRODUCCIÓN 22
1.1.1.1 IMPRESOR DE ALTA SEGURIDAD 22
1.1.1.2 FABRICACIÓN DE TARJETAS SOBRE DIVERSOS MATERIALES 23
1.1.1.3 CALIDAD Y RESPETO MEDIOAMBIENTAL 23
1.1.2 COMPONENTES ELECTRÓNICOS, SISTEMAS OPERATIVOS Y APLICACIONES 25
1.1.2.1 SEGURIDAD DE LOS COMPONENTES 25
1.1.2.2 TARJETAS ELECTRÓNICAS, INLAYS, E-STICKERS, E-COVERS 25
1.1.3 CERTIFICACIONES 26
1.1.3.1 ISO 9001, 14001, 27001 26
1.1.3.2 ISO 14298:2013 27
1.2 PROCESO DE FABRICACIÓN DE TARJETA 28
1.2.1 DISEÑO / ESTUDIO 28
1.2.2 PRUEBA DE COLOR 29
1.2.3 IMPRESIÓN 29
1.2.3.1 IMPRESIÓN EN OFFSET 29
1.2.3.2 IMPRESIÓN SERIGRÁFICA 31
1.2.4 ENSAMBLADO 31

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

Página/Folio No.11 de 843

1.2.5 LAMINADO 32
1.2.6 CORTE 33
1.2.7 PRE PERSONALIZACIÓN 34
1.2.7.1 ELÉCTRICA 34
1.2.7.2 GRÁFICA 34
1.2.8 CONTROL DE CALIDAD 35
1.2.9 EMBALAJE Y ALMACENAMIENTO 35
1.2.10 ENVÍO 36
1.2.11 DESTRUCCIÓN DE LOS PRODUCTOS SENSIBLES 37
1.3 PROPUESTA TARJETAS DE POLICARBONATO 38
1.3.1 LA TARJETA EN POLICARBONATO 38
1.3.1.1 CUERPO DE LA TARJETA 38
1.3.1.2 ESTRUCTURA DE LA TARJETA 39
1.3.2 TARJETA CON CHIP SIN CONTACTO 40
1.3.3 MIDDLEWARE 44
1.3.4 PERSONALIZACIÓN GRÁFICA 47
1.3.5 IMPRESIÓN DE SEGURIDAD 47
1.3.5.1 CERTIFICACIÓN PARA IMPRESORES DE SEGURIDAD 48
1.3.5.2 CREACIÓN DE UN DISEÑO GRÁFICO SEGURO 48
1.3.6 ELEMENTOS DE SEGURIDAD 49
1.3.6.1 NIVEL DE SEGURIDAD 50
1.3.6.2 IMPRESIÓN DE SEGURIDAD 50
1.3.6.2.1 GUILLOCHES 51
1.3.6.2.2 IMPRESIÓN EN ARCOÍRIS 52
1.3.6.2.3 MICROLÍNEAS DE AMPLITUD VARIABLE 53
1.3.6.2.4 MICROTEXTOS (POSITIVOS Y NEGATIVOS) 54
1.3.6.2.5 ERRORES DELIBERADOS 55
1.3.6.2.6 FONDOS NUMISMÁTICOS 56
1.3.6.3 TINTAS UV INVISIBLES 57
1.3.6.3.1 GUILLOCHES EN UV 58
1.3.6.3.2 MICROTEXTOS EN UV 58
1.3.6.3.3 ARCOIRIS EN UV 58
1.3.6.3.4 UV MALLA DE FONDO EN MICROTEXTO 58

1.3.6.4 TINTA ÓPTICAMENTE VARIABLE (OVI) 59
1.3.6.5 ELEMENTOS HOLOGRÁFICOS 60
1.3.6.6 ELEMENTOS TÁCTILES / RELIEVE SUPERFICIAL POSITIVO O NEGATIVO 61
1.3.6.7 MLI / CLI 63
1.3.6.8 VENTANA TRANSPARENTE 64
1.3.6.9 TINTAS INFRARROJAS ABSORBENTES/TRANSPARENTES 65
1.3.6.10 OTROS ELEMENTOS DE SEGURIDAD 66
ÍTEM II - ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN 67
2. ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN LASER 68
2.1 BENEFICIOS DE LA SOLUCIÓN 69
2.2 CRITERIOS DE DESEMPEÑO ÚNICOS 70
2.3 MÓDULO LASER CLM600 71
2.4 CARACTERÍSTICAS ADICIONALES 73
2.5 MÓDULO OPCIONAL PARA IMPRESIÓN A COLOR GET CP500 74
2.6 CONDICIONES DE GARANTÍA 75
GARANTÍA: 75
ÍTEM III - ESPECIFICACIONES TÉCNICAS DE LAS PKI - CA 78
3.1 GET TRUST – SOLUCIÓN DE PKI 79
3.1.1 ARQUITECTURA DEL SOFTWARE 79
3.2 GET AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA – CSCA 80
3.3 FIRMADO DE DOCUMENTOS GET TRUST (DOCUMENT SIGNER) 90
3.4 PKI CIUDADANA – PKI SUBORDINADA X509 92
3.5 INFRAESTRUCTURA GET TRUST 93
3.5.1 CARACTERÍSTICAS CLAVES 93
3.6 MÓDULO DE SEGURIDAD POR HARDWARE (HSM) 94
ÍTEM IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL 97
4.1 INTRODUCCIÓN - GET MOBILE ID 98
4.1.1 GET MOBILE ID 98
4.1.2 GET MOBILE ADMINISTRATOR 98
4.2 GET MOBILE ID – COMPONENTES 99
4.2.1 GET MOBILE ADMINISTRATOR 99
4.2.1.1 OPCIONES DE INTEGRACIÓN: 100
4.2.1.2 OPCIONES DE FIRMADO DIGITAL 102

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

Página/Folio No.13 de 843

4.2.1.3 MODELO DE DATOS Y CODIFICACIÓN. 103
4.2.1.4 PROCEDIMIENTO DE ACTIVACIÓN 103
4.2.2 GET MOBILE ID – APLICACIÓN MÓVIL 106
4.2.2.1 OPCIONES DE PERSONALIZACIÓN 107
4.2.2.2 CONTROL TOTAL Y PROTECCIÓN DE LA PRIVACIDAD 108
4.2.2.3 SIEMPRE ACTUALIZADO 109
4.2.2.4 INTEROPERABILIDAD 109
4.2.3 GET MOBILE VERIFIER 109
4.2.3.1 MODOS DE INTERACCIÓN 112
4.2.4 Herramientas de Desarrollo 113
4.2.5 INFRAESTRUCTURA 113
4.2.5.1 ARQUITECTURA DE ALTA DISPONIBILIDAD 113
4.2.5.2 DISPONIBILIDAD DEL 99.95% DE OPERACIÓN 115
ÍTEM V- KIT PERIFERICOS 116
ÍTEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO 127
6 PLAN DE MANTENIMIENTO PARA IMPRESORAS Y PERIFERICOS 128
6.1 PLAN DE MANTENIMIENTO PARA PKI 130
6.1.3 MODELOS DE SERVICIO Y SLA 130
6.1.4 SLA Y TIEMPOS DE RESPUESTA 131
6.1.5 PROCEDIMIENTO PARA LA APERTURA DE INCIDENTES POR PARTE DE LA JCE 132
6.3 MANTENIMIENTO PREVENTIVO Y CORRECTIVO 134
6.4 SEGURIDAD Y CUMPLIMIENTO 135
6.5 KPIS Y MÉTRICAS DE RENDIMIENTO 135
6.6 PLAN DE MANTENIMIENTO PARA TARJETA DIGITAL 136
6.6.1 INTRODUCCIÓN 136
6.6.2 ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA 136
6.6.3 MODELOS DE SERVICIO Y SLA 136
6.7 MANTENIMIENTO PREVENTIVO Y CORRECTIVO 138
6.7.1 ACTIVIDADES PERIÓDICAS 138
6.7.2 ACTIVIDADES DE MANTENIMIENTO PREVENTIVO 139
6.7.3 ACTIVIDADES DE RESPUESTA A INCIDENTES 139
6.7.4 MANTENIMIENTO CORRECTIVO 139
6.8 SEGURIDAD Y CUMPLIMIENTO 139

6.9 KPIS Y MÉTRICAS DE RENDIMIENTO....141
6.10 INVENTARIO....141
ÍTEM VII - CAPACITACIÓN....142
7. PLAN DE CAPACITACIÓN PARA IMPRESORAS....143
7.1 ENTRENAMIENTOS....143
7.11 PLAN DE CAPACITACION PARA PKI....145
7.11.1 CONTENIDO....145
7.11.2 METODOLOGÍA....145
7.11.3 DESCRIPCIÓN....145
7.12 PLAN DE CAPACITACION PARA TARJETA DIGITAL....151
7.12.1 CONTENIDO....151
7.12.2 METODOLOGÍA....151
7.12.3 DESCRIPCIÓN....151
VIII- OTRAS CONDICIONES....154
8. PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)....154
8.1 OBJETIVO DEL PLAN....154
8.2 2. ALCANCE....154
8.3 ANÁLISIS DE RIESGOS....154
8.4 ESTRATEGIAS DE CONTINUIDAD....155
8.4.1 INFRAESTRUCTURA DE RESPALDO:....155
8.4.2 PROTOCOLOS DE RESPALDO DE INFORMACIÓN:....155
8.4.3 GESTIÓN DE PROVEEDORES ESTRATÉGICOS:....155
8.4.4 PLAN DE RECUPERACIÓN ANTE CRISIS:....155
8.5 PROCEDIMIENTOS DE RESPUESTA Y RECUPERACIÓN....155
8.6 REQUISITOS DE PRODUCCIÓN Y TIEMPOS DE ENTREGA....157
8.7 INFRAESTRUCTURA DE PRODUCCIÓN Y UBICACIÓN DE LAS FÁBRICAS....157
8.9 CRONOGRAMA GENERAL DE PRODUCCIÓN Y ENTREGA....158
8.10 CRONOGRAMA DE TRABAJO....158

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

RESUMEN EJECUTIVO

La Junta Central Electoral (JCE) mediante la convocatoria de la presente Licitación Pública Internacional con el objetivo de modernizar el sistema de emisión de la Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) en la República Dominicana. Esta licitación busca la contratación de una empresa que suministre los equipos, materiales y servicios requeridos para garantizar un sistema de identificación seguro, eficiente y tecnológicamente avanzado.

En respuesta a esta convocatoria, se presenta una solución integral que cumple con los requerimientos técnicos, operativos y de seguridad exigidos en el pliego de condiciones. Nuestro enfoque está basado en la experiencia y capacidad de un equipo altamente especializado, garantizando un sistema confiable y escalable para la JCE.

La propuesta ofrece una serie de beneficios estratégicos para la JCE, alineados con su visión de modernización e innovación:

- Optimización en la emisión de cédulas, reduciendo tiempos y costos operativos.
- Mayor seguridad y confiabilidad, con tecnologías de protección contra fraudes y falsificaciones.
- Interoperabilidad con sistemas gubernamentales, facilitando la integración con otras plataformas digitales.
- Infraestructura de soporte técnico en República Dominicana, EE. UU. y Europa, garantizando mantenimiento y servicio especializado.
- Sostenibilidad operativa, con una red de distribución y mantenimiento ya establecida.

Para la ejecución de este proyecto, el consorcio cuenta con una amplia trayectoria en la implementación de soluciones de identidad seguras a nivel global. Su experiencia abarca la fabricación, integración y operación de sistemas de identificación, garantizando el cumplimiento de los más altos estándares de seguridad y confiabilidad.

A través de esta propuesta, se garantiza la viabilidad y sostenibilidad del proyecto, respaldado por un equipo altamente capacitado y una infraestructura tecnológica de primer nivel.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

PRESENTACIÓN DEL CONSORCIO

La Junta Central Electoral (JCE), a través de la presente licitación, busca adquirir una solución integral para la gestión de las cédulas de identidad en la República Dominicana. Esta iniciativa contempla la implementación de una infraestructura avanzada para la emisión de cédulas físicas y digitales, incorporando tarjetas de policarbonato con impresión láser, periféricos modernos y una plataforma PKI – CA que garantice autenticación y seguridad en el acceso a los servicios de identificación.

Para dar respuesta a esta necesidad, el Consorcio Cédula 4.0 RD fue conformado bajo el liderazgo de Copy Solutions International S.A. (CSI), con el objetivo de proporcionar una solución robusta, eficiente y alineada con los estándares tecnológicos y de seguridad establecidos por la JCE.

El Consorcio Cédula 4.0 RD está conformado por seis empresas de reconocimiento internacional, especializadas en la fabricación, integración y operación de sistemas de identificación. Gracias a esta estructura, la solución propuesta abarca desde la producción de credenciales seguras hasta la implementación de plataformas digitales para la gestión de identidad.

Las empresas que conforman el consorcio son:

- Copy Solutions International S.A. (CSI) – responsable principal del contrato y con capacidad instalada en la República Dominicana para la logística y operación del servicio.
- Grupo Get Group:
  - GET International FZCO – Especialista en tecnología de identidad y seguridad digital con experiencia en soluciones de autenticación y verificación de identidad.
  - GET Group Latin America S.A. – Enfocada en el desarrollo de plataformas para la emisión de documentos de identidad, pasaportes electrónicos y sistemas biométricos.
  - GET Secure ID Corp. – Dedicada a la fabricación de tarjetas de policarbonato con impresión láser y elementos de seguridad de alta resistencia.
  - Global Enterprise Technologies Corp. – Proveedor de tecnología y soluciones integradas para la personalización de documentos y autenticación digital.
- SELP S.A.S. – Especialista en la producción de documentos de identidad, con experiencia en impresión de alta seguridad y gestión de credenciales.

Cada una de estas empresas aporta su conocimiento en áreas específicas, garantizando una solución sólida, confiable y preparada para responder a los desafíos operativos y de seguridad de la JCE.

ALCANCE GEOGRÁFICO DE LA INFRAESTRUCTURA DE SERVICIOS QUE OPERARÁ EL FABRICANTE DE LA IMPRESORA

La cobertura de apoyo de servicios de CSI abarca, en la actualidad, el 100% de las Provincias de RD.

PROVINCIAS					
1- Azua	7- Elías Piña	13- Monseñor	19- Romana, La	25- San Juan de la Maguana	31- Valverde
2- Bahoruco	8- Espaillat	14- Montecristi	20- Her. Mirabal	26- San Pedro de Macorís	32- La Vega
3- Barahona	9- Hato Mayor	15- Monte Plata	21- Samaná	27- Santiago	
4- Dajabón	10- Independencia	16- Pedernales	22- San Cristóbal	28- Santiago Rodríguez	
5- Distrito nacional	11- Altagracia, La	17- Peravia	23- Sánchez Ramírez	29- Santo Domingo	
6- Duarte	12- María Trinidad	18- Puerto Plata	24- Ocoa	30- Seibo, El Seibo	

Clientes Actuales	Ubicacion Geografica del Clientes de Impresoras suplidas por CSI donde se cubre el servicio y soporte técnico en la actualidad EN Republica Dominicana																														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Edenorte Dominicana																																
Banco BHD	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Asociación La Nacional de Ahorros y Prestamos				✓	✓	✓	✓	✓	✓		✓	✓		✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Grupo CID	✓				✓										✓							✓					✓		✓			
Banco Promerica					✓						✓		✓						✓						✓		✓		✓			✓
Banco multiple Caribe				✓	✓						✓			✓				✓								✓	✓		✓			
Farmaco Químico Nacional					✓			✓			✓						✓	✓	✓							✓			✓			
Fenwal International																						✓										
Banco Union de Ahorro y Credito	✓		✓		✓			✓				✓		✓			✓		✓						✓	✓	✓					
Hotelera Bavaro											✓																					
Grupo Propagas																													✓			
Grupo Marti					✓																											
La Aurora (Grupo Leon Jimenes)											✓																					
Grupo SIM											✓																					
Punta Cana Holding (Secret)					✓													✓								✓			✓			
Print City																																
Grupo Ambar(Santo Domingo Motors)					✓								✓																✓			
DP World Caucedo																													✓			
Grupo JMMB					✓						✓																		✓			
Grupo Viamar				✓							✓															✓			✓			
Junta Central Electoral	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Procuraduria general de la Rep. Dominicana	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Senasa	✓	✓			✓			✓			✓	✓		✓				✓			✓						✓		✓			✓
Promipyme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitur				✓																												
Registro Inmobiliario					✓																								✓			
Medio Ambiente	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Camara de Diputados de la Rep Dom					✓																											
Senado de la Republica Dominicana					✓																											

CSI cuenta con más de 2,000 clientes de impresoras con tecnología láser en la RD y el desplazamiento a brindar el servicio de soporte técnico a sus localidades es tan común, que lo venimos sirviendo desde hace más de 20 años.

En la documentación adjunta detallamos un ejemplo de la infraestructura que disponemos en la actualidad. Lista muy distinguida en la que todos los meses se incluyen nuevas instalaciones

Nuestra presencia en el territorio nacional con seis (6) oficinas y una próxima en Azua, nos posiciona como el principal suplidor de soluciones tecnológicas en equipos de impresión y sistemas llave en

mano en la República Dominicana. Esto nos permite ofrecer el mejor tiempo de respuesta en servicio a nuestros clientes.

Cualquier otra oferta disponible actualmente está diseñada para brindar soporte exclusivamente desde el Distrito Nacional. Para ser realmente comparable, nuevas propuestas de servicio tendrían que replicar una plataforma de atención similar a la de CSI.

A continuación, se desglosa la distribución de nuestros clientes en el territorio nacional en relación con nuestras oficinas operativas, asegurando una cobertura eficiente y tiempos de respuesta óptimos para nuestros servicios.

BENEFICIOS INMEDIATOS PARA LA JUNTA CENTRAL ELECTORAL (JCE) CON LA IMPLEMENTACIÓN DE LA SOLUCIÓN DEL CONSORCIO CÉDULA 4.0 RD

- Optimización en la emisión de cédulas: La integración de un sistema holístico permite agilizar el proceso de emisión y renovación de cédulas, reduciendo tiempos y costos operativos.

- Actualización tecnológica: La incorporación de tecnología de vanguardia, como la impresión láser y plataformas digitales, asegura la modernización del sistema de identidad.

- Mayor seguridad y confiabilidad: La infraestructura robusta, que incluye una plataforma PKI – CA, fortalece la integridad de los datos y la autenticidad de las cédulas, generando mayor confianza en la ciudadanía.

- Soporte técnico especializado en RD: Con la red de instalada de soporte técnico de CSI a cargo del Fabricante para operar el mantenimiento, se garantiza un soporte técnico continuo y un mantenimiento eficiente, asegurando la operatividad de la plataforma al nivel más avanzado en SLAs.
- Soporte técnico especializado en EEUU: Con la red de instalada de soporte técnico de Get Group, miembro del consorcio CEDULA 4.0 RD y fabricante de la solución de impresoras, hoy suple servicios similares de soporte y mantenimiento al proyecto de Pasaportes de los EEUU desde las ciudades principales, se garantiza un soporte técnico continuo y un mantenimiento eficiente, al parque de impresión de la plataforma en ese país.

- Soporte técnico especializado en Madrid: Desde las oficinas de SELP en Madrid C/ Cronos 63,4-4 28037 Madrid, España. miembro del consorcio CEDULA 4.0 RD y suplidor de las tarjetas de Policarbonato, se centralizarán los servicios de soporte y mantenimiento a requerimientos de las impresoras del proyecto de la JCE en Europa.

- Interoperabilidad con otros sistemas: La solución digital facilita la integración con otras plataformas y sistemas gubernamentales, promoviendo la eficiencia en la gestión interinstitucional.

- Reducción de riesgos operativos: La experiencia y solvencia de las empresas integradas en el consorcio minimizan riesgos, asegurando la continuidad del servicio y la confiabilidad del proceso.

- Optimización logística: La amplia infraestructura de soporte y mantenimiento al usuario de la JCE de impresoras Láser será operado por el fabricante de las impresoras, tanto en la Republica Dominicana, en EE. UU. como España garantizando la atención oportuna y el soporte de los equipos y a sus usuarios sin necesidad de implementar e improvisar para el proyecto una infraestructura nueva en ninguna localidad.

- Mejora en la atención a la ciudadanía: Un sistema moderno, seguro y eficiente contribuye a elevar la calidad del servicio ofrecido a los ciudadanos, mejorando la imagen institucional de la JCE.
- Opción de COLOR con impresión Laser en Policarbonato: Nuestra propuesta contempla la capacidad de incorporar módulo de impresión a color de la fotografía para una combinación de impresión de tintas de pigmento solido e impresión laser utilizando la tecnología de imagen híbrida *LASMENT mediante impresión por re-transferencia* segura con grabado láser, logrando una característica única de personalización a color en tarjetas de policarbonato. El contar con esta opción le permitirá a la JCE redoblar la seguridad en el documento mientras se eleva la seguridad y calidad de este a estándares antes no vistos.

CREDENCIALES DE MIEMBROS DEL CONSORCIO CEDULA 4.0 RD

VISIÓN DEL PROYECTO, SUGERENCIAS Y RECOMENDACIONES

VISIÓN DEL PROYECTO

La modernización del sistema de emisión de la Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) en la República Dominicana responde a la creciente necesidad de un sistema de identidad seguro, eficiente e integrado con las nuevas tecnologías digitales. Esta transformación no solo es una evolución técnica, sino una respuesta a las dinámicas económicas y demográficas del país, que han incrementado la demanda de servicios de identificación y digitalización de procesos gubernamentales.

En las últimas décadas, la República Dominicana ha experimentado un crecimiento sostenido en su población, lo que ha generado una mayor presión sobre los sistemas de emisión de documentos de identidad. A esto se suma la expansión económica del país, con un crecimiento del PIB proyectado entre 4.5% y 5.0% para 2025, impulsado por el turismo, la inversión pública y el fortalecimiento del sector financiero.

Adicionalmente, el auge del turismo y la migración internacional ha elevado la necesidad de sistemas de identificación modernos, interoperables y seguros. Con ingresos turísticos que superan los 10,000 millones de dólares anuales, la República Dominicana se consolida como un hub internacional, albergando a ciudadanos de diversas nacionalidades que requieren servicios automatizados y verificación de identidad en múltiples sectores.

En este contexto, el Consorcio Cédula 4.0 RD presenta una solución que va más allá del cumplimiento de los requisitos del Pliego de Condiciones. Nuestra propuesta se fundamenta en las mejores prácticas internacionales en gestión de identidad, combinando seguridad, eficiencia operativa y facilidad de uso para los ciudadanos.

La implementación de este sistema permitirá a la JCE gestionar la identidad nacional con los más altos estándares de seguridad, interoperabilidad y escalabilidad. A través de la impresión láser en policarbonato, la autenticación digital y un esquema de soporte técnico integral, garantizamos un servicio sin interrupciones, adaptable al crecimiento del país y preparado para la evolución de los servicios digitales en el futuro.

SUGERENCIAS PARA LA IMPLEMENTACIÓN

La modernización del sistema de emisión de la Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) no solo debe responder a exigencias tecnológicas y de seguridad, sino también a las necesidades operativas reales de la Junta Central Electoral (JCE). La estabilidad y eficiencia del servicio dependen de factores estratégicos que van más allá del pedigrí y la experiencia internacional de los proveedores, incorporando factores críticos como la infraestructura nacional, la capacidad de respuesta local y la continuidad operativa garantizada.

En este sentido, el Consorcio Cédula 4.0 RD cuenta con una ventaja diferenciadora clave: la participación de un proveedor local con 21 años de experiencia en servicios tecnológicos y operativos en el país, de los cuales más de la mitad han sido en servicio directo a la JCE. Esta trayectoria no solo respalda la capacidad técnica del consorcio, sino que también aporta un conocimiento profundo de la realidad operativa dominicana, permitiendo la optimización de recursos, reducción de riesgos y una implementación eficiente.

Algunos de los factores clave que garantizan el éxito de la implementación incluyen:

Experiencia operativa comprobada en la JCE: Con más de 10 años de servicio directo a la institución, el proveedor local ha gestionado y mantenido infraestructura crítica para la emisión de documentos de identidad, asegurando continuidad operativa y eficiencia.

Infraestructura de soporte en todo el país: La cobertura a nivel nacional de los servicios técnicos permite una respuesta rápida y eficiente ante cualquier eventualidad, asegurando tiempos mínimos de inactividad.

Estabilidad eléctrica y conectividad garantizada: La infraestructura propuesta toma en cuenta la realidad energética y de telecomunicaciones de la República Dominicana, con planes de contingencia que minimizan el impacto de interrupciones en el servicio.

Capacidades de respuesta inmediata: Gracias a un esquema de reporte diario y monitoreo en tiempo real, la solución garantiza una evaluación constante de la operación, facilitando la identificación y resolución inmediata de cualquier incidencia.

ESTRATEGIAS PARA UNA IMPLEMENTACIÓN EFICIENTE

Para garantizar una transición fluida y sin interrupciones, el Consorcio Cédula 4.0 RD propone una estrategia de implementación escalonada, asegurando la correcta integración de los sistemas y la optimización del servicio.

Fase Piloto: Implementación inicial en una región específica para validar la interoperabilidad de los sistemas, identificar posibles mejoras y ajustar procesos antes de la implementación a nivel nacional.

Capacitación Especializada: Formación a los operadores y técnicos de la JCE sobre el manejo del nuevo sistema, combinando sesiones presenciales y virtuales, acompañadas de documentación técnica completa.

Integración con Otros Sistemas Gubernamentales: Implementación de interfaces de comunicación que permitan la validación en tiempo real de los datos de identidad con otras instituciones estatales, promoviendo la interoperabilidad del sistema.

Estrategia de Respaldo y Continuidad Operativa: Desarrollo de un esquema de redundancia y contingencia, asegurando la operatividad ininterrumpida del sistema ante cualquier evento imprevisto.

RECOMENDACIONES PARA LA JCE

Para maximizar la eficiencia y sostenibilidad del sistema, recomendamos:

Priorización de proveedores con experiencia operativa local comprobada: La experiencia internacional es importante, pero no suficiente cuando se trata de la continuidad operativa de la JCE. La gestión de un sistema de identificación nacional *requiere proveedores* que no solo cumplan con los estándares técnicos, sino que también comprendan las condiciones reales del país. Seleccionar proveedores con infraestructura local establecida y una trayectoria de servicio comprobada evita sobrecostos en adaptaciones, logística y gestión operativa.

Integración de capacidades nacionales para garantizar eficiencia y sostenibilidad: El éxito de la implementación no solo depende de la tecnología instalada, sino también de la capacidad operativa para sostenerla en el tiempo. Aprovechar la experiencia acumulada en el país reduce riesgos, optimiza costos y garantiza la adaptación del sistema a la demanda real de la JCE sin necesidad de inversiones adicionales en infraestructura de soporte.

Evitar proveedores que impliquen costos adicionales de implementación: Seleccionar un proveedor sin presencia establecida en el país podría significar inversiones adicionales en infraestructura, personal de soporte y contingencias operativas. Apostar por un modelo ya probado en la JCE y con capacidad instalada permite reducir el riesgo de fallas en la implementación, evitando gastos innecesarios y garantizando un servicio operativo desde el primer día.

Entrega de un producto final sobresaliente y sostenible: Además de cumplir con los requerimientos técnicos y operativos, el producto final debe representar un salto cualitativo en la identidad digital del país. La implementación de una cédula moderna, con capacidades digitales avanzadas, mecanismos de autenticación segura y opciones de interoperabilidad con otros servicios gubernamentales garantizará un sistema sostenible a largo plazo. La elección de un proveedor con experiencia local permite maximizar la eficiencia en este proceso, asegurando una implementación sin fricciones y con mejoras escalables en el tiempo.

Adopción de la Infraestructura de Seguridad PKI: La integración de la Plataforma de Infraestructura de Claves Públicas (PKI – CA) permitirá la firma digital y autenticación segura de documentos e identidades electrónicas, alineándose con estándares internacionales. Este sistema garantizará mayor seguridad en la identidad digital, reduciendo riesgos de fraude y facilitando la interoperabilidad con servicios gubernamentales y privados.

Optimización de Procesos de Emisión: Implementar medidas para reducir los tiempos de emisión y renovación de documentos, mejorando la experiencia del ciudadano y garantizando procesos más ágiles y eficientes. La reducción de tiempos de espera y la implementación de tecnologías que automaticen los procedimientos serán clave para aumentar la satisfacción del usuario final.

Mantenimiento Preventivo y Correctivo: Aplicar un plan de mantenimiento programado que garantice la disponibilidad y óptimo funcionamiento de los equipos de impresión y autenticación digital. Un mantenimiento preventivo estructurado minimizará tiempos de inactividad y reducirá costos operativos, asegurando que la infraestructura se mantenga en condiciones óptimas a largo plazo.

ESPECIFICACIONES TÉCNICAS GENERALES

La implementación del nuevo sistema de emisión de la Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) representa una transformación clave en la gestión de identidad en la República Dominicana. Más allá de la simple modernización tecnológica, esta iniciativa debe garantizar una transición fluida, una operación ininterrumpida y un servicio ágil para los ciudadanos, minimizando riesgos y optimizando los recursos disponibles.

Este desafío no solo implica la adopción de tecnologías de última generación, sino también la integración efectiva con la infraestructura existente de la Junta Central Electoral (JCE). La propuesta del Consorcio Cédula 4.0 RD ha sido diseñada para ofrecer una solución adaptable, sostenible y alineada con las necesidades operativas reales, asegurando que la implementación no afecte la continuidad del servicio ni genere costos adicionales imprevistos.

Nuestra solución está diseñada para cumplir con los más altos estándares de seguridad, interoperabilidad y eficiencia operativa, garantizando:

- Un sistema robusto y escalable, capaz de responder a la demanda actual y futura de emisión de documentos de identidad.
- Automatización y optimización de procesos, reduciendo tiempos de emisión y mejorando la experiencia del ciudadano.
- Interoperabilidad con otros sistemas gubernamentales, facilitando la validación en tiempo real de los datos de identidad.
- Estrategias de contingencia y respaldo operativo, asegurando la continuidad del servicio ante cualquier eventualidad.

El Consorcio Cédula 4.0 RD presenta una solución efectiva y probada, con una ejecución estructurada que prioriza la estabilidad del sistema y el cumplimiento de los entregables exigidos en el Pliego de Condiciones Específicas, garantizando así un sistema de identidad seguro, eficiente y preparado para el futuro.

CUMPLIMIENTO DE NORMATIVAS Y ESTÁNDARES INTERNACIONALES

El sistema propuesto cumple con las siguientes normativas:

NORMAS DE IDENTIFICACIÓN Y SEGURIDAD

- OACI Doc 9303 – Normativa internacional para documentos de viaje electrónicos.
- ISO/IEC 14443 A y B – Tarjetas de proximidad sin contacto.
  CWA 15374 y CWA 14641 – Documentos de seguridad e identidad digital.

NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- ISO 27001 – Seguridad de la información en sistemas de identidad.
- ISO 14298 – Seguridad en la impresión de documentos de alta sensibilidad.

NORMAS DE PRODUCCIÓN Y CALIDAD

- ISO 9001 – Gestión de calidad en la producción y personalización.
- ISO 14001 – Sostenibilidad y reducción de impacto ambiental.

ENTREGABLES Y CANTIDADES EXIGIDAS

A continuación, se presentan los entregables en cantidad, de acuerdo con los requisitos del Pliego de Condiciones Específicas:

- Producción y Personalización de Cédulas
- Cantidad total de tarjetas a emitir: 8 millones de cédulas en un período de 18 meses.
- Material: Policarbonato multicapa con grabado láser.
  Chip sin contacto: Compatible con autenticación biométrica y validación PKI.

EQUIPAMIENTO PARA LA EMISIÓN DE CÉDULAS

- Impresoras láser de personalización: Cantidad requerida según demanda nacional.
- Sistemas de captura biométrica: Con capacidad de integración en centros de emisión.
- Servidores y software de gestión: Infraestructura optimizada para emisión, almacenamiento y validación de datos de identidad.

INFRAESTRUCTURA PKI – CA

- Implementación de la Plataforma de Infraestructura de Claves Públicas (PKI – CA) para firma digital y autenticación segura de identidades.
- Compatibilidad con estándares ICAO y gobierno digital.

MANTENIMIENTO Y SOPORTE TÉCNICO

- Cobertura: Presencial y remota en todo el territorio nacional.
- Tiempo de respuesta: Cumple con los niveles de servicio (SLA) exigidos por la JCE.
- Soporte técnico: 24/7 con capacidad de monitoreo y diagnóstico remoto.

CAPACITACIÓN PARA PERSONAL DE LA JCE

- Modalidad: Presencial y virtual.
- Documentación: Manuales técnicos y operativos detallados.
- Certificación: Asegurando la correcta operación y mantenimiento del sistema.

SEGURIDAD Y PROTECCIÓN DE DATOS

- La solución garantiza altos niveles de seguridad mediante:
- Cifrado de datos AES-256 y RSA-4096.
- Autenticación biométrica y multifactor.
- Protección contra ataques cibernéticos y falsificación de identidad.
- Gestión de accesos con trazabilidad y auditoría continua.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

PLAN DE IMPLEMENTACIÓN Y ENTREGABLES EN FASES

- Fase 1 – Prueba Piloto: Implementación inicial en una región específica para validar la interoperabilidad y ajustar procesos.
- Fase 2 – Despliegue Nacional: Expansión de la infraestructura a nivel nacional, garantizando estabilidad operativa.
- Fase 3 – Soporte Continuo: Mantenimiento y optimización del sistema tras su implementación.

ÍTEM I - ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS

1. ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS

1.1 INTRODUCCIÓN

1.1.1 DISEÑO Y PRODUCCIÓN

1.1.1.1 IMPRESOR DE ALTA SEGURIDAD

SELP es una imprenta de alta seguridad, certificada por Intergraf y por la norma internacional ISO 14298. Esta certificación garantiza un entorno de alta seguridad, y permite la fabricación de documentos de alto valor.

Como impresor de alta seguridad, SELP también tiene acceso a software de diseño gráfico fiduciario. Nuestros diseñadores integran elementos de seguridad (guilloches, arco iris, marcas ocultas, fondos numismáticos...) en los visuales que envían a nuestros clientes.

Nuestro sistema de producción es moderno y eficiente. SELP imprime fundamentalmente en offset y serigrafía, utilizando tintas que cumplen con la norma ISO 18745 (durabilidad) y con una solidez a la luz mayor a 4 en la escala de las lanas azules. Entre las tintas utilizadas, están las de formulación específica para el sistema de impresión offset (Pantone, UV, etc). Para la impresión de ciertos elementos de seguridad, se tienen las de seguridad con pigmento sólido, las tintas ópticas variables, entre otras.

Las diferentes capas que componen las tarjetas se ensamblan, laminan y cortan siguiendo un procedimiento muy preciso y perfectamente controlado.

La impresión es frecuentemente complementada con un hot-stamping de elementos de seguridad como: material de scratch seguro o banda magnética.

1.1.1.2 FABRICACIÓN DE TARJETAS SOBRE DIVERSOS MATERIALES

SELP está especializada en la producción de tarjetas plásticas (PVC, PET, Policarbonato), pero nuestros talleres también manejan una gran variedad de materiales alternativos como cartón, PLA y estructuras de madera.

SELP tiene una sólida experiencia con este tipo de substratos, gracias a la producción de grandes pedidos por los diferentes proyectos realizados.

1.1.1.3 CALIDAD Y RESPETO MEDIOAMBIENTAL

SELP está ampliamente reconocida por la calidad de sus productos y servicios. Esta notoriedad es el resultado de un compromiso total de la empresa.

Durante la producción, nuestras tarjetas se controlan de tres maneras diferentes: por medios mecánicos (cámaras, sistemas de rechazo automáticos en las máquinas), muestreos sistemáticos según nuestros procedimientos internos y muestreos aleatorios según las especificaciones de los productos.

SELP está certificada ISO 9001 (sitios de Angulema, Puy-Guillaume, Mareuil y Mumbai) por su gestión de calidad, ISO14001 (sitio de Angulema) por su gestión medioambiental, e ISO 27001 (sitio de Angulema) por la seguridad en el manejo de datos.

Respetuosas con el medio ambiente, nuestras fábricas destruyen los restos y mermas de manera programada y maximizan el reciclado de materiales en bruto y deshechos.

1.1.2 COMPONENTES ELECTRÓNICOS, SISTEMAS OPERATIVOS Y APLICACIONES

1.1.2.1 SEGURIDAD DE LOS COMPONENTES

SELP produce tarjetas de fidelización, tarjetas prepago, tarjetas bancarias y todo tipo de tarjetas de identificación.

La seguridad, el volumen de datos para almacenar y las aplicaciones necesarias definen la estructura de tarjeta a usar en cada caso (banda magnética, Mifare, chip de contacto, sin contacto, interface dual...) así como la normativa ISO a cumplir.

1.1.2.2 TARJETAS ELECTRÓNICAS, INLAYS, E-STICKERS, E-COVERS

El componente se incorpora en la tarjeta (mediante ensamblado / laminado / encartado)

De manera alternativa, también puede ser integrado:

- Junto a un adhesivo para la producción de e-stickers (trazabilidad de vehículos),
- En una lámina plástica flexible para la fabricación de inlays (en colaboración con diferentes proveedores),
- Sobre papel o teslín para la producción de e-covers (Pasaportes electrónicos).

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

1.1.3 CERTIFICACIONES

Todas las certificaciones originales, así como las traducciones de éstas, se encuentran en la sección de Documentos Adicionales, “Certificaciones SELP”

1.1.3.1 ISO 9001, 14001, 27001

1.1.3.2 ISO 14298:2013

1.2 PROCESO DE FABRICACIÓN DE TARJETA

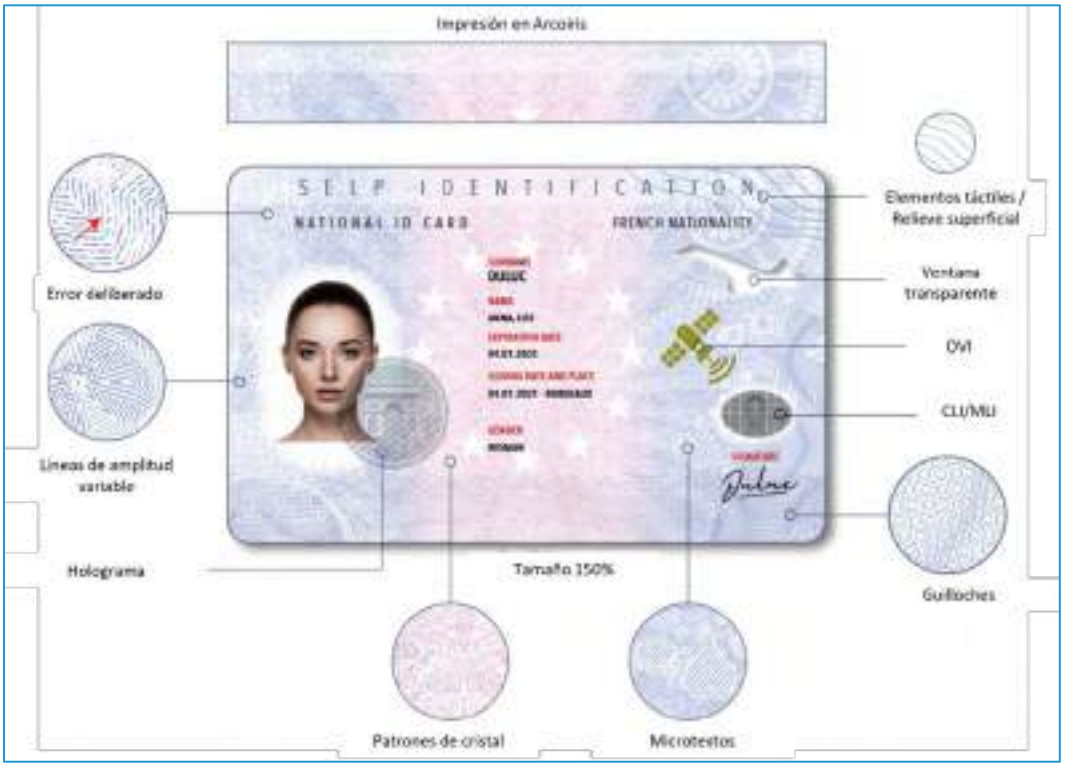
La fabricación de una tarjeta en SELP se divide generalmente en los siguientes pasos:

1.2.1 DISEÑO / ESTUDIO

El equipo DTP de SELP está al servicio de sus clientes para ofrecerles un diseño adaptado a sus necesidades. El diseño puede ser proporcionado por el cliente y adaptarse a las limitaciones de plástico, las dimensiones de la tarjeta, tintas offset, etc.

También podemos ofrecer un diseño original que luego se vuelve a trabajar en base a la retroalimentación del cliente, hasta obtener un visual satisfactorio. Cada planta de producción cuenta con una sala de DTP con varias estaciones de computadoras. Estas están equipadas con Adobe Suite (Illustrator, InDesign, Photoshop, Distiller 9 Pro y Acrobat 9 Pro), así como el software Prinergy Evo 5.1, Suitcase Fusion 3 Preps 6, QuarkXPress, XMF, Platón, FreeHand MX, Fortuna, EFI Colorproof XF.

El diseño es enviado como documento electrónico de baja resolución al cliente. Todos los elementos de seguridad se exponen. Elementos de seguridad especiales, tales como la exposición a lámparas UV se simulan en el documento. El cliente puede enviar rápidamente sus observaciones si los ajustes deben hacerse a nivel visual.



Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

Para este proyecto en específico, un diseño exclusivo para la tarjeta CIE y CI han sido creados de acuerdo con las especificaciones incluidas en el punto I.8 Características detalladas del ITEM I ESPECIFICACIONES TECNICAS DE LAS TARJETAS y de acuerdo a lo mencionado en el punto 1.27.7.1 Fases de diseño y puesta en marcha: “Cada oferente en su oferta debe entregar una propuesta de diseño gráfico de las nuevas tarjetas de República Dominicana en formato impreso y electrónico”.
Ambos diseños se están entregando junto con nuestra propuesta técnica, de manera física en formato booklet y en archivo electrónico.

1.2.2 PRUEBA DE COLOR

Una vez que el modelo visual es validado por el cliente, SELP crea un archivo de impresión completa del diseño en alta resolución (2400 ppp y superiores). Durante esta etapa, el diseño completo y cada elemento de seguridad se genera utilizando el software de seguridad dedicado y accesible sólo por organizaciones certificadas como Impresoras de alta seguridad (ISO 14298 INTERGRAF).

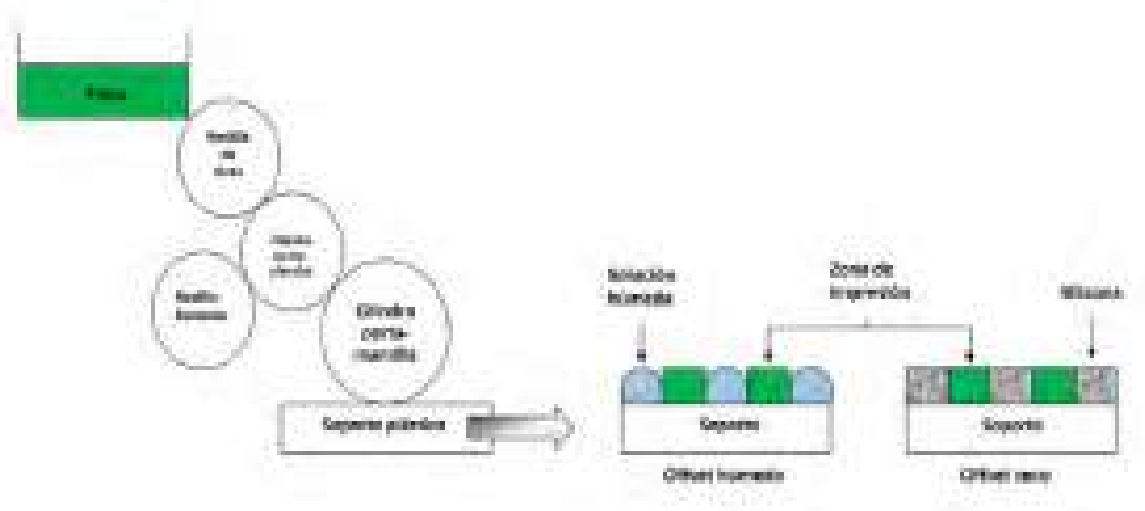
Este visual se imprime en papel satinado usando una impresora de alta calidad, calibrada de manera que los colores sean representados lo más cerca posible del resultado en el soporte de plástico.
Antes del inicio de la producción, esta primera hoja de plástico impresa con el diseño final se envía al cliente para ser validado y firmado.
Este paso también se puede realizar por el cliente directamente en la planta de producción SELP.

1.2.3 IMPRESIÓN

1.2.3.1 IMPRESIÓN EN OFFSET

Las características de seguridad gráficas son impresas en el soporte de plástico con la tecnología de impresión en offset, que requiere para su uso personal especializado. La calidad general de la impresión en offset está estrechamente relacionada con diversos parámetros que requieren un ajuste fino, tales como: hacer coincidir el color de tinta especificado (utilizando tintas de formulación específicas), minimizar el movimiento del soporte de plástico, minimizar la distorsión o el ruido de la imagen, tal como el polvo, verificar que las planchas impresas se soportan entre sí correctamente, etc.

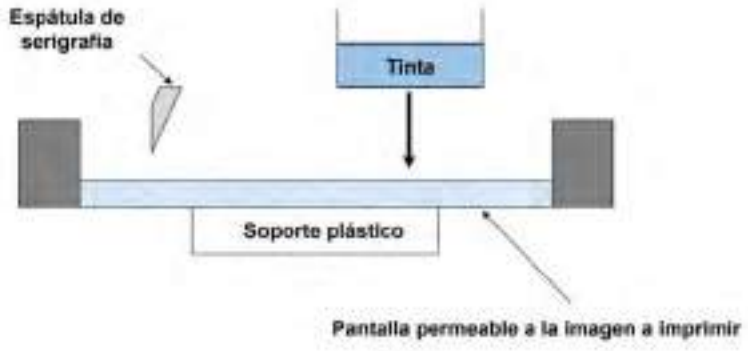
El nombre "offset" proviene del principio básico de esta técnica de impresión: la tinta es transferida de una plancha (imagen positiva) a una mantilla de caucho (imagen negativa) y luego al soporte a imprimir (como un positivo nuevamente). Cuando se hace una plancha de impresión, la imagen de impresión se convierte en receptora de tinta y repelente de agua, mientras que las áreas sin impresión son receptoras de agua y repelentes de tinta. Se pueden usar dos técnicas, "offset húmedo" u "offset sin agua", tal como está ilustrado abajo.



En la prensa de impresión, la plancha es montada en un cilindro portaplancha el cual, a medida que, rota, se pone en contacto con rodillos húmedos con agua (o solución humectante) y rodillos húmedos con tinta. La solución humectante humedece las áreas sin impresión e impide que la tinta penetre estas áreas. La tinta humedece las áreas de imagen, que son transferidas al cilindro portamantilla intermedio. El soporte de plástico capta la imagen a medida que este pasa debajo del cilindro portamantilla.

1.2.3.2 IMPRESIÓN SERIGRÁFICA

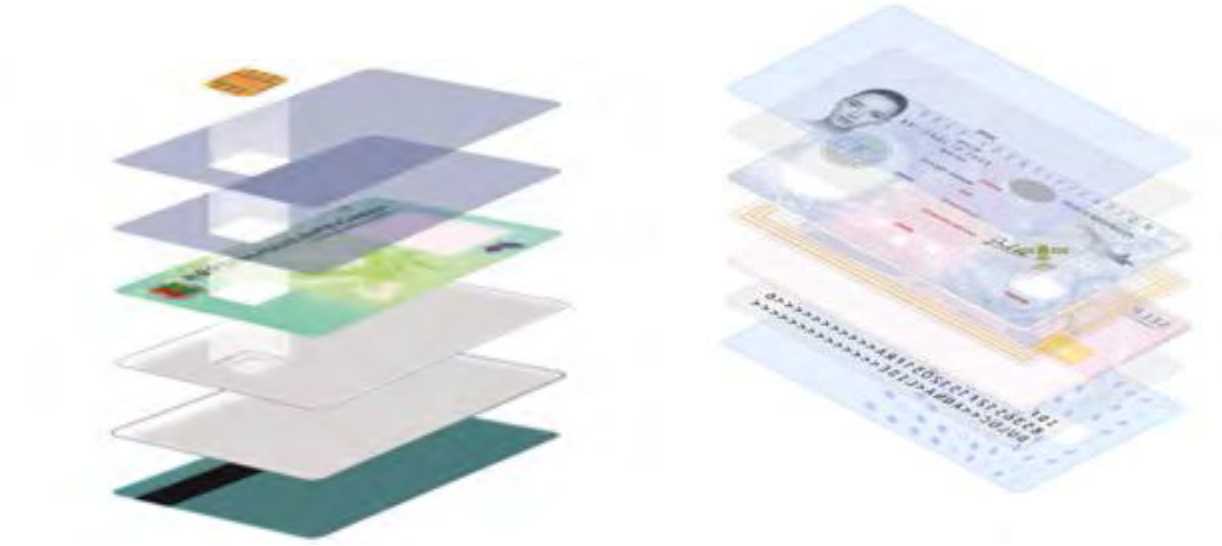
La serigrafía se usa para aplicar barnices o tintas especiales en el cuerpo de la tarjeta inteligente, una vez que el fondo principal ha sido impreso con offset. Una plantilla es aplicada a una pantalla de nailon o poliéster, mediante un procedimiento fotográfico, esparciéndola sobre un marco. Luego se escurre la tinta a través de la pantalla, depositándose la tinta sobre el soporte de plástico. Se necesita una pantalla distinta para cada color deseado.



1.2.4 ENSAMBLADO

Las tarjetas se componen generalmente de 5 a 8 capas de plástico u otros materiales, unidas entre sí. Las diferentes capas se ensamblan entre sí en un orden específico (dos capas externas, incrustaciones en el interior, y los componentes eléctricos en caso necesario. La composición de la estructura dependerá del material utilizado (PVC, policarbonato, PET, etc.), del tipo de tarjeta y del tipo de personalización que tendrá.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D



En nuestras soluciones, la construcción del cuerpo de la tarjeta está diseñada sin capas/materiales patentados que pudieran limitar el abastecimiento de materiales para cumplir con la producción de tarjetas de este proyecto.

1.2.5 LAMINADO

Cuando se tienen ensambladas las distintas láminas de material, se pegan entre sí mediante un proceso conocido como laminado. Se trata de un proceso durante el cual las láminas se calientan a cierta temperatura y presión para permitir que las diferentes capas, que inicialmente eran individuales, se adhieran entre sí y se unan permanentemente para formar un bloque sólido de material. Es durante el laminado que se puede dar a la tarjeta un acabado especial, como un efecto mate, espejo o satinado. Las tarjetas pueden grabarse incluso empleando placas de laminación. Esto se utiliza en los documentos de identidad para garantizar una seguridad aún mayor.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

1.2.6 CORTE

Una vez realizado el laminado, se procede al corte para obtener las tarjetas. Los formatos pueden variar según el documento.

1.2.7 PRE PERSONALIZACIÓN

El propósito de un documento de identidad es almacenar información personal que permita identificar a una persona con certeza. La certeza con la que se puede identificar a una persona no solo se deriva de la seguridad de la propia tarjeta, sino también de la forma en que los datos se almacenan de forma segura en la tarjeta.

1.2.7.1 ELÉCTRICA

Para las tarjetas que tienen un chip o una incrustación eléctrica, SELP realiza la pre personalización eléctrica de estos componentes. En general, esto consiste en cargar la aplicación que va a gestionar posteriormente los datos personales de cada individuo.
Esta pre personalización se puede realizar antes del montaje de la tarjeta, o después de este paso.

También tenemos, para las tarjetas bancarias, una máquina Datacard que permite hacer múltiples pasos en línea. Las tarjetas se montan y se cortan de antemano. A continuación, se colocan en la máquina que corta una ventana en la tarjeta, coloca el chip, lleva a cabo la pre personalización eléctrica del mismo, y prueba el componente en el extremo de la cadena.

1.2.7.2 GRÁFICA

En muchas ocasiones, se requiere hacer también una pre personalización gráfica. Normalmente consiste en imprimir algún número de serie utilizado para control de las tarjetas. Para este proyecto, cada tarjeta se identificará de manera individual durante el proceso de manufactura, mediante un número de serie en grabado láser.

1.2.8 CONTROL DE CALIDAD

SELP es reconocida por la calidad de sus productos y servicios. Esta notoriedad es la culminación del compromiso total de la empresa.

En la producción, nuestros productos se controlan de tres maneras distintas: mediciones automáticas (cámaras y sistemas de expulsión de máquinas), muestreo sistemático de acuerdo con nuestros procedimientos internos y muestreo aleatorio de acuerdo con las especificidades de los productos.

A lo largo de toda la fabricación, se realizan diferentes pruebas para corroborar la calidad de nuestros productos: dimensiones exactas (longitud, anchura y grosor), que el diseño de las tarjetas sea bien respetado, que la impresión no presente errores, pruebas de los componentes eléctricos, pruebas de materiales (resistencia física y química).

1.2.9 EMBALAJE Y ALMACENAMIENTO

De manera estándar, las tarjetas son empaquetadas en bandejas de 500 unidades. Posteriormente, estas bandejas se cubren con un film transparente y se embalan en paquetes de 10 unidades en cajas de cartón. Las cajas se sellan con un adhesivo SELP y se encintan para enseguida colocarlos en palés. Estos se recubren con una película transparente o negra, según las indicaciones del cliente, y se encintan. Finalmente, los palés se sellan para garantizar su inviolabilidad y trazabilidad.

Como la seguridad es una prioridad, particularmente en los sectores bancarios y de identidad, los palés se almacenan en una cámara de seguridad. SELP Secure dispone de amplios dispositivos de seguridad (cámaras de vídeo, enlaces con empresas de vigilancia, etc.) que le permiten manejar documentos sensibles.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

Para este proyecto en particular, se hará de acuerdo con lo especificado en las bases de la licitación. Las tarjetas serán empaquetadas en cajas que contendrán mil unidades correlativas, debidamente embaladas y selladas.

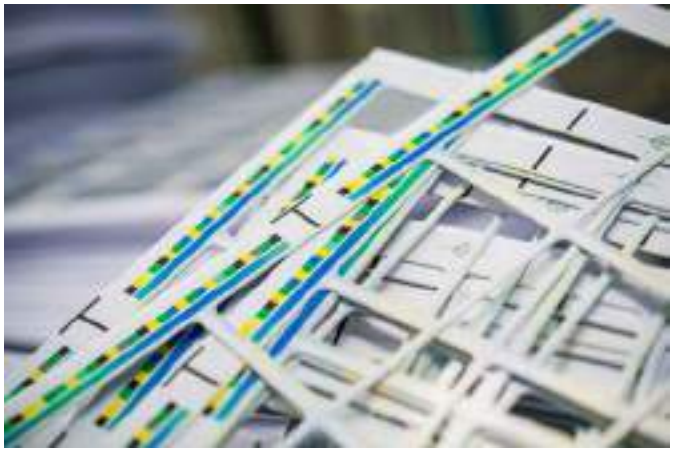
1.2.10 ENVÍO

Según el producto enviado, se elige el tipo de transporte (seguro o no). Para asegurar el transporte, tenemos varias esclusas entre la bóveda y el área de carga de tarjetas. No hay contacto entre el transportista y el interior de la planta de producción. Los palés se depositan en una esclusa intermedia; una vez que la esclusa se ha cerrado, el transportista carga los palés. El camión es liberado una vez que esté cerrado.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

1.2.11 DESTRUCCIÓN DE LOS PRODUCTOS SENSIBLES

Todos los residuos se procesan dentro de la planta de producción. Los materiales reciclables son recogidos para su reutilización y el resto de los residuos se destruyen en nuestro incinerador.



1.3 PROPUESTA TARJETAS DE POLICARBONATO

1.3.1 LA TARJETA EN POLICARBONATO

1.3.1.1 CUERPO DE LA TARJETA

Las tarjetas basadas en policarbonato propuestas por SELP cumplen con los más altos requerimientos de seguridad, cuando se escoge el grabado por láser para la personalización. El cuerpo multicapas de la tarjeta de policarbonato, laminado en caliente, se caracteriza por su alta durabilidad, seguridad y flexibilidad para esta tarjeta de última generación. Además, este tipo de material de tarjeta ofrece resultados de personalización superiores en términos de resolución y contraste entre el grabado por láser negro y los colores de fondo.

La tarjeta es laminada a partir de varias capas de películas, las cuales están todas hechas de materiales homogéneos. Este material es particularmente resistente al desgaste por uso y a la exposición a temperaturas altas. Comparado con otros materiales poliméricos, el policarbonato ofrece alta resistencia al esfuerzo mecánico, químico y térmico, así como a las influencias ambientales, lo que asegura una larga durabilidad de todas sus características.

Las composiciones del material y la tarjeta han sido optimizadas para satisfacer los requisitos de las técnicas de personalización por láser. Las películas exteriores en cada lado de la tarjeta son transparentes y protegen la impresión y personalización en las capas interiores.

Las características físicas de la tarjeta son, hasta donde es aplicable, totalmente conformes con las normas internacionales mencionadas más adelante. Esto se refiere a características tales como dimensiones de la tarjeta, rigidez a la flexión, resistencia a productos químicos, estabilidad dimensional de la tarjeta y deformación por temperatura/ humedad y por el uso normal, la exposición a la luz, la delaminación, la adhesión o el bloqueo y la transmisión luminosa.

El mejoramiento de la estructura del material brinda mejores resultados en la etapa de laminado, haciéndolo mucho más seguro. Después de 50,000 ciclos de torsión/flexión, la resistencia a la ruptura para la solución con material de policarbonato únicamente, es de ~ 200 N.

Las principales ventajas del policarbonato son las siguientes:

- Alta durabilidad,
- Alta flexibilidad y por lo tanto menor esfuerzo volumétrico.

1.3.1.2 ESTRUCTURA DE LA TARJETA

Las características físicas de la tarjeta son, hasta donde es aplicable, totalmente conformes con las siguientes normas internacionales mencionadas:

- ISO/IEC 7810
- ISO/IEC 7501-1
- ISO/IEC 7501-3
- ISO/IEC 10373-1
- ISO/IEC 7816

Las dimensiones de la tarjeta son las definidas por ISO/IEC 7810 capítulo 5. El tamaño y espesor corresponden al tipo de tarjeta ID-1 con las siguientes dimensiones:

- Largo: entre 85.47 mm y 85.72 mm
- Ancho: entre 53.92 mm y 54.03 mm
- Espesor: entre 0.68 mm y 0.84mm.

El cuerpo de la tarjeta y sus características de impresión están diseñados para una vida útil de 10 años en condiciones normales de desgaste y almacenamiento. Las tarjetas que fabricamos son conformes al perfil 3D de la norma ISO24789.

La tarjeta de policarbonato grabable por láser es un compuesto multicapas, es decir que es producido "fundiendo" entre sí varias capas durante un proceso de laminado en caliente. Las características de las capas y el proceso de laminado en caliente en sí aseguran una unión duradera, segura y flexible del compuesto. La tarjeta terminada tiene un espesor según los requisitos de ISO 7810 y, junto con las características especiales del material, ofrece una gran flexibilidad.

Por lo mismo, la deformación que se pudiera presentar es una deformación causada por el uso normal de la tarjeta. Nuestras tarjetas se someten a una fase de calificación durante su desarrollo, que resulta en pruebas de flexión/torsión de acuerdo a la norma ISO10373. Posteriormente en la fase de producción, las muestras se toman en lotes y se someten a las mismas pruebas de flexión/torsión, para asegurar su conformidad a las normas.

La durabilidad del material laminado excede las especificaciones de la norma ISO 10373. También excede la durabilidad y resistencia a la delaminación convencional.

Hablando de toxicidad, las tarjetas no presentan ningún riesgo tóxico en su uso normal de acuerdo a la norma ISO 7810. Las tarjetas, al cumplir con la norma ISO 10373 e ISO 7810, son resistentes a los efectos químicos inherentes al manejo y uso normales.

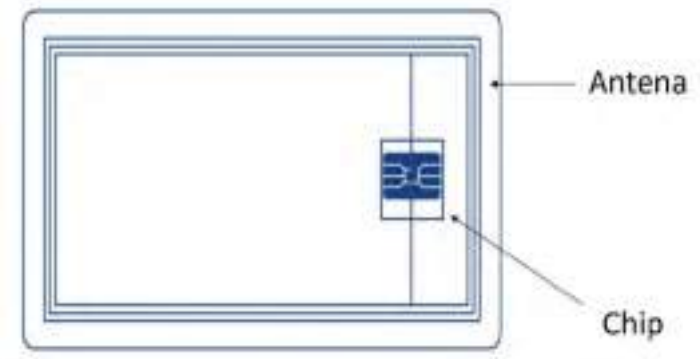
En cuanto a la estabilidad térmica, la tarjeta se mantendrá legible mecánicamente a temperaturas que oscilen entre -10°C y +50°C. La tarjeta no perderá su funcionalidad en caso de quedar expuesto a temperaturas que oscilen entre -35°C y +80°C.

Con respecto a la humedad, la tarjeta será legible mecánicamente a una humedad ambiente relativa del 5% al 95% y una temperatura máxima de bulbo húmedo de 25 °C. La tarjeta no perderá su fiabilidad en caso de quedar almacenada o expuesta a una humedad relativa ambiente del 0% al 100% (sin condensación).

1.3.2 TARJETA CON CHIP SIN CONTACTO

Las tarjetas con chip sin contacto tienen las mismas características funcionales que las tarjetas con microprocesador, pero con tecnología RFID (Identificación por radiofrecuencia) que permite intercambiar datos simplemente acercando la tarjeta a un lector compatible, sin necesidad de contacto físico. Están alimentadas por inducción (la inducción es un principio físico que transforma la energía mecánica [movimiento] colocada en un campo magnético en energía eléctrica) y equipados con una antena para comunicarse a distancias de unos pocos centímetros por radiofrecuencia (usualmente 13,56 MHz).

- El chip está conectado a la antena. Ambos están incrustados en el cuerpo de la tarjeta
- La comunicación con el chip se realiza únicamente a través de la antena
- La tarjeta se lee a distancia (de 0 a 10 cm)



En términos de fabricación, la estructura utilizada está compuesta por un prelam de policarbonato (incluido el chip y la antena) insertado entre varias capas de policarbonato. Las tarjetas con chip sin contacto cumplen, hasta donde es aplicable, con la norma ISO 14443.

El chip sin contacto para las tarjetas de esta licitación será conforme a las especificaciones detalladas en la Tabla 3.2 (NXP JCOP 4 o equivalente).

Las características principales del chip son:

- El mejor de su clase en términos de rendimiento y una excelente comunicación por radiofrecuencia
- Java Card v3.0.5 Edición Clásica
- GlobalPlatform:
  - Configuración de la identificación de GP v2.2
  - GP v2.2 Configuración de las directrices de mapeo v1.0.1
  - GP v2.3 Configuración de la implementación común v2.0
- ISO 7816-3 T=0, T=1
- ISO 14443 (hasta 848kbps)
- Soporte de doble interfaz

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

- Compatibilidad con DES, 3DES, AES, RSA, ECC y SHA mediante coprocesadores dedicados basados en hardware
- Sistema operativo ubicado en ROM que potencia el rendimiento de ejecución
- Memoria no volátil (NVM) disponible para aplicaciones y datos de personalización de hasta 180kB
- Certificación EAL 6+ de criterios comunes
- Aprobación EMVco
- Certificación FIPS

Aplicaciones incluidas:

- Documento nacional de identidad electrónico
- ePKI
- Firma Digital

Otras aplicaciones que se pueden cargar en este chip:

- Pasaporte electrónico
- Tarjeta electrónica de permiso de conducir
- Tarjetas electrónicas sanitarias y de prestaciones sociales
- Servicios electrónicos
- Pago y micropago
- Transporte público
- Acceso lógico y físico

Este chip albergará los aplicativos de Documento de viaje electrónico de acuerdo con ICAO 9303, Firma electrónica e Identificación Ciudadana.

Respecto a las especificaciones técnicas solicitadas para el chip, se presenta a continuación la información solicitada:

TABLA 3.2

	Respuesta	Comentarios adicionales
9.1 Características del chip sin contacto		
CPU de 16/32 bits	Cumplimos	
Certificación CC EAL5+ o superior (o equivalente)	Cumplimos	La certificación incluida es EAL6+ Favor de dirigirse a la sección de Documentos Adicionales, “Documentación Técnica Adicional”, donde se incluye la certificación solicitada.
Criptoprocesador hardware para operaciones criptográficas	Cumplimos	
Clave simétrica (Triple DES con clave de hasta 168 bits, AES hasta 256 bits)	Cumplimos	

Clave pública (RSA con longitud de clave de hasta 4096 y ECC con clave de hasta 512 bits)	Cumplimos	
Hash SHA1 y SHA2	Cumplimos	
Generador de números aleatorios de acuerdo a AIS31	Cumplimos	
Protección contra descargas ESD.	Cumplimos	
Número de serie único	Cumplimos	
Reloj interno asíncrono	Cumplimos	
Firewalls de seguridad entre particiones de memoria	Cumplimos	
Memoria no volátil necesaria para la incorporación de las aplicaciones requeridas y los datos especificados en el presente punto 1.2.4. Características electrónicas y del sistema operativo	Cumplimos	La memoria no volátil incluida en el chip es de 180k. Se considera suficiente de acuerdo a la información compartida por la JCE en los diferentes documentos de la presente licitación.
Retención de datos en memoria no volátil de al menos 10 años	Cumplimos	
Al menos 500.000 ciclos de lectura / escritura garantizados	Cumplimos	Típicamente 100.000.000 ciclos de lectura/escritura.
Interfaz de RF ISO/IEC 14443 A/B de hasta 848kbits/s, pudiendo ofrecer modos de transmisión RF mejorados	Cumplimos	Tipo A solamente. Compatible con VHBR (velocidad de transmisión muy alta)
9.2Características del Sistema Operativo		
Protocolo de transmisión de acuerdo con ISO/IEC 14443 A/B Interfaz de comandos de acuerdo a ISO/IEC 7816-4 y PCSC.	Cumplimos	
UID / PUPI aleatorio	Cumplimos para el UID	UID de 7 octetos. PUPI no aplica para Tipo A.
Certificación Common Criteria EAL4+ o superior (o equivalente).	Cumplimos	Favor de dirigirse a la sección de Documentos Adicionales, “Documentación Técnica Adicional”, donde se incluyen las certificaciones solicitadas del OS.
En caso de que el Sistema Operativo sea basado en JavaCard, se deberá bloquear la posibilidad del agregado de nuevas aplicaciones una vez incorporadas las aplicaciones requeridas.	Cumplimos	
Documento de Viaje Electrónico de acuerdo con ICAO 9303		
SAC (Supplemental Access Control).	Cumplimos	
EAC (Extended Access Control).	Cumplimos	
AA (Active Authentication)	Cumplimos	
Funcionalidad de Firma Electrónica		
Acceso protegido mediante PIN / PUK	Cumplimos	
Algoritmos de firma RSA y ECDSA	Cumplimos	
Soporte para claves RSA en formato CRT y en formato normal (exponente privado, exponente público y módulo).	Cumplimos	
Claves RSA con soporte para componentes p y q de longitud variable	Cumplimos	
Capacidad de almacenar, generar y usar claves RSA de, como mínimo, 4096 bits de longitud Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: Para el caso del tamaño de llaves de la Autoridad Ciudadana, tanto la Autoridad Raíz como la Autoridad Subordinada deben tener un tamaño de llaves de 4096 bits.	Cumplimos	

Para el caso de los certificados de usuario (ciudadanos) será de 2048 bits. Las claves que componen la "PKI de Firma Digital" y la "PKI de Firma de Documentos" deben estar basadas en los estándares X.509v3 y RFC 5280.		
Soporte de diversas curvas ECDSA, incluyendo las más habituales (NIST P-256, Brainpool, etc Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: Se debe tener la capacidad de soportar curvas elípticas NIST P-256, BrainpoolP256r1, entre otras, conforme con los estándares: • TR-03111 Elliptic Curve Cryptography (ECC) based on ISO 15946. Technical Guideline TR-03111, Version 2.0 • ISO15946-1 ISO/IEC. 15946-1. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General. 2002. • ISO15946-2 ISO/IEC. 15946-2. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures. 2002. • ISO15946-3 ISO/IEC. 15946-3: Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 3: Key establishment. 2002.	Cumplimos	
Operaciones de firma digital	Cumplimos	
Intercambio de claves de sesión o simétricas entre dos entidades basado en RSA/ECDSA/ECDH	Cumplimos	
Claves almacenadas en ficheros/elementos independientes	Cumplimos	
Condiciones de acceso independientes para cada clave/elemento	Cumplimos	
Estructura interna de ficheros según el estándar ISO/IEC 7816-15 (PKCS#15)	Cumplimos	
Deberá disponer de capacidad de memoria suficiente para almacenar hasta 4 certificados, con sus correspondientes claves, incluyendo el caso de claves RSA 4096 Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: El eID debe ser capaz de almacenar certificados x.509 que permitan a los ciudadanos gozar de los servicios de criptografía	Cumplimos	
Securización de los mensajes transmitidos entre la tarjeta y el terminal mediante canal seguro de acuerdo a CEN14890 o equivalente	Cumplimos	
Confidencialidad de los datos transmitidos mediante triple DES / AES	Cumplimos	
Autenticación de la información intercambiada entre las dos partes; incorporación de checksum criptográfico de tipo MAC según ANSI X9.19 y DES	Cumplimos	

Protocolo de establecimiento de las claves de sesión basado en el esquema propuesto en ISO/IEC 9798-3 Authentication SASL Mechanism Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: Para mayor claridad, la "Aplicación de Firma Electrónica" debe estar certificada según CC EAL5+, compatible con el conjunto y comandos ISO-7816	Cumplimos	
Claves de sesión derivadas a partir de información generada por las partes involucradas en el establecimiento del canal seguro; el cálculo de las claves se realiza según ANSI X9.63 Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: Para mayor claridad, la "Aplicación de Firma Electrónica" debe estar certificada según CC EAL5+, compatible con el conjunto y comandos ISO-7816	Cumplimos	
Software de gestión y drivers		
Drivers de la tarjeta (PKCS#11, CSP, Card Module, etc)	Cumplimos	Punto 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato"
Software de gestión que permita gestionar las operaciones más habituales con la tarjeta; por ejemplo, cambio de PIN, desbloqueo de PIN, borrado de certificados, etc. Deberá garantizar el funcionamiento del documento en distintos sistemas operativos (Windows, Linux, MacOS). Deberá garantizar el funcionamiento del documento en distintos navegadores	Cumplimos	Punto 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato"
Se deberán aportar librerías o SDKs que faciliten el desarrollo de aplicaciones para dispositivos móviles, con sistemas operativos Android e IOS	Cumplimos	Punto 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato"
El software suministrado deberá ser actualizado, adecuándolo a nuevos SO, Navegadores, corrección de bugs, etc., durante el tiempo de vida del proyecto	Cumplimos	Punto 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato"
Funcionalidad de Identificación Ciudadana		
Se almacenarán los datos de filiación del ciudadano de manera estructurada	Cumplimos	De acuerdo con el estándar ISO7816-4 file system
El acceso a los mismos se realizará por medios seguros	Cumplimos	Existen muchos mecanismos de seguridad estándar disponibles para garantizar la integridad, confidencialidad y autenticidad
Preferiblemente, de acuerdo con la Guía Técnica TR-03110 del BSI o similar Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: No es necesario control de acceso basado en roles basado EAC2 y/o Identificación Restringida para la función de elecciones.	Cumplimos	Cumplimos con la normativa eIDAS y somos compatible con TR-03110 v2.21, dentro del alcance implementado que incluye PACEv2 (incluyendo PACE con PIN), EACv1 y EACv2

Favor de referirse a la sección de Documentos Adicionales, "Documentación técnica adicional", donde se encontrará información adicional sobre el chip, así como las certificaciones Common Criteria solicitadas.

1.3.3 MIDDLEWARE

En la vida cotidiana existe una creciente necesidad de realizar acciones digitales con restricción de seguridad, que permita al ciudadano tener una burocracia inteligente y menos pérdida de tiempo. Las aplicaciones típicas se resumen en “Autenticación de sitio web” y “Firma digital”.

Con el fin de dar al ciudadano la posibilidad de utilizar la infraestructura digital, se le proveen tarjetas inteligentes / token, cuyo núcleo es un elemento seguro que contiene un certificado digital. Este certificado es accesible mediante un PIN, y por esta razón existe la necesidad de permitir también las funcionalidades de “Desbloquear PIN”, “Cambiar PIN”, “Cambiar PUK”.

Dado que hay muchos sistemas operativos diferentes y una gran variedad de tarjetas inteligentes y tokens, no es posible interconectarlos sin un componente de software externo. Todas las aplicaciones que se ejecutan en el sistema operativo utilizan la interfaz PKCS#11 (o CSP/TokenD) para ejecutar comandos criptográficos. Cada tarjeta inteligente habla en su propio idioma. De tal forma que el middleware es el traductor entre las aplicaciones (SO) y las tarjetas inteligentes.

Para esta licitación se contempla el Middleware Universal “UMW” u otro equivalente. El UMV es un conjunto de bibliotecas y herramientas estándar para interconectar varios dispositivos criptográficos, como tarjetas inteligentes y tokens PKI, con otros dispositivos (como PC de escritorio). UMW permite al usuario gestionar sistemas basados en certificados sin necesidad de tener un alto conocimiento de los mismos.

ESTRUCTURA DE MIDDLEWARE UNIVERSAL

El UMW consta de 2 componentes:

- Administrador de PKI:

Es una aplicación multiplataforma para la gestión de tarjetas que permite operaciones como cambio de PIN o PUK, desbloqueo de PIN, obtención de información sobre la tarjeta, importación o exportación de certificados.

- Bibliotecas del Middleware Universal:

Son una colección de archivos que contiene la implementación de los principales estándares criptográficos, por ejemplo, PKCS#11, MS CSP, MS CSP-NG, TokenD, CryptoTokenKit.

Las bibliotecas del UMW están compuestas por:

a) Un módulo de biblioteca que expone una API compatible con PKCS#11 v2.40/v3.0, totalmente compatible con los siguientes sistemas operativos: Windows, Linux y Mac OS X
b) Un módulo del sistema que expone una API compatible con la especificación del Proveedor de Servicios Criptográficos de Microsoft (MS CSP) (CryptoSPI / 2006) y con la API de criptografía de próxima generación (CNG o CSP-NG)
c) Un módulo del sistema "almacén de certificados" que implementa un mecanismo para la importación automática de certificados en el almacén "Personal" del usuario de Windows. Este mecanismo es compatible con el servicio de propagación de certificados de Windows.
d) Un módulo del sistema que expone una API compatible con el Apple TokenD para MacOS hasta 10.13.
e) Un módulo del sistema que expone una API compatible con Apple CryptoTokenKit para MacOS 10.13 o superior.

Dichos módulos proporcionan varias interfaces de programación, lo que permite en aplicaciones de terceros el uso de tarjetas inteligentes criptográficas y tokens.

Favor de referirse a la sección de Documentos Adicionales, “Documentación técnica adicional”, al documento “Datasheet Universal Middleware” donde se tiene información adicional sobre el Middleware.

1.3.4 PERSONALIZACIÓN GRÁFICA

La tarjeta propuesta puede ser personalizada gráficamente con una foto de alta resolución en escala de grises y el texto de los datos variables, con una impresora de grabado por láser.

El grabado por láser es un proceso mediante el cual, las capas de policarbonato del cuerpo de la tarjeta químicamente modificadas son carbonizadas con un haz de láser de alta precisión. Esta tecnología permite imprimir datos debajo de la superficie de la tarjeta. Combinado con el policarbonato, el grabado por láser también abre el camino a características de seguridad variables únicas, tales como grabado táctil, imagen fantasma perforada, impresión de microtexto variable o imagen láser cambiable/múltiple (CLI/MLI).

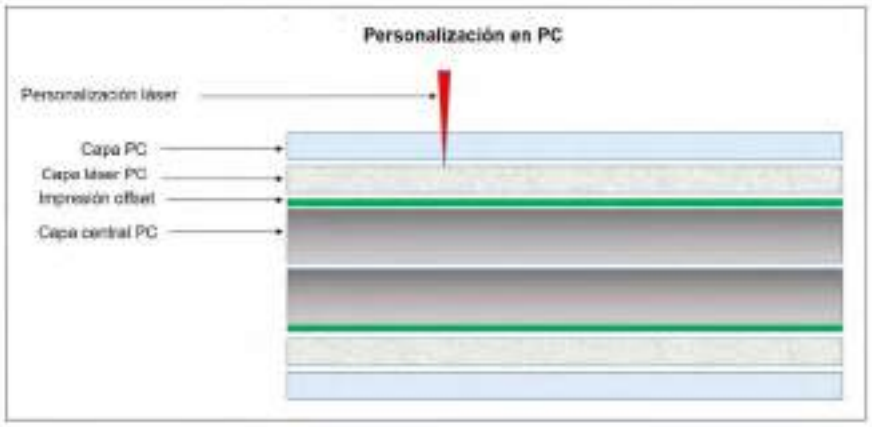


IMAGEN EXCLUSIVAMENTE ILUSTRATIVA

La tarjeta no debe ser expuesta al agua u a otros solventes que puedan debilitar su construcción, dejar rastros forenses o dañar el componente de microchip que pudiese tener. Tampoco debe ser conectada a dispositivos o sistemas para los cuales no está diseñada.

En las soluciones que ofrecemos, el cuerpo de la tarjeta en blanco y el proceso de personalización de esta, en combinación, no constituyen una solución dependiente o patentada que excluya a los proveedores de tarjetas y/o sistemas de personalización.

1.3.5 IMPRESIÓN DE SEGURIDAD

SELP tiene acceso a una experiencia única en la impresión de seguridad de diseños y de elementos de seguridad.

Esta sección presenta una lista de diversas certificaciones de seguridad que SELP puede reunir para diseñar un documento de identidad de alta seguridad personalizado basado en soportes de plástico tales como tarjetas inteligentes y páginas de datos electrónicas de pasaportes.

1.3.5.1 CERTIFICACIÓN PARA IMPRESORES DE SEGURIDAD

La certificación CWA 14641 para impresores de seguridad es un procedimiento implementado por la “International Confederation for Printing and Allied Industries” ("Confederación internacional para las industrias de la impresión y asociadas") (Intergraf). Esta da fe de que se han cumplido las reglas y reglamentos estrictos correspondientes a la seguridad del producto y la producción y de que satisfacen a los auditores.

Los criterios de certificación incluyen:

Seguridad del edificio, control de admisión, vigilancia por video, administración de llaves, elección y vigilancia de los empleados, comportamiento en caso de emergencias, contacto directo con la policía en caso de una alarma, gestión de productos y trazabilidad de los procesos de producción, el almacenamiento y la entrega, destrucción de maculación, seguridad EDP y gestión de datos, monitoreo de visitantes, etc.

SELP está certificado como un Sistema de gestión de alta seguridad para impresión segura con el ámbito de impresión de plásticos, fabricación e integración de tarjetas de alta seguridad.

1.3.5.2 CREACIÓN DE UN DISEÑO GRÁFICO SEGURO

Para la creación del diseño gráfico seguro que será impreso en el fondo de la tarjeta, SELP proporciona a su cliente toda su experiencia como impresor de plásticos de alta seguridad.

Creación del diseño gráfico y maqueta digital

La integración de diversas características de seguridad distintas dentro de un solo diseño gráfico requiere personal formado, tanto con experiencia técnica como con sensibilidad artística. El diseño gráfico final debe satisfacer a las limitaciones y requerimientos exclusivos de cada cliente, respetando las normas solicitadas (como ICAO para ciertos documentos), presentando elementos gráficos tales como:

- Diseño gráfico de un documento o tarjeta ya existente,
- Estándar internacional o regional,
- Monumentos nacionales,
- Jefes de Estado,
- Sitios geográficos excepcionales,
- Escudo y bandera,
- Mapa del país,
- Etc.

El diseño gráfico es enviado electrónicamente al cliente en forma de un archivo gráfico vectorial (en pdf) con cada elemento de seguridad detallado. Se simulan iluminaciones especiales - como la exposición a la luz UV. El cliente puede entonces rápidamente enviar su retroalimentación y si es necesario realizar cualquier ajuste al diseño gráfico.

Listo para imprimir e impresión en color real

Una vez que el diseño gráfico modelo es validado por el cliente, SELP crea un archivo de impresión completo del diseño gráfico en muy alta resolución (2400 dpi y superior). En esta etapa, todo el diseño gráfico y cada característica de seguridad son generados usando software de seguridad dedicado, solo accesible a organizaciones certificadas como Impresores de alta seguridad (CWA 14641) por la confederación internacional de impresores e industrias asociadas.

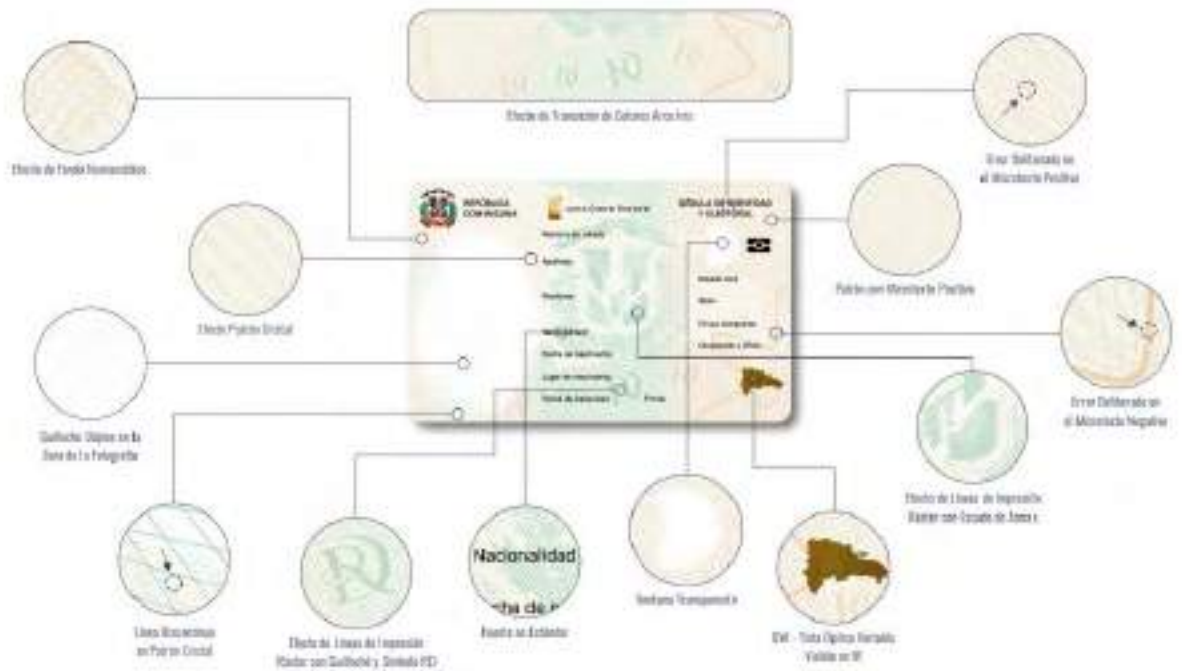
Este diseño gráfico es impreso en papel brillante con una impresora de alta calidad que ha sido calibrada para representar los colores lo más fielmente posible a cómo serán representados durante la producción en serie. Es encuadernado en dos folletos de presentación que son enviados al cliente para su aprobación.

Una vez aprobados, los diseños serán entregado en ficheros vectoriales de formato electrónico a la JCE, quien será la propietaria de todos los derechos sobre estos diseños.

Firma en la lámina lista para imprimir e inicio de la producción

Antes del inicio de la producción en volumen, la primerísima lámina de plástico impresa con el diseño gráfico final es enviada al cliente para validación y firma. Este paso también puede ser realizado por el cliente directamente en la fábrica SELP.

1.3.6 ELEMENTOS DE SEGURIDAD



En esta sección se describen los diferentes niveles de seguridad disponibles en el universo de elementos de seguridad utilizados en los documentos de identidad, así como la descripción detallada de cada uno de aquellos solicitados para las tarjetas de identidad en policarbonato. Todos estos elementos de seguridad se incluyen en los diseños exclusivos creados para la CIE y CI, objetos de esta licitación.

1.3.6.1 NIVEL DE SEGURIDAD

Los niveles de seguridad de autenticación de tarjetas son un enfoque estructurado para verificar la autenticidad de un documento, asegurando que cumpla con estándares estrictos en diferentes etapas de la inspección. Los niveles de seguridad y medios de verificación son los siguientes:

1.3.6.2 IMPRESIÓN DE SEGURIDAD

La impresión de seguridad utiliza técnicas de impresión gráfica sencillas, que son difíciles de reproducir, con el propósito de limitar la posibilidad de que los defraudadores copien o escaneen la tarjeta y recreen una

falsa. Estos elementos gráficos especiales constituyen la base de la seguridad de una tarjeta, y son los elementos de seguridad más utilizados en el sector de la identidad.

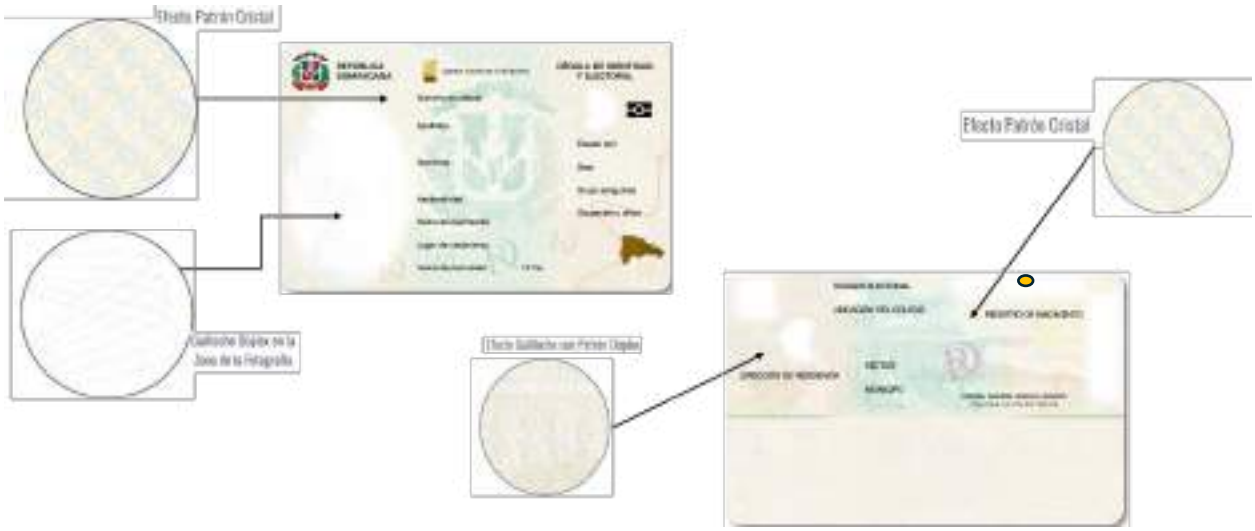
Incluyen guilloches, fondos iridiscentes, fondos numismáticos, motivos de cristal, microtextos, microlíneas.

1.3.6.2.1 GUILLOCHES

Los guilloches son elementos de seguridad gráficos elaborados exclusivamente con software de diseño de seguridad.

Un guilloche es un motivo compuesto de líneas muy delgadas entretejidas que forman una imagen única que solo puede ser recreada con el software del equipo y los parámetros usados en la creación del diseño original. El estilo gráfico del motivo guilloche consta de la interacción de líneas delgadas en motivos geométricos en aspectos positivo, negativo, radiante, deformación, marco o fondo.

El patrón cristal, el cual se puede visualizar en el diseño propuesto de CIE y CI, es un tipo de guilloche.



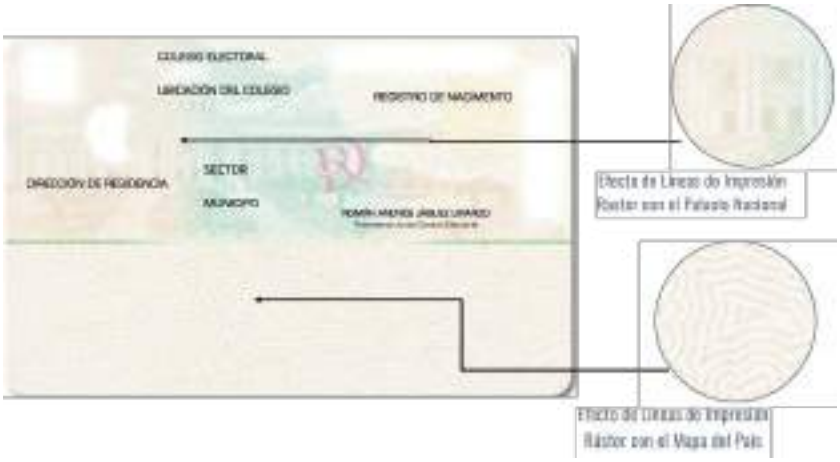
1.3.6.2.2 IMPRESIÓN EN ARCOÍRIS

Un fondo en arco iris se crea mezclando dos o cuatro colores sobre toda la superficie de la tarjeta. Los gradientes de color visibles o fluorescentes bajo radiación UV cambian continuamente de un color a otro. Es por ello que los bordes de color mezclándose entre sí representan una característica de seguridad que no puede ser copiada con las tecnologías de fotocopia o de digitalización en alta resolución.

1.3.6.2.3 MICROLÍNEAS DE AMPLITUD VARIABLE

Las microlíneas de amplitud variable, llamadas también Raster, son líneas muy pequeñas que se utilizan para crear tramas destinadas a impedir la copia de documentos de identidad, mediante el cambio de grosor y la distancia de las líneas, manteniendo constante la cobertura de tinta.

La idea detrás de este enfoque es que el proceso de falsificación no sería tan preciso y se verían diferentes tonos de color debido a la variación en el grosor del trazo y la distancia entre las líneas individuales.



1.3.6.2.4 MICROTEXTOS (POSITIVOS Y NEGATIVOS)

El microtexto es un texto muy pequeño que se extiende sobre el fondo de la tarjeta. Sólo puede leerse con una lupa y es imposible reproducirlos con las técnicas de impresión convencionales. Generalmente se utilizan para escribir el nombre de un país, su moneda, la autoridad que emite el documento o un mensaje. El objetivo de esta técnica es evitar la duplicación mediante fotocopia o escaneado.

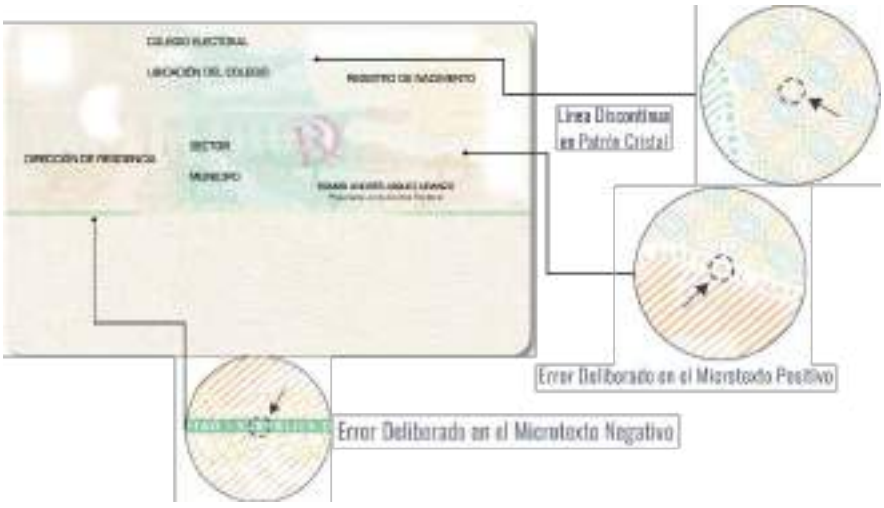
Reproducir microtextos con un alto grado de precisión y detalle es extremadamente complicado, ya que la finura de la impresión dificulta su producción y, por tanto, su reproducción. Al ser parte integrante del grafismo de la tarjeta y estar impreso al mismo tiempo que ésta, el microtexto es fácil de ocultar.

El microtexto suele ir unido a errores deliberados para crear zonas en la tarjeta que sean reconocibles y, por tanto, fáciles de comprobar.

1.3.6.2.5 ERRORES DELIBERADOS

Un error deliberado está pensado para eludir al falsificador: ya sea haciéndole creer que el documento que está copiando contiene un error de impresión, por lo cual no lo reproducirá en el documento falso (por ejemplo: un carácter no bien formado, un punto añadido, un corte en una línea delgada) o, por el contrario, ocultando un error deliberado que no será detectado por el falsificador, de modo que éste no lo reproducirá (por ejemplo: un carácter invertido en un microtexto, o una letra faltante).

Los errores deliberados son elementos de seguridad fáciles de incorporar y ocultar, pero también fáciles de comprobar por las autoridades competentes.



1.3.6.2.6 FONDOS NUMISMÁTICOS

Un fondo numismático usa una onda modulada que consta de líneas paralelas delgadas cuya orientación, grosor y espaciado varían a fin de generar un efecto de relieve y crear imágenes y / o texto de estas superficies elevadas. Una segunda serie de líneas a un ángulo de orientación distinta a la del primero (normalmente de un color diferente) puede reforzar eficazmente la impresión de relieve y crear un efecto tridimensional.

Esta característica gráfica ayuda a detectar la alteración de datos variables y documentos falsificados puesto que es difícil crear ambas líneas delgadas y los tonos de color que componen los diseños mediante escáneres y fotocopiadoras.

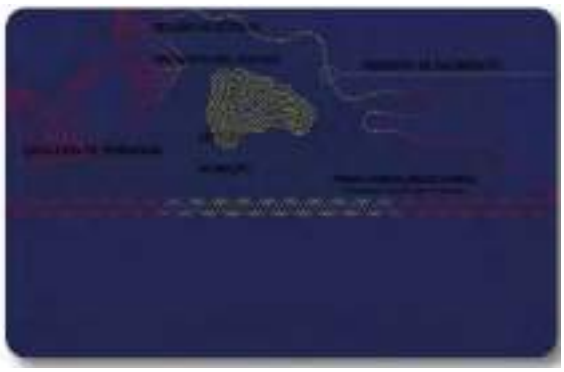
1.3.6.3 TINTAS UV INVISIBLES

Las tintas especiales con propiedades que reaccionan a la luz ultravioleta (UV) son una parte importante de la protección de un documento de identidad. Cuando se exponen a la luz UV, estas tintas cambian de color y se vuelven reflectantes.

Esta tecnología abre posibilidades creativas para mejorar la seguridad de los documentos impresos. Al incorporar estas tintas especiales durante el proceso de impresión, se pueden incorporar detalles ocultos en el documento, creando nuevos patrones estéticos o resaltando rasgos distintivos como escudos, lemas y otras sutilezas.

Este proceso de seguridad de segundo nivel ofrece una sólida protección contra la imitación y la falsificación. Combinando el uso de estas tintas reactivas a los rayos UV con complejos guilloches, la seguridad de los documentos aumenta aún más.

En resumen, el uso de tintas UV reactivas representa una forma segura y estéticamente discreta de añadir elementos de seguridad a los documentos impresos. Estas tintas ofrecen una solución rentable para combatir la falsificación y reforzar la integridad de los documentos oficiales.



1.3.6.3.1 GUILLOCHES EN UV

Finas líneas entrelazadas, generalmente de naturaleza geométrica, crean una imagen única que impide la reproducción sin las herramientas y configuraciones originales que reaccionan a la luz UV.

1.3.6.3.2 MICROTEXTOS EN UV

Los microtextos son elementos textuales sutiles y detallados. Es posible hacer microletras que reaccionan a la luz ultravioleta. Por ejemplo, cuando pasa una fuente de luz UV, se puede mostrar el nombre del país emisor, la moneda nacional, la entidad emisora o un mensaje específico.

1.3.6.3.3 ARCOIRIS EN UV

Un degradado sutil y gradual de dos a cuatro colores en todo el sustrato, similar al efecto visual de un arco iris reaccionando a la luz ultravioleta. Este proceso solo se puede llevar a cabo a través de prensas offset especializadas.

1.3.6.3.4 UV MALLA DE FONDO EN MICROTEXTO

Realizando una combinación de microtextos dispuestos sobre un fondo guilloche con cierta disposición y utilizando tintas UV invisibles, se puede tener una Malla de fondo en microtexto UV.

1.3.6.4 TINTA ÓPTICAMENTE VARIABLE (OVI)

La tinta ópticamente variable (OVI por Optical Variable Ink) es una tecnología de seguridad poco común pero muy eficaz para proteger los documentos de identidad, los billetes de banco y otros documentos oficiales como los carnés profesionales. Esta tinta contiene pigmentos que tienen la particularidad de presentar dos colores distintos según el ángulo desde el que se mire el documento. Por ejemplo, según la orientación del observador, el color de la tinta puede cambiar de dorado a azul, de magenta a verde, o muchas otras combinaciones.

El fenómeno del cambio de color en estas tintas se debe a la forma en que reflejan diferentes longitudes de onda de la luz blanca en función del ángulo de incidencia sobre su superficie.

Esto las convierte en una medida muy eficaz contra la falsificación, ya que esta característica dificulta la copia o el escaneado precisos de documentos seguros mediante dispositivos como fotocopiadoras o escáneres en color, ya que necesitan un ángulo específico para reproducir el cambio de color. El OVI puede tener diferentes opciones de seguridad y complejidad, para una máxima protección del documento. Todos los OVI son visibles a la radiación IR.

1.3.6.5 ELEMENTOS HOLOGRÁFICOS

Un holograma de seguridad es un componente impreso que reduce la posibilidad de fraude gracias a su diseño y tecnología, que son complejos y caros. Se crea mediante la superposición de capas impresas que se hacen visibles o no en función de los ángulos de visión. El holograma destaca como uno de los elementos más predominantes de los dispositivos utilizados para reforzar la seguridad de los documentos sensibles. En concreto, se utiliza mucho para autenticar documentos y tarjetas de identidad, billetes de banco y tarjetas de crédito o débito. Con estos hologramas pueden conseguirse diversos efectos, de color, estructura o visuales, lo que convierte a los hologramas en un importante detalle estético del documento.

Hay que tener en cuenta que los hologramas pueden ser extremadamente complejos, con diferentes niveles de seguridad en su interior, que van desde simples cambios de color y texto cromático, o la aparición/desaparición de un visual, hasta nanotextos que sólo pueden observarse con herramientas de laboratorio. Un holograma es imposible de duplicar con un escáner o una fotocopiadora en color. Tampoco puede imitarse mediante procesos de impresión estándar.

Para las tarjetas en policarbonato, se tienen diferentes opciones. Una de éstas son los hologramas 3D, que forman parte de los DOVID (dispositivo difractivo de imagen ópticamente variable). Estos introducen imágenes tridimensionales y son capaces de incorporar visuales que cambian en respuesta al ángulo con que los mira la persona, así como variaciones cromáticas. El DOVID es un elemento holográfico incrustado dentro de un documento de policarbonato. Los DOVID transparentes protegen la fotografía grabada con láser de modificaciones o sustituciones.

Una capa holográfica es un holograma de mayor tamaño y puede llegar a estar presente en todo el documento seguro (holograma de borde a borde). Esta es, con mucho, la versión más agradable estéticamente porque el holograma se puede adaptar al diseño gráfico del producto agregando detalles y colores, al tiempo que mantiene una importante utilidad protectora porque cubre datos más confidenciales.

Para esta licitación, el holograma propuesto es un DOVID 3D transparente de borde a borde, el cual se muestra a continuación. Este cumple con los requisitos especificados en el punto I.4, I.8.1.1 y I.8.1.4.

1. Efecto cinético lineal: este efecto aparece como una transición de un color a lo largo de la forma cuando se inclina el holograma.
2. Rejilla difractiva directa: el efecto es visible sólo en un ángulo determinado como una forma o superficie coloreada
3. Efecto cinético de expansión: este efecto aparece como una expansión de un color a lo largo de la forma cuando se inclina el holograma.

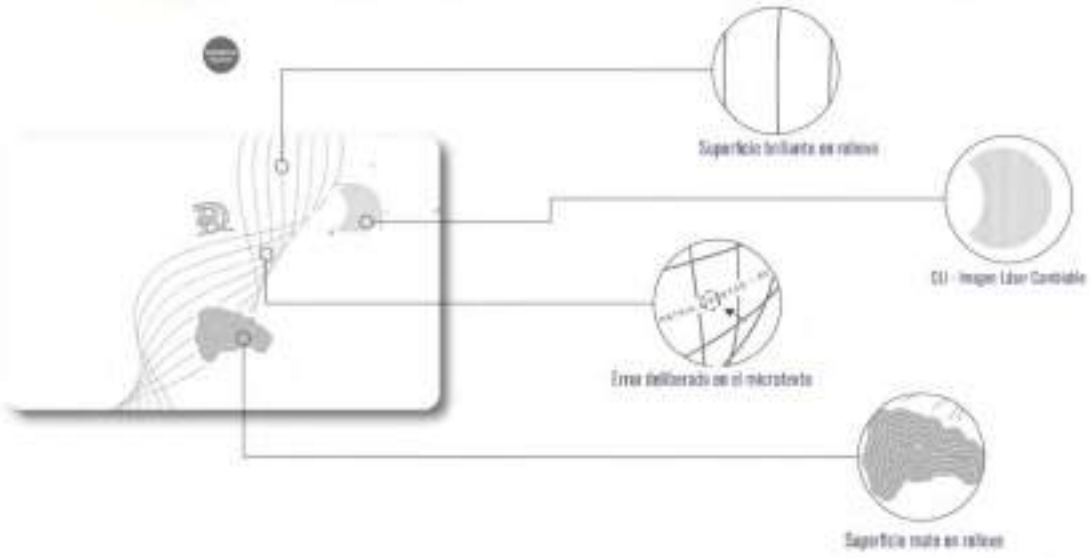
4. Efecto cinético lineal en un microtexto de 400 micras
5. Elemento óptico especial Axicona modificada: Aparece como múltiples líneas de colores que giran alrededor de su punto central y es visible desde cualquier dirección.
6. Bajorrelieve Pastel: Este se presenta coma un bajorrelieve 30 en color pastel reflectante con un alto nivel de detalle. La superficie de color pastel con brillo variado es muy visible bajo cualquier tipo de iluminación, incluida la luz diurna difusa. Es un elemento de seguridad muy fuerte. Se aplica al palmito que es el ave nacional de la República Dominicana
7. Rotación profunda: Un efecto 3D nítido sabre un motivo ornamental. Este efecto holográfico real, extremadamente brillante, aparece coma un objeto colorido de estructura alámbrica en 3D que flota de 3 a 5 mm por encima o por debajo de la superficie del holograma, incluido un objeto giratorio en 2D. La rotación del objeto es observable con una inclinación horizontal. IQ CHECK proporciona una autenticación inequívoca de un documento de identidad físico mediante un smartphone.
8. Efecto Ghost3D: El efecto holográfico real aparece coma un objeto de estructura alámbrica en 3D que flota a 100 mm por debajo de la superficie del holograma. El objeto es observable cuando se inclina horizontal y verticalmente. Solo es visible cuando el holograma se ilumina con una luz monocromática lateral. Este es un fuerte elemento de seguridad.
9. Imagen nanográfica y nanotextos: Este efecto permite la inscripción directa de una estructura de mapa de bits con una resolución de 254.000 dpi. Se utiliza para inscribir una imagen pequeña y nanotextos, que sólo son legibles con el uso de un microscopio forense

1.3.6.6 ELEMENTOS TÁCTILES / RELIEVE SUPERFICIAL POSITIVO O NEGATIVO

Los elementos táctiles de los documentos de identidad, como los contornos del país emisor, un emblema o cualquier otro elemento de diseño, se crean grabando las placas de laminación, aportando un terminado de alto o bajo relieve, así como una terminación mate o brillante. Estos pueden detectarse de forma táctil y visual cuando se inclina el documento. Esta técnica disuade la adición de capas fraudulentas, ya que cualquier modificación interfiere con la continuidad táctil del relieve.

Los microtextos son elementos textuales sutiles y detallados. Es posible hacer micro letras táctiles. Por ejemplo, se puede mostrar el nombre del país emisor, la moneda nacional, la entidad emisora o un mensaje específico. Los microtextos en relieve se colocan generalmente en forma de guilloche, pero se pueden controlar fácilmente con una lupa. También es posible incorporar errores deliberados. En nuestra propuesta se incluye un microtexto con error deliberado, tal y como se muestra en la figura siguiente.

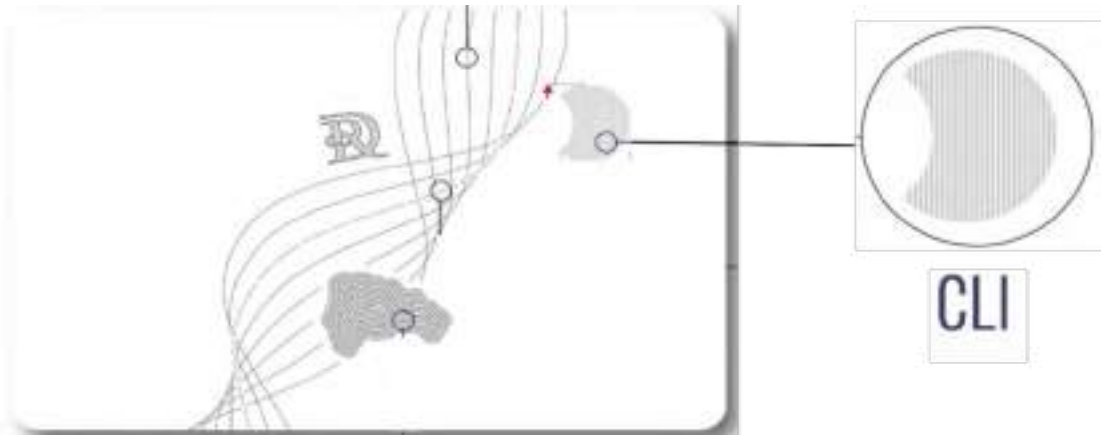
Superficie con Elementos en Relieve - Frente



1.3.6.7 MLI / CLI

El MLI o el CLI (Multiple Laser Image o Changeable Laser Image, respectivamente, por sus siglas en inglés), consisten en numerosas pequeñas lentes horizontales o verticales, respectivamente, incorporadas a la superficie de la tarjeta con placas de laminación especiales. Estos elementos de seguridad son personalizados posteriormente con láser. Según el ángulo de visión, el titular puede ver distintas partes de la información de la tarjeta, como la fecha de nacimiento, una pequeña foto, la firma, etc.

El CLI / MLI es el elemento de seguridad más eficaz contra la copia y la falsificación. No es posible reproducir los datos CLI / MLI grabados utilizando técnicas tradicionales como la fotocopia. La función CLI / MLI proporciona medios visuales y táctiles para verificar la autenticidad de la tarjeta.

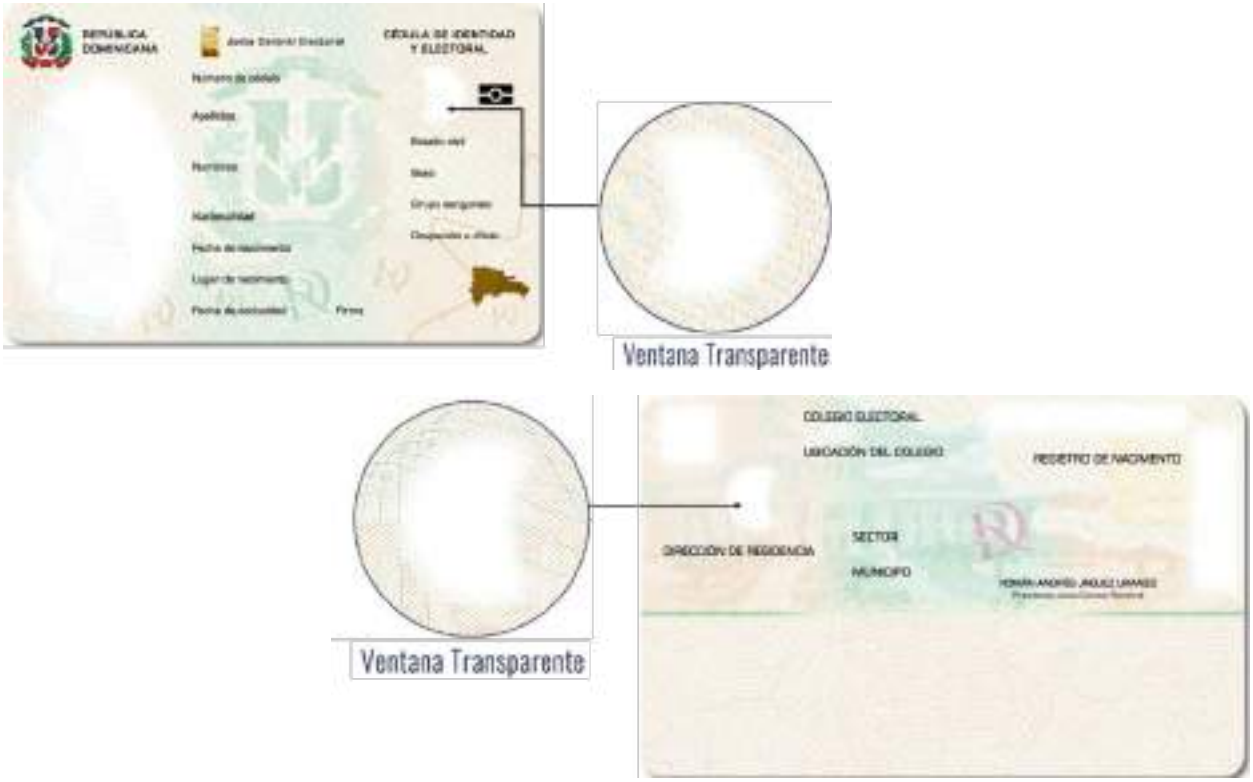


Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

1.3.6.8 VENTANA TRANSPARENTE

La ventana transparente es un área transparente realizada en el material mediante un proceso de producción específico y avanzado. Su integración en el documento complica cualquier intento de infracción, en particular al impedir la adición ilegítima de capas de materiales que contienen datos falsificados.

La ventana transparente puede incorporar elementos de seguridad adicionales como la integración del retrato del titular del documento, tintas específicas o elementos táctiles, aumentando su seguridad. Tal y como se puede distinguir en nuestra propuesta de diseño, un CLI está incorporado dentro de la ventana transparente.



1.3.6.9 TINTAS INFRARROJAS ABSORBENTES/TRANSPARENTES

Las tintas infrarrojas (IR) transparentes y absorbentes mantienen un aspecto uniforme bajo iluminación normal y son claramente visibles sin ayudas ópticas. Cuando se someten a una fuente de luz infrarroja específica, solo las tintas IR absorbentes revelan su presencia, lo que permite una detección selectiva. Lo contrario sucede con las tintas IR transparentes, las cuales son invisibles al someterlas a una fuente de luz infrarroja específica. Esto permite la lectura mecánica del documento, como requisito ICAO.

Este atributo hace que las tintas IR sean especialmente eficaces como defensa adicional contra la copia ilegal.

1.3.6.10 OTROS ELEMENTOS DE SEGURIDAD

En el contexto de un proyecto de muy alta seguridad, SELP puede utilizar una fuente no estándar, lo que hará aún más difícil de copiar el documento.

Para esta licitación, SELP ha realizado una proposición de diseño para la Cédula de Identidad y Electoral (CIE) y otro para la Cédula de identidad (CI), los cuales incluyen todas las características de seguridad mencionadas en el punto I.8.1 “Características de seguridad de la tarjeta”. Favor de referirse al Booklet “Proposición de diseño CIE y CI” donde se muestran cada uno de los elementos de seguridad, tanto en el anverso como en el reverso de cada documento.

Nota: La construcción del cuerpo de la tarjeta esta diseñada sin capas /materiales patentados que limitarían al abastecimiento de materiales de producción de tarjetas a proveedores dedicados. A su vez el cuerpo de la tarjeta en blanco y el proceso de personalización de la misma en combinación no constituirán una solución dependiente o patentada que excluya a los proveedores de tarjetas y/o sistemas de personalización.

ÍTEM II - ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN

2. ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN LASER

GET GROUP ofrece una solución modular de personalización de tarjetas que combina la impresión avanzada con capacidades de grabado láser para producir tarjetas láser en blanco y negro y a color en un proceso de personalización unificado para producir tarjetas de identificación gubernamentales seguras con características de seguridad complejas que no pueden manipularse ni sustituirse.

La solución de personalización CLM600 está disponible en un diseño compacto y liviano, y personaliza tarjetas de policarbonato en colores seguros con láminas holográficas personalizadas. Utiliza la tecnología de imagen híbrida LASMENT mediante impresión por re-transferencia segura con grabado láser.

Unidad de Impresión GET CLM600

El CLM600 es una unidad láser de fibra de 20 W confiable que brinda un rendimiento y una calidad óptimos en el grabado láser de tarjetas. El control del láser está integrado en una única placa altamente integrada con una pantalla gráfica a color para monitorear el estado y las operaciones.

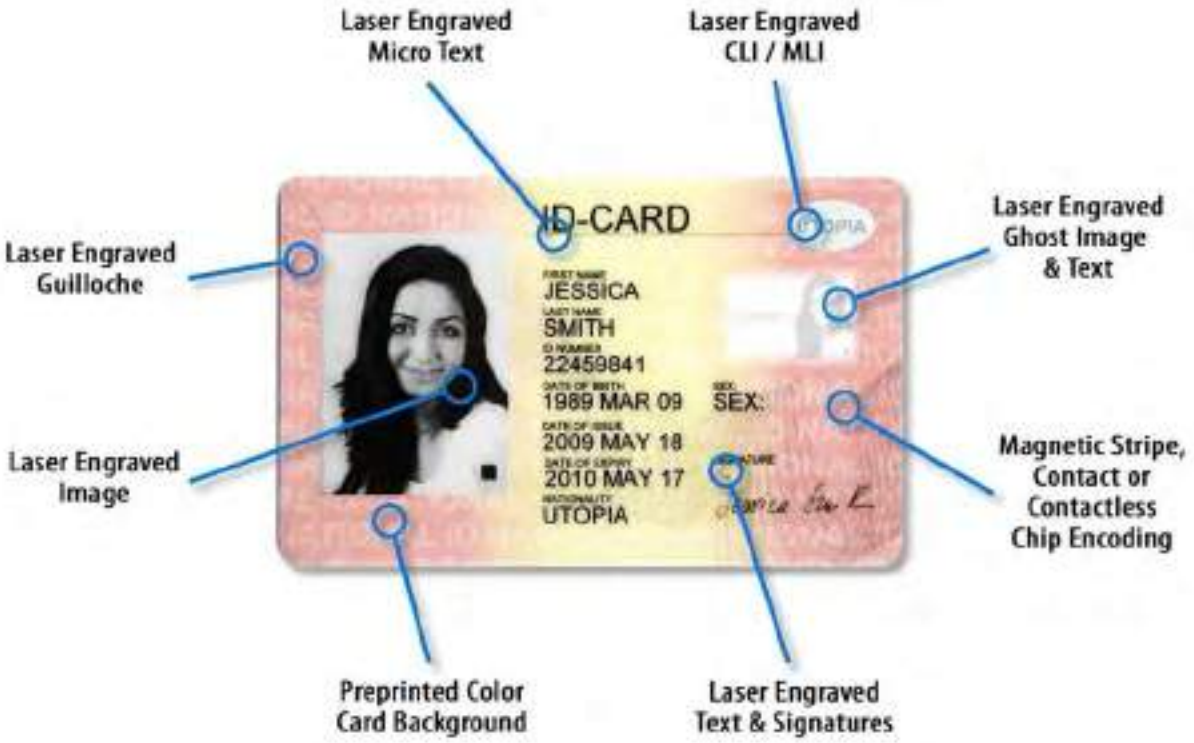
Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

2.1 BENEFICIOS DE LA SOLUCIÓN

Calidad, seguridad y simplicidad todo en un solo paso para impresión a doble cara.

Equipo modular para ser integrado en diferentes opciones de personalización laser.

- Funcionalidad de impresión a blanco y negro en laser de alta calidad.
- Resolución de 600 dpi para escala de grises.
- Sistema de personalización de escritorio ideal para personalización descentralizada.
- Diseño industrial de gran robustez para trabajo de alto tráfico de impresión, incluso por 24 horas.
- Grabación Laser que permite la máxima seguridad de la tarjeta a través de funciones de Nivel 1, Nivel 2 y Nivel 3:
    - Microtextos
    - Imagen fluorescente a todo color.
    - Grabado en Relieve (táctil) personalizable.
    - Código de Barra de 1D y 2D.
    - Impresión de imágenes, imagen fantasma y logotipos.
- Funciones de seguridad de ventana CLI/MLI.
- El control del láser integrado con una pantalla gráfica en color para supervisar el estado y las operaciones.
- Tecnología de imagen híbrida LASMENT.
- Personalización y Codificación de tarjetas en cumplimiento del estándar ICAO Documento 9303.
- Impresión personalizada de acuerdo con las especificaciones del formato solicitado Pliego de Condiciones, según punto II.2.1 Formato (Lay out) de las tarjetas CIE y punto II.2.2 Formato (Lay out) de las tarjetas CI.
    - Datos personales.
    - Fotografía a blanco y negro en escala de grises.
    - Firma y Foto fantasma.
    - Personalización CLI.
    - Zona de Lectura Mecánica (MRZ)
    - Códigos de Barras 1D y 2D.
- Capacidad de incluir componentes adicionales para controles de calidad adicionales que permiten garantizar una inspección completa de inicio a fin del proceso de impresión:
    - Control de posicionamiento de la tarjeta, mediante cámara, iluminación y software dedicado para reconocer los elementos de referencia.
    - Lectura OCR/OCV para verificación de los elementos impresos en la tarjeta.
    - Lectura de códigos de barras en la tarjeta.
    - Codificador para tarjetas:
        - Chip sin contacto: Antena y conectividad para interactuar con tarjetas RFID según ISO 14443 Parte I a IV, tipo A/B, CL y Mifare (opcional). La opción se puede conectar en un puerto USB y mediante protocolo PC/SC o a través del SDK.
        - Antena para verificación de calidad, para comprobación de calidad.



2.2 CRITERIOS DE DESEMPEÑO ÚNICOS

- Adaptación descentralizada: la configuración descentralizada de GET CLM600 ofrece al cliente las siguientes ventajas clave:
    - Escalabilidad: Fácilmente escalable a la demanda de producción de cada ubicación.
    - Operación: Cargas equilibradas y más bajas en cada sitio mantendrían un rendimiento de producción garantizado durante toda la duración del proyecto.
    - Riesgo distribuido: Los riesgos están distribuidos; por lo tanto, es muy poco probable que falle todo el sistema.
    - Entrega: La emisión dentro de la misma provincia garantizará plazos de entrega inmediatos o más cortos que una impresión centralizada.
    - Solución de problemas: fácil de definir, localizar y solucionar errores o problemas.
    - Configuración del sitio: pequeñas ubicaciones propiedad del gobierno podrían albergar el sistema de emisión.
    - Seguridad: La entrega directa de documentos seguros personalizados a los ciudadanos dentro de cada provincia minimiza cualquier riesgo de mal manejo.
    - Monitoreo: Esfuerzos moderados de monitoreo y supervisión.
    - Equipada con un sistema de alimentación ininterrumpida (UPS), asegurando al menos dos minutos de autonomía en caso de interrupciones eléctricas. Este respaldo permite la finalización segura de los procesos de impresión en curso, minimizando riesgos de fallas o pérdida de datos.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

2.3 MÓDULO LASER CLM600

El CLM600 es un sistema modular compacto de personalización de tarjetas de escritorio que ejecuta personalización de gráficos mediante grabado láser y ofrece opciones de codificación para banda magnética y chip de contacto y sin contacto.

El CLM600 es una unidad láser de fibra confiable de 20 W que proporciona un rendimiento y calidad óptimos en el grabado láser de tarjetas. El control láser está integrado en una única placa altamente integrada con una pantalla gráfica en color para monitorear el estado y las operaciones.

Las características relevantes del CLM600 son las siguientes:

CLM600	
Rendimiento (TPH)	Diseño industrial de hasta 60 tarjetas por hora (TPH) a doble cara, dependiendo del diseño, composición de la tarjeta y los requerimientos de codificación y verificación QA. Eficiencia productiva de más del 95%.
Personalización	Grabado Laser (Class 1), codificación de chip, banda magnética
Tecnología de personalización	Laser de Fibra 20W refrigerado por aire
Area de trabajo	Mayor a la especificada en el ID1/CR80, con un borde de 1.5 mm

Seguridad en Operación	Sistemas de bloque interno para evitar la apertura durante las operaciones.
Seguridad ambiental	Extractor de aire con filtro de carbón activo
CLI/MLI	MLI/CLI mediante desviación óptica (espejos)
Codificación de Banda magnética	Tracks 1, 2, 3 HiCo/LoCo read/write per ISO/IEC 7810, 7811
Codificación Chip de Contacto	Estación de contacto para ISO/IEC 7816 lectura y escritura, PC/SC
Codificación Chip sin Contacto	ISO 14443 Part I a IV, tipo A/B, CL y Mifare (opcional), PC/SC
Aseguramiento de calidad	Cámara con auto posicionamiento (5 Mpx, standard), Verificación OCR para lectura y códigos de barras (SW opcional)
Bandeja de alimentación de tarjetas	Alimentador de tarjetas con capacidad para entre 100 y 300 tarjetas
Administración de la tarjeta	Transporte sin rayones, modular, con volteo integrado
Bandeja de salida de tarjetas	Bandeja de 100 tarjetas Bandeja de rechazo de 10 tarjetas
Monitor de estado	Pantalla gráfica en color de 128x64 píxeles para acceso a operador.
Integración de Software	Integración de software multiplataforma mediante SDK propietario con licencia gratuita. Código fuente de ejemplo de integración. PC integrado WINDOWS. Incluye los elementos necesarios para desarrollar, compilar, depurar y probar las aplicaciones de personalización en un entorno de pruebas.
Control de Láser	Aplicación de control láser integrada (basada en PC, integrada)
Diagnóstico y Personalización	iCube (Id IDInterface), aplicación de configuración y monitoreo basada en web (web-based) para informes de producción. Personalización de datos personales almacenados de manera temporal, acorde a configuración.
Tamaño y peso	300 x 300 x 500(a) mm 29 Kgs./ Largo por ancho (0.09m²).;
Fuente de Alimentación	110/240V AC, 50/60Hz, 300W
Conectividad	Ethernet LAN

2.4 CARACTERÍSTICAS ADICIONALES

Las características relevantes del CLM600 son las siguientes:

CLM600	
El sistema de posicionamiento automático XY	El sistema de posicionamiento automático XY tiene como objetivo asegurar la posición exacta del grabado y consta de un conjunto de cámara en escala de grises, iluminación con LED múltiple y software dedicados a capturar la imagen, reconocer los elementos de referencia y medir su posición (orientación), ya sea para la tarjeta relativa al sistema, y para los elementos relativos a los otros elementos de la tarjeta.
Lectura OCR/OCV	Esta es una herramienta de software que permite implementar la lectura y verificación de texto impreso en documentos, por anverso y reverso de la tarjeta. La herramienta actualiza las funcionalidades del kit de cámara. Validación de textos impresos y ZLM (MRZ)
Lectura de códigos de barra	Esta es una herramienta de software que permite leer códigos de barras 2D/3D en documentos. La herramienta actualiza las funcionalidades del kit de cámara.
Aseguramiento de Calidad	El conjunto de lectura de OCR y/o códigos de barras, normalmente utilizado para identificar las tarjetas entrantes, también puede abordar el control de calidad, comprobando la coherencia de los datos gráficos y verificando la legibilidad de los datos grabados. Rechazo por la ausencia de los datos requeridos.
Codificación Chip sin Contacto	La opción de codificación de chip sin contacto proporciona la antena y la conectividad para interactuar con tarjetas RFID según ISO 14443 Parte I a IV, tipo A/B, CL y Mifare (opcional). La opción se puede conectar a un puerto USB y mediante protocolo PC/SC o mediante SDK. Opción también disponible desde el módulo de impresión a color CP500. Integrado al componente de Middleware incluido en esta propuesta. Control de Lectura a la entrada, que permite verificar la tarjeta a ser grabada antes de su proceso de codificación (ATS). Opcional: Control de lectura al final del proceso de codificación e impresión, por antena adicional.
Codificación Chip de Contacto	La opción de codificación de chip de contacto proporciona la conexión mecánica a tarjetas con chip ISO7816. El módulo de chip de contacto se puede conectar a un puerto USB y mediante el protocolo PC/SC o mediante el SDK.
Codificación de Banda Magnética	Este es un módulo dedicado capaz de codificar y leer TRK1, 2 y 3 (2 pistas en una sola pasada), separado del transporte principal, que funciona cargando la tarjeta desde la estación de volteo.
MLI/CLI Grabado inclinado	El grabado inclinado se realiza mediante un método patentado que utiliza espejos para desviar el rayo láser en un ángulo adecuado. La principal ventaja de esta solución es reducir el impacto de MLI/CLI en la productividad, ya que la tarjeta no se mueve de la posición de grabado estándar y el tiempo de ejecución corresponde al tiempo necesario para grabar dos entidades.

2.5 MÓDULO OPCIONAL PARA IMPRESIÓN A COLOR GET CP500

El módulo laser GET CLM600, tiene la opción de poder ser integrado con un módulo de impresión a color por re-transferencia térmica, lo que evoluciona al equipo denominado GET CP500LE. La CP500LE es una solución modular integrada de personalización de tarjetas que combina la impresión por re-transferencia inversa avanzada de la CP500 con capacidades de grabado láser de la GET CLM600 en un proceso de personalización unificado que produce tarjetas de identificación gubernamentales seguras con características de seguridad complejas que no se pueden manipular ni sustituir. La solución está disponible en un diseño compacto y liviano, y produce tarjetas de policarbonato a color seguras con láminas holográficas personalizadas en un solo paso.

1. Imágenes a full color en 600 dpi sobre tarjetas en policarbonato.
2. Estabilidad del color a largo plazo con tintas pigmentadas resistentes a la decoloración.
3. Opciones avanzadas de grabado láser.
4. Tecnología de imagen híbrida LASMENT.
5. Máxima seguridad de la tarjeta a través de funciones de Nivel 1, Nivel 2 y Nivel 3:
   - 5.1 Personalización variable UV
   - 5.2 Tinta variable reflectante Plus (RVI+)
   - 5.3 Microtextos
   - 5.4 Patrón de impresión único punto por punto
   - 5.5 Imagen fluorescente a todo color.
6. 10 años de resistencia a la decoloración.
7. Opción de Película holográfica de retransferencia segura.
8. Funcionalidad de impresión a blanco y negro en laser de alta calidad.

2.6 CONDICIONES DE GARANTÍA

Marcador láser CLM600

GARANTÍA:

- Reemplazar o reparar las piezas que se demuestren defectuosas durante el período de garantía, excepto las piezas sujetas a desgaste normal y las piezas consumibles.
- La garantía estándar cubre todas las piezas mecánicas y eléctricas.
- Tiempo de Garantía: 5 años posteriores a la entrega de equipos a la JCE.
- Tiempo de vida útil: Hasta 10 años, siempre y cuando se sigan las instrucciones y recomendaciones del fabricante en cuanto a instalación, operación, mantenimiento y uso de partes originales.

LIMITACIONES:

- La garantía cubre fallas de fabricación o mal funcionamiento durante el funcionamiento normal de la máquina.
- El Consorcio no se hace responsable de los defectos causados por una mala instalación, en los casos donde el consorcio no realice la instalación (ejemplo: luego de un mantenimiento), o por un uso incorrecto de la máquina o el desgaste de las piezas.
- La garantía no cubre los mal funcionamientos resultantes del grabado de cualquier otro material que no sea PC. Las tarjetas que no sean de policarbonato deben probarse y aprobarse con anticipación.

CONDICIONES QUE ANULA LA GARANTÍA:

A) Condiciones ambientales:

- humedad elevada
- temperatura elevada
- cualquier condición ambiental fuera de las Especificaciones Técnicas

B) Falta de mantenimiento regular.

C) La cantidad de ciclos o documentos producidos durante el uso normal de la máquina. (ver clasificación de repuestos)

CLASIFICACIÓN DE REPUESTOS:

Description
FUSE 5X20 10A (F)
EUROPEAN POWER CORD
POWER SUPPLY RWS300B-24
ON/OFF SWITCH
MAIN POWER PLUG AND FILTER
IDC 16G CONTROL BOARD ASSEMBLY
JPT FIBER LASER 20W WITH RED PILOT BEAM
IDC SCAN HEAD

“SCAPS” USC-1 BOARD WITH SOFTWARE
F-THETA LENS 160 1064 M39
Ø25.4mm MIRROR, BROADBAND 603&1064 nm
2.0 A-B 0,6m USB CABLE
CARD TRANSPORT SIGNAL CABLE IDC6
USC1-SCAN HEAD CABLE IDC6
USC1-DB37-IDX_CTRL CABLE IDC6
LASER SOL-IDX_CTRL CABLE IDC6
IDC CARD TRANSPORT
IDX INTERFACE BOARD 1
REPETEABLE TRANSPORT PARTS
BELT 60MXL025-75D ENCODER
MXL Z180 025 BELT
O-RING BELT Ø2.62X133
IDC RUBBER ROLLER Ø15
IDC O-RING PULLEY
IDC INPUT LOWER ROLLERS KIT
IDC PINCH ROLLER KIT
IDC OUPUT LOWER ROLLERS KIT
IDC FLIP OVER KIT
CARD TRANSPORT ELECTRICAL PARTS
CARD TRANSPORT PHOTOSENS. W\CABLE CARD
TRANSPORT STEP MOTOR W\CABLE
IDC DC MOTOR W/CABLE
*** VISION ***
IDX & IDC XY AUTOPOSITIONING GREYSCALE CAMERA KIT
CAMERA ILLUMINATOR
**** VISION CAMERA LICENSES ***
OCR/OCV READING TOOL (SINGLE LICENSE, 1 FOR EACH CAMERA)
BARCODE READING TOOL (SINGLE LICENSE, 1 FOR EACH CAMERA)
**** CLI / MLI MIRRORS *****
CLI/MLI MIRROR SPARE PART
**** MISCELLANEOUS ***
IDX INTERFACE BOARD 1
USB FEED THROUGH CONNECTOR
CENTRIFUGAL FAN 51x51 24Vdc
FAN 92x92x25 12Vdc
REED SWITCH SENSOR WITH UL CABLE
INTERLOCK MAGNET
DONGLE EXTERNAL INTERLOCK
LOCK ASSEMBLY + KEY
*** MACHINE KIT CABLE ***

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

IDC20 CABLES KIT
**** CONSUMABLE ***
ACTIVE CARBON FILTER FOR IDC

A) Corredores (RUN): piezas sujetas a desgaste y por tanto relacionadas con la carga de trabajo, por ejemplo:

- Rodillos
- Correas

B) Repetidores (RPT): piezas con vida limitada o con vida menor o cercana a la vida de la máquina, por ejemplo:

- Iluminador Led para Sistema de visión: 15.000hrs
- Diodo Láser: 30.000hrs
- Integridad de Datos Disco SSD: 15.000hrs
- Módulo Magnético: 750.000 Ciclos

C) Extraños (STR): piezas con tasa de fallos impredecible o con vida útil comparable a la vida del sistema, por ejemplo:

- Conjunto de Transporte de Tarjetas
- Resonador Láser
- Cabezal de Escáner Láser
- Láser de Radio Frecuencia
- Láser de Fibra
- Tarjetas Electrónicas

D) Consumibles (CNS): piezas que necesitan ser reemplazadas a intervalos regulares, por ejemplo:

- Filtro de carbón activo

NOTA:

Las horas de vida útil dependen en gran medida de las condiciones ambientales de trabajo y los parámetros de salida.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

3.1 GET TRUST – SOLUCIÓN DE PKI

En nuestra búsqueda de una solución de infraestructura de clave pública (PKI) sólida y segura, hemos implementado "GET Trust", que es compatible con los estándares de la ICAO (OACI). Este sistema PKI de vanguardia ha sido meticulosamente diseñado y ejecutado por nuestro equipo de PID (Departamento Comercial de Pasaportes e Identificación) para cumplir con los más altos estándares de seguridad y garantizar la integridad y autenticidad de las transacciones digitales.

3.1.1 ARQUITECTURA DEL SOFTWARE

GET Trust establece una estructura clara y jerárquica para nuestros certificados digitales. Incluye una Autoridad de Certificación de Firma de País (CSCA) de primer nivel para seguridad a nivel nacional, así como Autoridades de Certificación Técnica (CA Técnicas) para manejar certificados SSL y otros certificados técnicos.

Sus módulos se componen de varios submódulos propietarios de PKI de la OACI que se pueden utilizar para firmar información de forma segura en documentos electrónicos y proteger datos confidenciales como identidades digitales.

- Extensible

GET Trust es altamente extensible. Ofrece soporte para múltiples API criptográficas y se integra perfectamente con una variedad de dispositivos de módulo de seguridad de hardware (HSM), lo que garantiza adaptabilidad y compatibilidad en diversos entornos operativos.

- Escalable

GET Trust ha sido ingeniosamente diseñado como una arquitectura de microservicios, lo que garantiza flexibilidad y escalabilidad. Este sistema puede escalarse horizontalmente fácilmente agregando sin esfuerzo firmantes de datos adicionales cuando surja la necesidad.

- Registro

GET Trust, con su arquitectura de microservicios, también prioriza capacidades de registro sólidas. Proporciona funciones de registro amplias y configurables, lo que permite un seguimiento y análisis exhaustivos de las actividades del sistema para mejorar la seguridad y la resolución de problemas.

- Gestión de usuarios

La gestión de usuarios es un aspecto fundamental del conjunto de funciones de GET Trust. El sistema incluye sólidas funcionalidades de administración de usuarios, lo que permite a los administradores crear, administrar y controlar de manera eficiente el acceso, los permisos y los procesos de autenticación de los usuarios para operaciones seguras y sin inconvenientes.

- Mecanismo de confianza en la máquina (Machine Trust)

GET Trust incorpora un sofisticado mecanismo Machine Trust que aprovecha las autoridades de certificación técnicas (Technical CA) para emitir certificados SSL. Las claves generadas dentro de este mecanismo se almacenan de forma segura en Módulos de plataforma segura (TPM) y están diseñadas para no ser

exportables. Esta estricta medida de seguridad garantiza la máxima protección de los materiales criptográficos confidenciales, mejorando la postura de seguridad general del sistema.

3.2 GET AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA – CSCA

La Autoridad de Certificación de Firma de País (CSCA) de GET Trust permitirá las siguientes funcionalidades:

- Confidencialidad: garantía con certificados de cifrado
- Integridad: garantía con certificados de firma.
- Autenticación: garantía con certificados de autenticación
- No repudio: garantía con certificados de firma y autenticación
- Control de acceso: garantía con certificados de autenticación

El software ID-CA actúa en la solución propuesta como CSCA, como fabricante de certificados gestionando su ciclo de vida.

El objetivo del componente ID-CA es permitir una gestión centralizada y segura del ciclo de vida de los certificados gracias a las siguientes funcionalidades:

- Creación de autoridades de certificación.
- Creación de certificados de usuario (entidad final) por parte de las autoridades de certificación.
- Revocación de certificados por parte de las autoridades certificadoras.
- Creación automática de CRL (listas de revocación de certificados) para cada autoridad certificadora.
- Publicación de certificados de usuario (entidad final) y CRL en un directorio LDAP.

Una característica interesante de ID-CA es la multi entidad, que permite crear instancias de un número ilimitado de particiones (dominios), capaces de alojar una jerarquía PKI completa con CA raíz e intermedia. Estas particiones actúan como dominios separados y, por lo tanto, es posible implementar entornos de confianza de clientes completamente independientes dentro de la misma instancia de software.

Centrándose en la capacidad de abordar todo tipo de segmentos del mercado de identidad digital, ID-CA también ha sido diseñado para satisfacer todos los requisitos de las necesidades de Seguridad Corporativa y, en particular:

- Proporcionar una variedad de conectores de interfaz, permitiendo la integración en el sistema de TI de la empresa.
- Implementar una configuración altamente empaquetada y, por lo tanto, eliminar la complejidad de las implementaciones de PKI.
- Instalación y configuración del sistema fáciles de usar.

Como enfoque general, su desarrollo tuvo mucho cuidado en facilitar al máximo el uso de PKI. Por lo tanto, se han revisado todos los aspectos, desde los procedimientos de instalación hasta las tareas administrativas diarias, donde se guía y apoya al administrador durante la configuración y ejecución de la aplicación.

Considerando los esquemas de evaluación de seguridad de terceros como garantía de calidad, seguridad y robustez, ID-CA se somete a un proceso de certificación Common Criteria, dirigido al nivel EAL4+. Este enfoque es una apuesta clara por mantener continuamente el nivel de seguridad del software, como lo demuestran las certificaciones EAL3+ y EAL4+ obtenidas por productos anteriores.

GESTIÓN DEL ALMACÉN DE CLAVES

Un KeyStore es la configuración para acceder al contenedor de claves criptográficas de hardware o software.

Permite generar pares de claves criptográficas basadas en servicios criptográficos proporcionados por bibliotecas de software, tokens de tarjetas inteligentes (a través del middleware PKCS11) o mediante un Crypto Server (capa de abstracción de hardware), conectado a un HSM.

El tipo de algoritmos, parámetros y longitudes de clave dependen únicamente del recurso elegido. Por lo tanto, con el software o hardware adecuado, ID-CA admite RSA hasta 4096 bits y ECDSA hasta 512 (curvas NIST, Brain Pool y otros parámetros).

Los HSM compatibles son de la familia EVIDEN Trustway Proteccio, Safenet y Thales (nCipher). Cualquier otro HSM estándar basado en PKCS#11 puede ser compatible después de la calificación.

La gestión del KeyStore consiste en Creación, Edición, Actualización y Eliminación.

GESTIÓN DE DEPOSITOS EN GARANTIA

ID-CA integra la gestión de depósitos en garantía (Escrow Management) como función principal.

El depósito de claves es un acuerdo en el que las claves necesarias para descifrar datos cifrados se mantienen en depósitos de garantía y, en determinadas circunstancias, el propietario o un tercero autorizado puede obtener acceso a esas claves. El depósito en garantía se utiliza a menudo con la generación de claves centralizada (es decir, emisión de pares de claves en el lado de PKI), para limitar el riesgo de filtración de la clave.

La clave maestra para escrow, la clave simétrica y la clave de usuario final se generan en un recurso criptográfico de hardware, cada vez que existe una solicitud de generación de clave centralizada.

De forma predeterminada, la clave maestra es una clave RSA de 3072 bits y la CLAVE simétrica es una clave AES de 256.

Están disponibles las siguientes funciones:

- Creación de configuración de generación de claves: cree una configuración de generación de claves para la partición actual.
- Habilitar la generación centralizada de pares de claves en el perfil de certificado: habilite la generación de pares de claves mediante PKI (generación centralizada de pares de claves) para un perfil de certificado en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.

- Habilitar depósito en garantía en perfil de certificado: habilite el depósito en garantía para un perfil de certificado en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- Clave de depósito en garantía: deposita en custodia una clave para un certificado en una partición de destino.
- Recuperar clave en custodia: recupere una clave que ha sido en custodia para un certificado en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.

AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA

ID-CA permite una gestión de autoridades de certificación muy sofisticada y eficaz.

Una Autoridad de Certificación (CA) es la parte esencial de un sistema PKI. Su función principal es emitir certificados y gestionar su ciclo de vida. Una CA puede tener varios certificados, que deben tener el mismo DN (Domain Name).

Con ID-CA están disponibles las siguientes funciones de gestión de CA disponibles en el mercado:

- Generación de pares de claves de CA: genere un par de claves para un certificado de CA
- Creación de certificado de CA firmado localmente/renovación de certificado con nueva clave: crear un certificado de CA para una configuración de CA
- Creación de certificado de CA firmado externamente/renovación de certificado con nueva clave: cree una CSR para firmarlo externamente e importar el certificado resultante.
- Importar certificado de CA/renovación de certificado: importar un certificado de CA a una CA

ID-CA implementa una característica particular, el concepto *CA Group*, que permite una gestión de CA altamente flexible y segura.

CA Groups permite a los administradores gestionar varias CA en una sola entidad. En general, los *CA Groups* están formados por una sola CA y, por lo tanto, el concepto de grupo se oculta en aras de la simplicidad. Los *CA Groups* permiten:

- Garantizar que el servicio de firmas permanezca disponible incluso cuando el tráfico de firmas esté en su nivel más alto: una CA definida en un *CA Group* puede tener una cuota de firmas. Cuando una CA alcanza la cuota de firmas, el servicio de firma cambia a la siguiente *CA Group* que aún no ha alcanzado la cuota de firmas.
- Administrar las CRL (listas de revocación de certificados) para todas las CA dentro del *CA Group*.
- Predefina las CA antes de crear certificados de CA: los *CA Groups* se pueden crear y configurar antes de que se hayan creado los certificados de CA; luego los certificados de CA se pueden cargar cuando estén disponibles.

La función *CA Groups* es de particular interés para proyectos de identidad a gran escala donde se necesita producir una gran cantidad de certificados de ciudadanos (usuarios). De hecho, *CA Groups* evita ataques criptoanalíticos a una única clave privada de CA. *CA Group* se administra fácilmente mediante configuración y mecanismos GUI.

En detalle, están disponibles las siguientes funciones de *CA Group*:

- Creación de *CA Group* mediante la importación de un certificado: Cree un *CA Group* en la Partición actual o cualquier Partición en un nivel inferior de la rama del árbol, con dentro, una CA y un certificado importado.
- Creación de *CA Group* con certificado firmado localmente: cree un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol, con una CA interna y su certificado firmado por una CA local.
- Creación de *CA Group* con certificado firmado externamente: cree un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol, con dentro, una CA y su certificado firmado por una CA externa.
- Edición de *CA Group*: edite el *CA Group* en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- Importación de *CA Group*: cree un *CA Group* en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol, desde un archivo XML.
- Exportación de *CA Group*: exportación XML de un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- Eliminación de *CA Group*: elimine un *CA Group* que no tenga un certificado de CA en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.

ADMINISTRACIÓN DE PERFILES DE CERTIFICADOS

La principal tarea de una Autoridad de Certificación es, por definición, producir certificados digitales.

ID-CA realiza esta tarea con un enfoque particular en el rendimiento y la facilidad de uso, para permitir una rápida definición del perfil de certificado y la producción de certificados en gran volumen.

En lo que a tareas de administración se refiere, se puede:

- Crear/Editar perfiles de certificados
- Importar/exportar perfiles de certificados

La estructura de un certificado se puede crear de una manera muy sencilla mediante soporte GUI, en un proceso guiado que permite al usuario ingresar solo valores que no están predefinidos.

Además, y para poder combinarlo con productos anteriores de CA, es posible importar perfiles de certificados también en formato XML.

Para configurar rápidamente varios entornos, como ensayo, preproducción y producción, también se pueden exportar perfiles de certificados, así como otros datos de configuración, en formato XML.

Un perfil de certificado está asociado con una CA o un grupo de CA. Determina las propiedades del certificado, como el tamaño de la clave pública, el período de validez, el DN y los usos de clave para todos los certificados emitidos por la CA o el grupo de CA asociado con el perfil del certificado.

A través de la GUI, se puede definir, editar y modificar casi todos los elementos dentro de un perfil de certificado. La gestión del perfil del Certificado IDnomic ID-CA permite, en particular, definir libremente:

- El formato del certificado
- El algoritmo utilizado para el certificado.
- La firma del Grupo CA
- La información del certificado y cómo obtener esta información.

ADMINISTRACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS

Periódicamente se genera y publica una lista de revocación de certificados (CRL), a menudo en un intervalo definido.

ID-CA implementa todas las funciones de gestión de CRL necesarias para producir y distribuir información de revocación a todas las aplicaciones relevantes. Además de la publicación (automática), también se puede recuperar la CRL manualmente a través de la GUI.

Una CRL también se puede publicar inmediatamente después de que se haya revocado un certificado. La CRL siempre la emite la CA que emite los certificados correspondientes. Todas las CRL tienen una vida útil durante la cual son válidas. Durante el período de validez de una CRL, una aplicación habilitada para PKI puede consultarla para verificar un certificado antes de su uso.

También es posible generar una CRL Delta, que es la lista de cambios desde la última CRL.

Las funciones de Gestión de CRL de ID-CA consisten en:

- Configuración de generación de CRL en grupo CA: configure la información de CRL de un grupo CA para producir CRL (y opcionalmente Delta CRL).
- Producción automática de CRL: produzca periódicamente una CRL completa (y opcionalmente una CRL Delta) para todas las CA válidas de un grupo de CA.
- Producción automática de Delta CRL: produzca una Delta CRL periódicamente para todas las CA válidas en un grupo de CA.
- Producción manual de CRL: produzca periódicamente una CRL completa (y opcionalmente una CRL Delta) para todas las CA válidas de un grupo de CA.
- Descarga de CRL mediante GUI: descarga mediante GUI, la última CRL completa o Delta CRL de una CA en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- Descarga de CRL vía HTTP: Descarga vía HTTP, última CRL completa o Delta CRL de CA.

ADMINISTRACIÓN DE PUBLICACIÓN

La publicación de la información producida (certificados y CRL) es una tarea clave en los sistemas PKI para hacer que los datos públicos estén disponibles para verificar la identidad digital y su validez. La publicación en ID-CA está disponible tanto para Certificados como para CRL al ser datos públicos de una CA.

ID-CA tiene una gestión de publicaciones muy fácil de usar, que consiste en un proceso de configuración basado en GUI combinado con elementos de configuración. La publicación se puede realizar de forma automática o manual.

En particular, las características de ID-CA Publication Management consisten en todas las funciones del ciclo de vida, como creación, edición y eliminación para terminales, estrategia de publicación y política de publicación.

Además, ID-CA admite de forma nativa la política de publicación de enlaces para la publicación de certificados y CRL, así como la publicación automática.

Para configurar una publicación se necesitan varias configuraciones (Endpoint, Estrategia de publicación, Política de publicación).

ADMINISTRACIÓN DE CA DE CONFIANZA (TRUSTED CA)

El paradigma de seguridad de ID-CA se basa en el más alto nivel de confianza. Por lo tanto, una CA interna sólo se puede utilizar si es de confianza. Las CA confiables se utilizan para la autenticación de usuarios y la verificación de firmas de solicitudes de servicios web.

El concepto Trusted CA se implementa en toda la aplicación para permitir y controlar la comunicación segura y el acceso a las funciones del producto.

Los certificados de autenticación de usuario que permiten conexiones a la aplicación ID-CA deben haber sido emitidos por una autoridad de certificación (CA) en la que la aplicación ID-CA confíe para la autenticación de actores. ID-CA también debe poder verificar la cadena de confianza del certificado hasta un ancla de confianza.

Para la firma de solicitudes de certificados, las CA que emiten certificados que firman solicitudes de certificados deben ser confiables para la firma de solicitudes y la CA de ID debe poder verificar la cadena de confianza del certificado hasta un ancla de confianza.

Cuando se confía en una CA en una partición, también se confía en todas las particiones debajo de esta partición.

Trusted CA Management consiste en:

- Creación de CA de confianza externa: cree una CA de confianza en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- Edición de CA de confianza externa: edite la CA de confianza en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- Edición de CA de confianza interna: edite la CA de confianza interna en la partición actual o inferior

ADMINISTRACIÓN DE NOTIFICACIONES

En modo operativo, esta función de notificación es esencial para garantizar un alto nivel de disponibilidad de la aplicación PKI.

ID-CA ha integrado de forma nativa la gestión de notificaciones dirigidas a sus administradores.

El módulo de Notificación se utiliza para advertir a una persona sobre los diferentes eventos que ocurren en la plataforma o sobre entidades administradas por una CA. Las funcionalidades de Notificación ID-CA consisten en:

- Notificación de caducidad: notifica a un usuario acerca de un certificado que caducará pronto en la partición de destino.
- Configuración de notificación: configure la notificación para la partición actual y cualquier partición en un nivel inferior de la rama del árbol.

ADMINISTRACIÓN DE ACTORES

Los actores son Personas, Máquinas o Dispositivos que pueden acceder al sistema, normalmente identificados y autenticados mediante un certificado. Disponible para la asignación de doble factor de autenticación mediante OTP.

Están autorizados a realizar Acciones dependiendo del Rol que se les asigne en una Partición específica y sus hijos.

- Los roles (roles) son una colección de derechos. Los roles se definen para casos de uso específicos identificados de la aplicación y para garantizar la separación de funciones.
- Los permisos (rights) son una colección coherente de posibles acciones en el sistema para una característica específica. Actualmente, no es posible editar derechos ni crear roles (los roles y derechos son estáticos).

En resumen, el triplete de Rol, Partición y Actor es necesario para determinar si una acción está autorizada o no en el sistema, en una partición específica.

Rol	Descripción
Super Administrator	Posee todos los roles
Rights Administrator	Puede ver certificados y usuarios.
Connector Enroll	Puede crear y editar usuarios.
Connector Revoke	Puede realizar la inscripción de certificados a través del servicio web (SOAP)
Connector Recovery	Puede realizar la revocación de certificados a través del servicio web (SOAP)
Configuration Administrator	Puede realizar recuperación de claves a través del servicio web (SOAP)
Certificate Administrator	Puede realizar todas las tareas de configuración, así como ver certificados
Revocation Administrator	Puede realizar búsquedas, inscripciones y revocaciones de certificados a través de GUI
Recovery Administrator	Puede ver todos los ajustes de configuración, excepto los clústeres criptográficos. Puede ver, suspender, revocar y reactivar/reanudar certificados. Puede suspender, revocar y reactivar/reanudar certificados mediante servicios web
Key Administrator	Puede realizar la recuperación de claves a través de GUI
Audit Administrator	Puede gestionar funciones de generación de claves.

Tabla 1. Roles y Permisos.

ADMINISTRACIÓN DE AUDITORIA, REPORTES Y SUPERVISIÓN

ID-CA registra todos los eventos funcionales y técnicos. Los registros de auditoría se utilizan para monitorear la plataforma tanto a nivel de proceso comercial como a nivel técnico.

Se pueden diferenciar dos tipos de trazas:

- Seguimientos técnicos: Estos seguimientos son generados por los componentes internos (servidor web Apache, base de datos PostgreSQL, directorio LDAP, etc.) implicados en el funcionamiento de ID-CA. Accesibles como un archivo de texto a través del sistema de archivos, estos seguimientos proporcionan indicadores sobre el estado de ejecución de cada uno de estos componentes. Estos rastros son generados por los propios componentes según su propia lógica de aplicación.
- Seguimientos de aplicaciones: Para garantizar la trazabilidad y la rendición de cuentas, ID-CA genera seguimientos completos de las aplicaciones para cada una de las acciones realizadas. Cada rastro tiene un número único que permite seguir los eventos que originaron la emisión de este rastro y seguir las acciones realizadas posteriormente. Por ejemplo, a partir de un seguimiento generado durante la validación de una solicitud de tarjeta, será posible:
- Volver a la solicitud inicial.
- Seguimiento del futuro de la solicitud.

En general, cada rastro se compone de datos que especifican "quién" hizo "qué", "cuándo", "dónde" y "el resultado". Un seguimiento suele ir acompañado de los datos correspondientes (solicitudes, certificados, etc.).

Los seguimientos de aplicaciones de ID-CA se pueden interconectar con la herramienta Syslog.

La Gestión de Auditoría consiste en:

- Normalización de auditoría: normalice periódicamente los eventos de auditoría en la base de datos para realizar consultas en la base de datos.
- Vista de auditoría: vea información de auditoría en la partición actual o debajo
- Búsqueda de auditoría: busque registros de auditoría disponibles en la partición actual o debajo
- Exportación de auditoría: exporta registros de auditoría en la partición actual o debajo

En términos de funciones de informes, ID PKI puede manejar la siguiente información:

1. Para una fecha determinada, una tabla muestra el número total de certificados (emitidos antes de esta fecha) por partición o perfil y por estado:
- válido (no revocado en un período de validez)
- revocado (en un período de validez)
- aún no válido y no revocado
- aún no válido y revocado
- caducado y no revocado
- caducado y revocado
2. Por rango de tiempo, una lista de eventos relacionados con certificados por perfil o partición
- Inscribirse
- Revocación
- Vencimiento

A nivel global, cada administrador de sistemas necesita verificar el estado de las aplicaciones en ejecución.

ID-CA proporciona información básica sobre el estado de las aplicaciones y expone varios indicadores basados en los procesos de Monitoreo del sistema y Monitoreo de aplicaciones.

Los elementos de monitoreo del sistema son:

- CPU, RAM, uso del disco, tiempo de actividad del servidor,
- Estado de salud del repositorio LDAP, la base de datos y el agente JMS.

Los elementos de monitoreo de aplicaciones PKI son:

- Tiempo de actividad y estado del servidor
- Estado de salud de HSS (capa de abstracción de hardware criptográfico)
- Caducidad de CA
- Información de gestión de CRL
- Producción de CRL
- Publicación CRL
- Alerta de publicación de CRL

ADMINISTRACIÓN DE PARTICIONES

El sistema de partición permite implementar fácilmente el arrendamiento múltiple dentro de ID PKI. Permite configurar varios entornos CA completamente independientes dentro de una única instancia del software.

Las particiones se definen en una estructura de árbol, siendo cada nodo una partición en la que se pueden adjuntar recursos (por ejemplo, configuraciones, certificados, etc.). Según las necesidades del cliente podemos aislar o compartir recursos comunes.

Debido a la asociación de los roles y acciones del actor a una partición y sus hijos, es posible dedicar una partición completa a un cliente. Puede actuar como un entorno PKI individual.

El principio de partición lógica se describe a continuación:

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

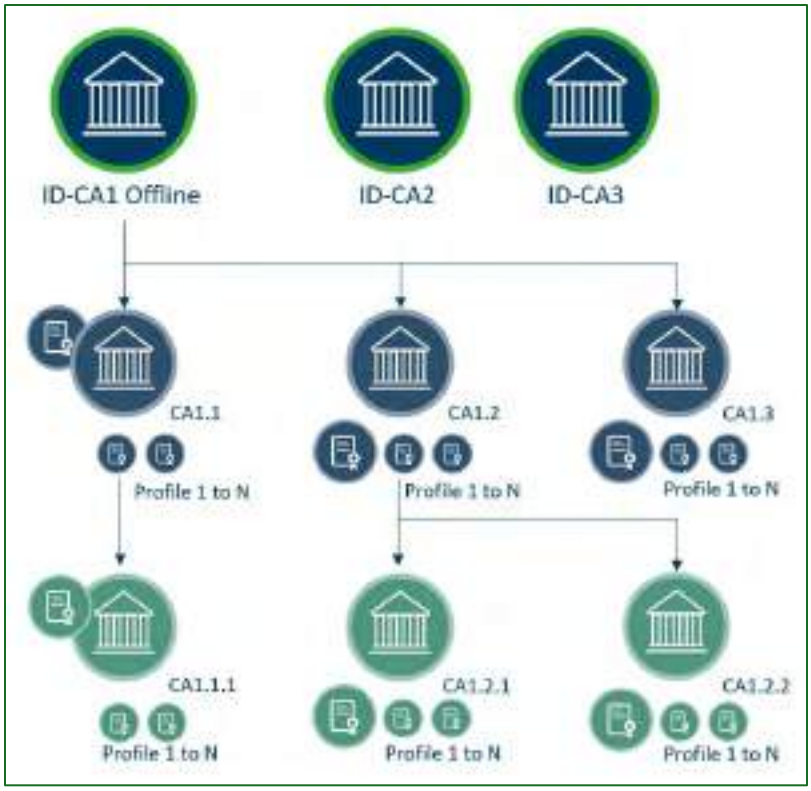


Ilustración 1. Principios de partición de datos.

La gestión de particiones consiste en:

- Creación de partición: creación de una nueva partición (son posibles estructuras anidadas)
- Edición de partición: edición de la partición actual o cualquier partición en un nivel inferior de la rama.

Es posible compartir (colocar recursos más arriba en el árbol) y aislar (crear ramas en el árbol de partición).

La gestión de particiones se realiza de una manera extremadamente fácil de usar, a través de una sencilla GUI mediante mecanismos de hacer clic, arrastrar y soltar. Para una mayor visibilidad, se puede asociar un logotipo a cada partición para resaltar mejor unas de otras.

SELLADO DE TIEMPO

El producto Time Stamping nos permite proporcionar tokens de tiempo certificados y fiables.

En combinación con una fuente de tiempo y un medio de firma digital, esto permitirá a los clientes garantizar, por ejemplo, la existencia de un documento en un momento preciso en el tiempo.

En términos de implementación, un cliente transmite solicitudes de sellado de tiempo a la plataforma, que determina con gran precisión la hora y la fecha, firma y envía esta información de vuelta al cliente.

El protocolo de comunicación subyacente para este procedimiento está definido en RFC 3161, al que el producto Time Stamping cumple plenamente.

La firma de los tokens de tiempo se basa en dispositivos criptográficos (módulos de seguridad de hardware) que admiten la interfaz PKCS#11.

El producto consta de dos servidores:

- Un servidor de administración, encargado de proporcionar servicios de gestión basados en GUI para operadores acreditados.
- Un servidor de firma, encargado de producir técnicamente los tokens (de tiempo) firmados.

Se admiten las siguientes funciones:

- Administración basada en GUI del servicio de sellado de tiempo
- Gestión de los espacios de trabajo del cliente, incluido el manejo de pares de claves criptográficas asociadas
- Gestión de entidades de sellado de tiempo, sus políticas y extensiones aceptadas
- Gestión de actores
- Auditoría y estadísticas

El acceso a los servidores solo se concede mediante autorización basada en autenticación mutua (HTTPS SSL/TLS).

Además, el sellado de tiempo ofrece las siguientes ventajas:

- Tokens producidos totalmente compatibles con IETF RFC 3161 e IETF RFC 5816
- Gestión flexible de particiones de clientes (cada una dedicada a un espacio de trabajo de sellado de tiempo)
- Máximo rendimiento
- Cumplimiento de la normativa Eidas

3.3 FIRMADO DE DOCUMENTOS GET TRUST (DOCUMENT SIGNER)

ADMINISTRACIÓN BASADA EN WEB

La interfaz de administración basada en web ofrece las siguientes funcionalidades:

- Gestión de espacios de trabajo (dominio del cliente)
- Gestión de entidades firmantes (comúnmente denominadas “Firmantes de documentos” o DS)
- Gestión de claves de firma (claves de firma de respuestas y sus certificados asociados)
- Gestión de los usuarios del servicio.
- Auditoría de operaciones de administración
- Consulta de estadísticas de producción.

Solo se puede acceder al sitio de administración mediante un certificado de usuario final (UE), que se puede almacenar en una tarjeta inteligente. El servidor web frontal autentica a la UE que se conecta. Para que la UE esté autorizada a acceder al sitio, la CA que emitió su certificado debe estar definida como una CA confiable del servidor web frontal.

Una vez que el Usuario Final haya sido autenticado por el servidor Web frontal, se abrirá la página de inicio de la plataforma DS. Dependiendo del perfil de Usuario final utilizado para conectarse al sitio, tendrá acceso a ciertas funcionalidades, pero no a todas.

Están disponibles los siguientes perfiles:

- Perfil "Gestión del espacio de trabajo": Otorga acceso al menú "Gestión del espacio de trabajo". Un Usuario Final con este perfil puede crear, seleccionar, ver o modificar un espacio de trabajo.
- Perfil "Gestión de claves": Otorga acceso al menú "Gestión de claves". Un Usuario Final con este perfil puede generar un par de claves en el equipo criptográfico y recuperar la solicitud de certificado emitido (CSR en formato PKCS#10).
- Perfil "Administración DS": Otorga acceso al menú "Administración DS". Un Usuario Final con este perfil puede registrar, ver, activar, desactivar y bloquear certificados DS.
- Perfil "Gestión de usuarios": Otorga acceso al menú "Gestión de usuarios". Un Usuario Final con este perfil puede registrar, activar, desactivar o bloquear usuarios y gestionar los derechos de los usuarios registrados.
- Perfil "Gestión de Auditoría": Otorga acceso al menú "Auditoría". Un usuario final con este perfil puede ver información relacionada con la auditoría, así como estadísticas de producción.

INTERFACE CON LA PLATAFORMA DE DS

La interfaz de la plataforma DS se basa en el enfoque de servicios web (XML sobre HTTP(S)) y permite, por lo tanto, una interfaz sencilla e independiente del contexto.

IDnomic proporciona al Cliente:

- Una documentación para la interfaz de especificación
- Apoyo a la integración

ESPECIFICACIONES DE LA PLATAFORMA DE DS

Software	Especificaciones
ICAO - DOCUMENT SIGNER®	La plataforma DS se suministra y puede configurarse. Normalmente se instala en el sitio de producción en interfaz directa con la cadena de personalización. Funciones principales: • Verificación de certificados DS. • Enrutamiento de una solicitud de firma a una clave disponible con control de cuota (número máximo de firmas por clave). • Generación de un lote de claves y DS CSR. • Realiza codificación ASN.1 y firma de SOD. Interfaz DS: servicio web (XML) sobre protocolo HTTP(S)

ALGORITMOS

- RSA 2048 y 4096
- SHA-1, SHA-256 y SHA-512
- ECDSA 256

3.4 PKI CIUDADANA – PKI SUBORDINADA X509

CA SUBORDINADA DE LA CA ROOT

Una CA subordinada es una CA que obtiene su certificado de una CA raíz (también conocida como CA principal). La CA subordinada podrá emitir certificados a otras entidades (ciudadanos), pero su certificado es verificado por la CA raíz.

PROCESO DE EMISIÓN DE CERTIFICADOS

El proceso de emisión de certificados en la PKI Ciudadana con una CA subordinada es el siguiente:

1. Solicitud de certificado: Una entidad (Ciudadano) solicita un certificado a la CA subordinada.
2. Verificación de identidad: La CA subordinada verifica la identidad de la entidad (Ciudadano) que solicita el certificado. (Tarea delegada al sistema de verificación de identidad de la JCE)
3. Generación de clave pública: La entidad genera un par de claves (pública y privada).
4. Solicitud de certificado a la CA raíz: La CA subordinada solicita un certificado a la CA raíz para la entidad.
5. Emisión de certificado x509: La CA raíz emite un certificado para la CA subordinada, que a su vez emite un certificado para la entidad.
6. Firma del certificado: El certificado es firmado digitalmente por la CA subordinada y la CA raíz.

ESTRUCTURA DEL CERTIFICADO X.509

Un certificado X.509 tiene la siguiente estructura:

- Número de versión: Indica la versión del certificado.
- Número de serie: Un número único que identifica el certificado.
- Algoritmo de firma: El algoritmo utilizado para firmar el certificado.
- Emisor: La entidad que emitió el certificado (CA subordinada).
- Sujeto: La entidad a la que se emitió el certificado.
- Clave pública: La clave pública de la entidad.
- Validez: La fecha de inicio y fin de validez del certificado.
- Extensiones: Información adicional sobre el certificado.

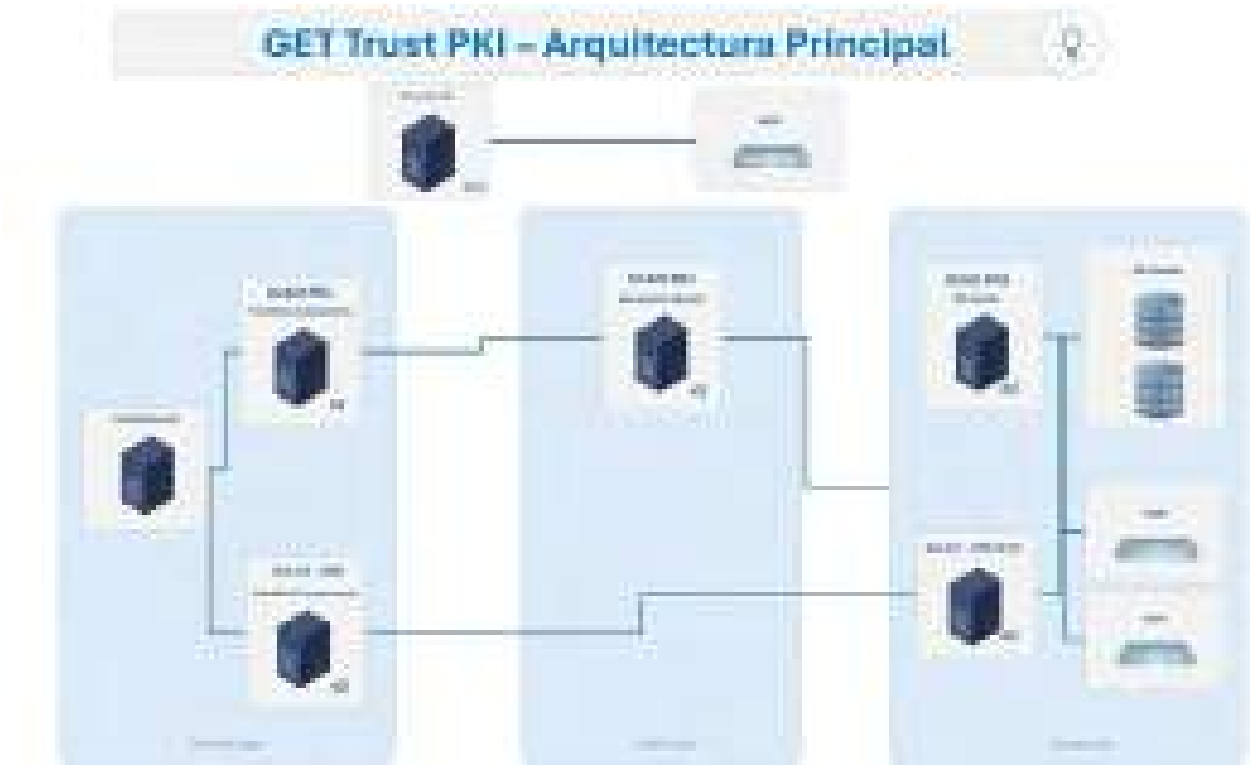
VENTAJAS DE LA PKI CON CA SUBORDINADA

La PKI con CA subordinada ofrece varias ventajas, como:

- Mayor flexibilidad: La CA subordinada puede emitir certificados para entidades específicas.
- Mejora la seguridad: La CA raíz puede revocar el certificado de la CA subordinada si es necesario.
- Reducir costos: La CA subordinada puede reducir los costos de emisión de certificados.

3.5 INFRAESTRUCTURA GET TRUST

La infraestructura de GET Trust está diseñada para permitir la comunicación digital segura, la autenticación y la protección de datos durante todo el proceso de personalización. La infraestructura que se describe a continuación comprende componentes esenciales del sistema y la intercomunicación entre ellos. Abarca la Autoridad de Certificación de Firma de País (CSCA), la Autoridad de Certificación Técnica (CA Técnica) responsable de los certificados SSL, los firmantes de datos y los sitios de emisión.



3.5.1 CARACTERÍSTICAS CLAVES

GET Trust cuenta con la notable capacidad de operar en entornos Windows y Linux y, al mismo tiempo, se adapta a diferentes estándares de API criptográfica, incluidos PKCS11, CNG y CSP. Además, la excepcional flexibilidad de GET Trust se extiende a su compatibilidad con módulos de seguridad de hardware (HSM) y soluciones de software HSM como el 'DB Crypto Engine'. Esta interoperabilidad dinámica garantiza que GET Trust pueda integrarse perfectamente en una amplia gama de infraestructuras de TI, brindando a las organizaciones la libertad de elegir las herramientas y plataformas que mejor se adapten a sus necesidades de seguridad.

- Máxima seguridad probada, Modulo CA certificado en CC EAL4+

- Multi-tenant por diseño: implemente, configure y administre varias PKI de forma independiente con una instancia de software.
- Cumplimiento de normas y estándares:
    - Cumplimiento del formato del certificado: X.509v3, RFC 5280 y RFC 3739
    - Solicitudes de certificados: PKCS#10, CSR, SPKAC
    - Algoritmos de firma RSA (1024 - 4096), (RSA PKCS#1 v1.5, RSA PSS PKCS#1 v2.1), ECDSA (192-521)
    - Algoritmos hash SHA-224, SHA-256, SHA-384, SHA-512, SHA-256 MGF1, SHA-384 MGF1, SHA512 MGF1
    - Contenido del certificado: UTF8, T61, imprimible, correo electrónico,
    - SAN (RFC822, UPN), etc.
- Cumplimiento:
    - Certificado RGS considerando todos los usos de los certificados y para todas sus clasificaciones (1, 2 y 3). LSTI N° 8029-1318-V3.0 / EN319411-1 V1.1.1
    - Cumple con eIDAS: obtención del Certificado LSTI N° 8029-1318-V3.0.

3.6 MÓDULO DE SEGURIDAD POR HARDWARE (HSM)

Nos permitimos ofrecer el modelo Eviden Trustway Crypt2pay, el cual presenta las siguientes características.

Eviden Trustway Crypt2pay ™ es un Módulo de Seguridad Hardware (HSM) que ofrece soluciones de software en un entorno altamente seguro y de alto rendimiento, permitiendo la ejecución de operaciones criptográficas muy sensibles. Este HSM combina medidas sólidas de seguridad física con un núcleo criptográfico que cumple con los estándares de seguridad más estrictos, lo que lo convierte en uno de los módulos criptográficos más certificados del mundo para integrarse en sistemas de información corporativos y servicios en la nube. Su implementación simplificada, diseñada para despliegue independiente, proporciona a los entornos críticos una solución ideal para garantizar la seguridad absoluta de sus datos sensibles, todo a un precio competitivo.

Algunas características clave de Eviden Trustway Crypt2pay incluyen:

- Nivel de seguridad alto: Diseño a prueba de manipulaciones (Anti-tampering) con un alto nivel de certificación.
- -Gestión sencilla: Fácil instalación y administración intuitiva.
- Disponibilidad alta: Mecanismos nativos para alta disponibilidad, conmutación por error y copias de seguridad.

- Protección de datos: Soluciones de protección de datos que le permiten cifrar, gestionar y controlar el acceso a sus datos, independientemente de su ubicación (local, virtual y en la nube).
- Autenticación: Eleva la seguridad de su aplicación mediante el control de acceso a sus datos y la protección de generadores de claves.
- Seguridad en la nube: Proporciona una raíz de confianza para servicios en la nube al asegurar la comunicación entre la nube privada y el sitio local, la encriptación de datos para soluciones locales y basadas en la nube, y servicios criptográficos bajo demanda.

  - APIs:
    - PKCS#11
    - OpenSSL
    - Java Cryptography Architecture/Extension (JCA/JCE)
    - Microsoft Crypto API (CSP), Cryptography Next Generation (CNG)
  - Diseño Anti-Tampering certificado en:
    - Common Criteria EAL4+ en cumplimiento con CWA 14167-2-PP
    - NATO SECRET
    - Cumple con eIDAS.
    - Qualification Renforcée (la más alta calificación de la ANSSI)
    - FIPS 140-2 level 3.
  - Algoritmos
    - DES: Triple DES
    - RSA: Keys up to 4069bits
    - 5 and PSS signature
    - SHA-1, SHA-2, SHA-3
    - HMAC
    - AES: 128, 192 and 256 bit keys
    - ECDSA: ANSI and Brainpool named curves
    - CHACHA & Poly1305
    - EdDS
  - Interfaces y características físicas
    - Performance: Crypt2pay XT: 100 to 3600 PVV tps
    - Voltage: 85 – 264 Vac
    - Red: 3 x 1Gb
    - 2 Hot Plug PSU
    - Frecuencia: 47 – 63 Hz
    - Humedad: 30% – 70% noncondensing
    - Temperatura de Operación: 10/45°C
    - Dimensiones: Crypt2pay XT: 442x346x76mm
    - Peso: Crypt2pay XT: 14 kg
  - Tipos de Llaves
    - Payment Industry keys.
    - Smart metering Industry keys.
    - PKCS#11 keys.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

- Generic secret keys.
- Import / Export keys feature.

ÍTEM IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL

4.1 INTRODUCCIÓN - GET MOBILE ID

La solución de identidad digital GET Mobile ID proporciona una identidad de alta seguridad en el dispositivo móvil de un usuario, que representa una alternativa conveniente, segura e instantánea a los documentos de identificación físicos tradicionales, y utiliza formidables algoritmos de cifrado de datos y medidas de seguridad de comunicación para reducir el robo de identidad y mejorar la privacidad de los ciudadanos.

4.1.1 GET MOBILE ID

Los ciudadanos quieren que sus documentos de identificación sean móviles y esperan poder administrar sus datos de identidad mejor que con las tarjetas de identificación físicas. GET Mobile ID brinda control de identificación por parte del usuario y permite una verificación de edad y una comprobación de identidad rápida y segura en todo tipo de negocios.

GET Mobile ID es el único producto en el mercado compatible con Android e iOS. Los gobiernos pueden emitir cualquier documento de identificación en GET Mobile ID. También permite que las organizaciones de todos los sectores (educación, empresa, comercio minorista y finanzas, así como instituciones públicas) acepten identificaciones digitales de alta seguridad. La autenticación es instantánea, las identidades son seguras, las interacciones están estandarizadas. Es la base para una amplia gama de servicios de identidad.

- La aplicación Direct to Consumer permite el control ciudadano del mID
- Tu identificación oficial en tu teléfono
- Totalmente compatible con ISO 18013-5
- Cambia cómo se protege la identidad
- No se puede falsificar

4.1.2 GET MOBILE ADMINISTRATOR

GET Mobile Administrator permite a los emisores de tarjetas de identificación del gobierno, hacer el cambio a lo digital de forma rápida y segura. Los gobiernos con visión de futuro podrán digitalizar sus documentos de identidad y dar a los ciudadanos el control de sus propios datos de identidad. GET Mobile ID cumple con la norma ISO/IEC 18013-5 de cinco estrellas con todos los canales de comunicación y modos de interacción estandarizados, dando como resultado la mejor experiencia de usuario y aceptación en la mayor cantidad de ubicaciones y casos de uso.

- Conectividad simple al sistema del JCE.
- Diseñado para Alta Disponibilidad.
- Conecta a los emisores para emitir identidades digitales en teléfonos móviles.
- Habilita todos los modos de interacción ISO 18013-5 en línea y fuera de línea
- Mantener actualizadas las identidades digitales
- Administrar el ciclo de vida de la identificación digital móvil

4.2 GET MOBILE ID – COMPONENTES

4.2.1 GET MOBILE ADMINISTRATOR

El módulo GET Mobile Administrator es fundamental para el concepto de producto mID, puesto que proporciona a la autoridad expedidora los siguientes servicios y funciones:

- Conectividad sencilla con el sistema de Identidad y Emisión del JCE.
- Diseñado para alta disponibilidad al 99,99% cuando se aloja en plataformas en nube o centros de datos redundantes y distantes.
- Conecta a los Emisores (el JCE) para que puedan emitir documentos de identidad firmados ISO 18013-5 en Teléfonos Móviles para sus ciudadanos.
- Incluye la más alta seguridad a nivel de pasaportes para la firma de datos mID a partir de su estructura de claves o de claves generadas
- Valida a los ciudadanos para garantizar que sólo reciben su documento de identidad.
- Permite solicitudes de verificadores compatibles con ISO 18013-5 en línea (WebAPI u OIDC).
- Mantiene los mID actualizados con los cambios de datos del Sistema del Emisor.

Los servicios prestados por GET Mobile Administrator son:

- Servicio de firma y gestión de claves: firma de forma segura los mID en nombre del emisor para transmitirlos a los dispositivos de los ciudadanos. Mediante la integración con la solución de PKI propuesta para el proyecto, se realizan los procesos de encripción sugeridos por la norma ISO 18013-5.
- Personalización y gestión de dispositivos: portal del consumidor para gestionar dispositivos, incluidos teléfonos perdidos, nuevos o actualizados.
- Fácil integración con sistemas de registro: conexiones API seguras con sistemas de registro que mantienen los datos actualizados.
- Gestión de Identidad y Acceso - Inicio de sesión y registro para verificadores que necesitan acceso a servicios ISO en línea.
- Caché mID – Puede mantener los datos mID durante un tiempo predeterminado para aligerar las solicitudes de los verificadores en la base de datos SOR.

4.2.1.1OPCIONES DE INTEGRACIÓN:

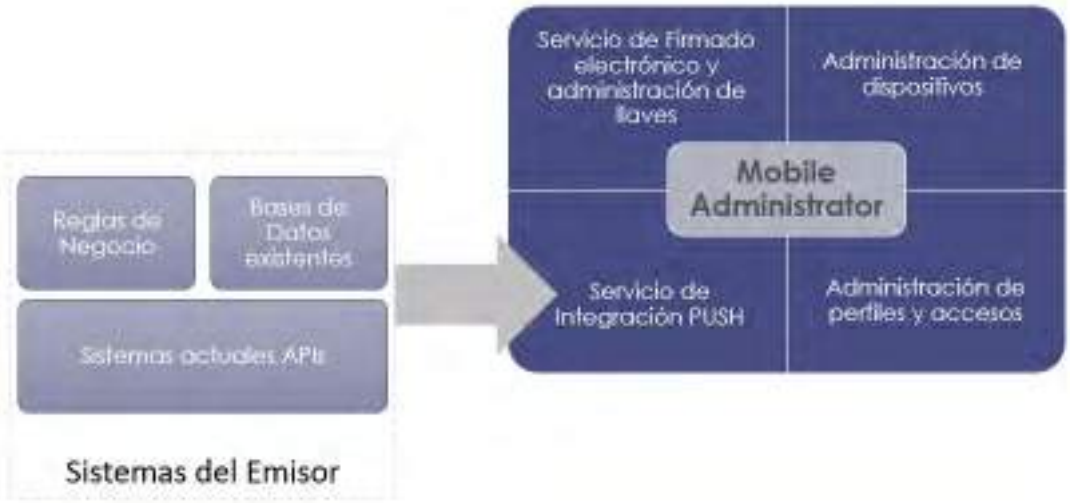
GET Mobile Administrator provee diferentes métodos de integración, buscando que la integración con el sistema de emisión del Emisor se pueda realizar de la forma más eficiente, y de esa manera, permitir un escalamiento progresivo en el desarrollo de casos de uso:

- Modelo sin integración: El modelo sin integración se basa únicamente en el aprovisionamiento diligenciado y aprobado por el administrador, se pueden aprobar nuevas solicitudes para Mobile ID sin una integración con la base de datos. El Administrador es responsable de revisar las solicitudes de mID, corregir cualquier error de datos, verificar la identidad y la confianza del solicitante y aprobar el mID que se proporcionará. Los datos mID están autocontenidos en la caché mID y el sistema se ejecuta basándose únicamente en esos datos.

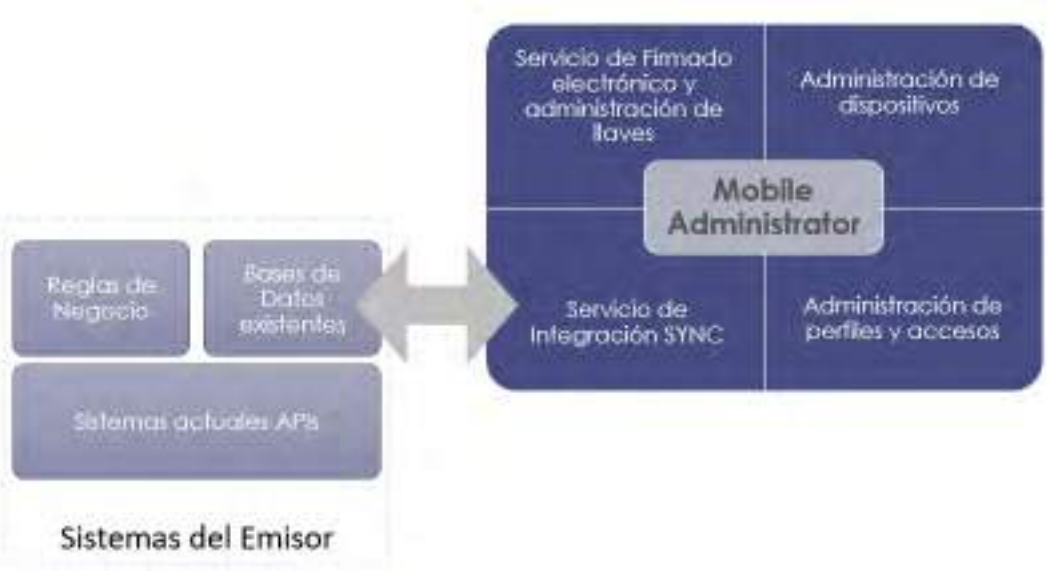
- Modelo Push: En el modelo Push, el sistema del emisor, como parte de su lógica empresarial, determina los momentos adecuados para llamar a GET Mobile Administrator con a través del API, usando un método de Creación de Licencia según los documentos de swagger para su instancia del software GET Mobile Administrator.

- Los documentos Swagger están disponibles al navegar a la URL de la instancia de la página GET Mobile Administrator Services del Emisor. Este modelo Push brinda el máximo control al entorno del sistema del emisor a expensas del tiempo de programación para la integración (el uso de la API es sencillo, rápido y fácil de usar según un enfoque tecnológico popular; el esfuerzo de programación puede variar dependiendo de la integración necesaria con los sistemas existentes).

El JCE puede crear sus propios informes a partir del software cuando utiliza este modelo porque tiene pleno conocimiento de qué mID están activos.

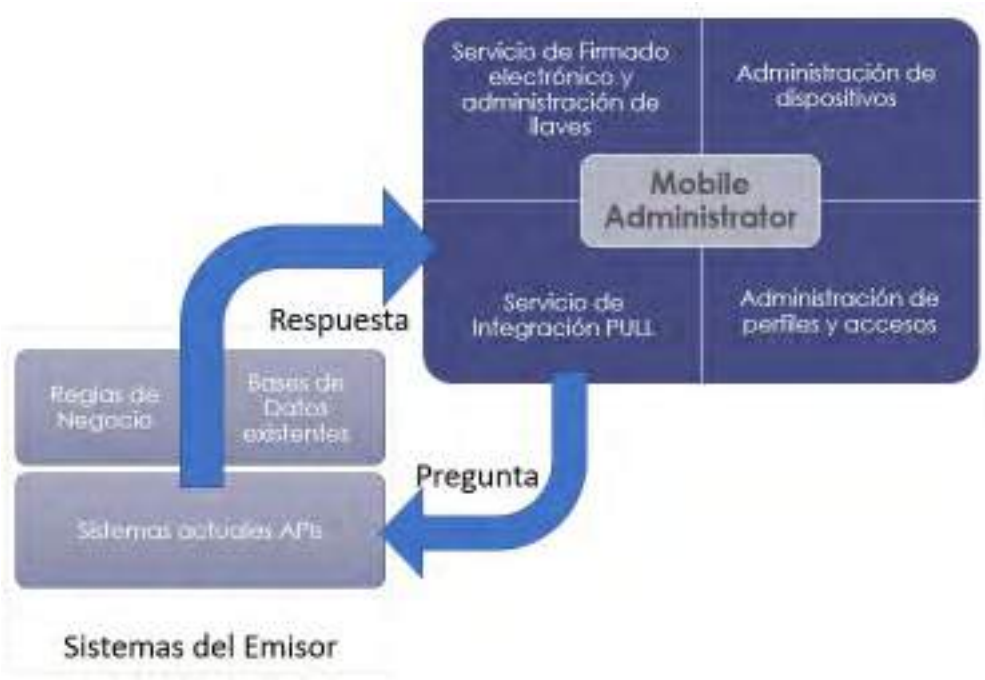


- Modelo SYNC: Para el modelo de sincronización, es posible realizar una conexión ODBC o similar entre el sistema del emisor y GET Mobile Administrator, cache que sincroniza el último registro del ciudadano en su registro en caché mID. La rutina de sincronización se puede configurar para sincronizar solo registros SOR estatales aprobados para mID, o para sincronizar todos los registros.



- Modelo Pull: En el modelo Pull, el administrador de GET Mobile se puede configurar para llamar a una API del sistema del emisor que busca registros actuales pendientes de emisión. La caché mID retiene registros de identidad para que el número de llamadas al sistema del emisor sea limitado.

La caché mID también se puede configurar para que no retenga datos. Si el sistema del emisor puede manejar los altos volúmenes de transacciones de los verificadores en el momento de uso, y existen requisitos contra el almacenamiento en caché de los registros más recientes detrás de la API en línea ISO (consulte la sección Medidas de seguridad para la API en línea a continuación), se puede configurar GET Mobile Administrator para llamar una API del sistema del Emisor que busca registros actuales. La carga completa de tráfico mID en el momento de uso (consulte la sección Tiempo de verificación (uso de mID) a continuación) alcanzará el SOR del emisor en esta configuración. (Cuando se hace referencia a SOR (Sistemas del Emisor), también puede ser un espejo local sincronizado de SOR).



4.2.1.2OPCIONES DE FIRMADO DIGITAL

La implementación de una identidad digital móvil ISO 18013-5 requiere llaves privadas del emisor que firmen los datos mID antes de que se aprovisionen en los dispositivos móviles. Estas llaves privadas pueden generarse a partir de la CA estatal. La CA no tiene que ser pública porque no existe una verificación de la cadena de certificados. Si se utiliza una CA estatal, se deben planificar ceremonias de certificación segura en el proyecto para obtener la clave privada en el servicio de firma o HSM. El Certificado Público IACA puede distribuirse por separado de la jurisdicción o colocarse en una "Lista Maestra" (también conocida como VICAL) con otros certificados confiables y ser distribuido por cualquier entidad. Los verificadores son responsables de garantizar que obtengan Listas Maestras confiables.

4.2.1.3MODELO DE DATOS Y CODIFICACIÓN.

JSON Identity Suite es el modelo de objetos sobre el que se construye Open ID Connect. Sus estructuras de datos JSON Web Token (JWT) están definidas en https://tools.ietf.org/html/draft-ietf-oauth-json-web-token-19 especificaciones IETF, con los campos de datos registrados en el registro JWT de la Autoridad de Números http://www.iana.org/assignments/jwt/jwt.xhtml. El estándar ISO 18013-5 ha ampliado el modelo de datos JWT con atributos de identidad específicos de las tarjetas de identificación (+ privilegios de conducción).

Este mismo modelo de datos JWT estándar se ejecuta a través de ISO 18013-5 y grupos de trabajo de OpenID Foundation (OIDF) para que las identidades digitales puedan ser utilizadas ampliamente y confiables por la más amplia gama de dispositivos autenticadores y dispositivos POS posible. La transmisión de datos "fuera de línea" ISO 18013-5 utiliza una representación compacta de objetos binarios (CBOR por sus siglas en ingles) de este modelo de datos JWT. Esto une los casos de uso en línea y en persona.

La codificación de los datos mID ha ser codificados en el dispositivo móvil, serán codificados de acuerdo al numeral 7.2 del estándar ISO 18013-5, campos que serán discutidos y coordinados con el JCE para que su integración tenga una correlación a los campos mencionados en el estándar. La definición de campos adicionales conlleva un análisis adicional para su inclusión y lectura por parte de los verificadores ISO 18013-5.

4.2.1.4PROCEDIMIENTO DE ACTIVACIÓN

Para el aprovisionamiento, o emisión y descarga de la identidad móvil en el dispositivo del ciudadano, GET Mobile Administrator presenta estas opciones de activación:

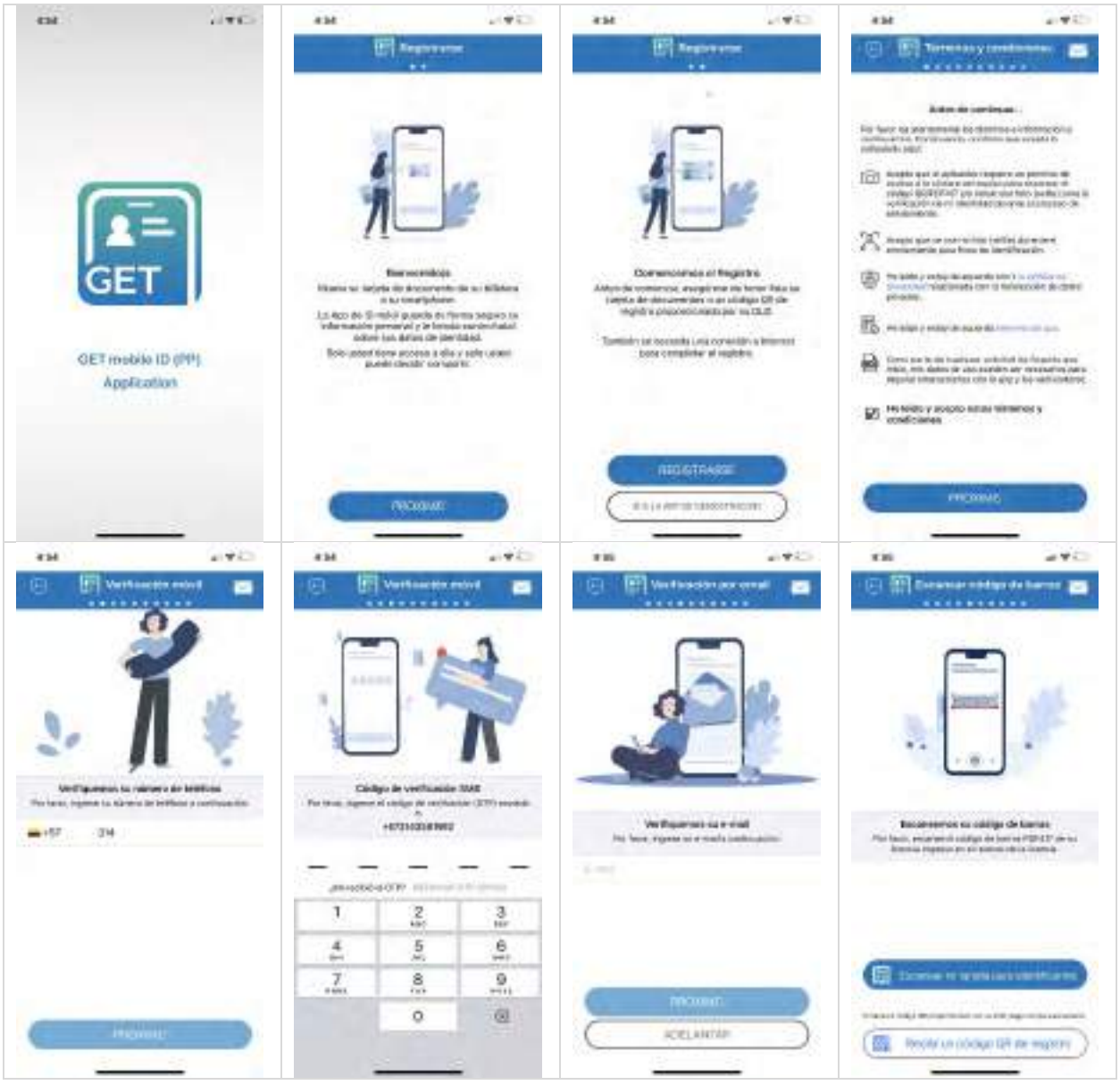
- Aprobador por Administrador: Para el aprovisionamiento aprobado por el administrador, los datos se ingresan a través de GET Mobile Administrator. El Administrador aprueba el registro verificando la identidad del solicitante e ingresa la información en el Administrador de GET Mobile ya sea de forma manual o automática desde el sistema del emisor (ver opciones de integración arriba). Una vez que se inserta el registro, los datos mID están listos para publicarse en la aplicación móvil. Es opción es ideal para un programa piloto, donde el titular puede recibir una invitación por correo electrónico para descargar la aplicación y luego completar un breve formulario para personalizar su aplicación con los datos de mID.

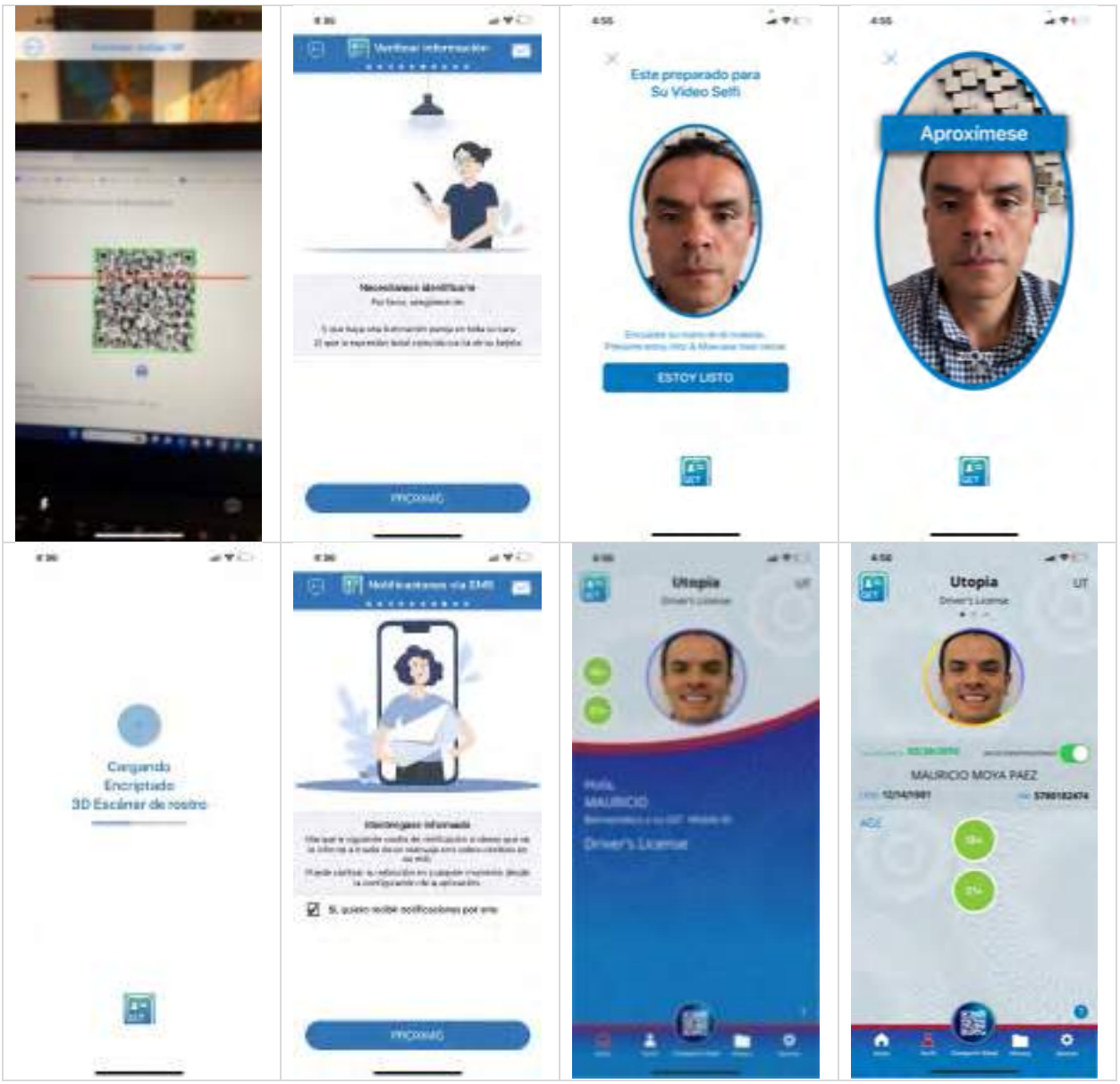
- Aprovisionamiento en Persona: Para el aprovisionamiento en persona supervisado por un operador, el administrador de GET Mobile o la aplicación del sistema del emisor del operador pueden mostrar un código QR que identifica un registro mID adecuado y permite que la aplicación GET Mobile ID acceda a ese registro mID adecuado para descargarlo en el dispositivo móvil. (personalización). Alternativamente, el titular puede rellenar un breve formulario para personalizar su aplicación con los datos mID.

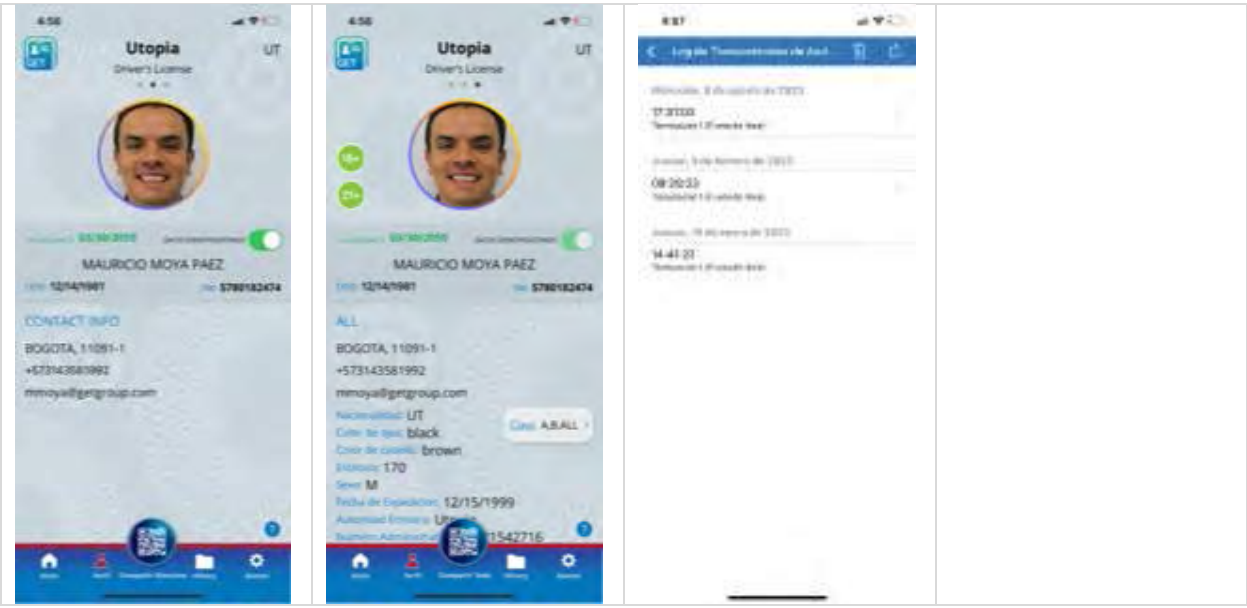
- Aprovisionamiento remoto: Para el aprovisionamiento remoto/selfie + liveness, la función del GET Mobile Administrator es verificar a una persona basándose en un escaneo de su identificación estatal emitida por el gobierno, o mediante la lectura de un código QR enviado por correo

electrónico, y una selfie en vivo, incluyendo validación de vida certificada ISO 30107-3 , ambas tomadas en el momento del proceso de inscripción de la aplicación GET Mobile ID. Esta opción incluye la instalación de un componente de que facilita la verificación de datos biométricos y demográficos durante el proceso de registro de emisión de mID. Luego de la emisión, se solicita al usuario digitar un PIN Personal, para permitir la apertura de la aplicación de forma segura. Se cuenta con la funcionalidad de Apple FaceID para realizar este proceso de autenticación.

DEMOSTRACIÓN DE APROVISIONAMIENTO REMOTO:




Este preparado para
Su Video Selfi
ESTOY LISTO
Aproximese
Cargando
Encriptado
3D Escáner de rostro
Utopia
Driver's License
Utopia
Driver's License
MAURICIO MOYA PAEZ



4.2.2 GET MOBILE ID – APLICACIÓN MÓVIL

GET Mobile ID estará disponible en las tiendas de aplicaciones públicas de cada plataforma móvil en el momento del lanzamiento. Dado que es una aplicación de consumo, se espera que las características del producto se aceleren continuamente y se les dé prioridad según las solicitudes de los ciudadanos/usuarios y lo que esté sucediendo en el mercado mID. El uso de una aplicación de las tiendas de aplicaciones proporciona la experiencia de aplicación que los usuarios esperan de sus bancos, emisores de tarjetas de crédito, proveedores de atención médica y entretenimiento. Todos los usuarios de la aplicación en todas las jurisdicciones experimentarán el mismo conjunto de funciones y se podrán implementar nuevas funciones en todo el país.

El CONSORCIO trabajará con el JCE para configurar (“personalizar”) el interior de la aplicación GET Mobile ID cuando un ciudadano lleva su credencial digital como mID. El sello estatal, los patrones de fondo entrecruzado, las fuentes de encabezado y las banderas, así como los tipos de licencia, están disponibles como configuraciones. El GET Mobile ID no es una tarjeta y no tiene una representación de tarjeta; está diseñado para ser intervenido, compartido y utilizado electrónicamente porque la prueba criptográfica de identidad es fácil de presentar utilizando ISO 18013-5.

El CONSORCIO se asegurará de que los campos de la credencial digital estén asignados a los campos ISO 18013-5. Si alguno permanece sin asignar, se puede agregar opcionalmente según se define en los campos específicos de las jurisdicciones, pero no podrán ser leídos por todos los dispositivos o aplicaciones lectores estandarizados. Por lo general, esto no es un problema en los casos de uso de identidad, ya que los campos específicos de la jurisdicción no suelen ser necesarios para aprobar transacciones generalizadas.

Soporte de cumplimiento y estándares

- Cumple con las especificaciones y directrices de la AAMVA
- Certificado de cumplimiento de las normas ISO/IEC18013
- Comunicación entre pares compatible con NFC, Bluetooth y WiFi nativos
- Manejo de llaves conforme a ICAO 9303
- Protección de acceso básica mejorada mediante clave de acceso dinámica

Soporte de comunicaciones

- HTTP/S
- Modo par NFC
- Modo Bluetooth Peer to Peer
- Wifi aware
- Código de barras 2D

Funciones de control de seguridad

- Seguridad redundante mediante almacenes de claves respaldados por hardware.
- Encripción de datos en reposo y transmisión encriptada basada en sesiones.
- Los datos de mID están firmados por la autoridad emisora de confianza a prueba de manipulaciones.
- La ofuscación de aplicaciones significa que el código ejecutable no se puede piratear.
- Protección de análisis estático y dinámico. Se logran protecciones integrales de análisis estático y dinámico a través de técnicas de encriptación y ofuscación en capas complementadas con verificaciones RASP automatizadas y defensas antimalware integradas. Protección contra jailbreaking y rooting.
- OAuth habilitado para autorización de agentes del orden.
- Revocación automática desde el GET Mobile Administrator.
- Criptografía soportada: RSA y Eliptic Curves.

4.2.2.1OPCIONES DE PERSONALIZACIÓN

GET utilizará componentes existentes sobre una base de desarrollo personalizado para crear una aplicación de emisor personalizada que funcione según los requisitos y el diseño del emisor. Una vez determinado el tamaño y el alcance de los requisitos de la aplicación, se procede con los ajustes de personalización. Además, si el JCE desea publicar la aplicación a través de su propia tienda de aplicaciones (también conocida como marca blanca), se requerirá una coordinación significativa con el personal de Desarrollo de productos de GET para coordinar las actualizaciones del servicio con las actualizaciones de la aplicación.

GET trabajará en conjunto con el JCE para presentar una propuesta de diseño que cumpla con los requerimientos de diseño de la marca JCE y de la marca PAIS.

Así mismo, el sistema GET Mobile Administrator, en conjunto con las aplicaciones móviles, permiten la generación de notificaciones PUSH, permitiendo la comunicación con los ciudadanos portadores del GET Mobile ID.

4.2.2.2CONTROL TOTAL Y PROTECCIÓN DE LA PRIVACIDAD

Todos los ciudadanos tienen el derecho básico a controlar su información de identidad. Deberían poder elegir qué datos comparten, ser transparentes en su uso y tener un registro claro de dónde han compartido sus datos. En línea o fuera de línea, GET Mobile ID permanece bajo el control del ciudadano y siempre se requiere su consentimiento para compartir datos, proporcionando un registro claro para el titular del mID de dónde se utilizaron los datos del mID y, cuando sea posible, por quién.

Actualmente, cuando una persona quiere acceder a un colegio de abogados, por ejemplo, está obligada a demostrar su edad. Sin embargo, al presentar un documento de identificación físico, el individuo se ve obligado a exponer toda su información personal (incluida la dirección y otros datos personales sensibles), algunos de los cuales tal vez desee mantener en privado. Al escanear los códigos de barras se crea un registro permanente de sus datos. Con el mID compatible con ISO de GET, un ciudadano puede proteger su privacidad eligiendo la cantidad y el tipo de datos que pueden transferirse a los verificadores. Sólo ciertos verificadores necesitan acceso a todos los elementos de datos. GET Mobile Verify puede limitar los niveles de acceso a datos según la función, la suscripción y la autorización del verificador.

4.2.2.3SIEMPRE ACTUALIZADO

Las aplicaciones móviles son dinámicas, a diferencia de las credenciales físicas estáticas, lo que permite definir una frecuencia para actualizar los datos mID. El Administrador de GET Mobile permite al Emisor establecer una política de actualización y aplica e implementa automáticamente esa política para que todos los mID conectados dentro de GET Mobile ID se actualicen de forma natural. Ni el ciudadano ni el administrador necesitan preocuparse por mantenerse al día. Además, GET Mobile Administrator admite múltiples mecanismos, a elección del Emisor, para transmitir datos de identificación modificados desde el sistema de registro (SOR) a los usuarios con mID.

Cuando el emisor cambia el estado de una identificación, el emisor transmite ese cambio al administrador de GET Mobile para que lo transmita inmediatamente al dispositivo móvil del usuario. Si un ciudadano reporta la pérdida de una tarjeta o un teléfono, es posible que se le dé de baja de forma remota. Más convenientemente, las funciones de teléfono perdido o extraviado disponibles en cada plataforma están completamente disponibles. Los usuarios pueden borrar los datos del teléfono utilizando sus inicios de sesión individuales en la plataforma. Estas funcionalidades de actualización también aplican en los escenarios de revocación que la Administración decida implementar.

4.2.2.4INTEROPERABILIDAD

El concepto de interoperabilidad en el marco de la norma ISO 18013-5 hace referencia la capacidad que deben tener las identidades móviles en poder ser usadas dentro de la jurisdicción del emisor (en este caso, la Republica Dominicana) y cualquier otra jurisdicción que requiere poder leer la información de una identidad digital.

Con relación a lo anterior, la norma ISO 18013-5 es la guía para que los gobiernos puedan emitir identidades móviles a sus ciudadanos de manera que están puedan ser leídas, comprobadas y verificadas dentro de otras jurisdicciones. Por ejemplo, en Colombia, país que ha implementado la identidad móvil digital desde el año 2020, a razón de haber implementado el estándar ISO 18013-5, es ahora permitido viajar en los diferentes países de la CAN y MERCOSUR con tan solo mostrar su identidad móvil en su teléfono inteligente, puesto que, al ser una identidad estandarizada, la interoperabilidad le permite identificar que la identidad sigue siendo original y sin modificaciones.

Es así que al decir que una solución de emisión de identidades móviles digitales se encuentra CERTIFICADA para el estándar ISO 18013-5, confirma que esta solución permite la interoperabilidad de las identidades emitidas por esta solución, en conjunto con las diferentes opciones de integraciones y API disponibles para acceder a información adicional y verificaciones.

4.2.3 GET MOBILE VERIFIER

Contrariamente a lo que se cree erróneamente, aceptar identificaciones móviles no significa mirar la pantalla del teléfono de sus clientes ni manipular su teléfono en absoluto. Las herramientas de manipulación de fotografías hacen que el uso visual no sea confiable y usted nunca debe asumir la responsabilidad de manipular el teléfono de su cliente.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

Los mecanismos de transmisión ISO 18013-5 permiten modos de interacción flexibles que mantienen a su cliente en control de su dispositivo y sus datos, al tiempo que le brindan al verificador prueba criptográfica indiscutible de la identidad de su cliente, incluso sin sobrecarga de datos.

Cuando intercambia datos electrónicos y valida pruebas criptográficas, ya no está sujeto a los requisitos de "línea de visión" de las tarjetas de identificación físicas.

A medida que la identificación se vuelve cada vez más digital, el mercado debe estar preparado para aceptar rápidamente identificaciones móviles desde cualquier parte del mundo como forma legal de identidad o verificación de edad. La aplicación GET Mobile Verify le proporcionará una transacción de cliente más fácil y segura.

- Aplicación directa a la parte que confía: verificar la edad y la identidad del titular.
- Lectura estándar ISO 18013-5 en línea y fuera de línea.
- Trabaja con todas las jurisdicciones a nivel mundial a través de una lista confiable
- Disponible para iOS y Android: GET Mobile Verify admite NFC, BLE, Wi-Fi Aware y WebAPI en plataformas iOS y Android. Disponible como motor para dispositivos Windows y POS.
- Reduce la complejidad de la inspección de documentos de identificación globales: mantenerse al día con los cambios de los documentos de identificación en constante cambio es difícil. ¿Cómo puedes saber qué es real o qué es simplemente una muy buena tarjeta de identificación falsa? Las identificaciones móviles mID presentan su prueba de identificación electrónicamente y de la misma manera siempre: grande, en negrita, mostrando prueba de edad o identificación. No requiere del entrenamiento laborioso del personal y hay menos errores cuando los documentos parecen ser legítimos.
- Obtiene una prueba criptográfica de identificación: el simple hecho de mirar los documentos de identificación, especialmente en dispositivos móviles, no descarta las identificaciones falsas. GET Mobile Verify solo acepta documentos de emisores de identificación gubernamentales conocidos, lo que reduce su responsabilidad y exposición.
- Respeta la confidencialidad de sus clientes: reducir los datos intercambiados durante las transacciones de identificación mejora la privacidad de sus clientes y alivia sus preocupaciones sobre privacidad y seguridad, al tiempo que reduce su exposición y responsabilidad de recopilar y almacenar datos personales.
- Transacciones de identidad más saludables: proteja la salud de sus empleados y clientes con transacciones de identificación sin contacto. Un toque o un escaneo desde la distancia social garantiza que no esté manipulando documentos de identidad ni asumiendo responsabilidad por el manejo de los teléfonos móviles de sus clientes. GET Mobile Verify permite a tus clientes comprobar su identidad desde una distancia segura y saludable.

El estándar ISO/IEC 18013-5 introduce dos pasos en una interacción mID: La interacción del dispositivo (Device engagement) es cuando el mID y el dispositivo lector negocian cómo conectarse en el intercambio de datos mID en línea; Y fuera de línea, a través de un canal de transmisión mutuamente compatible. Una vez elegido un canal, los dispositivos realizan la transmisión de datos mediante solicitud-respuesta.

Se admiten dos modelos: verificación offline (sin necesidad de Internet) y verificación de búsqueda en línea.

Los métodos de interacción con dispositivos admitidos: NFC, QR, BLE (según la extensión en evolución del borrador del estándar internacional ISO).

Canales de transmisión de datos admitidos: NFC sin conexión (Android completo e iOS en alfa), BLE, WIFI Aware (en versión beta disponible solo en Android 10 o posterior), en línea a través de WebAPI y Open ID Connect.

Simulación de Verificación de mID

Aplicación mID	Aplicación Mobile Verifier
 Se inicia la Aplicación GET Mobile ID	 Se inicia la aplicación GET Mobile Verifier
 El usuario elije los datos que desea compartir	
 El usuario selecciona Compartir	 Se escanea el QR compartido

<table>
<tr><td> </td><td>
Se transfieren los datos compartidos y se visualizan</td></tr>
<tr><td> </td><td>
Se verifican los datos de los certificados digitales</td></tr>
</table>

4.2.3.1MODOS DE INTERACCIÓN

Las combinaciones de interacción con el dispositivo, transferencia de datos y en línea/fuera de línea crean “interacciones” únicas que, si se implementan por completo, permitirán a los verificadores reconfigurar el flujo de trabajo para adaptarlo a su negocio y brindar un servicio ampliado y más personalizado a los clientes de mID en comparación con lo que se ofrece tradicionalmente con Tarjetas físicas.

Estos modos de interacción combinados se pueden resumir a continuación. El soporte de todos los modos de interacción pasa a ser responsabilidad del Emisor al elegir la tecnología mID. Múltiples modos de interacción brindarán la experiencia de usuario óptima para los titulares de mID y brindarán la mejor opción para los verificadores de mID.

Los verificadores deberían poder elegir el modo de interacción que mejor respalde su negocio.

Modo de Interacción	Vinculación de Dispositivo	Transferencia de Datos	Autorización de Usuario [Si es no atendida]	Descripción
Tap & Go	NFC	BLE		El toque NFC establece BLE para la transferencia de datos y el usuario puede alejar el mID mientras transfiere datos al lector
Tap & Request	NFC	Online		NFC contiene un token WebAPI que devuelve datos con el retrato (fotografía) para el operador
Tap & Hold	NFC	NFC		Interacción y transferencia de datos complete por NFC

Scan & Go	QR	BLE	El usuario sostiene el código QR mID frente a la cámara del lector y luego puede mover el mID mientras se transfieren datos a través de un método cercano
Scan & Request	QR	Online	El usuario sostiene el código QR mID en la cámara del Reader y los datos aparecen en el Reader después de una rápida recuperación en línea

Dar soporte a estos múltiples modos de interacción no requiere ningún esfuerzo por parte del JCE más allá de elegir e implementar la tecnología de aplicación GET Mobile ID y realizar una opción de integración estándar como se describe en este documento. Será una opción clave para los ciudadanos y para construir una plataforma en la que la identidad móvil pueda florecer verdaderamente.

4.2.4 Herramientas de Desarrollo

GET Mobile ID tiene la posibilidad de brindar un soporte adicional con relación a las herramientas de desarrollo disponibles para la implementación de la emisión de una identidad digital móvil basada en estándar ISO 18013-5, dentro de las cuales se encuentran:

- SDK's para la emisión de identidades, para Android y iOS.
- API para la conexión e integración en el proceso de emisión de identidades móviles.
- SDK's disponibles para la verificación de identidades móviles, basadas en estándares, para su implementación en Android, iOS, Windows o sistemas POS.

Durante el proceso de análisis de requerimientos se establecerán los compromisos necesarios para realizar la entrega de los SDK's solicitados de acuerdo con la necesidad de implementación del JCE.

4.2.5 INFRAESTRUCTURA

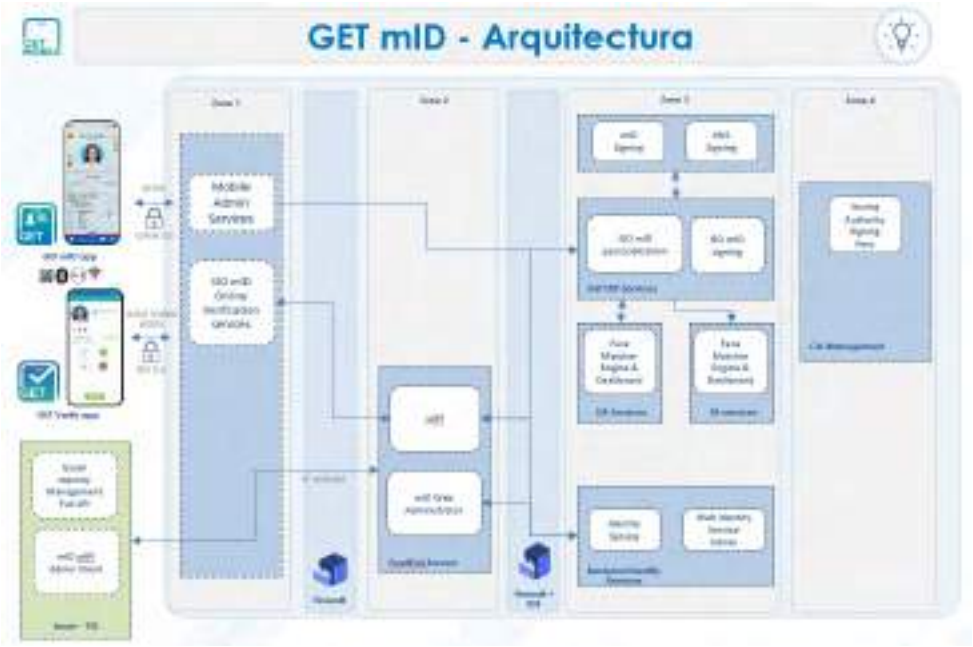
4.2.5.1ARQUITECTURA DE ALTA DISPONIBILIDAD

El diseño de la solución GET Mobile ID es un diseño innovador que está basado en la Alta Disponibilidad de cada uno de los componentes, en conjunto con el uso de diferentes zonas de seguridad para garantizar la implementación segura. El diseño de solución acá propuesto incluye la capacidad requerida para emitir al menos 5.000 GET Mobile ID por día.

Los módulos que componen la arquitectura de la solución son:

- Mobile Admin services: API para la Administración de la emisión en los teléfonos móviles.
- ISO mID Online Verification services: API para la verificación de identidades Mobile ID en línea.
- xAPI: API para el control de la emisión de identidades Mobile ID.
- mID Web Administrator: Modulo Web que permite la administración de la solución, su configuración, visualizar de eventos y auditoria, gestor de reportes.
- mID Signing: Modulo de firma de documentos digitales, utiliza las llaves del PKI para su función.
- JWS Signing: Modulo de firmado para archivos JSON.
- ISO mID Perso: API para emisión de identidades estándar ISO 18013-5
- ISO mID signing: API para el firmado ISO.

- Face matcher: Módulos de comparación y base de datos para la verificación biométrica y reconocimiento de vida.
- Identity Service: Modulo de administración de identidades.
- Web Identity Service Admin: Administración de usuario para módulos web.
- Issuing Authority Signing Keys: Solución PKI.



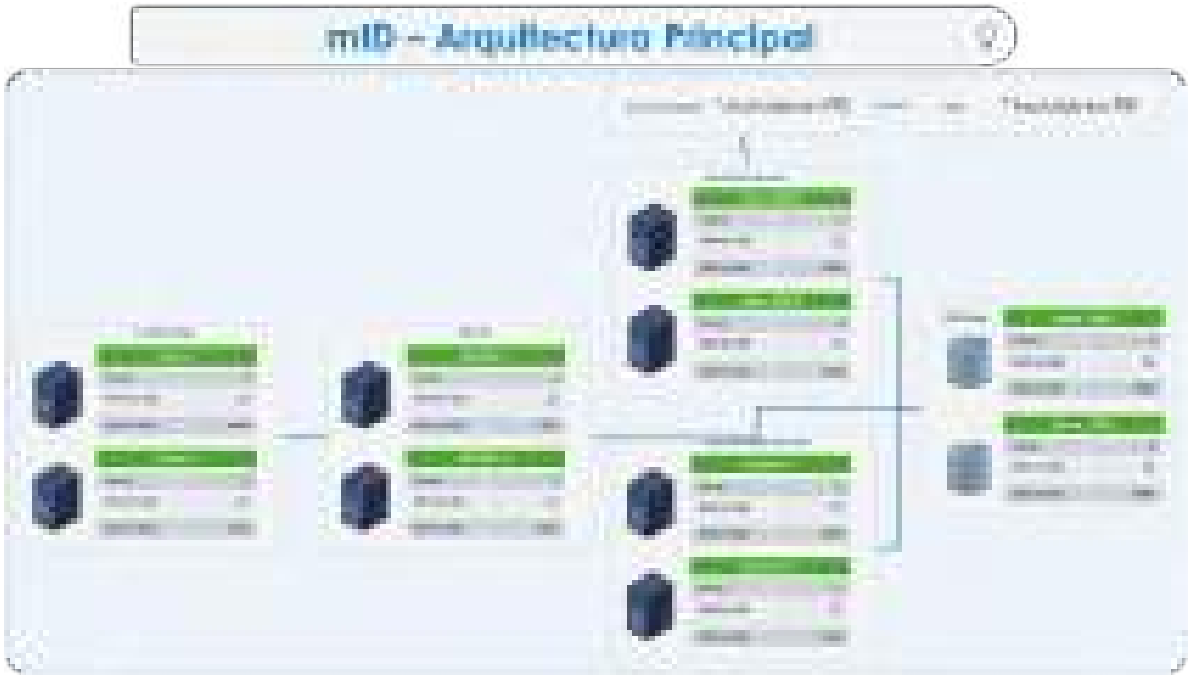
Se han tomado todas las previsiones del caso para poder brindar a la JCE una plataforma con mecanismos de alta disponibilidad del servicio tanto en hardware como en software contemplando los siguientes aspectos a nivel de diseño de la infraestructura para garantizar la continuidad de la operación:

Se dispondrá de una infraestructura Hiperconvergente el cual está diseñado con 4 nodos para brindar una redundancia y alta disponibilidad, además de una capa de interconexión media con dos switches en HA para realizar la configuración del ambiente de producción requerido. Esta solución de hiperconvergencia contempla una configuración vSAN para brindar alta disponibilidad a nivel de almacenamiento.

Esta solución contempla un esquema de respaldos sobre las máquinas virtuales requeridas para desplegar el servicio, el cual se define en 1 respaldo Full diario con retención de 30 días.
Además, se incluye una capa de red de borde compuesta por dos switches en configuración de alta disponibilidad y redundancia para brindar la interconexión entre la infraestructura de hiperconvergencia, la capa de seguridad dimensionada y la conexión hacia la infraestructura de la JCE.

A nivel de seguridad se contempla un diseño de alta disponibilidad de NG Firewalls, este es un componente crítico en la arquitectura de seguridad de redes modernas. Estos dispositivos desempeñan un papel fundamental en la protección de una organización contra amenazas cibernéticas, por lo que garantizar su continuidad operativa es esencial. Para lograr una alta disponibilidad, se implementan redundancias en la infraestructura del NG Firewall, lo que incluye configuraciones en clúster, así como elementos en su arquitectura física, como fuentes de poder redundantes.

Referente a la implementación del Web Application Firewall (WAF), el mismo es un elemento virtual dentro de la solución ofertada. De esta manera, teniendo lo anterior en consideración, es posible brindar todas las bondades de los ambientes de virtualización desarrollados en el presente diseño, lo que permite que el WAF tenga una alta disponibilidad en su infraestructura. Un Web Application Firewall (WAF) virtual de Alta Disponibilidad (HA) es una parte esencial de la estrategia de seguridad cibernética para proteger aplicaciones web y sitios web.



4.2.5.2DISPONIBILIDAD DEL 99.95% DE OPERACIÓN

Con el fin de garantizar un esquema de alta disponibilidad de operación durante las horas efectivas de producción definidas por el JCE el consorcio considera conveniente la inclusión de un recurso especializado en los equipos de procesamiento y seguridad en sitio para garantizar la atención inmediata de incidentes que se puedan presentar y reducir los tiempos de atención de la solución, esto en conjunto con los diseños explicados en el apartado de Infraestructura buscan garantizar al JCE el menor impacto posible en la operación y la continuidad del servicio.

ÍTEM V- KIT PERIFERICOS

5 INTRODUCCION

Como parte del compromiso del Consorcio Identidad 4.0 RD con la modernización y optimización del sistema de identificación de la Junta Central Electoral (JCE), se ha realizado un análisis exhaustivo de los dispositivos disponibles en el mercado, priorizando la eficiencia, seguridad y compatibilidad con la infraestructura existente.

En base a la amplia experiencia del consorcio en la implementación de soluciones tecnológicas para la gestión de identidad, se ha seleccionado el Canon imageFORMULA P-208II como el escáner ideal para la digitalización de documentos dentro del proceso de emisión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI).

Este escáner portátil de alto rendimiento destaca por su precisión en la captura de documentos oficiales, incluyendo tarjetas de identificación, licencias de conducir, contratos, fotografías y otros archivos esenciales para la personalización y validación de identidad. Su diseño compacto y su capacidad de escaneo a doble cara optimizan los tiempos de procesamiento, reduciendo significativamente los errores en la captura de datos.

El Canon imageFORMULA P-208II ha sido elegido estratégicamente debido a los siguientes factores clave:

- Experiencia del consorcio en la implementación de sistemas de escaneo de alta precisión, garantizando su integración óptima con los procesos de la JCE.
- Compatibilidad comprobada con los sistemas operativos y plataformas en la nube utilizadas en proyectos de identidad digital.
- Cumplimiento con estándares internacionales de calidad y seguridad, incluyendo normativas de protección de datos y eficiencia energética.
- Fiabilidad en entornos de alto volumen de escaneo, respaldada por casos de éxito en la implementación de este modelo en otros organismos gubernamentales y entidades de identificación ciudadana.

El imageFORMULA P-208II permite un escaneo intuitivo y eficiente mediante su función de "Conectar y Escanear", eliminando la necesidad de instalación de software adicional. Además, su tecnología de Reconocimiento Óptico de Caracteres (OCR) facilita la conversión de documentos físicos en archivos digitales estructurados, garantizando una gestión documental ágil y segura.

Debido a su compatibilidad con sistemas operativos Windows y Mac, así como su integración con plataformas en la nube como Google Drive™, OneDrive™ y Microsoft® SharePoint®, este escáner representa una solución flexible y escalable, perfectamente alineada con los requerimientos tecnológicos y operativos de la JCE.

Con una trayectoria comprobada en la integración de soluciones tecnológicas para identidad digital, el Consorcio Identidad 4.0 RD garantiza que la incorporación del Canon imageFORMULA P-208II fortalecerá la infraestructura de emisión de cédulas, asegurando una transición eficiente hacia un sistema moderno, seguro y de alta precisión.

DESCRIPCIÓN DE LOS PERIFÉRICOS

5.1 ESCÁNER DE DOCUMENTOS - CANON IMAGEFORMULA P-208II

El Canon imageFORMULA P-208II es un escáner de documentos compacto y portátil que permite la digitalización rápida de documentos de identidad, fotografías, contratos y otros archivos relevantes. Es ideal para su uso en entornos de oficina o en movilidad.

ESPECIFICACIONES TÉCNICAS

- Tipo: Escáner de documentos portátil.
- Alimentación de documentos: Automática o manual.
- Tamaño de documentos:
- Anchura: 2.0” a 8.5”
- Longitud: 2.8” a 14.0”
- Capacidad del alimentador: 10 hojas.
- Modos de escaneo: Color, escala de grises y blanco y negro.
- Resolución óptica: 600 ppp.
- Velocidades de escaneo:
- Blanco y negro: Hasta 8 páginas por minuto (ppm) / 16 imágenes por minuto (ipm).
- Escala de grises: Hasta 8 ppm / 16 ipm.
- Color: Hasta 8 ppm / 16 ipm.
- Interfaz: USB 2.0 de alta velocidad.
- Compatibilidad con sistemas operativos: Windows (XP, Vista, 7, 8, 10) y Mac OS X 10.6 en adelante.
- Software integrado:
- CaptureOnTouch: Optimización de escaneo con opciones avanzadas.
- OCR (Reconocimiento Óptico de Caracteres): Convierte documentos físicos en texto digital.
- Integración con la nube: Compatible con Google Drive™, Evernote™, Microsoft® SharePoint®, OneDrive™ y Dropbox™.

OTRAS CARACTERÍSTICAS:

- Detección automática de color y tamaño de documento.
- Corrección de desviación y eliminación de sombras.
- Detección de alimentación doble para evitar pérdida de datos.

BENEFICIOS

- Escaneo rápido y eficiente, optimizando el procesamiento de documentos en la JCE.
- Compacto y portátil, ideal para estaciones de trabajo con espacio limitado.
- Integración con los sistemas de la JCE, facilitando el almacenamiento seguro de documentos digitales.
- Alta calidad de imagen, asegurando legibilidad en documentos oficiales.

5.2 TABLETA DE FIRMA DIGITAL WACOM STU-540

Como parte de esta estrategia, y en base a la amplia experiencia del consorcio en la implementación de soluciones de autenticación digital y biométrica, se ha seleccionado la tableta de firma digital Wacom STU-540. Este dispositivo representa la opción más avanzada y confiable en la captura de firmas electrónicas manuscritas, asegurando precisión biométrica, seguridad criptográfica y una integración fluida con los sistemas existentes de la Junta Central Electoral (JCE).

La elección del Wacom STU-540 responde a los siguientes criterios estratégicos:

- Experiencia del consorcio en la implementación de sistemas de firma electrónica en entornos gubernamentales y de alta seguridad.
- Cumplimiento con estándares internacionales de cifrado y autenticación, garantizando la validez jurídica de las firmas electrónicas.
- Compatibilidad con infraestructuras de escritorio virtual (VDI), permitiendo su integración con plataformas como Citrix XenDesktop y XenApp.
- Fiabilidad y durabilidad en entornos de alto tráfico, asegurando un rendimiento óptimo en oficinas de atención al ciudadano.
- Autenticidad en la representación de la firma manuscrita, mediante la tecnología WILL™ (Wacom Ink Layer Language), que proporciona una apariencia natural y precisa de cada trazo.

El Wacom STU-540 ha sido seleccionado como la solución óptima para la captura de firmas electrónicas en el proceso de emisión de la Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI), gracias a su combinación de precisión biométrica, seguridad avanzada y robustez operativa.

Su pantalla LCD de 5 pulgadas con vidrio endurecido proporciona una experiencia de firma natural y ergonómica, replicando la sensación del papel y garantizando una durabilidad superior ante el uso intensivo en entornos de alta demanda. Además, su tecnología de captura con 1024 niveles de presión permite registrar con exactitud cada trazo de la firma manuscrita, asegurando una autenticación precisa, única y verificable.

Desde una perspectiva de seguridad y cumplimiento normativo, el Wacom STU-540 incorpora cifrado AES-256 y RSA-2048, garantizando la integridad y confidencialidad de cada transacción. Su Identificador Único de Hardware (UID) permite asociar de forma inalterable cada firma al dispositivo donde fue generada, fortaleciendo los mecanismos de auditoría, trazabilidad y prevención de fraude dentro del sistema de identidad de la Junta Central Electoral (JCE).

En términos de integración y escalabilidad, su conectividad flexible mediante USB, Virtual COM Port (VCP) y RS-232 facilita su implementación en infraestructuras de escritorio virtual (VDI), garantizando una interoperabilidad sin fricciones con los sistemas actuales de la JCE. Adicionalmente, su capacidad para almacenamiento y despliegue de imágenes permite utilizar el dispositivo como un canal de comunicación institucional, optimizando la difusión de información relevante para los ciudadanos.

La incorporación del Wacom STU-540 en la solución propuesta por el Consorcio Identidad 4.0 RD refuerza el compromiso con la innovación tecnológica y la seguridad en la gestión de identidad, asegurando un sistema de identificación digital eficiente, confiable y alineado con los más altos estándares internacionales.

5.3 LECTOR DE HUELLAS DIGITALES DIGITALPERSONA 4500

La autenticación biométrica es un pilar esencial en la modernización de los sistemas de identidad. Por ello, el DigitalPersona 4500 es el dispositivo ideal para garantizar la identificación precisa y segura en los procesos de emisión de la Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI). Este lector de huellas dactilares se distingue por su capacidad de capturar imágenes con alta fidelidad, su resistencia operativa y su compatibilidad con diversas plataformas tecnológicas.

El DigitalPersona 4500 destaca por sus características avanzadas:

- Escaneo óptico de alta precisión: Su tecnología óptica permite la captura de huellas con resolución de 500 dpi, asegurando un alto nivel de detalle y calidad en cada lectura.
- Fiabilidad en entornos exigentes: Equipado con una carcasa metálica robusta y un recubrimiento de silicona que mejora la adherencia de la huella, permite la identificación efectiva incluso con dedos húmedos, secos o rugosos.
- Seguridad criptográfica integrada: Implementa cifrado propietario de 32 bits con clave de rotación, protegiendo la integridad de los datos biométricos transmitidos.
- Interoperabilidad y escalabilidad: Compatible con múltiples sistemas operativos como Windows, Linux y Android, y optimizado para integrarse con los SDK de DigitalPersona.
- Facilidad de uso e implementación: Su interfaz USB 2.0 y su diseño compacto permiten una instalación sencilla y una experiencia de usuario intuitiva, ideal para entornos de alta demanda.

Desde el punto de vista normativo, el DigitalPersona 4500 cumple con certificaciones internacionales como FCC Class B, CE, ICES, BSMI, MIC, USB y WHQL, asegurando su idoneidad para sistemas de identidad gubernamentales. Su capacidad de rechazo de huellas falsas y latentes refuerza aún más la seguridad en el proceso de autenticación.

La implementación del DigitalPersona 4500 en la solución del Consorcio Identidad 4.0 RD representa un avance estratégico en la protección y validación de la identidad de los ciudadanos, alineado con los estándares internacionales de seguridad y eficiencia tecnológica.

5.4 IMPRESORA TÉRMICA STAR BSC10UD-24

En el marco de la optimización de los procesos de venta y servicio en entornos de retail y hospitalidad, la impresora térmica STAR BSC10UD-24 se posiciona como una solución esencial para la emisión rápida y fiable de tickets y recibos. Su diseño simple y robusto, junto con la innovadora tecnología de carga de papel sin mecanismos complicados, garantiza un rendimiento óptimo en condiciones de uso intensivo, reduciendo tiempos de inactividad y mejorando la experiencia del cliente.

CARACTERÍSTICAS TÉCNICAS Y BENEFICIOS

- Alta velocidad de impresión: Con una capacidad de hasta 250 mm/seg, la impresora permite la emisión de recibos de forma ultrarrápida, ideal para momentos de alta demanda.
- Resolución de 203 dpi: La tecnología de impresión térmica directa asegura textos y gráficos nítidos, fundamentales para una legibilidad impecable en ambientes comerciales.
- Interfaz dual (USB/RS232): Facilita su integración con diversos sistemas de punto de venta, garantizando compatibilidad con múltiples plataformas operativas.
- Diseño compacto y de fácil mantenimiento: Su innovador sistema de "drop-in & print" elimina la necesidad de mecanismos de carga complicados, reduciendo el tiempo de cambio de rollo y aumentando la fiabilidad operativa.
- Capacidad para rollos de 10 cm de diámetro: Esta característica permite utilizar hasta un 60% más papel en cada rollo, lo que se traduce en menores costos operativos y menos interrupciones por reposición.
- Compatibilidad con ESC/POS y suministro completo: Viene equipada con fuente de poder y es compatible con los estándares de emulación más utilizados en la industria, facilitando su implementación en infraestructuras digitales existentes.

VENTAJAS

• Incremento en la eficiencia operativa: La alta velocidad de impresión y la capacidad extendida del rollo reducen los tiempos de espera en el punto de venta.
• Reducción de costos: Menor frecuencia en el cambio de papel se traduce en ahorro en insumos y logística.
• Integración versátil: La interfaz dual y la compatibilidad con ESC/POS permiten una implementación sencilla en diferentes entornos tecnológicos.
• Fiabilidad y durabilidad: Su diseño robusto y fácil mantenimiento garantizan un funcionamiento constante incluso en condiciones de uso intensivo.
• Mejora en la experiencia del cliente: Un proceso de emisión de recibos ágil y sin contratiempos contribuye a una atención más fluida y satisfactoria.

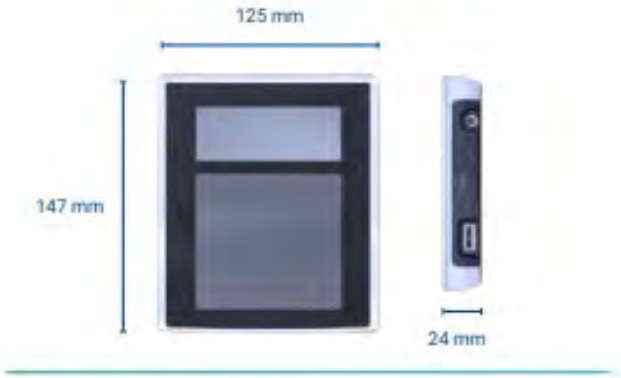
5.5 ESCÁNER DE HUELLAS DIGITALES LIVETOUCH QUATTRO

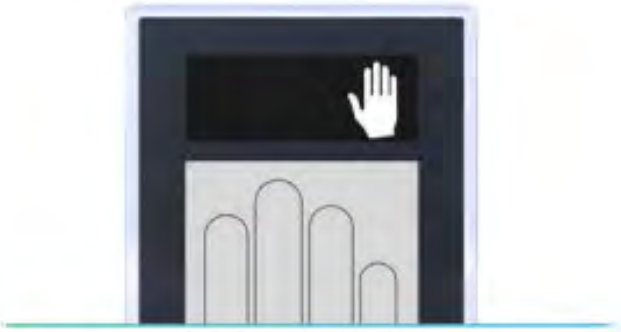
El LIVETOUCH QUATTRO responde a las exigencias de seguridad e interoperabilidad requeridas en los procesos de identificación nacional. Su integración dentro de los centros de emisión de documentos garantiza un registro biométrico confiable, alineado con estándares internacionales.

Su capacidad de captura rápida y su sistema de corrección visual reducen significativamente los tiempos de inscripción, permitiendo una experiencia más eficiente tanto para el personal de la JCE como para los ciudadanos.

CARACTERÍSTICAS TÉCNICAS Y BENEFICIOS

- Captura multifuncional de huellas: Permite la obtención de huellas planas, rodadas y el método 4-4-2, optimizando el registro de datos biométricos con alta precisión.
- Pantalla táctil interactiva: Incluye un sistema de guía visual que facilita el proceso de captura y minimiza errores de inscripción.
- Alta resolución de imagen: Sensor con 500 dpi, garantizando una calidad de imagen certificada por el FBI y BSI.
- Diseño compacto y portátil: Con dimensiones de 125 mm x 147 mm x 24 mm y un peso de solo 360 g, es ideal para integraciones en infraestructuras existentes.
- Conectividad avanzada: Compatible con USB 3.0 y 2.0, asegurando una transmisión de datos rápida y estable.
- Protección robusta y durabilidad: Recubrimiento de vidrio resistente a arañazos y certificación IP54, protegiendo contra polvo y salpicaduras.
- Captura de firmas digitales: Funcionalidad integrada que permite la recolección de firmas manuscritas sin necesidad de un dispositivo adicional.





5.6 CÁMARA CANON EOS REBEL T7

En el marco del fortalecimiento de los procesos de identificación, la captura de imágenes de alta calidad es un pilar fundamental para garantizar la precisión y confiabilidad en la documentación oficial. La Canon EOS Rebel T7 ha sido seleccionada como una solución tecnológica clave para la obtención de imágenes que

cumplan con los requerimientos técnicos de identificación, asegurando una captura fiel y detallada de cada ciudadano.

CARACTERÍSTICAS TÉCNICAS Y BENEFICIOS

- Calidad de imagen excepcional: Con un sensor CMOS de 24.1 MP, la cámara proporciona imágenes de alta resolución esenciales para la identificación digital y la verificación biométrica.
- Procesador de Imagen DIGIC 4+: Optimiza el rendimiento y garantiza una reproducción de color precisa, fundamental para la identificación oficial.
- Sistema de enfoque automático de 9 puntos: Facilita la captura de imágenes nítidas en condiciones de alta demanda, asegurando uniformidad y precisión.
- Pantalla LCD de 3.0 pulgadas: Permite visualizar y ajustar la toma en tiempo real, facilitando la operatividad en centros de emisión de documentos.
- Conectividad Wi-Fi y NFC: Permite la transferencia rápida de imágenes al sistema central de la JCE, agilizando los procesos administrativos.
- Compatibilidad con infraestructuras digitales: Integración eficiente con el sistema de captura y almacenamiento de datos de la JCE.

VENTAJAS

- Estandarización en la captura de imágenes para cédulas de identidad.
- Reducción de tiempos de procesamiento mediante transferencia inalámbrica.
- Alta fidelidad en la reproducción de detalles faciales, mejorando la autenticación visual.
- Facilidad de uso y configuración rápida, adaptándose a los entornos operativos de la JCE.
- Durabilidad y resistencia, garantizando un funcionamiento óptimo en condiciones de uso intensivo.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

5.7 CONDICIONES DE SUMINISTRO Y AJUSTE DE PRECIOS

El Consorcio Cédula 4.0 RD se compromete a suministrar los periféricos detallados en esta sección en un período de treinta (30) días calendario después de la solicitud formal de la Junta Central Electoral (JCE).

Los precios de los equipos podrán ajustarse anualmente conforme a la inflación, asegurando que las condiciones económicas reflejen las variaciones del mercado.

Además, la JCE tendrá la facultad de decidir la compra o no de estos equipos, de acuerdo con sus requerimientos operativos y disponibilidad presupuestaria.

ÍTEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

6 PLAN DE MANTENIMIENTO PARA IMPRESORAS Y PERIFERICOS

SERVICIO TÉCNICO

- Localidades: Las localidades incluyen la Republica Dominicana, EEUU y España.

- Infraestructura de Soporte: La infraestructura de Soporte consta de al menos:

- República Dominicana:

- Técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Hasta 15 técnicos locales del C4RD disponibles de forma presencial
- Cuatro (4) Regionales existentes en la actualidad desde donde se habilitará el servicio de manera estratégica. Allí, en la localidad, C4RD dispondrá de su estructura de soporte actual incluyendo la inclusión de personal técnico propio del fabricante cuando fuese necesario como la infraestructura de recursos en la localidad, transporte, taller y/o almacenes de repuestos debidamente equipados con las herramientas de trabajo, etc

- EEUU:

- 4 técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Hasta 70 técnicos locales del C4RD disponibles de forma presencial
- Regional existente en la actualidad desde donde se habilitará el servicio de manera estratégica, siendo Nueva York el punto de atención focal. Allí C4RD dispondrá de su estructura de soporte actual incluyendo, personal técnico propio del fabricante como la infraestructura de recursos en la localidad, transporte, taller y/o almacén de repuestos debidamente equipados con las herramientas de trabajo, etc.

- España:

- 4 técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Se contara con al menos 1 técnico local del C4RD disponibles de forma presencial
- Una (1) Region actualmente existente desde donde se habilitará el servicio de manera estratégica, incluyendo Madrid. Allí C4RD dispondrá de su estructura de soporte actual incluyendo, personal técnico propio del fabricante como la infraestructura de recursos en la localidad, transporte, taller y/o almacén de repuestos debidamente equipados con las herramientas de trabajo, etc

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

- Tiempos de Respuesta:

- Ocho (8) horas de tiempo de respuesta en localidades lejanas; desplazamientos mayores a 2 hrs.
- Cuatro (4) horas en localidades cercanas a los centros de servicios de C4RD; desplazamientos menores a 2 horas.

- Contingencia:

- Cada localidad regional de servicios de C4RD contara con al menos un equipo funcional disponible y referido de este lote para sustitución inmediato además de Trick de partes y piezas para reparación.
- Todos los recursos técnicos tienen disponibles medios de comunicación con alcance mundial disponibles, entre sí, con fuentes de información centralizada para consulta técnica; algunas de estas comprenden WhatsApp, llamadas locales y/o llamadas internacionales, etc
- Las fuentes de soporte de asistencia técnica del fabricante, a nivel mundial, están disponibles con respecto al horario laborable del hemisferio occidental, cubriendo entre 8 - 19 hrs diarias entre Domingo y viernes, aprovechando el centro de soporte de Dubái en el medio oriente y el de Bogotá en América Latina.
- 8-9 hrs en ventaja con el horario de apertura de labores con NY, Santo Domingo durante el año.
- 1-2 hrs con el horario de cierre de labores con NY, Santo Domingo durante el año.

- Registro del Incidentes:

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.
- Incluir la siguiente información:
- Nombre de la entidad reportante (JCE.RD, JCE.EEUU o JCE.UE).
- Fecha y hora del incidente.
- Identificar como Impresora o Periférico
- Serie del equipo
- Descripción detallada del problema.
- Componentes afectados
- Nivel de urgencia del incidente

- Protocolos de Escalamiento y Gestión de Incidentes:

- Definición de niveles de escalamiento con tiempos de respuesta específicos según la criticidad del incidente.
- Disponibilidad de un equipo de soporte de segundo y tercer nivel para atender problemas complejos de hardware y software.

6.1 PLAN DE MANTENIMIENTO PARA PKI

6.1.1 INTRODUCCIÓN

Este documento establece los lineamientos para garantizar la continuidad y estabilidad de la infraestructura PKI-CA suministrada por el consorcio C4RD a la Junta Central Electoral (JCE). La infraestructura PKI es un pilar fundamental para la seguridad digital y la confianza en las transacciones electrónicas, permitiendo la autenticación, el cifrado y la firma digital de documentos.

Garantizar un plan de soporte técnico robusto es esencial para mantener la disponibilidad y la integridad de la plataforma. La implementación de GET Trust, junto con las mejores prácticas de mantenimiento y monitoreo, permite el cumplimiento de normativas internacionales y la continuidad operativa del sistema.

6.1.2 ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA DEL PKI – CA

La JCE depende de la gestión técnica de C4RD para administrar la infraestructura PKI-CA, que abarca la generación y revocación de certificados, el monitoreo de riesgos y el cumplimiento de estándares globales. A través de este esquema, a la JCE se le garantiza la seguridad de sus procesos digitales, mientras que C4RD implementa además medidas para prevenir fallos y responder ante cualquier incidente.

Este programa de soporte y mantenimiento cubre los siguientes aspectos clave:

- Infraestructura PKI-CA: responsable de la gestión de claves, la generación y revocación de certificados, así como la administración de la Autoridad de Certificación (CA).
- Monitoreo y gestión de incidentes: Se implementan herramientas de auditoría y supervisión que permiten a la JCE detectar y reportar riesgos en tiempo real, mientras que C4RD ejecuta las acciones correctivas necesarias.
- Seguridad y cumplimiento: C4RD garantiza la adhesión a los estándares internacionales, como EAL4+, eIDAS y FIPS 140-2, asegurando la protección de la información manejada por la JCE.

El mantenimiento efectivo de la infraestructura PKI-CA es clave para preservar la autenticidad de los procesos digitales. Su robustez depende de una gestión eficiente del ciclo de vida y de la respuesta oportuna ante cualquier incidencia.

6.1.3 MODELOS DE SERVICIO Y SLA

Para garantizar tiempos de respuesta óptimos, la JCE contara con un esquema de soporte técnico proporcionado por C4RD en tres niveles: desde la resolución de consultas básicas hasta la intervención especializada. Los acuerdos de nivel de servicio (SLA) permitirán a la JCE operar sin interrupciones, asegurando que los incidentes sean atendidos según su nivel de criticidad.

Para garantizar la eficiencia y disponibilidad del sistema, C4RD ha definido tres niveles de soporte:

- Nivel 1 (L1): Atención inicial y resolución de consultas básicas.

- Nivel 2 (L2): Gestión de incidencias técnicas y soporte especializado.
- Nivel 3 (L3): Intervención de ingeniería avanzada y escalamiento a proveedores.

6.1.4 SLA Y TIEMPOS DE RESPUESTA

Los tiempos de atención se han definido para minimizar el impacto de las incidencias, en horario 7:00AM a 6:00PM de lunes a viernes y los sábados de 8:00 a 1:00 PM

- Incidentes críticos (P1): Respuesta en menos de 2 horas.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
- Incidentes mayores (P2): Respuesta en menos de 6 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
  -
- Incidentes mayores (P3): Respuesta en menos de 8 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
  -
- Incidentes menores (P4): Respuesta en menos de 1 día.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.

Estos niveles de servicio garantizan la operatividad de la infraestructura y evitan interrupciones en la emisión y validación de certificados digitales.

6.1.5 PROCEDIMIENTO PARA LA APERTURA DE INCIDENTES POR PARTE DE LA JCE

El protocolo de soporte a la JCE requiere el seguir un protocolo estructurado para reportar incidentes a C4RD, incluyendo la clasificación por nivel de urgencia y el envío de información detallada para un diagnóstico preciso. C4RD, a su vez, evalúa cada caso y asigna recursos especializados para su resolución, garantizando una comunicación fluida con la JCE hasta la solución del problema.

Este modelo de soporte robusto gestionado por C4RD, con más de 15 años de experiencia en procesos críticos de negocios del sector privado y público probado ante exigencias de trafico de alta demanda del sector financiero nacional y de servicios públicos opera 24/7 para atenderá cualquier incidencia que afecte la infraestructura PKI-CA.

Este capítulo describe la metodología de categorización y escalamiento de problemas, asegurando que la JCE cuente con un servicio confiable y eficiente en la resolución de inconvenientes técnicos. La metodología implementada por C4RD se basa en un enfoque estructurado de gestión de incidentes, que incluye la identificación, registro, clasificación por niveles de criticidad (P1 a P4), diagnóstico inicial, asignación de recursos especializados, resolución y documentación del incidente.

Además, están establecidos procedimientos de escalamiento para garantizar que, en caso de problemas complejos, los niveles de soporte superiores intervengan de manera oportuna, minimizando el impacto en las operaciones de la JCE.

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

6.2 CUADRO DE ESCLAMEINTO INCLUYENDO

Matriz de Escalamiento Mesa de Servicios - TIC							
Niveles	Soporte	Tiempo de Respuesta	Puesto	Nombres	Contacto	Móvil	Correo
1	L1	De 1 a 30 Minutos	Técnico Especialista 1 - CSI	Mesa de Servicio CSI	809-567-0022 Ext. 282	Técnico de Turno	ServiciosTIC@grupocsi.com.do
2		30 Minutos a 60 Minutos	Técnico Especialista 2 - CSI	Mesa de Servicio CSI	809-567-0022 Ext. 262	(849) 886 2012	jli.infante@grupcsi.com.do
3		60 Minutos (1 Horas) a 120 Minutos (2 Horas)	Gerente de Servicios TIC - CSI	Federico Norberto	809-567-0022 Ext. 281	(809) 443 1502	f.norberto@grupocsi.com.do
4		2 a 3 Horas	VP Comercial - CSI	Ruben Cordero	809-567-0022 Ext. 239	(809) 603 8696	r.cordero@grupocsi.com.do
5		3 a 4 Horas	Presidente - CSI	Manuel Infante	809-567-0022 Ext.222	(809) 430-7242	jm.infante@grupocsi.com.do
6	L2	4 Horas o Mas	Mesa de Servicios GetGroup				soportelatam@getlatamprojects.com

Cuando la JCE identifique un problema en la infraestructura PKI-CA, deberá seguir el siguiente procedimiento para reportarlo a C4RD:

1. Registro del Incidente

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.
- Incluir la siguiente información:

    - Nombre de la entidad reportante (JCE).
    - Fecha y hora del incidente.
    - Descripción detallada del problema.
    - Componentes afectados dentro de la infraestructura PKI-CA.
    - Capturas de pantalla o logs relevantes.
    - Nivel de urgencia del incidente.

2. Clasificación del Incidente

    - Máxima (P1): El servicio de PKI-CA está completamente inoperativo.
    - Alta (P2): Falla parcial que afecta la operación de la JCE.
    - Media (P3): Problemas que afectan el rendimiento sin impacto inmediato.
    - Baja (P4): Incidentes menores atendidos en la siguiente ventana de mantenimiento.

3. Evaluación y Diagnóstico Inicial

    - C4RD realizará un análisis preliminar y solicitará información adicional si es necesario.

4. Resolución y Seguimiento

    - C4RD asignará un técnico según la criticidad del incidente.
    - Se mantendrá una comunicación constante con la JCE hasta la resolución.
    - Se emitirá un informe con causas y medidas correctivas.

6.3 MANTENIMIENTO PREVENTIVO Y CORRECTIVO

La continuidad operativa de la infraestructura PKI-CA de la JCE está respaldada por un plan de mantenimiento estructurado por C4RD. Las tareas preventivas incluyen auditorías de seguridad, actualizaciones de software y revisión de certificados, mientras que el mantenimiento correctivo aborda fallos imprevistos para minimizar el impacto en los servicios digitales de la JCE.

El mantenimiento preventivo, ejecutado por C4RD, incluye:

- Renovación y revocación programada de certificados.
- Verificación de integridad del HSM.
- Simulacros de incidentes y evaluaciones de rendimiento.
- Revisión de certificados y actualización de software.
- Pruebas de penetración y seguridad.

El mantenimiento correctivo responde a fallas imprevistas mediante:

- Atención inmediata de fallos críticos.
- Sustitución de hardware según acuerdos con proveedores.
- Monitoreo de la integridad de certificados emitidos y revocados.

6.4 SEGURIDAD Y CUMPLIMIENTO

Con la JCE, C4RD trabajaremos en conjunto para mantener la infraestructura PKI-CA alineada con estándares internacionales de seguridad, protegiendo la integridad de los datos y la identidad digital. C4RD implementara auditorías periódicas y monitoreo constante para detectar posibles vulnerabilidades, asegurando que la misma cumpla con los requisitos regulatorios en la gestión de certificados digitales.

Para garantizar la seguridad de la infraestructura PKI-CA, C4RD implementa:

- Auditorías internas propias y externas via terceros.
- Monitoreo continuo para prevenir accesos no autorizados.
- Políticas de control de acceso basado en roles.
- Procedimientos de respuesta a incidentes de seguridad.

6.5 KPIS Y MÉTRICAS DE RENDIMIENTO

Para evaluar la efectividad del soporte técnico, la JCE y C4RD dejaran definidos indicadores claves de rendimiento (KPIs) como la disponibilidad del sistema, el tiempo de respuesta ante incidentes y la satisfacción del cliente. El monitoreo constante de estos parámetros permite optimizar los procesos y garantizar la fiabilidad de la infraestructura PKI-CA.

Se emitirán informes mensuales de rendimiento del mes anterior y se ejecutarán conferencias recurrentes de análisis de estos.

Para evaluar la efectividad del soporte, se establecen los siguientes indicadores:

- Disponibilidad del sistema: >99.9%.
- Cumplimiento del SLA: >95% de los incidentes resueltos dentro del tiempo.
- Tiempo promedio de resolución: Optimización de respuestas según la criticidad.
- Satisfacción del cliente: Evaluaciones continuas para mejora del servicio.

Este programa garantizara la estabilidad, seguridad y disponibilidad de la infraestructura PKI-CA, reforzando la confianza de la ciudadanía en los servicios de la JCE

6.6 PLAN DE MANTENIMIENTO PARA TARJETA DIGITAL

6.6.1 INTRODUCCIÓN

El presente documento define el Programa de Soporte y Mantenimiento para la plataforma de Cédula de Identidad Digital basada en GET Mobile ID, instalada e implementada por GET Group para la JCE. Dado que esta plataforma es crítica para la gestión de identidad nacional, se establece un esquema de soporte robusto y alineado con las mejores prácticas de la industria, garantizando alta disponibilidad (99.95%), seguridad avanzada y continuidad operativa.

Este programa contempla modelos de servicio y SLA, mantenimiento preventivo y correctivo, cumplimiento con regulaciones de seguridad, y métricas de rendimiento que permitan monitorear y optimizar el funcionamiento de la plataforma.

6.6.2 ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA

El soporte y mantenimiento de la plataforma GET Mobile ID abarca las siguientes áreas clave:

- Infraestructura Tecnológica: Servidores, almacenamiento, red y elementos de seguridad como NG Firewalls y WAF.
- Software y Aplicaciones: Mantenimiento de GET Mobile Administrator, GET Mobile ID y GET Mobile Verify.
- Base de Datos y Firmado Digital: Gestión del ciclo de vida de los certificados digitales, claves de firma y bases de datos vinculadas al sistema de identidad digital.
- Monitoreo y Respuesta a Incidentes: Supervisión proactiva de los servicios para garantizar alta disponibilidad.
- Gestiones con la Junta Central Electoral (JCE): Coordinación para integraciones, actualizaciones y cambios en los procedimientos de identidad digital.

El servicio está diseñado para operar en un modelo 24/7 con distintos niveles de soporte técnico, asegurando la resolución eficiente de incidentes y la actualización continua de la plataforma.

6.6.3 MODELOS DE SERVICIO Y SLA

El servicio de soporte se estructura en distintos niveles, con acuerdos de nivel de servicio (SLA) bien definidos para cada categoría de incidencia en horario 7:00AM a 6:00PM de lunes a viernes y los sábados de 8:00 AM a 1:00 PM:

- Nivel 1 (Soporte Básico y Atención al Cliente): Resolución de consultas, asistencia básica y gestión de usuarios.

- Nivel 2 (Soporte Técnico Especializado): Diagnóstico avanzado de problemas, configuraciones de software y ajustes de red.
- Nivel 3 (Soporte de Infraestructura y Seguridad): Resolución de incidentes críticos, recuperación ante desastres y gestión avanzada de seguridad.

6.6.4 ACUERDOS DE NIVEL DE SERVICIO (SLA):

- 4. Acuerdos de Nivel de Servicio (SLA):
- Incidentes críticos (P1): Respuesta en menos de 2 horas.
    - El procedimiento de registro de incidentes incluirá:
    - ▪ Recepción y Registro del incidente.
    - ▪ Análisis y clasificación del incidente.
    - ▪ Investigación y Diagnostico.
    - ▪ Resolución del incidente.
    - ▪ Verificación y cierre.
- Incidentes mayores (P2): Respuesta en menos de 6 hora.
    - El procedimiento de registro de incidentes incluirá:
    - ▪ Recepción y Registro del incidente.
    - ▪ Análisis y clasificación del incidente.
    - ▪ Investigación y Diagnostico.
    - ▪ Resolución del incidente.
    - ▪ Verificación y cierre.
- Incidentes mayores (P3): Respuesta en menos de 8 hora.
    - El procedimiento de registro de incidentes incluirá:
    - ▪ Recepción y Registro del incidente.
    - ▪ Análisis y clasificación del incidente.
    - ▪ Investigación y Diagnostico.
    - ▪ Resolución del incidente.
    - ▪ Verificación y cierre.

  Incidentes menores (P4): Respuesta en menos de 1 día.
    - El procedimiento de registro de incidentes incluirá:
    - ▪ Recepción y Registro del incidente.
    - ▪ Análisis y clasificación del incidente.
    - ▪ Investigación y Diagnostico.
    - ▪ Resolución del incidente.
    - ▪ Verificación y cierre.

Cuando la JCE identifique un problema en el servicio de la infraestructura Cedula Digital, deberá seguir el siguiente procedimiento para reportarlo a C4RD:

REGISTRO DEL INCIDENTE

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.

- Incluir la siguiente información:
  - Nombre de la entidad reportante (JCE).
  - Fecha y hora del incidente.
  - Descripción detallada del problema.
  - Componentes y/o servicio afectado dentro de la infraestructura Cedula Digital.
  - Capturas de pantalla o logs relevantes.
  - Nivel de urgencia del incidente.

6.6.5 CLASIFICACIÓN DEL INCIDENTE

- Máxima (P1): El servicio de Cedula Digital está completamente inoperativo.
- Alta (P2): Falla parcial que afecta los servicios o la operación de la JCE.
- Media (P3): Problemas que afectan el rendimiento sin impacto inmediato.
- Baja (P4): Incidentes menores atendidos en la siguiente ventana de mantenimiento.

5. Evaluación y Diagnóstico Inicial
   - C4RD realizará un análisis preliminar y solicitará información adicional si es necesario.
6. Resolución y Seguimiento

- C4RD asignará un técnico según la criticidad del incidente.
- Se mantendrá una comunicación constante con la JCE hasta la resolución.
- Se emitirá un informe con causas y medidas correctivas.

6.7 MANTENIMIENTO PREVENTIVO Y CORRECTIVO

Para garantizar el funcionamiento óptimo de la plataforma, se establecen los siguientes tipos de mantenimiento:

6.7.1 ACTIVIDADES PERIÓDICAS

- Revisión de certificados: Verificar la validez y vigencia de los certificados emitidos, incluyendo los certificados de la Autoridad de Certificación (CA) raíz y subordinada.
- Actualización de software y firmware: Mantener actualizados los sistemas y aplicaciones que utilizan la solución de emisión de credenciales digitales.
- Revisión de políticas de seguridad: Verificar que las políticas de seguridad estén actualizadas y sean efectivas para proteger la solución de emisión de credenciales digitales.

- Realización de copias de seguridad: Realizar copias de seguridad regulares de la solución de emisión de credenciales digitales, incluyendo los certificados, las claves privadas y los registros de transacciones.
- Pruebas de penetración y vulnerabilidades: Realizar pruebas de penetración y vulnerabilidades periódicas para identificar y corregir cualquier debilidad en la solución de emisión de credenciales digitales.

6.7.2 ACTIVIDADES DE MANTENIMIENTO PREVENTIVO

- Revisión de los registros de transacciones: Verificar los registros de transacciones para detectar cualquier actividad sospechosa o irregular.
- Monitoreo de la integridad de los certificados: Verificar la integridad de los certificados emitidos y revocados.
- Actualización de la lista de revocación de certificados (CRL): Actualizar la lista de revocación de certificados (CRL) para reflejar los certificados revocados.
- Revisión de la configuración de la solución de emisión de credenciales digitales: Verificar la configuración de la solución de emisión de credenciales digitales para asegurarse de que esté configurada correctamente y sea segura.

6.7.3 ACTIVIDADES DE RESPUESTA A INCIDENTES

Procedimientos de respuesta a incidentes: Están establecidos procedimientos de respuesta a incidentes para manejar cualquier incidente de seguridad que afecte la solución de emisión de credenciales digitales.

- Notificación de incidentes: Notificar a las partes interesadas relevantes en caso de un incidente de seguridad.
- Análisis de incidentes: Realizar un análisis detallado de cualquier incidente de seguridad para identificar la causa raíz y tomar medidas correctivas.
- Recuperación de la solución de emisión de credenciales digitales: Recuperar la solución de emisión de credenciales digitales después de un incidente de seguridad, incluyendo la restauración de los certificados y las claves privadas.

6.7.4 MANTENIMIENTO CORRECTIVO

- Solución de Errores Críticos: Reparación inmediata ante caídas del sistema.
- Reemplazo de Componentes: Sustitución de módulos afectados por fallos.
- Corrección de Brechas de Seguridad: Ajustes urgentes en respuesta a ataques o vulnerabilidades detectadas.

6.8 SEGURIDAD Y CUMPLIMIENTO

Dado que GET Mobile ID maneja información altamente sensible, el programa de mantenimiento prioriza la seguridad mediante:

- Cifrado y Protección de Datos: Uso de criptografía RSA y curvas elípticas.
- Autenticación Multifactor (MFA): Para el acceso administrativo y operación segura se implementarán mecanismos de autenticación y autorización seguros para garantizar que solo los usuarios autorizados puedan acceder a la solución de emisión de credenciales digitales.
- Firewall de Nueva Generación (NGFW) y WAF: Control avanzado contra ataques cibernéticos.
- Cumplimiento Normativo: Asegurar que la solución de emisión de credenciales digitales cumpla con los requisitos de seguridad establecidos en la norma ISO 18013-5, ISO 27001 y regulaciones nacionales de protección de datos.
- Monitoreo de Amenazas: Detección temprana de intrusiones y análisis de comportamiento.
- Gestión de claves: Implementación de una gestión de claves segura y eficiente para proteger las claves privadas y los certificados.
- Registros de auditoría: Mantener registros de auditoría detallados y precisos para permitir la trazabilidad y la responsabilidad de las acciones realizadas en la solución de emisión de credenciales digitales.

6.9 KPIS Y MÉTRICAS DE RENDIMIENTO

Para evaluar la eficiencia del soporte y mantenimiento, se definen indicadores clave:

- Disponibilidad del Sistema: Tiempo efectivo de operación (meta: 99.95%).
- Tiempo Medio de Resolución (MTTR): Promedio de tiempo para resolver incidentes.
- Tiempo Medio entre Fallas (MTBF): Periodo promedio entre fallas críticas.
- Tasa de Resolución en Primera Llamada (FCR): % de incidencias resueltas sin escalamiento.
- Cumplimiento de SLA: % de incidentes resueltos dentro de los tiempos acordados.
- Incidentes de Seguridad: Número de alertas de seguridad atendidas y resueltas.
- Uso de Recursos: Análisis de carga en servidores y almacenamiento.

Estos KPIs se revisarán periódicamente, cada trimestre, para identificar oportunidades de mejora y garantizar que la plataforma opere de manera segura y eficiente.

6.10 INVENTARIO

Para garantizar la continuidad operativa y evitar interrupciones en la personalización de documentos de identidad, el Consorcio Identidad 4.0 RD mantendrá un stock de inventario equivalente a un mínimo del 3% Este inventario permitirá una respuesta inmediata en caso de fallas técnicas o necesidades de reposición, asegurando el cumplimiento ininterrumpido del servicio.

ÍTEM VII - CAPACITACIÓN

7. PLAN DE CAPACITACIÓN PARA IMPRESORAS

7.1 ENTRENAMIENTOS

El consorcio Cedula 4.0 RD ha diseñado un plan de entrenamiento sin costo que inicia durante la fase de implementación con un entrenamiento general de todas las funciones de la solución de impresión y acompañamiento directo del fabricante durante el proceso. El entrenamiento será divido en 2 fases un entrenamiento básico de operación para el personal que replicará esta capacitación en los centros de atención que incluye:

- Guía básica de operación de la solución
- mantenimiento preventivo
- validación de calidad de impresión
- resolución de incidencias básicas

Adicional a esto se entregará una guía de referencia rápida para uso básico de la solución y un video interactivo con material que apoya y guía al usuario en como operar la solución esta guía se recomienda que sea realizado en conjunto con la JCE con la solución final aprobada.

De igual forma se realizará un *entrenamiento* más especializado para el *personal técnico de la JCE a* fin de asegurar su conocimiento sobre las *características* técnicas de los equipos, *configuraciones*, y demás aspectos técnicos y operativos de la solución instalada. Dicho entrenamiento será realizado en las mismas instalaciones de la JCE por el personal directo del fabricante del hardware.

7.2 TÓPICOS DE ENTRENAMIENTO:

PREPARACIÓN DEL EQUIPO Y CONFIGURACIÓN INICIAL

Instalación del software: Asegúrate de tener instalado el software adecuado para el modelo de impresora láser. Verifica que los controladores sean los más recientes.

Calibración de la impresora: calibración inicial para asegurarse de que el láser y los componentes mecánicos estén correctamente alineados.

Configuración de la calidad de impresión: Ajusta los parámetros de resolución, velocidad de impresión, y otros aspectos técnicos a las necesidades del proyecto.

PREPARACIÓN DE LAS TARJETAS DE POLICARBONATO

Selección de tarjetas: Asegúrate de que las tarjetas sean del tamaño adecuado y estén libres de imperfecciones. Las tarjetas de policarbonato deben estar diseñadas específicamente para ser impresas con láser.

Limpieza: Es importante limpiar las tarjetas de cualquier polvo o suciedad para evitar manchas o fallas de impresión.

7.4 ENTRENAMIENTO DE LA IMPRESORA (PRUEBAS DE IMPRESIÓN)

Prueba inicial de impresión: Imprime una tarjeta de prueba para evaluar la calidad de la impresión. Revisa la nitidez de las imágenes y la correcta alineación del diseño.

Ajustes: Si los resultados no son satisfactorios, ajusta la configuración si las condiciones del área de impresión esta fuera del requerimiento mínimo de operación.

7.5 ALIMENTACIÓN DE PLATICOS DE POLICARBONATO

Las tarjetas de policarbonato CIE / CI

7.6 VERIFICACIÓN DE LA CALIDAD DE LA IMPRESIÓN

Inspección visual: Verifica la precisión del color, la nitidez del texto y los gráficos, y la consistencia de la impresión.

7.4 MANTENIMIENTO REGULAR

Limpieza del equipo: Mantén el equipo limpio, especialmente los mecanismos láser y de alimentación de tarjetas, para evitar fallos durante la impresión.

Rutina de mantenimiento preventivo para operadores

Rutina de mantenimiento personal técnico JCE.

7.4 RESOLUCIÓN DE INCIDENCIAS

Se realizará un entrenamiento practico con el personal técnico que incluye un manual de servicio para resolución de problemas para fines de consulta.

7.10 CANALES DE ATENCIÓN.

- Página web para registro de incidencias: https://www.grupocsi.com.do/soporte-tecnico-hardware/
- Centro de atención para recepción de reportes telefónicos con horario: lunes a jueves de 7:00 am a 6:00 pm viernes de 8:00 am a 5:00 pm sábado de 8:00 am a 1:00 pm.

7.11PLAN DE CAPACITACION PARA PKI

7.11.1 CONTENIDO

Los cursos que se describen a continuación ofrecidos y organizados por nuestros formadores para la solución de PKI, GET Trust.

- PKI Basics: formación sobre conceptos básicos de PKI e introducción
- CMS: formación sobre el Sistema de Gestión de Credenciales (CMS): En conjunto con ID PKI
- ID PKI: formación sobre software de ID PKI, incluyendo ID CA
- ID CA: formación sobre software de ID CA
- Instalación de ID PKI: formación sobre instalación de software de ID PKI, incluyendo instalación de ID CA
- Instalación de ID CA: formación sobre instalación de software de ID CA
- ID RA para Operadores: Introducción a PKI + uso de ID RA y EE para operadores. Gestión del ciclo de vida de los certificados
- BAC: formación sobre el módulo BAC
- Firmado electrónico: formación sobre el software de firma electrónica IDnomic Sign

Además de estas formaciones estándar, se puede establecer un programa específico con el cliente para cubrir necesidades específicas, como una formación en profundidad para un grupo especifico de usuarios.

7.11.2 METODOLOGÍA

Nuestros formadores son profesionales de la formación, especializados en nuestro campo de especialización. Ponemos énfasis en los intercambios interactivos y el desarrollo de habilidades a través de la implementación operativa de nuestras soluciones. Como tal, cada sesión incluye conferencias, sesiones de preguntas y respuestas y trabajos prácticos para poner en práctica los conceptos presentados.

7.11.3 DESCRIPCIÓN

Referencia	PKI Basics
Objetivo	• Descubra los certificados y su ciclo de vida • Comprenda las tecnologías y las normas criptográficas • Comprenda la organización de PKI
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Este curso de capacitación proporciona los conocimientos mínimos necesarios para comprender completamente los demás módulos de capacitación impartidos.
Prerequisitos	Formación universitaria básica o ingeniero informático o equivalente mediante experiencia.
Plan	- Fundamentos de criptografía - Implementación de la criptografía

	- Introducción a los conceptos de PKI - PKI y organización - La estructura de la PKI - Jerarquía de autoridad - Autoridad de certificación - Marco legal y regulatorio
Duración	4 horas

Referencia	Sistema de Gestión de Credenciales (CMS)
Objetivo	- Comprender los certificados y las tarjetas inteligentes. - Cómo utilizar tarjetas inteligentes en una infraestructura de gestión de certificados. - Implementar el CMS y sus módulos - Configurar y administrar el CMS - Comprender los componentes clave para utilizar el CMS con todos los demás componentes de PKI.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de CMS o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - - Curso TRN.BASICS
Plan	Día 1: - Introducción al CMS y sus componentes - Instalación e inicialización del software CMS - 1ª conexión en modo "Bootstrap" - Inicialización de la configuración - Inicialización de la seguridad (firma de certificados internos de módulos) - Configuración - Protección de datos, claves de almacenamiento (creación e implementación) - Conexión a directorios, creación de fuentes de datos, definición de perfiles de autenticación, aplicaciones (autenticación, firma de correo electrónico y cifrado) - Medios: políticas de PIN, personalización gráfica, fabricantes, gestión de secretos, creación de perfiles para tokens de entrenamiento - Tarjetas inteligentes: arquitectura y concepto, gestión de secretos - Creación de perfiles para tokens de entrenamiento - Presentación del cliente CMS - Generación de archivos XPI - Instalación del cliente CMS - Configuración del navegador para tokens

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

	- Creación de un perfil de gestión de tarjetas "SelfEnroll" para administradores, gestión de números de serie de confianza - Definición y uso de procesos / flujos de trabajo: - Solicitud de certificado de administrador designado - Control de acceso (zonas, grupos, gestión de derechos de zona y módulo) - Inicio de sesión con certificado de administrador designado - Preparar un Configuración de usuario final - Creación de perfil de Badge Office - Fuente de datos interna, creación y aprovisionamiento Día 2: - Creación de un perfil de gestión de tarjetas - Emisión por lotes, envío de correo - Creación de perfil, adición de derechos, creación de tokens, revocación, desbloqueo, seguimiento, desbloqueo de medios sin conexión... - Copia de seguridad/restauración - Administración funcional de CMS, gestión de registros
Duración	14 horas (2 días)

Referencia	Instalación
Objetivo	- Instalar manualmente el software de ID CA. - Conocer los componentes que conforman el producto, las arquitecturas típicas a implementar y las diferentes etapas de una instalación. - Identificar los prerrequisitos para la instalación. - Poner en marcha la solución y acceder a las interfaces de administración.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de CMS o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Introducción a ID PKI y sus componentes técnicos - Arquitectura técnica de la solución - Requisitos previos - Instalación de ID CA - Ejercicios prácticos: - Verificar los requisitos previos - Instalar ID CA - Verificar la instalación correcta - Iniciar servicios y arrancar PKI - Analizar
Duración	7 horas

Referencia	HSM Proteccio Training
Objetivo	- Presentación, preparación e integración de Proteccio HSM en el contexto de un proyecto PKI - Introducción a una ceremonia de entrega de llaves
Audiencia	Cualquier persona involucrada en la implementación de una solución PKI, incluido un HSM de Proteccio (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes), especialmente futuros administradores de PKI o gerentes de soluciones PKI involucrados en la Ceremonia de entrega de claves.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Descripción general de Proteccio HSM, arquitectura de hardware y funciones; - Presentación de los diferentes roles y funciones disponibles para cada uno; - Instalación de equipos y creación de tarjetas maestras SO y maestras de auditoría; - Configuración de red y TLS; - Administración local de equipos; - Instalación de la herramienta de administración en una estación de trabajo Windows y en una estación de trabajo Linux - Actualizaciones de software; - Creación de decks de instalación Shamir; - Creación, configuración y personalización de HSM virtuales; - Gestión de objetos de HSM virtuales; - Gestión de HSM virtuales; - Migraciones de tarjetas inteligentes; - Implementación del modo de balanceo de carga; - Guía de resolución de problemas, mantenimiento de rutina de Proteccio HSM; - Preguntas varias. - Ceremonia de llave con Keyseed - Objetivos de un KC - Procedimiento de KC - Procedimientos y herramientas - • Cierre de un KC
Duración	7 horas

Referencia	BAC Training
Objetivo	- Entender el pasaporte electrónico - Conocer los procesos de solicitud de certificados y su ciclo de vida. - Cómo utilizar tecnologías y estándares criptográficos - Cómo implementar/operar la solución BAC

Audiencia	Cualquier persona involucrada en la implementación técnica de una solución PKI para pasaportes incluyendo el componente BAC (Gerentes de Seguridad, CISOs, Gerentes de Proyecto, Arquitectos, Administradores de Sistemas y Redes), y más particularmente futuros administradores de PKI o referentes de soluciones PKI.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	Día 1: - Introducción a la criptografía y PKI - Historia y evolución del pasaporte - Descripción del pasaporte electrónico - Presentación del producto BAC - Descripción general del producto CSCA - Configuración de CSCA - Ejercicios prácticos: - Creación de particiones - Creación de almacén de claves - Creación de CA - Gestión de CA de confianza - Creación y gestión de perfiles de certificados - Gestión de CRL - Renovación de CSCA - Día 2: - Configuración del producto DS - Ejercicios prácticos: - Creación de un área de clientes - Creación de administradores DS - Declaración de usuario de cliente DS - Gestión de claves - Creación de DS - Firma de certificados por DS - o Gestión de estadísticas
Duración	14 horas (2 días)

Referencia	Firmado Digital
Objetivo	- Entender las firmas electrónicas - Conocer el proceso de verificación de firmas mediante certificados - Conocer los diferentes tipos de firma electrónica - Cómo utilizar tecnologías y estándares criptográficos - • Implementar y operar la solución.
Audiencia	Cualquier persona involucrada en la implementación técnica de una solución PKI para pasaportes incluyendo el componente BAC (Gerentes de Seguridad, CISOs, Gerentes de Proyecto, Arquitectos, Administradores de Sistemas y Redes), y más

	particularmente futuros administradores de PKI o referentes de soluciones (integradores) PKI.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Descripción general del producto - Configuración - Ejercicios prácticos: - Parte de configuración - Conexión de HSM - Creación de clave maestra - Conexión a PKI - Configuración de CA de confianza - Configuración de importación y exportación - Configuración de la sección de gestión - Creación de usuarios - Creación de políticas de firma - Creación de claves y perfiles de firma - Configuración de firmas - Creación de visuales - Configuración de preferencias de firma - Gestión de auditorías
Duración	7 horas

7.12 PLAN DE CAPACITACION PARA TARJETA DIGITAL

7.12.1 CONTENIDO

Los cursos que se describen a continuación ofrecidos y organizados por nuestros formadores para la solución de tarjeta digital, GET mID.

- ISO 18013-5 Basics: formación sobre conceptos básicos de ISO 18013-5
- Formación de emisión de credenciales digitales ISO 18013-5.
- Instalación y Configuración de GET Mobile Administrator.
- Aplicación Móvil GET Mobile ID.
- Aplicación Móvil GET Mobile Verifier.

7.12.2 METODOLOGÍA

Nuestros formadores son profesionales de la formación, especializados en nuestro campo de especialización. Ponemos énfasis en los intercambios interactivos y el desarrollo de habilidades a través de la implementación operativa de nuestras soluciones. Como tal, cada sesión incluye conferencias, sesiones de preguntas y respuestas y trabajos prácticos para poner en práctica los conceptos presentados.

7.12.3 DESCRIPCIÓN

Referencia	ISO 18013-5 Basics
Objetivo	Descubra los conceptos básicos de ISO 18013-5 y como su implementación impacta la innovación digital y su ecosistema.
Audiencia	- Cualquier persona involucrada o interesada en implementar una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes, áreas funcionales de emisión de documentos, Planificación e innovación). - Este curso de capacitación proporciona los conocimientos mínimos necesarios para comprender completamente los demás módulos de capacitación impartidos.
Prerequisitos	Formación universitaria básica o ingeniero informático o equivalente mediante experiencia.
Plan	- Resumen ISO 18013-5 - Alcance del ISO 18013-5 - Avances innovadores en el mundo - Relación de la PKI con el ISO 18013-5 - Usos e innovaciones - Marco legal y regulatorio
Duración	4 horas

Referencia	Formación de emisión de credenciales digitales ISO 18013-5.

Objetivo	- Comprender los sistemas y procedimientos involucrados en la emisión de una credencial digital. - Cumplimiento del estándar ISO 18013-5 en su implementación.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de GET Mobile ID o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Conocimientos generales de sistemas Android/iOS e infraestructura API o contenidos formativos. - Curso ISO 18013-5 Basics
Plan	- Flujo de emisión de credenciales. - Componentes e integraciones con sistemas CMS. - Integraciones e interacciones.
Duración	4 horas

Referencia	Instalación y Configuración de GET Mobile Administrator.
Objetivo	- Comprender el modelo de instalación, sus ubicaciones y demás configuraciones aplicadas al proyecto. - Operación de la solución. - Modelo de datos. - Integraciones disponibles.
Audiencia	Futuros administradores de CMS o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso ISO 18013-5 Basics - Formación de emisión de credenciales digitales ISO 18013-5.
Plan	- Arquitectura técnica de la solución - Requisitos previos - Instalación de los componentes en el proyecto. - Integraciones disponibles:
Duración	4 horas

Referencia	Aplicaciones Moviles GET
Objetivo	Aplicación de los conceptos adquiridos para el uso de las aplicaciones móviles finales.
Audiencia	Cualquier persona involucrada en la implementación de una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de

	sistemas y redes), especialmente futuros administradores de CMS o gerentes de soluciones CMS.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Conocimientos generales de sistemas Android/iOS e infraestructura API o contenidos formativos. - Curso ISO 18013-5 Basics
Plan	- Descripción general de las aplicaciones móviles. - Despliegue de soluciones móviles. - Funcionalidades posibles. - Taller Practico.
Duración	3 horas

8. PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)

8.1 OBJETIVO DEL PLAN

Este plan es presentado a la Junta Central Electoral con el propósito de garantizar la operación ininterrumpida en la producción y personalización de las Cédulas de Identidad y Electoral. Una de las empresas locales que conforman el Consorcio Identidad 4.0 RD, con 21 años de operación ininterrumpida, ha desarrollado estrategias efectivas para mitigar cualquier riesgo que pueda comprometer la entrega de estos documentos esenciales. Además, esta misma empresa ha sido proveedor de la cédula durante 10 años, lo que refuerza el compromiso y la capacidad de ejecución del presente proyecto, basándose en su experiencia comprobada en la producción e implementación del documento de identidad nacional

8.2 2. ALCANCE

Este plan cubre todas las actividades relacionadas con la producción, personalización, impresión, almacenamiento y distribución de las cédulas, incluyendo:

- Operaciones en los centros de producción.
- Infraestructura tecnológica y seguridad de datos.
- Suministro de materiales e insumos.
- Procesos de impresión y personalización de documentos.
- Coordinación entre seis sucursales estratégicamente ubicadas a nivel nacional, con la sede principal en el Distrito Nacional, que ha operado de manera ininterrumpida durante 21 años, asegurando estabilidad y continuidad en los procesos.

8.3 ANÁLISIS DE RIESGOS

Se han identificado los siguientes riesgos clave para la Junta Central Electoral (JCE):

- Fallas técnicas: Posibles disrupciones en los equipos de impresión y en el sistema de personalización de cédulas, lo que podría comprometer la emisión oportuna de los documentos de identidad.
- Eventos de fuerza mayor: Desastres naturales como terremotos, incendios o inundaciones que podrían afectar las instalaciones de la JCE y los centros de producción.
- Ciberamenazas: Riesgo de ataques cibernéticos que puedan comprometer la integridad de los registros ciudadanos, generar accesos no autorizados o alterar la base de datos de identidad.
- Disrupciones en la cadena de suministro: Retrasos en la provisión de materiales esenciales, como tarjetas en blanco, tintas de seguridad y componentes tecnológicos críticos para la emisión de cédula

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

8.4 ESTRATEGIAS DE CONTINUIDAD

Para garantizar la operatividad ininterrumpida de la JCE, se implementarán las siguientes estrategias:

8.4.1 INFRAESTRUCTURA DE RESPALDO:

- Implementación de servidores redundantes y almacenamiento en la nube para asegurar la integridad y disponibilidad de los datos.
- Establecimiento de centros de producción secundarios para asegurar la continuidad del servicio en caso de fallas críticas.
- Activación de seis sucursales estratégicamente ubicadas como puntos de contingencia operativa.
- Para garantizar la continuidad operativa, se dispone de una fábrica adicional plenamente equipada para asumir la producción en caso de contingencias, en cumplimiento con los requisitos del Pliego de Condiciones.

  Dirección: 187 Allée des Plagnes, 24300 Mareuil-en-Périgord, Francia

8.4.2 PROTOCOLOS DE RESPALDO DE INFORMACIÓN:

- Respaldo automatizado de bases de datos de identidad con encriptación avanzada para prevenir accesos no autorizados.
- Mecanismos de recuperación rápida de información ante posibles incidentes tecnológicos.

8.4.3 GESTIÓN DE PROVEEDORES ESTRATÉGICOS:

- Acuerdos con múltiples proveedores para diversificar la fuente de insumos críticos y evitar dependencias exclusivas.
- Implementación de un esquema logístico eficiente para la distribución de materiales a los centros de emisión de cédulas.

8.4.4 PLAN DE RECUPERACIÓN ANTE CRISIS:

- Realización de pruebas de recuperación de datos y operatividad para garantizar una respuesta eficiente en situaciones de emergencia.
- Establecimiento de protocolos claros de acción para asegurar la continuidad del servicio de emisión de cédulas.

8.5 PROCEDIMIENTOS DE RESPUESTA Y RECUPERACIÓN

Ante una eventual interrupción del servicio, se activará el siguiente protocolo de actuación:

1. Activación del Plan: Identificación inmediata del incidente y notificación a los equipos de respuesta.
2. Gestión de Contingencias: Evaluación del impacto en la emisión de documentos y aplicación de medidas correctivas en tiempo real.

3. Restauración de Operaciones: Puesta en marcha de procedimientos de recuperación para garantizar la continuidad del servicio.
4. Tiempo Máximo de Recuperación (RTO): Restauración completa de operaciones esenciales dentro de un lapso de 24 a 48 horas.
5. Análisis Post-Incidente: Evaluación integral del evento, documentación de aprendizajes y aplicación de mejoras en los procedimientos internos.

ROLES Y RESPONSABILIDADES

- Comité de Seguridad y Continuidad Operativa Responsable de la coordinación de respuestas estratégicas ante eventos disruptivos.
- Departamento de Tecnología y Seguridad: Encargado de la protección y recuperación de los sistemas de información y los datos de la JCE.
- Unidad de Producción y Logística: Responsable de garantizar la continuidad en la fabricación y distribución de cédulas en los distintos puntos de emisión.

7. PRUEBAS Y SIMULACROS

- Ejecución de simulaciones periódicas para evaluar la efectividad del plan y su capacidad de respuesta.
- Realización de ensayos de recuperación ante ciber amenazas y fallos técnicos en los sistemas de emisión.
- Auditorías anuales para fortalecer la resiliencia operativa y asegurar el cumplimiento de estándares tecnológicos y de seguridad.

8.6 REQUISITOS DE PRODUCCIÓN Y TIEMPOS DE ENTREGA

INTRODUCCIÓN

El Consorcio Identidad 4.0 RD se compromete a garantizar una producción eficiente, segura y confiable de las Cédulas de Identidad y Electoral (CIE) para la Junta Central Electoral (JCE). Con una infraestructura de producción avanzada, estrictos protocolos de calidad y una logística optimizada, se asegura el cumplimiento de los plazos estipulados en el Pliego de Condiciones, minimizando riesgos y asegurando la disponibilidad ininterrumpida de los documentos.

8.7 INFRAESTRUCTURA DE PRODUCCIÓN Y UBICACIÓN DE LAS FÁBRICAS

El Consorcio Identidad 4.0 RD cuenta con centros de fabricación de alta tecnología, ubicados estratégicamente para optimizar los tiempos de producción y entrega.

UBICACIÓN DE LAS FÁBRICAS Y OFICINAS EN EL EXTERIOR

- Centro principal de producción: Angoulême, Rue Louis Pergaud, 16000 Angoulême, Francia.
- Fábrica de respaldo: 187 Allée des Plagnes, 24300 Mareuil-en-Périgord, Francia
- Oficinas regionales y centros de distribución:

- Estados Unidos – Centro logístico para coordinación internacional.
- Europa – Oficina para soporte técnico y distribución.
- República Dominicana – Sede operativa y de implementación. José Andrés Aybar Castellanos No. 153. La Esperilla

RED DE SUCURSALES DE CSI

- CSI cuenta con seis oficinas operativas en República Dominicana y una en desarrollo en Azua.
- Infraestructura de asistencia técnica presente en el 100% de las provincias del país.

8.8 MEDIDAS DE SEGURIDAD EN LA PRODUCCIÓN

- Control de acceso biométrico y videovigilancia 24/7 en todas las fábricas y centros logísticos.
- Procedimientos de validación digital y trazabilidad para cada documento producido.
- Protocolos de encriptación avanzada en bases de datos para evitar accesos no autorizados
- El Consorcio cuenta con dos plantas de producción estratégicamente ubicadas para garantizar la fabricación segura y eficiente de los documentos de identidad:

- Planta Principal: SELP – Angoulême, Rue Louis Pergaud, 16000 Angoulême, Francia.
- Planta de Respaldo: SELP – Mareuil-en-Périgord, 187 Allée des Plagnes, 24300 Mareuil-en-Périgord, Francia.

  Ambas plantas cuentan con certificaciones internacionales en seguridad de impresión, control de acceso biométrico y videovigilancia 24/7, garantizando la integridad y trazabilidad del proceso de producción.

8.9 CRONOGRAMA GENERAL DE PRODUCCIÓN Y ENTREGA

Fase de Entrega	Cantidad de Cédulas	Tiempo Máximo
Entrega inicial (prueba)	2,000 tarjetas	Semana 16
Primera producción masiva	300,000 tarjetas	Semana 22
Segunda producción masiva	500,000 tarjetas	Semana 26
Tercera producción masiva	1,200,000 tarjetas	Semana 30
Producción continua	1,000,000 tarjetas cada 4 semanas	Desde Semana 34 hasta la 54

8.10 CRONOGRAMA DE TRABAJO

El cronograma de trabajo establece una planificación general y estratégica para la ejecución del proyecto, asegurando el cumplimiento de los plazos establecidos en el Pliego de Condiciones. Funciona como cronograma madre, ya que proporciona una visión estructurada de las principales fases de producción, implementación y entrega de las Cédulas de Identidad y Electoral (CIE).

Es importante destacar que el cronograma definitivo se elaborará en conjunto con la Junta Central Electoral (JCE), lo que permitirá realizar ajustes y optimizaciones según las necesidades específicas del cliente final. Este proceso garantizará una planificación alineada con las expectativas operativas y los objetivos de la JCE.

Nota: La versión completa del cronograma de trabajo se encuentra en la sección de Anexos, detallando cada actividad clave, sus tiempos de ejecución y los hitos de entrega.

Línea	TAREA	DEPENDENCIA	RESPONSABLE				ETAPA 1	+6	ETAPA 2
			CSI	GET	SELP	JCE			
1	**ETAPA 0**								
2	***Firma del contrato***		X	X	X	X			
3	***Planificación del Proyecto***	1	X	X	X	X			
	ETAPA 1								
	EJECUCIÓN								
	1. Suministro de Tarjetas en Policarbonato								
3	Entrega de diseños por parte de la JCE/ Definición de especificaciones portarios de periféricos *1	1			X	X	*4		
4	Generación del diseño (BAT) y entrega de diseño de seguridad en .pdf	3			X				
5	Aprobación de BAT	4				X			
6	Generación Pruebas de color / Envío muestra de impresión de la "Prueba de color"	5			X				
7	Aprobación "Prueba de color"	6				X			
8	Entrega 2,000 tarjetas genéricas de FC con chip, para pruebas (llaves "test")				X				
9	Aprovisionamiento de materia prima (modulos, PC, placas de laminación, hologramas, etc)	5			X				
10	Impresión y ensamblado de tarjetas	9			X				
11	Elaboración de BAP (Llaves producción)				X				
12	Aprobación de BAP (JCE y el Consorcio)	11		X	X	X			
13	Entrega por parte de la JCE del plan de numeración para la pre-personalización del número de serie de las tarjetas de identidad					X			
14	Pre-personalización eléctrica y gráfica (laser)	10,13,19			X				
15	Pruebas de durabilidad (laboratorio externo)	10			X				
16	Envío y entrega de 500,000 tarjetas acompañado de certificado de test independiente	14,15			X				
	2. Suministro de impresoras								
17	Levantamiento de cumplimiento de requerimientos mínimos de instalación de impresoras		X						
18	Reacondicionamiento para el cumplimiento de requerimientos mínimo de instalación de impresoras					X			
19	Entrega física de 2 impresoras de policarbonato a JCE *3	2			X	X			
20	Instalación in situ	17	X						
21	Adaptación del SDK de la impresora al sistema de la JCE	17		=		X			
22	Pruebas unitarias, de integración, de pre-producción con las impresoras, las tarjetas, personalizando la tarjeta	19		=		X			
	3. Implementación GET PKI								
23	Definición y entrega de requisitos para implementación PKI	1		=		X	*4		
24	Definición de CA y nombramiento de dominios	1		X		X			
25	Plan de configuración	24			=				
26	Habilitación de área de cómputo para la entrega de la infraestructura	2				X			
27	Instalación y entrega de infraestructura física	26	X						
28	Recepción de la infraestructura física	27				X			
29	Preparación de VMs	28		=					
30	Ceremonia de llaves - Preproducción	29		=		X			
31	Instalación y configuración - Preproducción	30		=					
32	Pruebas de aceptación	31		=		X			
33	Ceremonia de llaves - Producción	32		=					
34	Instalación y configuración - Producción	33		X					
35	Instalación y configuración - Disaster recovery	34		=					
	4. Implementacion GET Mobile ID								
36	Reunion de proyecto - Inicio de documento de requerimientos	1,2		X					
37	Revisión de plan de implementación	36		=		X			
38	Definición de diccionario de datos	36		X		X			
39	Guía de integraciones / Interfaces	36		X		X			
40	Requerimientos de seguridad	39		=		X			
41	Discusión sobre branding TSE	36		=		X			
42	Habilitación de área de cómputo para la entrega de la infraestructura (JCE)					X			
43	Instalación y entrega de infraestructura física *6	42	X						
44	Recepción de la infraestructura física	43				X			
45	Definicion de personalización del CMS	39		=		X			
46	Aprobación de personalización del CMS	45				X			
47	Implementación de UI IOS/Android	46		=					
48	Verificador IOS/Android mID Verifier	47		X					
49	Desarrollo de interfaces con sistema de emisión TSE	48		=					
50	Despliegue mobile administración versión pre-productiva	44		=					
51	Configuración de mID en servidores	50		X					
52	GET Mobile administrator: Instalación			X					
53	Key Management Services	43		X					
54	Perso & Device Management			X					
55	Integración de Sistema de Emisión de la JCE con el mID *2	53				X			
56	ID & Access Management	39		=					
57	ISO Online LookUp API	56		X					
58	UAT - GET Mobile Administrator UAT *8	52		X		X			
59	UAT - GET mID UAT	52		X		X			
60	UAT - GET Verifier UAT	43		X		X			
61	UAT signoff	60				X			
	5. Capacitación								
63	Coordinación Solucion de Inmotion laser con la JCE para generar grabación de entrenamientos en SD incluyendo personal de la JCE, solucion de impresion y bateria de periféricos para simulacion de area de trabajo y dar mayor flexibilidad al contexto mismo de la grabación		X			X			
63	Entrenamiento de la Solución de Impresión Presencial en Casa Central de JCE (Nacional e Internacional) - Personal Operadorativo y Técnico nivel 2. - Guia básica de operación de la solución - Mantenimiento preventivo - Verificación de calidad de impresión - Resolución de incidencias básicas - Módulo sobre respuesta ante fallas y continuidad del negocio (PCN)		X	X					
64	Entrenamiento PKI Presencial en Casa Central de JCE RD (Nacional e Internacional): - PKI Básico (Mirona) - Sistema de gestión de Credenciales (CMS) (1 días - 7 horas) - Instalación (7 horas) -HSM Protocolo Training (7 horas) -SAC Training (1 día - 7 horas) -Firmado Digital (7 horas)	34	X	X		X			
65	Entrenamiento Mobile ID Presencial en Casa Central de JCE RD (Nacional e Internacional) - ISO 18013-5 Basico (4 horas) - Formación de emisión de credenciales digitales ISO 18013-5 (4 horas) - Instalación y Configuración de GET Mobile Administrator (4 horas) - Aplicaciones Moviles GET (3 horas)	60	X	X		X			
66	Edición grabación de entrenamientos en SD incluyendo personal de la JCE	60,64,65	X						
67	Subida de la grabación al portal de la JCE	66	X			X			
	ETAPA 2								
	EJECUCIÓN								
	1. Suministro del inventario de tarjetas para la cedulación nacional.								
68	500,000 Tarjetas de policarbonato a los 36 semanas despues de la firma de contrato.					X			
69	1,000,000 tarjetas de policarbonato a las 30 semanas despues de la firma de contrato.					X			
70	1,000,000 tarjetas de policarbonato a las 34 semanas despues de la firma de contrato.					X			
71	1,000,000 tarjetas de policarbonato a las 38 semanas despues de la firma de contrato.					X			
72	1,000,000 tarjetas de policarbonato a las 42 semanas despues de la firma de contrato.					X			
73	1,000,000 tarjetas de policarbonato a las 46 semanas despues de la firma de contrato.					X			
74	1,000,000 tarjetas de policarbonato a las 50 semanas despues de la firma de contrato.					X			
75	1,000,000 tarjetas de policarbonato a las 54 semanas despues de la firma de contrato.					X			
76	Planificacion de entregas para Etapa 3					X			
	2. Suministro de Impresoras Nacional e Internacional								
77	Entrega 2 de impresoras - Cantidad 12 / ja *3		X	X					
78	Entrega 3 de impresoras - Cantidad 100, en batches por cantidades acorde a la orden solicitada / 6s *3		X	X					
79	Entrega 4 de impresoras - Cantidad 100, en batches por cantidades acorde a la orden solicitada / 5s *3		X	X					
	3. Puesta en marcha del mantenimiento nacional e internacional de las impresoras en período de garantía								
80	Mantenimiento preventivo de la solucion de impresión - Inspección - Ajuste - Calibración - Limpieza - Lubricación y remplazo del fibra (una vez al año) Periodicidad: Cada 6 meses					X			
81	Soporte a incidencias reportadas a través de los canales de atención. Detalles en anjeto de actividades de respuesta a incidentes de la propuesta técnica.					X			
	ETAPA 3								
	EJECUCIÓN								
	1. Suministro de tarjetas de identidad								
82	Despacho y entrega de 1,000,000 de tarjetas de identidad, siempre un 10% G en la oficina Central de la JCE, segun el plan acordado				X				
83	Planificacion de entregas (4 meses antes) para Periodo de años 5-10 y emision de OC subsecuentes para fabricacion, despacho y entrega de tarjetas de policarbonato	75	X			X			
	2. Mantenimiento del sistema de la solución de impresión en República Dominicana y en Madrid - USA								
84	Mantenimiento preventivo de la solución de impresión - Inspección - Ajuste - Calibración - Limpieza - Lubricación y remplazo del fibra (una vez al año) Periodicidad: Cada 6 meses.		X	X					
85	Soporte a incidencias reportadas a través de los canales de atención. Detalles en anjeto de actividades de respuesta a incidentes de la propuesta técnica, a partir de primera Etapa		X						
	2. Mantenimiento PKI, Sistemas y Cédula Digital								
86	Mantenimiento PKI - Renovación y revocación programada de certificados. - Verificación de integridad del HSM. - Simulacros de incidentes y evaluaciones de rendimiento. - Revisión de certificados y actualización de software. - Pruebas de penetración y seguridad. Periodicidad: Cada 6 meses.		X	X				*10	
87	Infraestructura - Servidores, almacenamiento, red y elementos de seguridad como NSS Firewalls y WAF. *7 Periodicidad: Cada 6 meses.	38 y 44	X	X				*10	
88	Cedula Digital - Revisión de certificados. - Actualización de software y firmware. - Revisión de políticas de seguridad. - Realización de copias de seguridad. - Pruebas de penetración y vulnerabilidades. Periodicidad: Cada 6 meses		X	X				*10	

Notas:

*1 *Entrega de periféricos a los treinta (30) días máximo después de la solicitud de la JCE. Detalles en Pliego de Condiciones, Pág 36, Item 5 Especificaciones Kit de Periféricos, Subtitulo V.6 Cámara.*

*2 *Prerrequisito de habilitación y aseguramiento de la disponibilidad del sistema de emisión de la JCE.*

*3 *Validación certificación impresores por parte del fabricante*

*4 *Tras completar la entrega en 19 semanas, las semanas 20 a 25 están destinados a la estabilización operativa, optimización de procesos y entrenamientos. Este período permitirá realizar pruebas adicionales, afinar configuraciones y garantizar un inicio de producción sin interrupciones, asegurando el máximo rendimiento del sistema desde el primer día. (Buffer)*

*5 *Validar procedimientos de contingencia durante la prueba UAT (PCN)*

*6 *Asegurar redundancia de servidores y respaldo en la implementación (PCN)*

*7 *Prueba de recuperación de datos y sistemas en caso de fallo (PCN)*

*8 *El consorcio Cedula 4.0 R.D. iniciará el cronograma de trabajo a la semana siguiente de la firma del contrato con la JCE, sin depender del anticipo del 20%.*

*9 *Plaificacion recurrente de forma annual (gestion de planificacoin con JCE)*

*10 *Pre-Run para S20*

Matriz de cumplimiento del pliego Punto a Punto

MATRIZ DE CUMPLIMIENTO
CONSORCIO "IDENTIDAD 4.0 RD"

PARA EL PROCESO DESTINADO A LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARALA IMPRESIÓN DE LA NUEVA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI) DE REF.: JCE-CCC-LPI-2024-0001.

Junta Central Electoral
Santo Domingo de Guzmán, Distrito Nacional, República Dominicana.

RNC: 101038652
Santo Domingo, R.D.

Contenido

CAPITULO I 3
GENERALIDADES 3
ESPECIFICACIONES TÉCNICAS ITEM I 17
TARJETAS 17
ESPECIFICACIONES TÉCNICAS ITEM II 28
MÁQUINAS DE IMPRESIÓN 28
ESPECIFICACIONES TÉCNICAS ITEM III 37
PKI 37
ESPECIFICACIONES TÉCNICAS ITEM IV 44
TARJETA DE IDENTIDAD DIGITAL 44
ESPECIFICACIONES TÉCNICAS ITEM V 52
KIT DE PERIFÉRICOS 52
ESPECIFICACIONES TÉCNICAS ITEM VI 58
MANTENIMIENTO 58
ESPECIFICACIONES TÉCNICAS ITEM VII 66
CAPACITACIONES 66
OTROS REQUERIMIENTOS 68
CAPITULO II 94
CAPITULO III 97
CAPITULO IV 106
CAPITULO V 111
CAPITULO VI 121
CAPITULO VII 126
CAPITULO VIII 130

Página/Folio No.171 de 843

CAPITULO I
GENERALIDADES

Página/Folio No.172 de 843

1.1 Objetivos y Alcance

Requerimiento	Respuesta Consorcio Identidad 4.0 RD
El objetivo del presente documento es establecer el conjunto de cláusulas jurídicas, económicas, técnicas y administrativas, de naturaleza reglamentaria, por el que se fijan los requisitos, exigencias, facultades, derechos y obligaciones de Las Partes, en el proceso llevado a cabo por la JUNTA CENTRAL ELECTORAL, Referencia: JCE-CL-LPI-2024-01, destinado a la contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI). Este documento constituye la base para la preparación de las ofertas por parte de las empresas nacionales o extranjeras, que deseen participar en la licitación de referencia. Si el Oferente/Proponente omite suministrar alguna parte de la información requerida en el presente Pliego de Condiciones o presenta una información que no se ajuste sustancialmente al mismo, el riesgo estará a su cargo y el resultado será el rechazo de su propuesta.	Entendemos y aceptamos.

1.2 Definiciones e Interpretaciones

Requerimiento	Respuesta Consorcio Identidad 4.0 RD
A los efectos de este Pliego de Condiciones Específicas, las palabras y expresiones que se inician con letra mayúscula y que se citan a continuación, tienen el siguiente significado: **Agentes Autorizados:** Personas físicas designadas por los Oferentes/Proponentes a los fines de realizar, en nombre de ellos, los trámites requeridos en el proceso de licitación. **Bienes:** Materiales, equipos, mobiliarios, maquinarias, que el Oferente esté obligado a suministrar a la Entidad Contratante. **Caso Fortuito:** Acontecimiento que no ha podido preverse, o que no ha podido evitarse, por ser extraño a la voluntad de las personas. **Circular:** Aclaración que la entidad contratante, a través de los organismos correspondientes, emite de oficio, o para dar respuesta a las consultas planteadas por los Oferentes/Proponentes con relación al contenido del Pliego de Condiciones Específicas, formularios, anexos u otra Circular y que siempre se hará de conocimiento de todos los Oferentes/Proponentes, los cuales en su contenido serán vinculantes a los fines de la licitación.	Entendemos y aceptamos.

Página/Folio No.173 de 843

Comité de Compras y Contrataciones: Órgano de la Entidad Contratante responsable de la evaluación y calificación de las propuestas, así como de la organización, conducción y ejecución de la integridad del proceso de licitación, encargándose también de dar respuestas a las consultas, recepción de propuestas, calificación de Oferentes/Proponentes, aprobación de las propuestas con la opinión de la Comisión Técnica, preparación del informe con las recomendaciones de lugar, y todo acto complementario, conveniente y válido a los fines de valorar las propuestas para la adjudicación.

Comisión de Asesoría y Asistencia Técnica: Cuerpo integrado por áreas o personas expertas en la materia respecto del proceso. Son designados por la Entidad Contratante para colaborar, asesorando y analizando propuestas, evaluando datos, confeccionando documentos para el sustento de las decisiones que deba adoptar el Comité de Compras y Contrataciones.

Comprobante de Pago: Recibo numerado que entregará la Entidad Contratante al Oferente/Proponente como constancia del pago realizado para cubrir los gastos administrativos generados durante todo el proceso de licitación, incluyendo la elaboración del Pliego de Condiciones. Esta suma, no es reembolsable bajo ninguna circunstancia.

Contrato: Documento o instrumento legal suscrito entre la Entidad Contratante y el adjudicatario en que se fijan las obligaciones y derechos de ambas partes. De éste, formarán parte el Pliego de Condiciones, la Resolución de Adjudicación y la Orden de Compra u Orden de Servicios (según corresponda).

Consorcio: Asociación de personas jurídicas que no constituyen un ente con personalidad jurídica independiente y que se establece con el objeto de participar en la licitación. En todo caso, debe intervenir entre sus integrantes un acuerdo bajo firma privada de constitución de consorcio, que haga a sus miembros corresponsables de las acciones de este.

Consulta: Comunicación escrita por un Oferente/Proponente, remitida conforme al procedimiento establecido y recibida por el Comité de Compras Contrataciones, solicitando aclaración, interpretación o modificación sobre aspectos relacionados con el Pliego de Condiciones.

Credenciales: Documentos que un Oferente/Proponente presenta, en la forma establecida en el Pliego de Condiciones, a fin de ser evaluados y calificados por el Comité de Compras Contrataciones, durante la etapa de selección de los Proponentes Habilitados para presentar propuestas.

Cronograma: Cronología del proceso de licitación.

Página/Folio No.174 de 843

Enmienda: Comunicación escrita, remitida por el Comité de Compras Contrataciones, con el fin de modificar el contenido del Pliego de Condiciones Específicas, formularios, anexos u otros y que se hace de conocimiento de todos los Oferentes/Proponentes.

Entidad Adquiriente: La Junta Central Electoral.

Estado: Estado Dominicano.

Fuerza Mayor: Cualquier evento o situación que escape al control, que se considere imprevisible e inevitable, y sin que esté envuelta su negligencia o falta, como son, a manera enunciativa pero no limitativa, actos de autoridades gubernamentales o militares, regulaciones o requerimientos estatales, epidemias, guerras, actos terroristas, huelgas, fuegos, explosiones, temblores de tierra, accidentes, catástrofes, inundaciones y otras perturbaciones ambientales mayores, condiciones severas e inusuales del tiempo o actos u omisiones de terceras personas que escapen del control de las partes.

Interesado: Cualquier persona jurídica que tiene interés de presentar credenciales o propuestas en el procedimiento de licitación.

Licitación Pública Internacional: Es el procedimiento administrativo mediante el cual se realiza un llamado público y abierto dentro y fuera del territorio nacional, convocando a los interesados para que formulen propuestas, de entre las cuales se seleccionará la que se encuentre más conforme a los Pliegos de Condiciones y sea considerada como la más conveniente a la institución.

Líder del Consorcio: Persona jurídica del consorcio que ha sido designada como tal.

Oferente/Proponente: Persona jurídica, legalmente capacitada para participar, presentando oferta o propuesta en la licitación, dentro del marco del presente pliego.

Pliego de Condiciones Específicas: Documento que contiene todas las condiciones por las que habrán de regirse las partes en la presente licitación y que formará, conjuntamente con la Orden de Compra o de Servicios, del Contrato definitivo.

Proveedor: Oferente/Proponente que habiendo presentado oferta en la licitación, resulta adjudicatario del contrato para suministrar los productos y/o servicios de acuerdo a los requerimientos del Pliego de Condiciones Específicas.

Representante Legal: Persona física o jurídica acreditada como tal por el Oferente/ Proponente.

Sobres: Paquetes que contienen las credenciales de los Oferentes/Proponentes y las Propuestas Técnicas o Económicas.

Página/Folio No.175 de 843

Suministro: Selección, adquisición y distribución de los bienes y/o servicios objetos de la licitación, los cuales serán llevados a cabo de acuerdo a las especificaciones detalladas en el presente Pliego de Condiciones Específicas.	

Requerimiento	Respuesta Consorcio Identidad 4.0 RD
Definiciones de las Especificaciones Técnicas A continuación, se incluye una lista de definiciones a ser tomadas en cuenta para el desarrollo de ofertas para esta licitación. A esta lista se agregan por referencia las definiciones contenidas en el Documento 9303 de la OACI, 8a Edición 2021. En caso de duda o contradicción respecto a su interpretación o aplicación, tendrán preponderancia las definiciones contenidas en el Documento 9303 antes citado. **OACI:** Organización de Aviación Civil Internacional. **AFIS:** Siglas en inglés del sistema de identificación automatizado de huellas dactilares. **Cédula de Identidad digital o CD**: Cédula en el celular. **CIE:** Cédula de Identidad y Electoral. Mayores de edad que no pertenecen a los grupos que tienen CI. **CI:** Cédula de Identidad. Menores de dieciocho (18) años de edad, Extranjeros, Militares y Policías. La particularidad es que no votan. **CMS:** Sistema Central de Gestión de Tarjetas. **CSCA:** Siglas en inglés de autoridad nacional de certificación de firmas electrónicas conforme a especificaciones de OACI. **CVCA:** Siglas en inglés de autoridad nacional de verificación de firmas electrónicas conforme a especificaciones de OACI. **Doc 9303 de la OACI 7a edición o posterior:** Documento emitido por la OACI que establece las normas y especificaciones que deberán utilizarse en la emisión de documentos de viaje, incluyendo tarjetas electrónicas. **DTC:** Digital Travel Credential. Estándar ICAO de documento de viaje en móvil. **Enrolamiento:** Captura de los datos biográficos y biométricos de los ciudadanos, introduciéndolos en una base de datos por diversos medios.	Entendemos y aceptamos.

COPY CONTROL INTERNACIONAL SA
RNC. 101038652
Santo Domingo, R.D.

ECMS: Sistema de gestión de tarjetas.

Guilloche: Técnica gráfica decorativa en la cual un patrón de diseño repetitivo y complejo es grabado mecánicamente en un material subyacente con gran precisión y detalle.

IEC: Siglas en inglés de Comisión Electrotécnica Internacional.

Intaglio: Técnica de impresión que consiste en la generación de un dibujo o composición artística en tres dimensiones sobre una plancha de metal, el cual es rellenado con tinta y luego transferido a un papel, dejando el dibujo en alto relieve.

INTERGRAF ISO 14298:2013: Es un estándar de seguridad altamente reconocido por los productores de documentos de valor que emplean funciones de seguridad añadidas, diseñadas para proteger contra la falsificación de sus características ("security printers").

ISO 18013-5: Estándar que establece especificaciones de interfaz para la aplicación de un documento de identificación (permiso de conducción particularmente) en asociación con un dispositivo móvil. Este estándar especifica la interfaz entre el mDL (mobile driving license) y el lector de mDL y la interfaz entre el lector de mDL y la infraestructura de la autoridad expedidora.

ISO/IEC23220: Especifica arquitecturas genéricas de sistemas y fases genéricas del ciclo de vida de los sistemas de identificación electrónica móvil en términos de bloques de construcción para infraestructuras de sistemas de identificación electrónica móvil. Normaliza interfaces y servicios para aplicaciones mdoc y aplicaciones móviles de verificación.

ISO/IEC 19794-2: Estándar que especifica un concepto y formatos de datos para la representación de huellas dactilares utilizando la noción fundamental de minucias. Este estándar describe cómo los puntos de las minucias serán determinados, define los formatos de datos para contener los datos para el uso general y de tarjeta inteligente, y detalla la información de la conformidad. Las pautas y los valores para los parámetros de combinación y decisión se proporcionan como anexo informativo.

ISO/IEC 19794-4: Estándar que especifica un formato de intercambio de registros de datos para almacenar, registrar y transmitir la información de imágenes de dedos o palmas.

ISO/IEC 19794-8: Estándar que describe todas las características de una huella dactilar en un pequeño registro de datos; permite la extracción de información espectral (orientación, frecuencia, fase, etc.) y características (minucias, núcleo, número de crestas, etc.). Se basa en las características comunes compartidas entre el patrón espectral y las minucias por medio de la codificación de las crestas de una forma que el esquema de crestas proporcione las bases para detectar minucias.

Página/Folio No.177 de 843

ISO/IEC FCD 19794-3: Formato de intercambio basado en patrones del dedo - Este estándar de bosquejo especifica que una imagen de la huella dactilar está dividida en una grilla de células solapadas o no solapadas. En cada célula, el patrón del dedo será representado por una estructura de célula. Un método para obtener la estructura de la célula es descomponer cada una de las células en una representación espectral de dos dimensiones tal como la Transformada Discreta de Fourier (Discrete Fourier Transform, DFT) de dos dimensiones. La descomposición produce los componentes espectrales, donde cada componente se puede caracterizar por una longitud de onda horizontales (x) y verticales (y), en dirección, amplitud, y fase.

ISO/IEC FCD 19794-5: Especifica los requisitos de la escena, fotográficos, de la numeración y del formato para las imágenes de caras de ser utilizado en el contexto de la verificación humana y del reconocimiento automatizado por computadora.

ISO/IEC FCD 19794-7: Para los propósitos de la verificación y/o de las identificaciones biométricas, este estándar especifica un formato de intercambio del concepto y datos del comportamiento dinámico de la firma, capturados bajo la forma de serie de tiempo usando los dispositivos tales como tabletas (pad) que convierten a digital o sistemas avanzados de la pluma.

ISO/IEC 27001:2013: Especifica requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de los sistemas de información.

ISO 14001: Esta norma de Sistemas de Gestión Ambiental (SGA) consigue que las empresas puedan demostrar que son responsables y están comprometidas con la protección del medio ambiente. Anteriormente hemos mencionado que lo consiguen a través de la gestión de los riesgos medioambientales que puedan surgir del desarrollo de la actividad empresarial.

ISO 9001: Es una norma de sistemas de gestión de la calidad (SGC) que se centra en todos los elementos de administración de calidad con los que una organización debe contar para tener un sistema efectivo que le permita administrar y mejorar sus productos y servicios.

ISO: Siglas en inglés de Organización Internacional de Estándares.

JCE: Junta Central Electoral de la República Dominicana. Emisor de la Cédula de Identidad y Electoral y Cédula de Identidad.

MRZ: Siglas en inglés de zona legible por máquina, es el código de barras alfanumérico en una zona específica de la tarjeta susceptible de ser reconocido por un lector óptico.

MRTD: Por sus siglas en inglés, Machine Readable Travel Document, Documento de viaje de lectura mecánica emitido de acuerdo a las normas contenidas en el Doc 9303 de la OACI.

Página/Folio No.178 de 843

Mobile ID: Tarjeta de Identidad digital, en un celular. **NFIQ:** Siglas en inglés de calidad de imagen de huella dactilar del Instituto Nacional de Estándares y Tecnología (NIST) USA. **OACI:** Organización de Aviación Civil Internacional. **OSE:** Oficina de Servicio Exterior donde se enrola y se entregan tarjetas en el exterior del país. **Personalización o Elaboración:** Es la impresión de los datos del titular de la tarjeta CIE o CI, incluido sus diversos componentes, una vez que los datos biográficos y biométricos del ciudadano han sido verificados y autorizados. La impresión comprende el uso de diversos métodos físicos y químicos. **Plan de Continuidad del Negocio**: Es un plan preparado y probado para que una organización pueda recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas, dentro de un tiempo predeterminado, después de una interrupción no deseada, catástrofe natural, ataque de delincuentes o causa similar. **Proceso:** Conjunto de actividades relacionadas lógicamente, llevadas a cabo para generar productos o servicios que, generalmente, atraviesan varias áreas funcionales de una organización. **Servicio**: Conjunto de actividades que buscan responder a las necesidades de un cliente, en este documento, el ciudadano. **Servicios de Apoyo:** Conjunto de actividades que buscan responder a las necesidades de un funcionario público que presta un servicio al ciudadano. **WSQ:** Siglas en inglés de cuantificación escalar de ondículas, es una norma de compresión diseñada y especificada por el FBI (Buró Federal de Investigaciones de Estados Unidos) para la compresión de imágenes de huellas dactilares de alta resolución en escala de grises.	

Requerimiento	Respuesta Consorcio Identidad 4.0 RD
Para la interpretación del presente Pliego de Condiciones Específicas: • Las palabras o designaciones en singular deben entenderse igualmente al plural y viceversa, cuando la interpretación de los textos escritos lo requiera.	Entendemos y aceptamos.

Página/Folio No.179 de 843

• El término "por escrito" significa una comunicación escrita con prueba de su recepción. • Toda indicación a capítulo, numeral, inciso, circular, enmienda, formulario o anexo se entiende referida a la expresión correspondiente de este Pliego de Condiciones Específicas, salvo indicación expresa en contrario. Los títulos de capítulos, numerales, formularios y anexos son utilizados exclusivamente a efectos indicativos y no afectarán su interpretación. • Las palabras que se inician en mayúscula y que no se encuentran definidas en este documento se interpretarán de acuerdo a las normas legales dominicanas.Toda cláusula imprecisa, ambigua, contradictoria u oscura a criterio de la Entidad Adquirente, se interpretará en el sentido más favorable a ésta. • Las referencias a plazos se entenderán como días calendario, salvo que expresamente se utilice la expresión de "días hábiles", en cuyo caso serán días hábiles de acuerdo con la legislación dominicana.	

1.3 Conocimiento y Aceptación del Pliego de Condiciones:

Requerimiento	Respuesta Consorcio Identidad 4.0 RD
El sólo hecho de un Oferente/Proponente participar en la licitación, implica pleno conocimiento, aceptación y sometimiento por él, por sus miembros, ejecutivos, Representante Legal y Agentes Autorizados, a los procedimientos, condiciones, estipulaciones y normativas, sin excepción alguna, establecidos en el presente Pliego de Condiciones Específicas, el cual tiene carácter jurídicamente obligatorio y vinculante. El Pliego de Condiciones estará disponible para su adquisición en las oficinas del Comité de Compras y Contrataciones, ubicadas en la Av. Gregorio Luperón esq. Av. 27 de Febrero, Edificio Administrativo, ala Este, 2do. Nivel, en la fecha indicada en el Cronograma de la Licitación y podrá consultarse en la página Web de la Junta Central Electoral (www.jce.do) y en el Portal Transaccional administrado por la Dirección General de Contrataciones Públicas. Los interesados en participar en la presente licitación deberán formalizar su inscripción (CON CARÁCTER OBLIGATORIO) mediante el llenado y presentación del Formulario FL-01 (Inscripción de Oferente), el cual se encuentra anexo al presente Pliego de Condiciones, y se podrá retirar en las oficinas del Comité de Compras y Contrataciones o descargarse de la página web de la Junta Central Electoral o del Portal Transaccional de la Dirección General de Contrataciones Públicas. El plazo para inscripción o registro de oferentes vence a las 4 horas de la tarde (4:00 P.M.) del día 17 de mayo del 2024.	Entendemos y aceptamos.

1.4 Normativa aplicable

Requerimiento	Respuesta Consorcio Identidad 4.0 RD

Página/Folio No.180 de 843

El proceso de Licitación, el Contrato, la Orden de Compras o de Servicios y su posterior ejecución se regirán por: la Ley Orgánica de Régimen Electoral No.20-23, el Reglamento Interno emitido por el pleno de la Junta Central Electoral, el Reglamento Interno para las Compras de Bienes y Contrataciones de Obras y Servicios aprobado por el Pleno de la Junta Central Electoral, el presente Pliego de Condiciones y las normativas vigentes en materia de compras y contrataciones, en todo lo que es aplicable a la Junta Central Electoral y no afecte su autonomía administrativa, dispuesta en la Constitución de la República y ratificada por la Sentencia No.TC-305-14, de fecha 29/04/2014, del Tribunal Constitucional. Todos los documentos que integran el Contrato serán considerados como recíprocamente explicativos. En caso de existir controversias, se aplicará para su resolución el siguiente orden de prelación: • Ley Orgánica de Régimen Electoral No. 20-23. • El Reglamento Interno para las Compras de Bienes y Contratación de Obras y Servicios, de la JCE. • El presente Pliego de Condiciones Específicas. • Sentencia del Tribunal Constitucional No. TC/0305/14. • Ley de Compras y Contrataciones Públicas No. 340-06, y sus modificaciones. • La Adjudicación. • La Orden de Compra o Servicio. • El Contrato.	Entendemos y aceptamos.

1.5 Modalidad de la Contratación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
La presente contratación se realizará por Licitación Pública Internacional, conforme a las disposiciones vigentes.	Entendemos y aceptamos.

1.6 Objeto de la Licitación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Constituye el objeto de la presente convocatoria la contratación por parte de la Junta Central Electoral de la empresa que se encargará de suplir los equipos, materiales y servicios para la nueva "Cédula de Identidad y Electoral y Cédula de Identidad". **1.6.1 Alcance**	Entendemos, aceptamos y cumplimos.

Página/Folio No.181 de 843

El proyecto contempla la impresión de unos ocho (8,000,000) millones de CIE y CI, durante los primeros dieciocho (18) meses de ejecución. Por su parte, los Proponentes deben garantizar el suministro oportuno de los equipos, materiales y servicios necesarios para el cumplimiento de esa meta.

1.6.2 Objetivo de General

Incorporar nuevas tecnologías que aporten mayores niveles de seguridad, para de esa manera, dar seguimiento a la estrategia diseñada por las actuales autoridades de la Junta Central Electoral, vinculada a la modernización y mejoramiento de los servicios que ofrece a la ciudadanía, relacionados con la función electoral y las atribuciones que la Carta Magna le otorga, en materia del Registro Civil y de la Cédula de Identidad.

1.6.3 Objetivos Específicos:

a. Actualizar la información personal y biométrica del ciudadano en el sistema de Cedulación de la Junta Central Electoral.
b. Garantizar la autenticidad y seguridad del documento de identidad para prevenir fraudes y falsificaciones.
c. Facilitar el acceso a servicios públicos y privados que requieran una identificación válida mediante la construcción de un ecosistema interoperable que permita contar con tecnología API REST en nubes públicas o privadas que sean capaces de verificar la autenticación de un documento a partir de la validación de credenciales verificables (VC) del W3C generadas en aplicaciones móviles mediante la lectura de la electrónica del chip y la verificación facial (1 a 1) exitosa. La (VC) del W3C se podrá representar en formato de código QR para facilitar su intercambio y verificación. El contenido del código QR suele ser una representación codificada de la VC en un formato específico, como JSON-LD.
d. Los componentes de la licitación cubren los siguientes elementos:
   1. Tarjetas CIE y CI.

- Plásticos electrónicos en policarbonato

   2. Máquinas de Impresión
   3. Cédula Digital (en el celular)
   4. PKI con establecimiento de Autoridad de Certificación
   5. Kits periféricos

- Escáner
- Lector de firma
- Lector de huellas
- Impresora punto de venta
- Lector de huellas digital persona
- Cámara

   6. Servicio de Instalación y Mantenimiento
   7. Capacitación

Página/Folio No.182 de 843

1.7 Características y Especificaciones Técnicas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
REQUERIMIENTOS	Entendemos, aceptamos y cumplimos.

Ítem	Cantidad	Artículos	Descripción
I	8,000,000	Tarjetas para Cédulas	Ver detalle en las especificaciones técnicas
II	214	Máquinas de Impresión	
III	1	PKI - CA	
IV	1	Cédula de Identidad Digital	
V	1	Kit de periféricos	
VI	-	Servicio de Instalación y Mantenimiento	
VII	-	Capacitación	

ESPECIFICACIONES TÉCNICAS GENERALES

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
a) Estándares aplicables Para completar esta Licitación, las ofertas deberán cumplir y conformarse a las siguientes recomendaciones y estándares internacionales, según corresponda: **b) Estándares OACI que prevalecen** • Documento 9303 8th edición 2021 de OACI. • PKI firmas digitales para MRTD **c) ISO / IEC 14443 Tarjetas de identificación de circuito integrado sin contacto** El estándar ISO/IEC 14443 consta de cuatro partes y se describen dos tipos de tarjetas: tipo A y tipo B. Las principales diferencias entre estos tipos se encuentran en los métodos de modulación, codificación de los planes (parte 2) y el protocolo de inicialización de los procedimientos (parte 3). Las tarjetas de ambos tipos (A y B) utilizan el mismo protocolo de alto nivel (llamado T=CL) que se describe en la parte 4. El protocolo T=CL especifica los bloques de datos y los mecanismos de intercambio: • Bloque de datos de encadenamiento • Tiempo de espera de extensión • Múltiple activación	Entendemos, aceptamos y cumplimos.

Página/Folio No.183 de 843

d) ISO 14001, ISO 9001, ISO 27001

Los Objetivos de Desarrollo Sostenible (ODS) son un conjunto de metas globales que fueron adoptadas por las Naciones Unidas en 2015. Los ODS se centran en 17 áreas clave, incluida la protección del planeta.

El compromiso de las Naciones Unidas y OACI con la protección del planeta, se refleja en el ODS 13, que tiene como objetivo "adoptar medidas urgentes para combatir el cambio climático y sus efectos". La gestión ambiental ISO 14001 es una norma internacional que proporciona un marco para que las organizaciones gestionen su impacto ambiental. La norma ISO 14001 se basa en los principios de prevención, precaución, responsabilidad, transparencia y participación.

La Norma ISO 9001:2015 determina los requisitos para un Sistema de Gestión de la Calidad, que pueden utilizarse para su aplicación interna por las organizaciones, sin importar si el producto y/o servicio lo brinda una organización pública o empresa privada, cualquiera que sea su rama, para su certificación o con fines contractuales.

ISO/IEC 27001 es un estándar para la seguridad de la información (Information security, cybersecurity and privacy protection - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por la ISO y por la International Electrotechnical Commission y la última versión fue publicada en octubre de 2022.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información según el Ciclo de Deming, o ciclo PHVA (acrónimo de Planificar, Hacer, Verificar, Actuar).

e) ISO 14298 INTERGRAF Nivel Gubernamental

ISO 14298 es un estándar de seguridad altamente reconocido por los productores de documentos de valor que emplean funciones de seguridad añadidas, diseñadas para proteger contra la falsificación de sus características.

ISO 14298 reúne una amplia variedad de controles, incluyendo la seguridad lógica, seguridad física, control de calidad y la seguridad financiera para garantizar la máxima seguridad durante todo el proceso de impresión. Con el uso de esta Norma Internacional, la organización establece, documenta, implementa y mantiene un sistema de gestión de la impresión de seguridad que se revisa regularmente para mejorar continuamente su eficacia.

f) ISO 50001

ISO 50001 es una normativa internacional que tiene como objetivo mantener y mejorar un sistema de gestión de energía en una organización, cuyo propósito es

COPIA SOLUCIONES SMART S.A. RNC. 131636052 Santo Domingo, R.D.

Página/Folio No.184 de 843

el de permitirle una mejora continua de la eficiencia energética, la seguridad energética, la utilización de energía y el consumo energético con un enfoque sistemático. Este estándar apunta a permitir a las organizaciones mejorar continuamente la eficiencia, los costos relacionados con energía, y la emisión de gases de efecto invernadero.

g) CWA 15374:2018

El certificado CWA 15374 confirma el reconocimiento mundial como proveedor de la industria de impresión de seguridad. Garantiza que los aspectos de seguridad y el sistema de gestión serán revisados por terceros independientes (reducción de auditorías externas). Las auditorías se centran en el sistema de gestión de la seguridad. El certificado asegura la diferenciación en el mercado.

h) ISO 15408: PKI Compatible con ICAO para establecer un SOD activado en los datos del chip.

ISO/IEC 15408-1:2009 establece los conceptos y principios generales de la evaluación de la seguridad de las TI y especifica el modelo general de evaluación dado por varias partes de ISO/IEC 15408 que, en su totalidad, está destinado a ser utilizado como base para la evaluación de las propiedades de seguridad de los productos de TI.

Página/Folio No.185 de 843

ESPECIFICACIONES TÉCNICAS ITEM I

TARJETAS

COPY SOLUTIONS INTERNATIONAL, S.A.
RNC: 101028652
Santo Domingo, R.D.

Página/Folio No.186 de 843

I.1 Características generales

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El diseño de todas las características y elementos de seguridad debe ser utilizando soluciones tecnológicas especializadas en la industria de la identidad y deben cumplir con las normativas de OACI Doc 9303. Las tarjetas constituyen un elemento clave y deben ser fabricadas por un integrante del consorcio. Se solicitan tarjetas de policarbonato para las nuevas CI y CIE, con chip sin contacto (contactless) con funcionalidad de Documento de Viaje Electrónico, Firma Electrónica e Identificación Ciudadana. Las características técnicas de las tarjetas se detallan a continuación	Entendemos, aceptamos y cumplimos. Ver punto 1.3 de la propuesta técnica, ITEM I de "Especificaciones Técnicas De Las Tarjetas"

I.2 Tipos de tarjetas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El adjudicatario deberá suministrar los siguientes tipos de tarjetas: • Tarjeta para la Cédula de Identidad y Electoral. • Tarjeta para la Cédula de Identidad. Las tarjetas deben tener las mismas características físicas estipuladas para las dos tarjetas variando únicamente en cuanto al color de la tarjeta (Fondos Preimpresos) y su personalización en el reverso.	Entendemos, aceptamos y cumplimos. Ver el anexo "Diseño de la tarjeta".

I.3 Formato del documento

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Las dimensiones y sus tolerancias vendrán especificadas por el formato ID-1 tal y como se especifica en las normativas ISO/IEC 7816:2019 / ISO/IEC 7810:2019. Las dimensiones, son las siguientes:	Entendemos, aceptamos y cumplimos. Ver propuesta técnica, ITEM I de "Especificaciones Técnicas De Las Tarjetas" en los siguientes puntos:

Página/Folio No.187 de 843

Característica	Valor Mínimo	Valor Máximo	1.3.1.2 Estructura de la tarjeta
Espesor	0.68 mm	0.84 mm	
Largo	85.47 mm	85.72 mm	
Ancho	53.92 mm	54.03 mm	
Será una tarjeta sin contacto conforme normas ISO/IEC 14443 vigentes.			1.3.2 Tarjeta con chip sin contacto

I.4 Materiales

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Tarjeta de polímero termoplástico (policarbonato) de gran resistencia, formada por varias capas (mínimo 5) fusionadas mediante laminación en caliente resistente a la división.	Entendemos, aceptamos y cumplimos. Ver propuesta técnica, ITEM I de "Especificaciones Técnicas De Las Tarjetas" en los siguientes puntos: Capas :1.2.4. , laminado:1.2.5 y Cuerpo: 1.3.1.1
• Tintas de formulación específicas para el sistema de impresión offset.	Tintas: 1.1.1.1, Impresión: 1.2.3.1
• Tintas de seguridad con pigmento sólido.	Tintas:1.1.1.1
• Tintas ópticamente variables.	Tintas:1.1.1.1, Impresión serigráfica 1.2.3.2, OVI:1.3.6.4
• Elemento holográfico de borde a borde.	Holograma propuesto: 1.3.6.5
Todas las tintas deberán cumplir la normativa de durabilidad (ISO 18745) y deberán tener una solidez a la luz de 4 en la escala de las lanas azules. **Requerimiento modificado o aclarado mediante "RESPUESTAS TÉCNICAS A OFERENTES GRUPO 2", No. 1.:** **Modificación/Respuesta:** *"Para favorecer la competencia, se elimina el requisito (de borde a borde) y que sea solo Opcional "Elemento holográfico de borde a borde o 2 elementos holográficos o OVD, uno que proteja la fotografía y otro en cualquier otro lugar de la tarjeta".*	Tintas: 1.1.1.1 *Se cumple con el requerimiento, ofreciendo en nuestra propuesta el elemento holográfico de borde a borde*

I.5 Características de seguridad principales

Página/Folio No.188 de 843

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Los diseños de seguridad del documento serán entregados por el adjudicatario a la JCE en ficheros vectoriales de formato electrónico. La JCE será la propietaria de todos los derechos sobre estos diseños.	Entendemos, aceptamos y cumplimos. Ver propuesta técnica, ITEM I de "Especificaciones Técnicas De Las Tarjetas" en los siguientes puntos:
De manera resumida, explicitado con mayor detalle más adelante, las tarjetas tendrán:	
• Diseño exclusivo de los fondos de seguridad a imprimir en offset, contemplando guilloches, microtextos combinados con motivos o imágenes alegóricas a la República Dominicana constituidos a partir de líneas finas continuas con modulación de su espesor u otras tramas de alta seguridad.	Diseño: 1.2.1, Diseño gráfico seguro: 1.3.5.2, Impresión Offset: 1.2.3.1, Impresión de seguridad: 1.3.6.2, 1.3.6.2.1, 1.3.6.2.4, 1.3.6.2.3, y 1.3.6.2.6
• Motivos impresos en al menos dos colores de tinta visible, los cuales deberán presentar fluorescencia en el anverso al menos ante la exposición de una fuente de luz ultravioleta.	Impresión de seguridad: 1.3.6.2, Tintas UV invisible: 1.3.6.3
• Embozados superficiales en relieve mediante laminación a registro.	Elementos táctiles: 1.3.6.6. Laminado: 1.2.5.
• Estructura lenticular para poder personalizar un CLI o MLI.	MLI /CLI: 1.3.6.7
Ventana Transparente a definir su forma y posición en la tarjeta para imprimir medidas de seguridad que contenga la solución como es la fotografía y la fecha de caducidad de la tarjeta.	Ventana transparente: 1.3.6.8 Así mismo, en la propuesta de Diseño para la CIE y CI, se pueden apreciar cada uno de estos elementos.

I.6 Respecto al sistema de personalización

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Personalización de datos variables mediante grabado láser, siendo para la fotografía láser con impresión en escala de grises.	Entendemos, aceptamos y cumplimos. Ver punto 1.3.4 de la propuesta técnica, ITEM I de

Página/Folio No.189 de 843

	"Especificaciones Técnicas De Las Tarjetas".

I.7 Otras características

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Inclusión de chip sin contacto con funcionalidad de documento de viaje electrónico OACI (ver características del documento lógico sobre características electrónicas y del sistema operativo del presente).	Entendemos, aceptamos y cumplimos. Ver punto 1.3.2 de la propuesta técnica, ITEM I de "Especificaciones Técnicas De Las Tarjetas".

I.8 Características detalladas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
I.8.1 Características de seguridad de la tarjeta **I.8.1.1 Nivel 1 - Características de seguridad que se detectan y verifican mediante simple inspección visual:**	Entendemos, aceptamos y cumplimos. Ver los siguientes puntos del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato":
• Impresión en iris: líneas que durante su recorrido cambian paulatinamente de color sin interrupción del trazo.	1.3.6.2.2
• Guilloches: movimientos lineales ornamentales que se conforman de múltiples curvas entrecruzadas, elaboradas simultáneamente, formando complejos diseños creados mediante software de seguridad.	1.3.6.2.1
• Numismáticos: conjunto de líneas que en su trayecto sufren una deformación y su combinación otorga la sensación de relieve o volumen.	1.3.6.2.6
• Tinta ópticamente variable: aquella que contiene en su estructura finas partículas que dotan el efecto óptico de variabilidad cuando se cambia el ángulo de incidencia de la luz y de observación. Son visibles a la radiación IR.	1.3.6.4
• Elemento difractivo ópticamente variable, situado en el interior de la tarjeta, ocupando parcialmente la zona de la fotografía del titular. Como se explica más adelante, este elemento también puede incluir medidas de nivel 2 y en algunos casos de nivel 3.	1.3.6.5

COPY CSIO SELP S.A. RNC: 101058602 Santo Domingo, R.D.
Página/Folio No.190 de 843

• Elementos táctiles en alto o bajo relieve o con acabado mate, integrados en la superficie de la tarjeta.	1.3.6.6
• Personalización en relieve con el láser de la personalización del nombre y del número de tarjeta.	1.3.4 Asimismo, en la proposición de Diseño para la CIE y CI, se pueden apreciar cada uno de estos elementos.
I.8.1.2 Nivel 2 - Características de seguridad que requieren para su detección del uso de instrumentos simples como lupas de aumento y lámparas de luz:	Entendemos, aceptamos y cumplimos. Ver los siguientes puntos del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato":
• Microtextos. Impresión positivo y negativo.	1.3.6.2.4
• Microtexto de fluorescencia.	1.3.6.3.2
• UV Malla de fondo en microtexto.	1.3.6.3.4
• Errores deliberados en el documento.	1.3.6.2.5
• Tinta invisible que fluórese bajo luz ultravioleta.	1.3.6.3
• Impresión arcoíris visible (impresión arcoíris offset).	1.3.6.2.2
• Impresión arcoíris invisible (impresión arcoíris de fluorescencia UV).	1.3.6.3.3
• Fondos de seguridad visibles e invisibles en la zona de la fotografía, para detectar posibles manipulaciones o sustituciones de esta.	1.3.6.2.1 (imagen) 1.3.6.3.1 (imagen)
• Tipo de fuente no estándar para elementos de texto impresos.	1.3.6.10 Asimismo, en la proposición de Diseño para la CIE y CI, se pueden apreciar cada uno de estos elementos.
I.8.1.3 Nivel 3 - Características de seguridad forensicas que requieren su detección en laboratorio:	Entendemos, aceptamos y cumplimos. Ver los siguientes puntos del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato":
• Tarjeta Multicapa 5 capas mínimo.	1.2.4, 1.3.1.1, 1.3.1.2

Página/Folio No.191 de 843

• Tintas invisibles en el infrarrojo (para permitir la lectura mecánica del documento. Requisito ICAO).	1.3.6.9
• Nanotextos integrados en el elemento difractivo.	1.3.6.5 punto 9
• Fondos de seguridad visibles e invisibles en la zona de la fotografía, para detectar posibles manipulaciones o sustituciones de esta.	1.3.6.2.1 (imagen) 1.3.6.3.1 (imagen) Asimismo, en la proposición de Diseño para la CIE y CI, se pueden apreciar cada uno de estos elementos.
I.8.1.4 Otras características de seguridad • **Elemento óptico variable difractivo:** Parche difractivo transparente de diseño exclusivo para la JCE, combinadas con líneas de Nanotextos y textos de formas moduladas en líneas sinusoidales. Las imágenes deberán poseer textos ocultos visibles en determinados ángulos de observación, pudiendo ser estos, cambiantes en más de un ángulo.	Entendemos, aceptamos y cumplimos. Ver los siguientes puntos de la propuesta técnica, ITEM I "Especificaciones Técnicas de las Tarjetas": 1.3.6.5
• **Elementos Táctiles:** Deberán ser integrados en la estructura de la tarjeta, en el anverso de esta, durante el proceso de fabricación. El diseño de estos elementos deberá ser aceptado por la JCE.	1.3.6.6
• **Ventana Transparente**: Deberá incluir una ventana transparente.	1.3.6.8
• **Estructura Lenticular**: Deberá incluir una estructura lenticular para personalización de un CLI.	1.3.6.7
• **Protección del Retrato del titular**: Mediante elemento ópticamente variable de tipo difractivo transparente, parcialmente coincidente con el retrato del titular.	1.3.6.5
• **Numeración de la Tarjeta**: Se identificará individualmente cada tarjeta mediante número de serie de tarjeta pre personalizado en grabado láser.	El número de serie de tarjeta será pre personalizado en grabado láser como se muestra en los diseños propuestos para la CIE y CI:

RNC: 101038632
Santo Domingo, R.D.

	Asimismo, en la proposición de Diseño para la CIE y CI, se pueden apreciar cada uno de estos elementos.
I.8.1.5 Resistencia de la Tarjeta de acuerdo con ICAO • **Durabilidad:** Se garantizará la durabilidad del soporte por un período de 10 años. • **Deformación:** De tal naturaleza la deformación causada por el uso normal, puedan enderezarse con el equipo de lectura sin afectar el uso de la tarjeta ni su funcionamiento. • **Toxicidad:** No deberá presentar ningún riesgo tóxico en su uso normal. • **Resistencia a productos químicos:** Será resistente a los efectos químicos inherentes al manejo y uso normales, salvo cuando se le haya dotado de sensibilidad química por razones de seguridad. • **Estabilidad térmica:** Se mantendrá legible mecánicamente a temperaturas que oscilen entre -10 °C y +50 °C. La tarjeta no perderá su funcionalidad en caso de quedar expuesto a temperaturas que oscilen entre -35 °C y + 80 °C. • **Humedad:** La tarjeta será legible mecánicamente a una humedad relativa a ambiente del 5 % al 95 % y una temperatura máxima de bulbo húmedo de 25 °C. La tarjeta no perderá su fiabilidad en caso de quedar almacenada o expuesta a una humedad relativa ambiente del 0 % al 100 % (sin condensación).	Entendemos, aceptamos y cumplimos Ver punto 1.3.1 de la propuesta técnica, ITEM I "Especificaciones Técnicas de las Tarjetas"

I.9 Características electrónicas y sistema operativo

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Las funcionalidades electrónicas serán operativas una vez se haga una activación mediante la comparación 1:1 al recoger su tarjeta el ciudadano. Esto es para garantizar que el extravío de una tarjeta no sea de utilidad para el malhechor ya que esa tarjeta no estará activada y será inútil. Además de dar de baja el plástico que tiene su numeración desde que sale de la fábrica donde se compone, el chip añade una seguridad adicional al no estar activa su funcionalidad hasta la recogida por su titular. Las funcionalidades electrónicas de las que estará dotada la nueva tarjeta son tres: • Documento de Viaje Electrónico. • Firma Electrónica. • Identificación Ciudadana. Para adaptarse a un número considerable de posibilidades de lectura eficiente y ágil mediante tecnologías sin contacto como el bluetooth, se ha decidido que la interfaz de comunicaciones sea únicamente por radiofrecuencia. Esto posibilitará su utilización en dispositivos móviles mediante interfaz NFC, además de su utilización en computadoras.	Entendemos, aceptamos y cumplimos. Ver el punto 1.3.2 y 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato" Ver el punto ITEM II ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN - 2.4. Características adicionales "Codificación Chip sin Contacto"

Página/Folio No.193 de 843

No se prevé que el documento pueda cambiar o ampliar su funcionalidad una vez se haya entregado al ciudadano, con excepción de los certificados de firma digital que podrán tener un vencimiento diferente al documento físico en cuyo caso se deberá prever la administración de todo el ciclo de vida de los mismos (generación, actualización y revocación) en la electrónica de los documentos, para el resto de las funcionalidades y como queda claro en el apartado siguiente que describe las características tanto del chip (hardware) del Sistema Operativo que corra sobre él (software asociado), imprescindible para utilizar algunas de las funcionalidades descritas.	
I.9.1 Características del chip sin contacto • CPU de 16/32 bits. • Certificación CC EAL5+ o superior (o equivalente). • Criptoprocesador hardware para operaciones criptográficas. • Clave simétrica (Triple DES con clave de hasta 168 bits, AES hasta 256 bits). • Clave pública (RSA con longitud de clave de hasta 4096 y ECC con clave de hasta 512 bits). • Hash SHA1 y SHA2. • Generador de números aleatorios de acuerdo a AIS31 Protección contra descargas ESD. • Reloj interno asíncrono Número de serie único. • Firewalls de seguridad entre particiones de memoria. • Memoria no volátil necesaria para la incorporación de las aplicaciones requeridas y los datos especificados en el presente punto 1.2.4. Características electrónicas y del sistema operativo. • Retención de datos en memoria no volátil de al menos 10 años. • Al menos 500.000 ciclos de lectura / escritura garantizados Interfaz de RF ISO/IEC 14443 A/B de hasta 848kbits/s, pudiendo ofrecer modos de transmisión RF mejorados.	Entendemos, aceptamos y cumplimos. Ver punto 1.3.2 de la propuesta técnica, ITEM I "Especificaciones Técnicas de las Tarjetas".
I.9.2 Características del Sistema Operativo • Protocolo de transmisión de acuerdo con ISO/IEC 14443 A/B Interfaz de comandos de acuerdo a ISO/IEC 7816-4 y PCSC. • UID / PUPI aleatorio. • Certificación Common Criteria EAL4+ o superior (o equivalente). • En caso de que el Sistema Operativo sea basado en JavaCard, se deberá bloquear la posibilidad del agregado de nuevas aplicaciones una vez incorporadas las aplicaciones requeridas. **Deberá incluir las siguientes funcionalidades:** • Documento de Viaje Electrónico de acuerdo con ICAO 9303. • Firma Electrónica. • Identificación Ciudadana.	Entendemos, aceptamos y cumplimos. Ver punto 1,3.2 de la propuesta técnica, ITEM I "Especificaciones Técnicas de las Tarjetas".

Página/Folio No.194 de 843

Funcionalidad de documento de viaje electrónico: Deberá poder soportar: • SAC (Supplemental Access Control). • EAC (Extended Access Control). • AA (Active Authentication)	
Funcionalidad de Firma Electrónica: • Acceso protegido mediante PIN / PUK. • Algoritmos de firma RSA y ECDSA. • Soporte para claves RSA en formato CRT y en formato normal (exponente privado, exponente público y módulo). • Claves RSA con soporte para componentes p y q de longitud variable. • Capacidad de almacenar, generar y usar claves RSA de, como mínimo, 4096 bits de longitud. • Soporte de diversas curvas ECDSA, incluyendo las más habituales (NIST P-256, Brainpool, etc. • Operaciones de firma digital. • Intercambio de claves de sesión o simétricas entre dos entidades basado en RSA/ECDSA/ECDH. • Claves almacenadas en ficheros/elementos independientes. • Condiciones de acceso independientes para cada clave/elemento. • Estructura interna de ficheros según el estándar ISO/IEC 7816-15 (PKCS#15). • Deberá disponer de capacidad de memoria suficiente para almacenar hasta 4 certificados, con sus correspondientes claves, incluyendo el caso de claves RSA 4096. • Securización de los mensajes transmitidos entre la tarjeta y el terminal mediante canal seguro de acuerdo a CEN14890 o equivalente. • Confidencialidad de los datos transmitidos mediante triple DES / AES. • Autenticación de la información intercambiada entre las dos partes; incorporación de checksum criptográfico de tipo MAC según ANSI X9.19 y DES	Entendemos, aceptamos y cumplimos. Ver punto 1,3.2 y 1.3.3. de la propuesta técnica, ITEM I "Especificaciones Técnicas de las Tarjetas".

Página/Folio No.195 de 843

• Protocolo de establecimiento de las claves de sesión basado en el esquema propuesto en ISO/IEC 9798-3 Authentication SASL Mechanism. • Claves de sesión derivadas a partir de información generada por las partes involucradas en el establecimiento del canal seguro; el cálculo de las claves se realiza según ANSI X9.63. • Software de gestión y drivers: o Drivers de la tarjeta (PKCS#11, CSP, Card Module, etc). o Software de gestión que permita gestionar las operaciones más habituales con la tarjeta; por ejemplo, cambio de PIN, desbloqueo de PIN, borrado de certificados, etc. Deberá garantizar el funcionamiento del documento en distintos sistemas operativos (Windows, Linux, MacOS). Deberá garantizar el funcionamiento del documento en distintos navegadores. o Se deberán aportar librerías o SDKs que faciliten el desarrollo de aplicaciones para dispositivos móviles, con sistemas operativos Android e iOS. o El software suministrado deberá ser actualizado, adecuándolo a nuevos SO, Navegadores, corrección de bugs, etc., durante el tiempo de vida del proyecto.	
Funcionalidad de Identificación Ciudadana: • Se almacenarán los datos de filiación del ciudadano de manera estructurada. • El acceso a los mismos se realizará por medios seguros. • Preferiblemente, de acuerdo con la Guía Técnica TR-03110 del BSI o similar.	Entendemos, aceptamos y cumplimos. Ver punto 1.3.2 y 1.3.3 de la propuesta técnica, ITEM I "Especificaciones Técnicas de las Tarjetas".
Muestras: El oferente deberá, en el momento de entregar las ofertas, suministrar diez (10) tarjetas genéricas de policarbonato, con las mismas especificaciones técnicas que se solicitan para esta licitación y con el detalle y la explicación de las medidas de seguridad que el oferente está ofreciendo, explicando en un documento, cuáles son los requisitos técnicos cumplidos y las medidas de seguridad ofertadas, excepto el diseño. Este es un requisito obligatorio (mandatorio) no subsanable.	Para las muestras solicitadas, entendemos, aceptamos y cumplimos. Se entregan 10 tarjetas en Policarbonato junto con un documento donde se explica cada uno de los elementos de seguridad solicitados y que se encuentran presentes en por lo menos una de las tarjetas enviadas.

Página/Folio No.196 de 843

ESPECIFICACIONES TÉCNICAS ITEM II
MÁQUINAS DE IMPRESIÓN

Página/Folio No.197 de 843

II.1 Máquinas de impresión

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Máquina de impresión modular. • La tecnología de personalización deberá ser de grabado láser, siendo para la fotografía láser con escala de grises. • El sistema de personalización propuesto será un sistema de escritorio. • Tiene que ser un sistema de producción industrial sólido, para funcionamiento de la máquina en producción de 3 turnos (24 horas) si así se requiere. • La máquina debe estar equipada con una conexión de alimentación monofásica de 110/220 V para su funcionamiento. • La máquina debe estar equipada con una conexión de alimentación monofásica de 230 V para su funcionamiento. **Requerimiento modificado o aclarado mediante "RESPUESTAS TÉCNICAS A OFERENTES GRUPO 1", No. 7.:** **Consulta:** En el bullet 5 se especifica alimentación monofásica de 110/220V y en el bullet 6 se menciona que la alimentación monofásica debe ser 230V. Solicitamos a la JCE aclarar y especificar cuál aplica. **Modificación/Respuesta:** *Aplica 110/220V.*	Entendemos, aceptamos y cumplimos. Ver propuesta técnica, ITEM II de "Especificaciones técnicas de las máquinas de impresión" en os siguientes puntos: 2.1. Beneficios de la Solución y 2.3 Módulo Laser
• Cada impresora de personalización debe estar equipada con una fuente de alimentación ininterrumpida para cubrir los PC integrados y la producción durante al menos dos minutos.	Ver propuesta técnica, ITEM II 2.2 Criterios de desempeño únicos.
• El peso de cada máquina debe ser de 80 kg máximo. Su volumen máximo no debe exceder de 0,70 m2. • El sistema debe estar equipado con una pantalla para la visualización de los trabajos.	2.3 Módulo Laser. Ver "Tabla de características" de la CLM600
• Debe estar disponible un módulo de codificación de chip. Debe permitir la codificación de tarjetas inteligentes basadas en contacto y sin contacto según ISO 14443 tipo A y B.	2.4 "Características Adicionales"
• El sistema debe poder grabar imágenes, firmas, textos y códigos de barras (códigos de barras 1D y 2D), así como microtexto, imágenes fantasma y logotipos en tamaños variables. • El sistema debe admitir el marcado láser táctil, así como la personalización de la función de la tarjeta CLI.	2.1. Beneficios de la solución

Página/Folio No.198 de 843

• Para garantizar la calidad, se debe integrar un sistema de control óptico de la tarjeta para una inspección completa de la tarjeta en el anverso y el reverso de forma independiente. Además, el sistema de control óptico debe realizar un proceso de inspección antes del grabado láser para alinear el diseño del grabado con el tipo de tarjeta especial. La función de detección de CLI también debe estar disponible y debe funcionar independientemente de los demás procesos de inspección de tarjetas. Se requiere una alineación de grabado láser individual del proceso de calidad CLI.	2.4. Características Adicionales Ver: • El sistema de posicionamiento automático XY • Lectura OCR/OCV • Lectura de códigos de barra Aseguramiento de Calidad
Es necesario que los componentes de inspección sean ajustables para procesar diferentes diseños de tarjetas mediante el uso de una unidad de iluminación LED múltiple con diferentes longitudes de onda. **Requerimiento modificado o aclarado mediante "RESPUESTAS TÉCNICAS A OFERENTES GRUPO 4", No. 107.: Consulta:** ¿Solicitamos a la JCE confirmar nuestro entendimiento de que el LED múltiple se refiere a los componentes del sistema de iluminación? **Modificación/Respuesta:** *Es correcto. El término "LED múltiple" en el requisito mencionado se refiere a los componentes del sistema de iluminación.*	ITEM II 2.4 "Características Adicionales" "Sistema de posicionamiento automático XY"
• La máquina debe tener su propio PC integrado con su propio sistema operativo y software de la maquina. • El sistema operativo de la máquina debe ser WINDOWS. **Requerimiento modificado o aclarado mediante "RESPUESTAS TÉCNICAS A OFERENTES GRUPO 3", No. 27.:** **Modificación/Respuesta:** *El sistema operativo de la PC debe de ser Windows. Las impresoras pueden ser WINDOWS o LINUX.*	2.3 Módulo Laser Ver "Tabla de caracteristicas" de la CLM600
• Debido a una integración de red obligatoria, los sistemas propuestos necesitan tener una interfaz TCP/IP para funcionar con ellos como una estación de trabajo completa con su propia dirección IP, que puede definirse y ajustarse.	2.3 Módulo Laser Ver "Tabla de características" de la CLM600
• La solución propuesta debe ser capaz de identificar los registros inconsistentes antes de proceder con la impresión de la tarjeta. Si el registro enviado por la interfaz de integración está incompleto, por la ausencia de alguno de los datos requeridos, el registro debe ser rechazado.	2.4 "Características Adicionales": "Aseguramiento de calidad"

Página/Folio No.199 de 843

• La solución propuesta solo debe almacenar los datos de forma temporal. El almacenamiento temporal se refiere a que en ningún momento la solución almacenará registros por más de un día. Es decir, una vez impresa y entregada la tarjeta, el registro debe eliminarse de forma criptográfica de todos los servidores de la solución donde este almacenada. El procedimiento de eliminación de los registros ya procesados debe ser aprobado por la JCE.	ÍTEM II - Módulo láser acápite: opciones de la CLM 600 - aseguramiento de calidad.
• El tipo de láser debe ser láser de fibra mínimo de 10W. **Requerimiento modificado o aclarado mediante "RESPUESTAS TÉCNICAS A OFERENTES GRUPO 1", No. 8.:** **Modificación /Respuesta:** *Se acepta la propuesta. Se requiere 20W del láser de las impresoras.*	2.3 Módulo Laser Ver "Tecnología de personalización" en tabla de características de la CLM600
• Deberá ser posible definir los ejes de referencia sobre el insumo a fin de configurar el posicionamiento para el marcado láser. Esta definición deberá ser tanto automática como plausible de definirla por una interfase accesible por los técnicos de la JCE.	2.4 "Características Adicionales", El sistema de posicionamiento automático XY.
• Los módulos que integran el equipamiento deberán poder recibir modificaciones tales que permitan reubicar estaciones o agregar instancias productivas sin necesidad de reemplazar el equipamiento. **Requerimiento modificado o aclarado mediante "RESPUESTAS A OBSERVACIONES TÉCNICAS GRUPO 3", No. 14.:** **Consulta:** No entendemos la necesidad de módulos o agregar instancias productivas, agradeceríamos a la convocante si pudiera damos más contexto sobre este requerimiento. **Modificación /Respuesta:** *Se aclara que este requerimiento se elimina.*	N/A
La eficiencia productiva de la solución tecnológica ofrecida deberá ser superior al NOVENTA POR CIENTO (90%), calculada según cantidad de tarjetas efectivas producidas por hora / capacidad de máquina por hora informada por el fabricante.	2.3. Módulo Láser Ver Rendimiento (TPH)

Página/Folio No.200 de 843

• La calidad de las impresoras debe mantenerse a lo largo de los diez años de la contratación. Tendrán garantía mínima por dos (2) años. Cada oferente, debe indicar en su propuesta, la vida útil de la pieza de cada impresora que produce el láser y queda comprometido a que su solución de impresión mantendrá la calidad de las impresoras durante todo el tiempo que lo exige el contrato, obligándose a reemplazar lo necesario y las veces que sea conveniente para cumplir con esta exigencia de calidad de las impresoras. **Requerimiento modificado o aclarado mediante "RESPUESTAS A TÉCNICAS A OFERENTES GRUPO 4", No. 112.:** **Preguntas:** Favor confirmar que lo siguiente: "Cada oferente, debe indicar en su propuesta, la vida útil de la pieza de cada impresora" se debe interpretar de forma correcta como sigue: "Cada oferente, debe indicar en su propuesta, la vida útil de las piezas de cada impresora" **Respuesta JCE:** *Es correcto*	2.6 Condiciones de garantía
• Los equipos deberán disponer de un control de calidad y registrar los eventos identificados, garantizando: o Evaluación de funcionamiento del chip antes de su personalización. o Correcto grabado del chip después de su personalización. o Control de información grabada durante la personalización de la tarjeta de policarbonato. o Control de espesor, orientación de la tarjeta y referencia. o Control de MRZ (ZLM). o Control de texto. o Control de los datos del chip. o Control de los datos gráficos.	2.4 "Características Adicionales"Ver Aseguramiento de Calidad.
• El fabricante deberá describir el flujo de trabajo y los diferentes criterios que podrían ser utilizados para el control de calidad adicional. Las impresoras deben contener un módulo de administración de diagnósticos de impresión para el control de cantidades de tarjetas impresas por cada hora de uso. **Requerimiento modificado o aclarado mediante "RESPUESTAS A TÉCNICAS A OFERENTES GRUPO 4", No. 111.:** **Consulta:** ¿Solicitamos a la JCE confirmar nuestro entendimiento de que el LED múltiple se refiere a los componentes del sistema de iluminación? **Modificación/Respuesta:** *Es correcto. Este requerimiento debe ser cumplido como parte de la solución completa de personalización. Los controles de calidad son dispuestos por la solución de personalización como parte de la implementación del controlador del equipo como sistema. Esto asegura que se mantenga un alto nivel de control de calidad en todo el proceso de impresión, garantizando que las impresoras administren de manera eficiente los diagnósticos y el control de cantidades de tarjetas impresas por cada hora de uso.*	2.1. Beneficios de la solución

Página/Folio No.201 de 843

• Control ATS (Answer To Select) a la entrada, para verificación del correcto funcionamiento del chip de la tarjeta.	2.4 "Caracteristicas Adicionales" Ver: Codificacion Chip sin contato
• Los equipos deberán coniar con los accesorios, equipos auxiliares y cualquier otro implemento necesario para su operación según las prestaciones especificadas en el presente pliego.	Entendemos, Aceptamos y Cumplimos.
• Deben permitir el rechazo de credenciales defectuosas por inspección y control de chip.	2.4 "Características Adicionales"Ver: Aseguramiento de Calidad y Codificación Chip sin Contacto

II.2 Personalización

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• La tecnología de personalización deberá ser de grabado láser, siendo para la fotografía láser en escala de grises mínimo 600 DPI.	Entendemos, aceptamos y cumplimos. Ver los siguientes puntos: 2.1. Beneficios de la solución
• Alimentador Automático min 100 Tarjetas. • Bandeja salida mínimo 100 tarjetas.	2.3. Módulo Láser, Tabla de características relevantes.
• Velocidad MÍNIMO 50 por hora incluyendo laser a doble cara, codificación, verificación QA.	2.3. Módulo Láser Ver Rendimiento (TPH)
• Personalización de los datos (según punto II.2.1). • Conjunto mínimo de datos personales y del documento de acuerdo con la normativa OACI (Doc. 9303). • Líneas de lectura mecánica en la zona inferior del reverso de la tarjeta (zona de lectura mecánica o ZLM). • Imagen facial en escala de grises. • Imagen fantasma o secundaria en escala de grises, en posición a definir.	2.1. Beneficios de la solución

Página/Folio No.202 de 843

• El sistema deberá disponer de un acceso de nivel de operador. • Cada entrada del operador deberá quedar reportada, con el fin de identificar cada usuario que accede a la máquina. • El sistema de personalización debe diseñarse para un manejo de documentos fácil y amigable para el operador con una separación de entrada de tarjeta sin fricción y solo la persona autorizada puede acceder a la entrada.	2.3. Módulo Láser Ver - Monitor de estado - Diagnóstico
• El proceso de personalización de las tarjetas deberá ser tipo modular, de tal forma que la tarjeta sea trasladada automáticamente de una etapa a otra y hasta el final de su personalización (en línea) sin intervención manual del operador. La impresora deberá imprimir ambas caras de la tarjeta en un sólo proceso completo de impresión, sin volver a pasarla por el proceso.	2.1. Beneficios de la solución.
• Dada la obligatoriedad de integración a una red, los sistemas propuestos deberán disponer de interfaz TCP / IP para trabajar con ellos como una estación de trabajo completa con su propia dirección IP, la cual podrá ser definida y ajustada oportunamente. • El sistema de personalización (software y maquinaria) debe ser capaz de imprimir diferente información acorde al menos el lay out según punto II.2.1; deberá personalizar, según sea necesario, personas mayores de edad, menores de edad, naturalizadas, extranjeras, etc. Debe ser posible la edición del lay out accesible por la JCE. • La interfaz del equipo de personalización deberá recibir un XML con los datos a personalizar. Este XML será generado por la plataforma de tarjetas de la JCE y almacenado en un servidor de archivos entre la plataforma y los equipos de personalización. El equipo deberá preparar los datos para realizar la personalización de las credenciales de forma totalmente automática. Además de la interfaz, cada sistema deberá incluir una PC interna con sistema operativo vigente.	2.3. Módulo Láser Ver "Diagnóstico" "Ver Integración de Software"
• A efectos del desarrollo de aplicaciones de personalización del chip, el fabricante deberá proporcionar un sistema de desarrollo de software. Este sistema incluirá todos los elementos hardware y software necesarios para desarrollar, compilar, depurar y probar las aplicaciones de personalización en un entorno de pruebas completamente aislado de la máquina de producción real. Los elementos de software deberán ser: un SDK de desarrollo con los plug-ins, librerías o módulos adecuados para desarrollar aplicaciones de personalización del chip (para ser utilizado por la JCE o terceros). • Además del sistema de desarrollo y emulación descrito anteriormente, el fabricante proporcionará toda la documentación necesaria, incluidos ejemplos descriptivos funcionales, para facilitar el desarrollo de estas aplicaciones a desarrolladores entrenados.	"Ver Integración de Software"

Página/Folio No.203 de 843

• En el caso de que el fabricante proporcione la aplicación de personalización del chip, deberá aportar el código fuente de este, que deberá ser plenamente funcional tanto en la máquina de producción real como en el entorno de desarrollo. **Requisito modificado o aclarado por:** *RESPUESTAS TÉCNICAS A OFERENTES, GRUPO 3, PREGUNTA 34.* **Modificación/Respuesta:** *La nueva impresora tendrá un SDK (Software Development Kit) para que se pueda integrar con el sistema de captura de datos de la JCE. Se refiere por tanto al SDK de personalización para la integración de la impresora con el sistema de captura de datos que deberá ser proporcionado por el licitante. No será necesario aportar el código fuente, siempre y cuando el fabricante suministre un SDK para la interacción con la impresora.* • Los sistemas de personalización deben estar equipados con el software interno de gestión de datos, que proporciona interfaces de usuario claras e iguales para la integración en la red del proyecto. El equipo deberá preparar los datos para realizar la personalización de las credenciales de forma totalmente automática.	
• El sistema de personalización debe ser capaz de imprimir medidas de seguridad definidas en este pliego. Deberá contar con medidas de seguridad Nivel 1, Nivel 2 y Nivel 3.	2.1. Beneficios de la Solución
• Se incluirá la generación de informes de producción, a definir por el organismo (por ejemplo, informes de la producción de un determinado DNI, Informes de la producción por máquina -cantidad y detalle de CI y CIE-, o informes de la producción en un período de tiempo definido por el usuario en una determinada máquina - cantidad y detalle de CI y CIE -). En cada sistema de personalización se debe crear y almacenar información histórica de listas de trabajos y estadísticas de producción durante un periodo de al menos cuatro semanas.	2.3. Módulo Láser Ver Diagnóstico
II.2.1 Formato (Lay out) de las tarjetas CIE **II.2.2 Formato (Lay out) de las tarjetas CI**	Entendemos, aceptamos y cumplimos.

Página/Folio No.204 de 843

Estos formatos (Lay out) son sugeridos, pero no es el diseño final a falta de aprobación en el momento de la fabricación de la nueva cédula.

Página/Folio No.205 de 843

ESPECIFICACIONES TÉCNICAS ITEM III

PKI

Página/Folio No.206 de 843

III.1 Características generales PKI

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El proveedor tendrá que implementar la siguiente PKI.	Entendemos, aceptamos y cumplimos.
PKI para seguridad: En el caso de documentos electrónicos, la PKI se utiliza principalmente para garantizar la autenticidad del documento electrónico y la integridad de los datos almacenados en el chip del mismo. Esto implica verificar la autenticidad del documento electrónico, así como garantizar que los datos no hayan sido modificados desde su emisión.	Ver Item III Especificaciones técnicas de las PKI – CA en los siguientes puntos
PKI para Firma Digital: La PKI utilizada para la firma digital se utiliza para garantizar la autenticidad, integridad y no repudio de documentos electrónicos. Se utiliza para firmar electrónicamente documentos como contratos, formularios, transacciones financieras, entre otros. El objetivo es proporcionar una forma segura de verificar la identidad del firmante y asegurar que el documento no haya sido alterado después de ser firmado. **Requisito modificado o aclarado por:** *RESPUESTAS TECNICAS A OFERENTES, GRUPO 1, PREGUNTA 3.* **Modificación/Respuesta:** *1. La "PKI de Firma Digital" tiene el objetivo de habilitar a los ciudadanos con certificados que les permitan gozar de los servicios de la criptografía.* *La "PKI de Firma Digital" debe tener su propia cadena de confianza completa, y respectivamente para sus niveles debe estar en línea o fuera de línea, de acuerdo con la infraestructura que el proveedor seleccionado ofrezca en su propuesta técnica. La PKI que emitirá certificados y permitirá firmar documentos a los ciudadanos (PKI ciudadana) debe prever implementar 2 tipos de Autoridades certificadoras (AC): a) la AC raíz, que será la AC del JCE y se empleará únicamente para emitir certificados de ACs subordinadas (operativas); b) La AC subordinada u operativa se encargará de emitir los certificados a los ciudadanos. Asimismo, se precisa que la PKI ciudadana no requiere compatibilidad con ICAO, debido a que su uso será para firmar en aplicaciones de la JCE o comerciales de terceros*	3.4. PKI Ciudadana – PKI Subordinada x509
En resumen, aunque ambas utilizan una infraestructura de clave pública (PKI) para garantizar la seguridad y la autenticidad, las implementaciones específicas difieren en función del uso y los requisitos de seguridad de cada sistema.	3.5. Infraestructura GET Trust

Página/Folio No.207 de 843

Conforme a las especificaciones de la OACI establecidas en el Doc 9303 vigente, el adjudicatario deberá implementar la infraestructura de criptografía basada en claves públicas (PKI), para emitir y revocar certificados digitales que se utilizarán para firmar electrónicamente las tarjetas electrónicas (CSCA) y para verificar tarjetas electrónicas (CVCA). La infraestructura de llave publica será utilizada para la emitir los certificados y firmar digitalmente las identidades digitales, y poder asegurar el ciclo de vida de los certificados y las verificaciones de identidad que menciona el estándar ISO 18013-5. **Requisito modificado o aclarado por:** *RESPUESTAS TECNICAS A OFERENTES, GRUPO 1, PREGUNTA 3.* **Modificación/Respuesta:** 1. *La "PKI de Firma Digital" debe ser una infraestructura independiente que permita la firma electrónica de los Documentos de Identificación electrónicos siguiendo las recomendaciones del Doc 9303 de la OACI para los mecanismos de acceso de Control de Acceso Básico (BAC), Control de Acceso Suplementario con el Protocolo de Establecimiento de Conexión con Contraseña (SAC-PACE). Las características técnicas generales de las aplicaciones en las que se podría integrar firma electrónica son principalmente aplicaciones web que pueden consumir servicios tipo APIRest. Se debe prever por el proveedor que la tecnología propuesta para la PKI ciudadana deberá poder ser integrada a las aplicaciones de la JCE. Por lo que debe proveerse de los APIS y web Services necesarios para su integración a aplicaciones de la JCE.*	3.2. GET Autoridad de certificación de confianza – CSCA
Deberá cumplir con ISO 15408 - Nivel de Garantía de Evaluación de Criterios Comunes (EAL) 4+ o superior.	3.2. GET Autoridad de certificación de confianza – CSCA Se adjunta Certificado - Common Criteria EAL4+
El hardware deberá responder a los requerimientos para implementar la infraestructura de criptografía basada en claves públicas (PKI). **Requisito modificado o aclarado por:** *RESPUESTAS TECNICAS A OFERENTES, GRUPO 1, PREGUNTA 10.* **Modificación/Respuesta:** *3. Componentes en premisa:* ▪ *Módulos de Seguridad de Hardware (HSMs)* ▪ *Autoridad de Certificación (CA)* ▪ *Autoridad de Certificación de Firma de País (CSCA)* ▪ *Autoridad de Certificación de Firma de Documentos (DSCA)* ▪ *Infraestructura de Gestión de Claves Seguras (KMI)* *En la nube (compatible con los servicios en la nube de Azure):* ▪ *Sistema de Gestión de Certificados (CMS)* ▪ *Lista de Revocación de Certificados (CRL) / Protocolo de Estado de Certificado en Línea (OCSP) Respondedor*	3.2. GET Autoridad de certificación de confianza – CSCA (CSCA, CA, KMI, CMS, CRL, Repositorio de PKI 3.3. Firmado de Documentos GET Trust (DSCA) 3.6. Módulo de Seguridad por Hardware (HSM)

Página/Folio No.208 de 843

▪ *Repositorio de PKI* *Servicios adicionales no críticos*	
El oferente deberá incluir en su propuesta, toda la infraestructura física necesaria para la implantación, ejecución y mantenimiento de la PKI.	Ver: 3.6. Módulo de seguridad por Hardware (HSM)
El software deberá responder a los requerimientos para implementar la infraestructura de criptografía basada en claves públicas (PKI) descrita anteriormente, y los respectivos hardware y software requeridos para cargar los firmantes de documentos y los CRL, conforme a las especificaciones funcionales de la OACI establecidas en el Doc. 9303 vigente.	3.3. Firmado de Documentos GET Trust Ver ICAO Document Signer
En concreto se solicita:	3.2. GET Autoridad de certificación de confianza – CSCA
• CSCA (Country Signing Certificate Authority): Autoridad encargada de firmar certificados para entidades gubernamentales o documentos de importancia nacional. • El CSCA utilizará algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante. • El CSCA utilizará algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante. • El CSCA deberá elaborar una lista de revocación de certificados ICAO 9303.	
• El CSCA debe trabajar en un entorno sin conexión.	3.5. Infraestructura GET Trust
• El CSCA utilizará una autenticación multifactorial para el inicio de sesión en la interfaz de administración.	3.3. Firmado de Documentos GET Trust Ver Autenticación basada en WEB
• El CSCA será capaz de emitir certificados VDS Signer conformes a la OACI 9303.	3.3. Firmado de Documentos GET Trust Ver ICAO Document Signer
• El CSCA debería ser capaz de emitir certificados de firmante de lista maestra.	3.2. GET Autoridad de certificación de confianza – CSCA (Escrow Management)
• DS (Document Signer): Entidad específica para la firma de documentos digitales, garantizando su autenticidad e integridad.	Ver: 3.3. Firmado de Documentos GET Trust
• El DS dispondrá de un servicio web SOAP al que llamar para la generación de SOD y creará un SOD conforme a la OACI 9303.	Ver: 3.3. Firmado de Documentos GET Trust (ICAO Document Signer)

Página/Folio No.209 de 843

• El DS utilizará algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante.	Ver: 3.6. Módulo de seguridad por Hardware (HSM)
• El DS que deberá utilizar una autenticación multifactorial para el inicio de sesión en la interfaz de administración debería avisar claramente antes de que finalice el tiempo de uso de la clave del certificado actualmente utilizado.	Ver: 3.3. Firmado de Documentos GET Trust Ver Autenticación basada en WEB
• Se utilizará un DS separado para firmar los DTC para la aplicación Tarjeta Digital de la JCE. Este DS independiente requerirá una interfaz para acceder al sistema back-end de la JCE. **Requerimiento adicionado:** *RESPUESTAS TECNICAS A OFERENTES, GRUPO 1, PREGUNTA 3.* **Modificación/Respuesta:** *4. La "PKI de Firma de Documentos" Se confirma que si se requiere que el proveedor considere una Autoridad de sellos de tiempo (TSA) como parte de los componentes de la PKI ciudadana, que pueda ser sincronizada con la hora oficial de la República Dominicana y que las llaves del servicio puedan estar almacenadas en software o hardware. Asimismo, que las timestamps sea parte de los elementos que tiene cada firma electrónica*	Ver: 3.2. Autoridad de Certificación de Confianza – CSCA "Sellado de Tiempo"

III.2. Autoridad de Certificación (CA) de firma de país (CSCA)

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El adjudicatario deberá implementar una CA con especificaciones y un marco que deberá cumplir con el Documento 9303 de la OACI vigente sobre el esquema de Firmas Digitales PKI propuesto para autenticar la tarjeta electrónica que ofrece acceso de sólo lectura de Chip de Circuito Integrado (IC).	Entendemos, aceptamos y cumplimos. Ver los siguientes puntos del Item III Especificaciones técnicas de las PKI – CA 3.3. Firmado de Documentos GET Trust Ver ICAO Document Signer

Página/Folio No.210 de 843

El adjudicatario instalará para la JCE, y en las propias instalaciones de la JCE, los sistemas y equipos necesarios para generar conjuntos de claves para diferentes periodos de tiempo que se utilizarán para computar las Firmas Digitales que se aplicarán para la firma de los Certificados. Los sistemas o instalaciones propuestos deberán estar bien protegidos de cualquier acceso externo o no autorizado a través del diseño inherente y las instalaciones de seguridad de hardware. La ubicación de los sistemas o instalaciones propuestos será divulgada al adjudicatario	Item III Especificaciones técnicas de las PKI – CA
Los certificados de CA de firma de país se generarán en una infraestructura de CA sin conexión, altamente protegida. El oferente deberá presentar la infraestructura aportando justificaciones adecuadas para su selección. Es necesaria la compatibilidad en la generación de certificados digitales X509. El oferente debe de incluir en su propuesta la inclusión, instalación, configuración y puesta en marcha de un dispositivo HSM certificado con FIPS 140-2 o mayor, que será instalado en las instalaciones de la ICE. Toda la infraestructura adicional (racks, cableado, etc.), deberá de suministrarla el proveedor adjudicado con las siguientes características (similares o superiores):	3.4. PKI Ciudadana – PKI Subordinada x509

Requerimiento		Respuesta Consorcio "Identidad 4.0 RD"
Módulos de Seguridad por Hardware (HSM)		Entendemos, aceptamos y cumplimos. Item III Especificaciones técnicas de las PKI – CA **Ver:** **3.6. Módulo de Seguridad por Hardware (HSM)**
APIS criptográficos (podrá soportar)	• PCKCS#11 • Java • Microsoft CAPI y CNG • OpenSSL.	
Algoritmos criptograficos asimétricos(podrá soportar)	• RSA • DSA • ECC • ECDSA • ECDH • Ed25519 • ECIES • Brainpool curves (nombrados y definidos por el usuario) • Diffie Hellman (DH)	

Página/Folio No.211 de 843

Algoritmos criptográficos simétricos(podrá soportar)	• AES • AES-GCM • DES • 3DES • ARIA • SEED • RC2 • RC4 • RC5 • CAST	
Condiciones de Operación	• Voltajes de operación: 110/220 V. • Temperatura de operación: 10°C- 40°C. • Humedad relativa no condensada: 20% a 90% • MTBF mínimo 150,000 horas a 25°C / 77°F	
Certificaciones de seguridad	• FIPS 140-2 Nivel 3 – Password and Multi-Factor (PED) • eIDAS CC EAL4+	
Características Generales	• Generación de números aleatorios reales (TNRG) • Copia de seguridad de la tarjeta inteligente del material clave • Doble conector de red • Administración remota (vía red) • Administración local • Soportar interface gráfica del HSM • Opciones múltiples para autentificación y control de acceso. • Múltiple integración para aplicaciones de PKI, servicios de encriptación • Separación de tareas • Sistemas operativos soportados: Windows y Linux • Rendimiento nominal mínimo (firmas RSA /segundo, 2048 bit, modo Bulk): 25 • Habilitado para operación en cluster (alta disponibilidad). • Debe permitir la importación / exportación de llaves internas a través de un método seguro, desde y hacia otro HSM. • El HSM deberá proveer mecanismos de detección de apertura llamados "Tamper Evidence" y ser resistentes al forzado, característica denominada "Intrusion Resistant".	
La clave privada de la CA firmante del país se utilizará para firmar certificados de firmante de documentos. El certificado DS será emitido por la CSCA. La PKI será responsable de la generación de claves/certificados de seguridad requeridos. El adjudicatario mantendrá la infraestructura actualizada anualmente y deberá garantizar su conformidad cuando sea requerida por una puesta al día de las normas y especificaciones contenidas en el Documento 9303, o cuando sea requerido por la JCE.		**Ver: 6.1. Plan de mantenimiento para PKI**

Página/Folio No.212 de 843

ESPECIFICACIONES TÉCNICAS ITEM IV
TARJETA DE IDENTIDAD DIGITAL

Página/Folio No.213 de 843

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El oferente deberá proveer un sistema completo de emisión de credenciales contenidas en dispositivos móviles, La solución debe contener todo el software, hardware, licencias y cualquier otro requisito necesario para implementar el servicio de identificación digital en dispositivos móviles y cumplir con los estándares ISO18013-5 así como estar preparada para cumplir con el estándar de la OACI ("Guiding Core Principles for the Development of Digital Travel Credential (DTC) de octubre de 2020"). Para garantizar la seguridad del documento, este debe estar confeccionado siguiendo lineamientos para la creación de estructuras de datos lógicos para documentos de identificación (ICAO DOC 303-10). **Requisito modificado o aclarado por:** *RESPUESTAS, ACLARACIONES Y ENMIENDAS ADMINISTRATIVAS, GRUPO 4, PREGUNTA 34.* **Modificación/Respuesta:** **DONDE DICE:** *ICAO DOC 303-10* **DEBE DECIR:** *ICAO DOC 9303*	Entendemos, aceptamos y cumplimos. Item IV Especificaciones técnicas de la Tarjeta de Identidad Se adjuntan certificados: • ISO 18013 IOS • ISO 18013 Android UL Verification Services Inc.- Global Enterprise Technologies Corp. 18013 Parte 5
El oferente deberá implementar la solución de identidad digital antes de 26 SEMANAS tras la firma del contrato que será administrado por la JCE integrada a su vez al sistema nacional de identidad mediante el uso de API'S, para la identificación y verificación de la identidad de los ciudadanos.	Ver carpeta 2/ seccion 3 / N°1 Se adjunta Cronograma
La tarjeta digital podrá ofrecer (si las leyes lo permiten) las mismas garantías jurídicas al titular que el CEI o CI. Los datos entregados deberán ser firmados electrónicamente. Esta firma electrónica certificada de los datos permitirá que terceros puedan validar la integridad y procedencia de los datos que presenta el ciudadano. Los datos entregados deberán ser firmados electrónicamente por la JCE. Esta firma electrónica certificada de los datos permitirá que terceros puedan validar la integridad y procedencia de los datos que presenta el ciudadano, tanto la firma de los datos como la validación de estos, se realizará usando los certificados electrónicos administrados por la JCE, como Autoridad Certificadora descrita en el apartado Infraestructura de clave pública.	Ver 4.2.1. GET Mobile Administrator
Para facilitar la lectura de los datos en formato electrónico, la aplicación que desarrolle el oferente deberá mostrar un código bidimensional con los datos y su respectiva firma electrónica certificada. La aplicación debe permitir al usuario seleccionar la lista de campos de la tarjeta que desee compartir a través del código bidimensional.	Ver 4.2.3. GET Mobile Verifier

Página/Folio No.214 de 843

IV.1 Aspectos generales de la Tarjeta Digital

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Al menos debe cumplir con los puntos siguientes:	Entendemos, aceptamos y cumplimos.
• La solución debe incluir el sistema de gestión del ciclo de vida de las credenciales digitales, de forma que se registren los eventos de acceso a cada credencial, así como proporcionar las aplicaciones o interfaces necesarias para la implantación de nuevas soluciones. • La solución debe disponer de un canal de comunicación que utilice algoritmos de cifrado, como medio de conexión entre los dispositivos, para ejecutar el proceso de verificación. El uso de diferentes transmisiones debe incluir los protocolos NFC (Near Field Communication) y BLE (Bluetooth Low Energy) y el cumplimiento de la norma ISO 18013-5.	Item IV Especificaciones técnicas de la Tarjeta de Identidad Ver 4.2. GET Mobile ID Componentes
• La solución debe tener las funciones de recepción, almacenamiento y proteccion segura de credenciales digitales en aplicaciones móviles, así como el uso de notificaciones PUSH para enviar mensajes masivos o personalizados al titular de la credencial digital.	Ver 4.2.1 GET Mobile Administrator
• La solución debe utilizar durante el proceso de emisión o activación de la identidad digital, el mecanismo de detección de liveness (prueba de vida), para prevenir ataques de presentación. • Las aplicaciones móviles deberán proporcionar al titular del documento de identidad digital el desbloqueo de la App mediante autenticación de dos factores (2FA), al menos el uso de un PIN y/o verificación facial.	Ver 4.2.1.4 Procedimiento de activación
• Las aplicaciones móviles tendrán que funcionar sin conexión, para permitir la visualización local de los datos de las credenciales digitales, utilizando un método de verificación de la autenticidad de la identidad digital. También deberá tener la capacidad de realizar consultas en línea, en caso de que se requiera llevar a cabo algún tipo de verificación de la información del titular de la identidad digital.	Ver 4.2.3 GET Mobile Verifier

Página/Folio No.215 de 843

• Las aplicaciones móviles deben permitir la visualización del documento de identidad digital, preferiblemente en modo de pantalla completa del dispositivo móvil, cambiando de anverso a reverso al tocar la credencial y mostrando los mismos datos del documento de identidad físico. • Las aplicaciones móviles deben tener la capacidad de compartir únicamente la información que el titular de la identidad digital desee compartir, en el momento de la verificación de la identidad.	Ver 4.2.2 GET Mobile ID – Aplicación Móvil Ver 4.2.2.2 Control total y protección de la privacidad
• Las aplicaciones móviles deben informar al titular cuando su identidad digital ha sido revocada, mediante una alerta al entrar en la App, indicando el cambio en la validez de su documento digital.	Ver 4.2.2 GET Mobile ID – Aplicación Móvil
• La solución debe ser modular, escalable y fácilmente optimizable para adaptarse a la evolución de la demanda de este tipo de documentos.	Ver 4.2.5 Infraestructura
• La solución debe incluir mecanismos de hardening y protección contra ataques que incluyan, entre otros, ingeniería inversa, manipulación de código, detección de rooting/jailbreak/debugging, etc.	Ver 4.2.2 GET Mobile ID – Aplicación Móvil (Funciones de control de seguridad)
• La solución debe poseer la capacidad de incorporar información en las imágenes de los solicitantes como medidas de seguridad complementarias.	Ver 4.2.2 GET Mobile ID – Aplicación Móvil (Opciones de personalización)
• El proveedor de la solución debe haber realizado con éxito un mínimo de un proyecto de identidad digital.	Se adjunta Certificación de Experiencia – Utah mDL
Adicionalmente, la solución de identificación móvil debe cumplir con las siguientes capacidades mínimas:	Item IV Especificaciones técnicas de la Tarjeta de Identidad.
• Certificación: ISO/IEC 18013 Parte. La solución ofrecida debe contar con la certificación ISO/IEC 18013 Parte 5.	Se adjuntan certificados: • ISO 18013 IOS • ISO 18013 • AndroidUL Verification Services Inc. -Global Enterprise Technologies Corp. 18013 Parte 5

Página/Folio No.216 de 843

• Herramientas de Desarrollo: Facilitar SDK y API. Uso por personal técnico o terceros.	Ver 4.2.1 GET Mobile Administrator – Opciones de Integración) Ver 4.2.4 Herramientas de desarrollo
• Integración de Servicios: Integración con sistemas de identificación de la JCE. El oferente debe presentar un plan de integración.	Cronograma (Sección 4. Implementación GET Mobile ID)
• Infraestructura PKI: la solución debe implementar infraestructura PKI para emisión de certificados. El oferente debe presentar las especificaciones de la infraestructura PKI ofrecida.	Ver ÍTEM III - ESPECIFICACIONES TÉCNICAS DE LAS PKI - CA
• Aplicaciones Móviles: La solución debe incluir la implementación de aplicaciones móviles multiplataforma compatibles con iOS y Android. El oferente debe presentar el plan de implementación de aplicaciones móviles.	Cronograma (Sección 4. Implementación GET Mobile ID)
• Seguridad: La solución debe incluir Protección contra ingeniería inversa y clonación. El oferente debe presentar los mecanismos de seguridad implementados.	4.2.2. GET Mobile ID – Aplicación Móvil. Ver Funciones de control de seguridad
• Liveness Detection: La solución debe utilizar liveness detección para el proceso de activación de identidad digital remota para la Prevención de suplantación de identidad de acuerdo con el estándar de referencia: ISO 30107-3. El oferente deberá presentar la Certificación de cumplimiento de ISO 30107-3.	Ver 4.2.1.4 Procedimiento de Activación, Aprovisionamiento Remoto Se adjunta Certificación ISO 30107-3
• Alta Disponibilidad: La plataforma debe contar con un esquema de alta disponibilidad de servicio.	Ver 4.2.5 Infraestructura

Página/Folio No.217 de 843

• Interoperabilidad: La plataforma debe permitir la interoperabilidad y escalabilidad del servicio para la implementación de diferentes mecanismos de control de dispositivos. El oferente debe presentar la descripción de módulos o componentes. **Requisito modificado o aclarado por:** *RESPUESTAS A OBSERVACIONES TÉCNICAS Y ADMINISTRATIVAS, GRUPO 4, PREGUNTA 5.* **Modificación/Respuesta:** QUIERE DECIR "Interoperabilidad: La plataforma debe permitir la interoperabilidad y escalabilidad del servicio ~~para la implementación de diferentes mecanismos de control de dispositivos~~. El oferente debe presentar la descripción de módulos o componentes." Ver pág. 32 del pliego.	Ver 4.2.2.4. Interoperabilidad Ver 4.2. GET Mobile ID - Componentes
• Intercambio de Datos: La aplicación de identidad móvil debe permitir intercambio de datos personales iniciado por el titular de acuerdo con la norma ISO/IEC 18013-5. El oferente debe demostrar los Métodos de intercambio (QR, NFC, Bluetooth).	Item IV Especificaciones técnicas de la Tarjeta de Identidad Ver 4.2.3.1 Modos de interacción
• Selección de Datos: La aplicación de identidad móvil debe permitir selección de campos específicos para compartir y las Categorías de campos. El oferente debe demostrar la Funcionalidad de selección en la aplicación a implementar.	Ver 4.2.3 GET Mobile Verifier
• Administración de Emisiones: La solución debe Incluir el sistema para administración de la emisión de identidades digitales para evidenciar el registro de eventos y accesos incluir las interfaces necesarias para nuevas soluciones.	Ver 4.2.1.1. Opciones de Integración
• Seguridad de Comunicaciones: Asegurar todas las comunicaciones entre aplicaciones móviles, incluyendo las interacciones en línea y fuera de línea. El oferente debe demostrar los Mecanismos de seguridad de comunicación.	Ver 4.2.3.1 Modos de interacción
• Canales de Comunicación: Utilizar algoritmos de encriptación en canales de comunicación. Se deben incluir las especificaciones de algoritmos utilizados. Se require al menos el uso de protocolos NFC y BLE.	Ver 4.2.3.1 Modos de interacción
• Funcionalidades de App: La solución deberá proveer las Funciones para recibir, guardar y proteger credenciales digitales. Se debe demostrar el uso de Notificaciones PUSH y almacenamiento seguro.	Ver 4.2.2 GET Mobile ID – Aplicación Móvil
• Autenticación: Las aplicaciones móviles deberán permitir el desbloqueo de la App mediante autenticación de dos factores 2FA, como mínimo PIN y verificación facial.	Ver 4.2.1.4 Procedimiento de Activación

Página/Folio No.218 de 843

• Funcionalidad Online / Offline: Las aplicaciones móviles deberán permitir el funcionamiento offline para visualización de datos Debe permitir también las Consultas en línea.	Ver 4.2.3.1 Modos de interacción
• Visualización de Documentos: Visualización de documentos de identificación digital en pantalla completa y el cambio de anverso a reverso	Ver 4.2.2 GET Mobile ID – Aplicación Móvil
• Compartir Información: Capacidad de compartir información seleccionada durante verificación de identidad.	Ver 4.2.2 GET Mobile ID – Aplicación Móvil Ver 4.2.3 GET Mobile Verifier
• Notificaciones de Revocación: Informar al titular sobre la revocación de su identidad digital mediante alertas en la App	Ver 4.2.2.3 Siempre actualizado
• Capacidad de Servicio: Atender al menos 5,000 solicitudes diarias de credenciales digitales. La solución debe ser Modular y escalable para adaptarse a la evolución en la demanda de este tipo de documentos. El oferente deberá proporcionar información de dimensionamiento de la plataforma.	Item IV Especificaciones técnicas de la Tarjeta de Identidad Ver 4.2.5 Infraestructura
• Interfaces de Comunicación: Utilizar e integrar con interfaces de comunicación existentes para el envío de orden de emisión por parte de la JCE.	Ver 4.2.1.1. Opciones de Integración
• Consistencia de Datos: Mantener consistencia de estados entre soluciones para el Proceso de actualización y sincronización al sistema institucional para la identificación de personas.	Ver 4.2.1.1. Opciones de Integración
• Disponibilidad de operación: Disponibilidad del 99.95% durante horas de producción, excepto por razones atribuibles a la JCE. El oferente deberá presentar un Plan de operación y mantenimiento	Ver 4.2.5.2. Disponibilidad del 99.95% de operación

Página/Folio No.219 de 843

IV.2 Prueba de Concepto (obligatoria)

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El oferente deberá realizar en Santo Domingo, de forma obligatoria, en las propias instalaciones del oferente o de un local rentado por el oferente (en el tiempo a determinar durante el proceso de licitación), una prueba de concepto funcional para la emisión de identificación física y digital. La prueba de concepto debe incluir: • Con diez (10) muestras de tarjetas vírgenes, el proveedor deberá realizar el enrolamiento de personas en vivo y al menos imprimir en una de sus tarjetas. Al terminar de personalizar una tarjeta, se realizará la generación de una cédula digital a partir de la tarjeta personalizada. Deberá incluir en dicha prueba de concepto, una aplicación móvil de verificación (mediante QR seguro generado desde la aplicación), la funcionalidad de compartir todos los datos o compartir un grupo de datos específicos seleccionados por el ciudadano. **Requisito modificado o aclarado por:** MATRIZ CON LOS CRITERIOS Y ACLARACIÓN DE LA PUNTUACIÓN DE LA PRUEBA DE CONCEPTO POC **Modificación/Respuesta:** 	Entendemos, aceptamos y cumplimos.

Página/Folio No.220 de 843

ESPECIFICACIONES TÉCNICAS ITEM V
KIT DE PERIFÉRICOS

Página/Folio No.221 de 843

Los oferentes tendrán que ofertar un kit (conjunto completo) de periféricos con características similares o superiores, que se listan a continuación:

V.1 Escáner

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Tipo: Escáner móvil personal. • Alimentación de documentos: Automática o manual. • Escala de grises: 8 bits. • Color: 24 bits. • Fuente de luz: LED RGB. • Modos de operación: Color, escala de grises, blanco y negro. • Resolución óptica: 600 ppp. • Resolución de salida: 150/200/300/400/600 ppp. • Velocidades de escaneo: 8 ppm/16 ipm. • Interfaz: Hi-Speed USB 2.0. **Otras características:** • Detección automática de color. • Detección automática de tamaño de página. • Configuración automática de resolución. • Suavizamiento de fondo. • Corrección de desviación. • Énfasis de borde. • Reducción del efecto muaré. • Corrección de fotografía. • Escaneo previo. • Eliminación de fondo/prevención de sangrado. • Recorte del sombreado. • Omisión de página en blanco. • Mejoramiento de texto. • Reconocimiento de la orientación del texto. • Software incluido para Windows: Controladores WIA/TWAIN. • Sistemas operativos compatibles: Windows 10, Windows 11. **Nota: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.**	Entendemos, aceptamos y cumplimos. 5.1. Escáner Móvil Personal – Canon imageFORMULA P-208II. Ver ÍTEM V- KIT PERIFÉRICOS

Página/Folio No.222 de 843

V.2 Lector de firma

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Dimensiones del producto (aproximadas, similar o superior): 156 x 126 mm. • Interface de comunicación: USB. • F-STN, monocromático, reflectante. • Tamaño de pantalla: +- 4". • Resolución nativa (aproximada, similar o superior): 800 x 480. • Niveles de presión del lápiz: 512/1024. • Resolución del sensor: 2540 líneas por pulgada. • Precisión de coordenadas: ± 0,5 mm (centro). • Bolígrafo sin pilas: Sí. • Bolígrafo inalámbrico: Sí. • Velocidad de transmisión (aproximada, similar o superior): 200pps. **Nota: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.**	Entendemos, aceptamos y cumplimos. 5.2.. Lector de Firma Digital – Wacom STU-540. Ver ÍTEM V - KIT DE PERIFÉRICOS – Sección de lector de firma.

V.3 Lector de huellas (Compatible con NEUROtechnology, porque la JCE dispone de sistemas y software que usan esta tecnología).

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Tamaño de la ventana de escaneado de huellas dactilares: aproximado de 66 mm x 84 mm. • Área de escaneo óptico (aproximada, similar o superior): 81 mm x 81 mm. • Resolución de la imagen (aproximada, similar o superior): 1600 x 1600 píxeles, 500 dpi. • Profundidad de bit: 8 bit, 256 niveles de gris. • Tamaño del archivo Raw de la imagen de la huella dactilar comprimido en WSQ aprox. 2,5 MB aproximadas, similar o superior 0,4. • Interfaz (aproximada, similar o superior): USB 2.0 de alta velocidad con cable USB estándar de alrededor de 1,8 metros. • Fuente de luz diodos emisores de luz: (LED) infrarroja. • Fuente de alimentación: Preferiblemente USB. • Indicar certificaciones. **Nota: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.**	Entendemos, aceptamos y cumplimos. 5.3.. Lector de Huellas Digitales – DigitalPersona 4500. Ver ÍTEM V - KIT DE PERIFÉRICOS – Sección de lector de **huellas.**

Página/Folio No.223 de 843

V.4 Impresora punto de venta

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Ancho: 20. • Alto: 15. • Largo: 25. • Calidad de impresión: Alta resolución. • Dimensiones (aproximadas, similar o superior): 20X20X25. • Cantidad de puertos USB: 1. • Largo del cable (aproximado, similar o superior): 1.8. • Compatible con Windows. • Tipo de inyección: Láser. • Color: negro. • Conectividad/conexión: USB. • Formato de papel: A7. • Cantidad de bandejas: 1. • Entrada: USB. • Velocidad de la impresión a blanco y negro (aproximada, similar o superior): 20. • Tipo de impresión: Láser monocromática **Nota: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.** **Requisito modificado o aclarado por:** *RESPUESTAS A OBSERVACIONES TÉCNICAS Y ADMINISTRATIVAS. GRUPO 4, PREGUNTA 34.* **Modificación/Respuesta:** FE DE ERRATAS: Donde dice IMPRESORA PUNTO DE VENTA quiere decir IMPRESORAS TÉRMICAS DE PUNTO DE VENTA. Se exige una impresora de punto de venta como se especifica en el pliego V.4 Impresora punto de venta. Pueden cumplir con esas características técnicas o superiores y se requiere muestra del equipo propuesto.	Entendemos, aceptamos y cumplimos. 5.4. Impresora de Punto de Venta – STAR BSC10UD-24. Ver ÍTEM V - KIT DE PERIFÉRICOS – Sección de impresora de punto de venta.

V.5 Lector de huella digital persona

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Voltaje de suministro: 5,0 V ±5 % suministrado mediante USB. • Corriente de alimentación: escaneo (aproximada, similar o superior) < 100 mA (típico). • Corriente de alimentación: en reposo (aproximada, similar o superior) 120 mA (típico).	Entendemos, aceptamos y cumplimos. 5.5. Lector de Huellas Digitales – LIVETOUCH

• Corriente de alimentación: modo suspensión (aproximada, similar o superior) < 0,5 mA (máximo). • Inmunidad contra descarga electrostática. • (ESD, por sus siglas en inglés) >15 kV, montado en la caja. • Temperatura de operación: 0 - 40 °C. • Humedad de almacenamiento: 20 % - 90 % sin condensación. • Información escaneada: Escala de grises de 8 bits. • Indicar cumplimiento de normas. • Peso (aproximado, similar o inferior): 105 gramos. • Interfaz: Dispositivo USB 2.0 de velocidad máxima, de alta potencia **Nota: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.**	QUATTRO. Ver ÍTEM V - KIT DE PERIFÉRICOS – Sección de lector de huellas .

V.6 Cámara

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Sensor: CMOS. • Tecnologías: Wi-Fi® y NFC** integradas. • Sistema de AF de 9 puntos y el modo AF Servo AI. • Visor óptico con una cobertura del visor de aproximadamente 95% (aproximado, similar o superior). • Alta definición real (Full HD) de 30p (aproximada, similar o superior). • Balance automático de blancos con "Prioridad de blancos". • Puerto USB (para el control del dispositivo/otra tecnología existente para la obtención de la imagen desde una PC). • Característica de auto enfoque. • Filtros creativos que incluyen el efecto ojo de pez y el efecto miniatura. **Nota: Pueden cumplir con estas características técnicas o superiores, requerido muestra del equipo propuesto.**	Entendemos, aceptamos y cumplimos. 5.6.1. Cámara Digital – Canon EOS Rebel T7. Ver ÍTEM V - KIT DE PERIFÉRICOS – Sección de cámara.

Página/Folio No.225 de 843

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Este desglose deber ser detallado y unitario. El proveedor se compromete a suministrar dichos periféricos en un periodo de treinta (30) días calendario después de la solicitud de la JCE. Los precios podrán ser ajustados anualmente de acuerdo con la inflación. La JCE tiene la decisión de comprarlos o no.	Entendemos, aceptamos y cumplimos. Ver ÍTEM V - KIT DE PERIFÉRICOS. 5.7. Condiciones de Suministro y Ajuste de Precios

Página/Folio No.226 de 843

ESPECIFICACIONES TÉCNICAS ITEM VI

MANTENIMIENTO

VI.1 Especificaciones técnicas del mantenimiento

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El adjudicatario deberá dar un soporte preventivo y correctivo durante toda la etapa del contrato, incluyendo a todas las impresoras, la PKI, la tarjeta digital y soluciones de software implementadas para integración de APIS de las impresoras con el actual sistema de identidad de la JCE.	Entendemos, aceptamos y cumplimos Ítem VI Especificaciones Técnicas del Mantenimiento

Página/Folio No.227 de 843

El adjudicatario deberá disponer o instalar de un centro regional de mantenimiento y reparación en República Dominicana, otro en USA y otro en Europa, y deberá tener en stock de inventario para reparaciones, como mínimo un 3% de inventario de suministro de las máquinas de personalización.	6.10. Inventario. Ver ITEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO
Para dar un correcto mantenimiento a la JCE, tanto en los centros de impresión en República Dominicana, USA y resto del mundo, el oferente deberá proponer un equipo de mantenimiento, con experiencia comprobada para dar tal mantenimiento.	Ver 6.1 Plan de Mantenimiento para PKI
Para dar mantenimiento a la PKI, se deberá proveer soporte de experiencia comprobada.	Ver carpeta 2 / sección 3 / N°6 Affidavit
El mantenimiento de las impresoras de tarjetas, al ser un elemento clave, debe ser ofrecido y operado por el fabricante de las impresoras tanto en sitio como de forma remota.	Ver item VI - Especificaciones Técnicas del Mantenimiento
El nivel de calidad del servicio se medirá mediante el SLA (Service Level Agreement).	Entendemos, aceptamos y cumplimos

Página/Folio No.228 de 843

VI.2 Nivel de Servicio (SLA)

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Habrá dos niveles de servicio: • Un nivel de servicio en garantía, que será durante el primer año de servicio desde la instalación de los equipos de impresión, el PKI o la tarjeta digital, donde el proveedor tendrá que ir en sitio, a las oficinas de la JCE tanto a nivel nacional o internacional, dando soporte a nivel 3, es decir, es la JCE quien registra la incidencia de los funcionarios (nivel 2), resuelve o escala a los técnicos de la JCE para que resuelvan la incidencia (nivel 2) y si no se resuelve con los técnicos de JCE, se re-escala al proveedor donde tendrá que ir a las oficinas en sitio (nivel 3) o podrá resolver de forma remota (si fuera posible). • Un nivel de servicio de mantenimiento (no en garantía) en la sede central de la JCE (para equipos de impresión en Rep. Dominicana o en el centro designado por la JCE en Nueva York o Madrid). Para PKI y tarjeta digital tendrá que ir al sitio central de la JCE o de forma remota.	Entendemos, aceptamos y cumplimos. ÍTEM VI - Especificaciones técnicas del mantenimiento Acápite: Nivel de Servicio (SLA).
VI.2.1 Clasificación del nivel de servicio (SLA) **VI.2.1.1 Primer Nivel de Soporte (Hot Line o Línea Directa JCE)** Cada tipo de incidente, que está relacionado con el equipo, debe ser informado a un sistema de boleta de servicio técnico o al servicio de atención en el centro de servicio central de la JCE en República Dominicana. El operador de la mesa de la JCE recoge la mayor cantidad posible de información sobre el incidente y brinda asistencia directa por teléfono. El formato de comunicación elegido para este nivel de soporte será: • Email • Teléfono Este nivel de soporte será ofrecido por la JCE.	Entendemos, aceptamos y cumplimos
VI.2.1.2 Segundo Nivel de Soporte (Especialista JCE) El soporte de segundo nivel será provisto por un técnico de JCE con un conocimiento más completo y especializado en los componentes del sistema. El técnico apoyará al iniciador ya sea por teléfono o por acceso remoto. En el caso de que el incidente no se pueda resolver, el técnico especializado activa el soporte de tercer nivel en el sitio. Este nivel de soporte será ofrecido por la JCE.	Ver ÍTEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO – Sección de Nivel de Servicio (SLA).

Página/Folio No.229 de 843

VI.2.1.3 Tercer Nivel de Soporte (Soporte en-sitio)

Este nivel de soporte será ofrecido por el proveedor adjudicado.

En caso de que un incidente no pueda resolverse por medio del soporte de segundo nivel, JCE abrirá un ticket de incidencia en el sistema de ticketing de JCE donde reportará la incidencia al proveedor adjudicado. Un experto especializado del proveedor debe de estudiar la incidencia, ponerse en contacto con JCE y organizar como resolver la incidencia, si de forma remota o yendo al sitio.

Ver ÍTEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO – Sección de Nivel de Servicio (SLA).

VI.2.1.4 Prioridades de incidentes

Nivel de prioridad	Impacto/Métricos		Descripción
	Componentes Centrales (PKI, Tarjeta de identidad digital)	**Componentes Descentralizados (Impresoras, etc.)**	
Crítica	La capacidad de salida de todo el sistema se ve afectada y se reduce a 0%.	La capacidad de salida del sistema local se ve afectada y se reduce a 0%	Un error en un elemento central (hardware o software del centro de datos) que detiene por completo la capacidad de realizar un procesamiento de extremo a extremo o en una sede o consulado
Alta	La capacidad de salida del sistema se ve afectada y se reduce en >50%	La capacidad de salida del sistema local se ve afectada y se reduce en >50%	Una falla en un elemento de los sistemas instalados que limita o reduce significativamente la capacidad de realizar el procesamiento de documentos de extremo a extremo.
Mediana	La capacidad de salida del sistema se	La capacidad de salida del sistema local se ve	Una falla en un elemento de los sistemas instalados

Ver ÍTEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO – Sección de Nivel de Servicio (SLA).

Página/Folio No.230 de 843

	ve afectada y se reduce en >10%	afectada y se reduce en	que limita o reduce la capacidad de realizar el procesamiento de documentos de extremo a extremo.
Baja	Defecto menor, la capacidad de salida del sistema no se ve afectada ni se ve afectada por	Defecto menor, la capacidad de salida del sistema local no se ve afectada o se ve afectada por <10%	Una falla en un elemento de los sistemas instalados que no / casi no limita o reduce la capacidad de realizar el procesamiento de documentos de extremo a extremo

VI.2.2 Definición de nivel de servicio en periodo de garantía para el proveedor

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
VI.2.2.1 Nivel de servicio para oficinas en Santo Domingo **VI.2.2.1.1 Tiempo de soporte en -sitio- Oficinas Santo Domingo**	Entendemos, aceptamos y cumplimos

Métrica: Soporte en el sitio - Tiempo de respuesta al incidente					
Definición métrica	Medidas de tiempo para que el adjudicatario llegue al sitio o resuelva la incidencia de forma remota, después de que se active el tercer nivel de soporte por parte de la JCE				
Horas de cobertura del servicio	Horario comercial: República Dominicana: de lunes a viernes, de 7:00 a.m. a 6:00 p.m., sábados de 8:00 am a 1:00 pm hora local (CST)				
Horas de medición		Prioridad Critica	Prioridad Alta	Prioridad Media	Prioridad Baja
		Horas de Negocio	Horas de Negocio	Horas de Negocio	Horas de Negocio
Nivel de Servicio	El 97% in situ en Santo Domingo	2 horas	6 horas	8 horas	1 día
Metodología de Medición					
Puntos de Medición	1. El momento de la solicitud de presencia en el sitio de un ingeniero de servicio para el adjudicatario es el momento en que se informa una solicitud a través de la mesa de servicio de JCE 1. La hora de "llegada al sitio" es la hora en que el técnico				

Página/Folio No.231 de 843

	de servicio documenta su llegada al sitio a través del servicio del adjudicatario.
Estimación	El tiempo de respuesta del incidente se mide como el tiempo entre: El momento de la notificación de la solicitud al servicio de atención al adjudicatario. La hora de "llegada al en-sitio" o "resolución de forma remota"
Frecuencia de medición	Medido para cada Incidente con una presencia solicitada en el sitio.
Fuente de Datos	Sistema de ticketing de JCE
Responsabilidad de medición	Sistema de ticketing de JCE el cual el proveedor tendrá acceso.
Periodo de Medición	Mensual

VI.2.2.2 Niveles de servicios para oficinas en República Dominicana

VI.2.2.2.1 Tiempo de apoyo en sitio - Oficinas De República Dominicana

Métrica: Soporte en el sitio - Tiempo de respuesta al incidente					
Definición métrica	Medidas de tiempo para que el adjudicatario llegue al sitio o resuelva la incidencia de forma remota, después de que se active el tercer nivel de soporte por parte de la JCE				
Horas de cobertura del servicio	Horario comercial: República Dominicana: de lunes a viernes, de 7:00 a.m. a 6:00 p.m., sábados de 8:00 am a 1:00 pm hora local (CST)				
Horas de medición		Prioridad Critica	Prioridad Alta	Prioridad Media	Prioridad Baja
		Horas de Negocio	Horas de Negocio	Horas de Negocio	Horas de Negocio
Nivel de Servicio	El 97% in situ en Santo Domingo	4 horas	8 horas	3 días	5 día
Metodología de Medición					
Puntos de Medición	• El momento de la solicitud de presencia en el sitio de un ingeniero de servicio para el adjudicatario es el momento en que se informa una solicitud a través de la mesa de servicio de JCE. • La hora de "llegada al sitio" es la hora en que el técnico de servicio documenta su llegada al sitio a través del servicio del adjudicatario.				
Estimación	El tiempo de respuesta del incidente se mide como el tiempo entre: • El momento de la notificación de la solicitud al servicio de atención al adjudicatario. • La hora de "llegada al en-sitio" o "resolución de forma remota"				

Página/Folio No.232 de 843

Frecuencia de medición	Medido para cada Incidente con una presencia solicitada en el sitio.
Fuente de Datos	Sistema de ticketing de JCE
Responsabilidad de medición	Sistema de ticketing de JCE el cual el proveedor tendrá acceso.
Periodo de Medición	Mensual

VI.2.2.3 Nivel de servicio para las oficinas de los Estados Unidos de América y resto del mundo.

VI.2.2.3.1 Tiempo de apoyo en-sitio - Oficinas de los Estados Unidos de América y resto del mundo

Métrica: Soporte en el sitio - Tiempo de respuesta al incidente					
Definición métrica	Medidas de tiempo para que el adjudicatario llegue al sitio o resuelva la incidencia de forma remota, después de que se active el tercer nivel de soporte por parte de la JCE				
Horas de cobertura del servicio	Horario comercial: República Dominicana: de lunes a viernes, de 7:00 a.m. a 6:00 p.m., sábados de 8:00 am a 1:00 pm hora local (CST)				
Horas de medición		**Prioridad Critica**	**Prioridad Alta**	**Prioridad Media**	**Prioridad Baja**
		Horas de Negocio	Horas de Negocio	Horas de Negocio	Horas de Negocio
Nivel de Servicio	El 97% in situ en Santo Domingo	3 días	5 días	7 días	9 días
Metodología de Medición					
Puntos de Medición	• El momento de la solicitud de presencia en el sitio de un ingeniero de servicio para el adjudicatario es el momento en que se informa una solicitud a través de la mesa de servicio de JCE 1. • La hora de "llegada al sitio" es la hora en que el técnico de servicio documenta su llegada al sitio a través del servicio del adjudicatario.				
Estimación	El tiempo de respuesta del incidente se mide como el tiempo entre: • El momento de la notificación de la solicitud al servicio de atención al adjudicatario. • La hora de "llegada al en-sitio" o "resolución de forma remota"				

Página/Folio No.233 de 843

Frecuencia de medición	Medido para cada Incidente con una presencia solicitada en el sitio.
Fuente de Datos	Sistema de ticketing de JCE
Responsabilidad de medición	Sistema de ticketing de JCE el cual el proveedor tendrá acceso.
Periodo de Medición	Mensual

Página/Folio No.234 de 843

ESPECIFICACIONES TÉCNICAS ITEM VII

CAPACITACIONES

Página/Folio No.235 de 843

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El oferente deberá presentar un plan de capacitación completo. Deberá cubrir todos los aspectos técnicos de la puesta en marcha del proyecto de renovación. Debe incluir todos los productos y servicios incluidos en su oferta. Debe incluir una capacitación al personal que vaya a gestionar las máquinas.	Entendemos, aceptamos y cumplimos. ÍTEM VII - Capacitación

Otros Requerimientos

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
a) Cronograma de trabajo: El oferente deberá presentar un plan de trabajo detallado que cubra las tres (3) etapas del proyecto. (ver 1.27.2). b) El tiempo de implementación mínimo debe ser de veintiséis (26) semanas. **Requisito modificado o aclarado por:** *RESPUESTAS, ACLARACIONES Y ENMIENDAS ADMINISTRATIVAS, GRUPO 4, PREGUNTA 7.* **Modificación/Respuesta:** *"b) El tiempo de implementación* **MÁXIMO** *debe ser de veintiséis (26) semanas.*	Entendemos, aceptamos y cumplimos. **Ver los siguientes puntos: Cronograma (Sección 4. Implementación GET Mobile ID)**
c) gEl fabricante de la tarjeta debe tener en vigor y presentar conjuntamente con su propuesta técnica, las siguientes certificaciones: • ISO 9001:2015. • ISO 27001:2013. • ISO 14001 o equivalente. • ISO 14928 INTERGRAF o equivalente nivel gobierno.	Ver carpeta 2 /Seccion 4 /N°11

Página/Folio No.236 de 843

OTROS REQUERIMIENTOS

Página/Folio No.237 de 843

1.8 Esquema de Adquisición de Equipos y Suministros "Impresión de Cédulas"

1.8.1 Modalidad Adquisición de Equipos y Suministros:

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Oferente debe presentar una propuesta técnica con todas las características mencionadas anteriormente, para suplir las impresoras y los plásticos o tarjetas requeridas. Quedando entendido, que los plásticos deben ser propuestos con las impresoras que correspondan. En cualquier caso, el Oferente que resulte adjudicatario, reconoce que la Junta Central Electoral, será el operador directo ante el ciudadano y deberá garantizar el suministro de los equipos, material gastable, reparación y el soporte técnico necesario para mantener la infraestructura nacional de impresión de la cédula, sin interrupciones. La emisión, selección y diseño de la cédula, será siempre una atribución exclusiva de la Junta Central Electoral.	Entendemos, aceptamos y cumplimos.

1.9 Fuente de recursos

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
La Junta Central Electoral cuenta con un monto referencial que sustentará el precio de los productos y servicios a ser adjudicados mediante la presente licitación. Las partidas de fondos, para liquidar las entregas, estarán debidamente especializadas para tales fines, siendo cubierta con los recursos consignados en el presupuesto de la entidad contratante para el año 2024 y 2025, a efecto de que las condiciones contractuales no sufran ningún tipo de variación durante el tiempo de ejecución del mismo. Para cada periodo de ejecución del Contrato, se actuará de igual manera. Es decir, se consignarán las partidas correspondientes en los respectivos presupuestos anuales.	Entendemos, aceptamos y cumplimos.

1.10 Condiciones de pago

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"

Página/Folio No.238 de 843

Es intención de la Junta Central Electoral, lograr condiciones que le permitan cubrir mediante pagos diferidos por entrega de cada etapa del proyecto, las obligaciones que genere la adquisición de los productos y servicios objetos de esta licitación para el año 2024 y 2025. Cada oferente podrá especificar cualquier otra modalidad de pago en su propuesta siempre que se acojan a las prácticas normales del comercio. La Junta Central Electoral, está en disposición, si así se le requiriere, de otorgar un anticipo no mayor del 20% del monto presupuestado y adjudicado para las partidas iniciales del proyecto. En cuanto a la duración total del contrato la Junta Central Electoral realizará los pagos de facturas de cada pedido realizado y justificados mediante órdenes.	Entendemos, aceptamos y cumplimos. **Ver FL-05 Presentación de Oferta Económica**

1.11Fases de la licitación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
La presente licitación se divide en dos (2) fases principales: **Fase I:** Se inicia con el proceso de Acreditación y Solvencia. En esta primera etapa los Oferentes/Proponentes deberán hacer entrega del "Sobre A", conteniendo los documentos de acreditación y solvencia, y la propuesta técnica, a los fines de su apertura y evaluación, así como la entrega del "Sobre B" contentivo de la Propuesta Económica, en la fecha que se indica en el cronograma. Esta fase concluye con la resolución de calificación, previo a la evaluación de la Comisión de Asesoría y Asistencia Técnica y ponderación del Comité de Compras y Contrataciones la cual emitirá el Acta de Validación. **Fase II:** Se inicia con la invitación a los Oferentes/Proponentes que hayan resultado habilitados en la Fase I, a presentarse al acto de Apertura del "Sobre B" Propuestas Económicas y concluye con la adjudicación de la Licitación. A tal efecto, el Comité de Compras y Contrataciones con la asesoría de la Comisión de Asesoría y Asistencia Técnica emitirá el Acta de Adjudicación definitiva.	Entendemos, aceptamos y cumplimos.

1.12Idioma

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"

Página/Folio No.239 de 843

El idioma oficial de la presente licitación es el español, por tanto, todas las correspondencias y documentos relativos a ella que intercambien el Oferente/Proponente y el Comité de Compras y Contrataciones, deben ser presentados en este idioma. De encontrarse en idioma distinto, deberán ser traducidos al español, por un intérprete judicial debidamente autorizado, traducción cuyas firmas deberán ser legalizadas por ante la Procuraduría General de la República Dominicana.	Entendemos, aceptamos y cumplimos.

1.13 De la publicidad

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
La invitación a presentar Ofertas en la presente licitación se hará mediante la publicación, en al menos, dos (2) diarios de circulación nacional, dos (2) diarios en el extranjero de amplia circulación, por término de dos (2) días consecutivos, en la página Web y las redes sociales de la Junta Central Electoral y en el portal administrado por la Dirección General de Contrataciones Públicas.	Entendemos y aceptamos.

1.14 Cronograma de la Licitación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"

Actividad	Periodo de Ejecución
Publicación del llamado a licitación	Los días 25 y 26 de abril, 2024
Registro de oferentes y adquisición (formal) del Pliego de Condiciones Específicas (Obligatorio)	Desde el 25 de abril, hasta el 17 de mayo, 2024 a las 4:00 P.M.
Período para realizar consultas por parte de los oferentes registrados	Hasta el 24 de mayo, 2024
Plazo para emitir respuestas, por parte del Comité de Compras y Contrataciones, mediante Circulares	Hasta el 10 de junio, 2024
Acto de recepción y apertura de credenciales, Propuesta Técnica y muestras "Sobres A" y recepción de propuestas económicas "Sobres B"	El 25 de junio, 2024 10:00 A.M.
Verificación y evaluación de documentos y propuestas técnicas	Desde el 25 de junio, 2024
Realización prueba de concepto	A partir del 27 junio, 2024
Notificación de errores de naturaleza subsanable	Hasta el 8 de julio, 2024
Período de subsanación	Hasta el 22 de julio, 2024 4:00 P.M.

Entendemos y aceptamos.

Página/Folio No.240 de 843

Notificación resultados de evaluación de documentos y propuestas técnicas y oferentes habilitados	Hasta el 29 de julio, 2024
Acto de apertura de propuestas económicas "Sobres B"	El 6 de agosto, 2024 10:00 A.M.
Evaluación de Ofertas Económicas "Sobres B" y	Desde el 6 de agosto, 2024
Adjudicación	
Acto de adjudicación	El 13 de agosto, 2024
Notificación de adjudicación	Hasta 5 días hábiles luego de la adjudicación
Plazo para constituir Garantía de Fiel Cumplimiento	Hasta 5 días hábiles luego de la notificación de adjudicación

Requisito modificado o aclarado por:
Ver CCC-351/2024
Modificación/Respuesta:

1) El acto de recepción y apertura de documentos para acreditación, Propuestas Técnicas y muestras (Sobres A), y recepción de Propuestas Económicas (Sobres B), se realizará el **martes 25 del mes de febrero del año 2025, a las 10:00 A.M.**, en el Auditorio de la Junta Central Electoral, sito en el primer (1er.) nivel de la sede principal, ubicada en la Av. Gregorio Luperón, esq. Av. 27 de Febrero, Plaza de la Bandera, Santo Domingo, D.N.

2) En lo relativo a la fecha de la prueba de concepto, se realizará a los quince (15) días hábiles contados a partir del 25 del mes de febrero del año 2025, iniciando el día diecinueve (19) de marzo del año 2025.

1.15 Disponibilidad y Adquisición del Pliego de Condiciones

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Pliego de Condiciones estará disponible para su adquisición en las oficinas del Comité de Compras y Contrataciones, ubicadas en la Av. Gregorio Luperon esq. Av. 27 de Febrero, Edificio Administrativo, ala Este, 2do. Nivel, en la fecha indicada en el Cronograma de la Licitación y podrá consultarse en la página Web de la Junta Central Electoral (www.jce.gob.do) y en el Portal Transaccional de la Dirección de Contrataciones Públicas. Los interesados en participar en la presente licitación, deberán aportar la suma de Tres Mil Dólares Estadounidenses con 00/100 (USD$3,000.00) - NO REEMBOLSABLES -, a ser saldados mediante cheque certificado o transferencia bancaria a nombre de la Junta Central Electoral, contra la entrega del recibo emitido por la Dirección Financiera y el retiro del Pliego de Condiciones Especificas en las oficinas del Comité de Compras y Contrataciones, conforme se indica precedentemente. Estos recursos son para cubrir los gastos administrativos generados durante todo el proceso de licitación, incluyendo la elaboración del Pliego de Condiciones Específicas. Esta suma no será reembolsable en ningún caso.	Entendemos y aceptamos. **Ver carpeta 1/ Seccion 2/ N°19 - Comprobante de pago para cubrir gastos administrativos (3,000 usd)**

Requisito modificado o aclarado por: *RESPUESTAS A RESPUESTAS, ACLARACIONES Y ENMIENDAS ADMINISTRATIVAS, ADMINISTRATIVAS, PREGUNTA 5.* **Modificación/Respuesta:** *Basta con que una de las empresas consorciadas esté inscrita. Sin embargo, las empresas ya inscritas individualmente y que se presenten en consorcio posterior a la inscripción, el pago no es reembolsable.*	

1.16Órgano Rector

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Pleno de la Junta Central Electoral, como un primer nivel y órgano de dirección de la Junta Central Electoral.	Entendemos y aceptamos.

1.17Ejecución del Proceso de Licitación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Comité de Compras y Contrataciones será el cuerpo encargado de evaluación y calificación, de la integridad del proceso de licitación y estará asistido de la Comisión de Asesoría y Asistencia Técnica, la cual, en cada caso será integrada por expertos en la materia de que se trata.	Entendemos y aceptamos.

1.18Atribuciones

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Sin que la presente indicación resulte limitativa, el Comité de Compras y Contrataciones tendrá las siguientes funciones: • Garantizar la integridad del proceso, desde la presentación del Pliego de Condiciones, respuestas a las consultas, propuestas de Oferentes/Proponentes, evaluación de propuestas contando con la Comisión de Asesoría y Asistencia Técnica, preparación de informes con las recomendaciones de lugar y todo acto complementario, conveniente y válido, a los fines de la adjudicación. • Llevar registros de las operaciones y todo lo relacionado con el proceso de licitación.	Entendemos y aceptamos.

Página/Folio No.242 de 843

• Modificar, en cualquier momento, respetando los plazos establecidos en el Cronograma de la Licitación, el Pliego de Condiciones Específicas, mediante enmiendas dadas a conocer a todos los Oferentes/Proponentes. • Cancelar, suspender, declarar desierto o nulo, total o parcialmente el concurso, por las causas que considere pertinentes. • Las decisiones que adopte el Comité de Compras y Contrataciones deberán ser por mayoría de votos, procediendo a tales efectos, a levantar el acta correspondiente, en la que hará constar las incidencias que se hayan presentado.	

1.19Exención de Responsabilidades

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Comité de Compras y Contrataciones no estará obligado a declarar habilitado a ningún Proponente que haya presentado sus credenciales y/u ofertas, si las mismas no demuestran que cumplen con los requisitos establecidos en el presente Pliego de Condiciones. En caso de presentarse esta situación, el Comité de Compras y Contrataciones simplemente informará su no habilitación. La no habilitación de un Oferente/Proponente, la decisión de modificar el Pliego de Condiciones, de cancelar, suspender o declarar desierta o nula la licitación, no conllevará responsabilidad alguna para dicho Comité, ni dará lugar a reclamo alguno por parte de los Oferentes/Proponentes, ni implicará responsabilidad para la Junta Central Electoral, el Comité de Compras y Contrataciones, sus asesores o cualquier entidad, organismo o funcionario del Gobierno de la República Dominicana. Estas decisiones no podrán motivar reclamos de cualquier naturaleza por gastos, honorarios, reembolsos, retribuciones, derechos de ningún tipo y/o indemnizaciones por parte de los Oferentes/Proponentes, excepto lo establecido expresamente en el presente Pliego de Condiciones.	Entendemos y aceptamos.

1.20Prácticas Corruptas o Fraudulentas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Las prácticas corruptas o fraudulentas comprendidas en el Código Penal o dentro de la "Convención Interamericana contra la Corrupción", o cualquier acuerdo entre Proponentes o con terceros, que establecieren prácticas restrictivas a la libre competencia, serán causales determinantes del rechazo de la propuesta en cualquier estado del procedimiento de selección, o de la rescisión del contrato, si éste ya se hubiere celebrado. A los efectos anteriores se entenderá por: "Práctica Corrupta", es el ofrecimiento, suministro, aceptación o solicitud de "práctica fraudulenta", una tergiversación de los hechos con el fin de influir en un proceso de	Entendemos y aceptamos.

contratación o en la ejecución de un contrato de obra pública en perjuicio del contratante; la expresión comprende las prácticas colusorias entre los licitantes (con anterioridad o posterioridad a la presentación de las ofertas) con el fin de establecer precios de ofertas a niveles artificiales y no competitivos y privar al contratante de las ventajas de la competencia libre y abierta.	

1.21 De los Oferentes/Proponentes Hábiles e Inhábiles

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Toda persona física o jurídica, nacional o extranjera que haya adquirido el Pliego de Condiciones y que se encuentre inscrita en el Registro de Proveedores del Estado Dominicano, tendrá derecho a participar en los procesos de adquisiciones que celebre la Junta Central Electoral, siempre y cuando haya sido calificada y reúna las condiciones exigidas y no se encuentre inhabilitada o afectada por el régimen de prohibiciones establecido en el presente Pliego de Condiciones.	Entendemos y aceptamos.

1.21.1 Prohibición de Contratar.

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
No podrán participar como Oferentes/Proponentes, en forma directa o indirecta, las personas físicas o sociedades comerciales que se relacionan a continuación: 1. El Presidente y Vicepresidente de la República; los Ministros y Viceministros del Estado; los Senadores y Diputados del Congreso de la República; los Magistrados de la Suprema Corte de Justicia y de los demás tribunales del orden judicial; del Tribunal Constitucional, del Tribunal Superior Electoral, de la Cámara de Cuentas y de la Junta Central Electoral; los Alcaldes y Regidores de los Ayuntamientos de los Municipios y del Distrito Nacional; el Contralor General de la República y el Sub- Contralor; el Director de Presupuesto y el Subdirector; el Director Nacional de Planificación y el Subdirector; el Procurador General de la República y los demás miembros del Ministerio Público; el Tesorero Nacional y el Sub.-Tesorero y demás funcionarios de primer y segundo nivel de jerarquía de las instituciones descritas en la Ley 340-06, del sector gubernamental central. 2. Los jefes y subjefes de Estado Mayor de las instituciones militares del Ministerio de Defensa, así como el Director y Subdirectores de la Policía Nacional, ni de otros cuerpos policiales o militares. 3. Los funcionarios públicos con injerencia o poder de decisión en cualquier etapa del procedimiento de contratación administrativa. 4. Todo personal de la entidad Adquiriente.	Entendemos, aceptamos y cumplimos.

Página/Folio No.244 de 843

5. Los parientes, por consanguinidad hasta el tercer grado o por afinidad hasta el segundo grado, inclusive, de los funcionarios relacionados con la contratación cubierta por la prohibición, así como los cónyuges, las parejas en unión libre, las personas vinculadas con análoga relación de convivencia afectiva o con las que hayan procreado hijos, y descendientes de estas personas.

6. Las personas jurídicas en las cuales las personas naturales a las que se refieren los enunciados anteriores, cuando tengan una participación superior al diez por ciento (10%) del capital social, dentro de los seis (6) meses anteriores a la fecha de la convocatoria.

7. Las personas físicas o jurídicas que hayan intervenido como asesoras en cualquier etapa del procedimiento de contratación o hayan participado en la elaboración de las especificaciones técnicas o los diseños respectivos, salvo en el caso de los contratos de supervisión.

8. Las personas físicas o jurídicas que hayan sido condenadas mediante sentencia que haya adquirido la autoridad de la cosa irrevocablemente juzgada por delitos de falsedad o contra la propiedad, o por delitos de cohecho, malversación de fondos públicos, tráfico de influencia, prevaricación, revelación de secretos, uso de información privilegiada o delitos contra las finanzas públicas, hasta que haya transcurrido un plazo igual al doble de la condena. Si la condena fuera por delito contra la administración pública, la prohibición para contratar con el Estado será perpetua.

9. Las empresas cuyos directivos hayan sido condenados por delitos contra la administración pública, delitos contra la fe pública o delitos comprendidos en las convenciones internacionales de las que el país sea signatario.

10. Las personas físicas o jurídicas que se encontraren inhabilitadas en virtud de cualquier ordenamiento jurídico.

11. Las personas que suministraren informaciones falsas o que participen en actividades ilegales o fraudulentas relacionadas con la contratación.

12. Las personas naturales o jurídicas que se encuentren sancionadas administrativamente con inhabilitación temporal o permanente para contratar con entidades del sector público, de acuerdo a lo dispuesto por las normativas vigentes en materia de Compras y Contrataciones Públicas.

13. Las personas naturales o jurídicas que no estén al día en el cumplimiento de sus obligaciones tributarias o de la seguridad social, de acuerdo con lo que establezcan las normativas vigentes.

14. Las personas naturales o jurídicas que al momento actual estén realizando

Página/Folio No.245 de 843

trabajos para organizaciones políticas de la República Dominicana. **PÁRRAFO I**: Para los funcionarios contemplados en los Numerales 1 y 2, la prohibición se extenderá hasta seis (6) meses después de la salida del cargo. **PÁRRAFO II**: Para las personas incluidas en los Numerales 4, 5 y 6 relacionadas con el personal referido en el Numeral 3, la prohibición será de aplicación en el ámbito de la institución en que estos últimos prestan servicios.	

1.21.2 Declaraciones de Capacidad para Contratar

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Los Oferentes/Proponentes deben demostrar que: • Al momento de adquirir el Pliego para esta licitación, no están embargados; que durante el proceso no se encuentran en estado de quiebra o en proceso de liquidación; que sus negocios no han sido puestos bajo administración judicial, y que sus actividades comerciales no han sido suspendidas ni se ha iniciado procedimiento judicial en su contra por cualquiera de los motivos precedentes.	Entendemos, aceptamos y cumplimos. Ver los siguientes puntos. Carpeta 1 / sección 1 / N°15 Carpeta 4 / sección 5/ N°28 Carpeta 3 / sección 1 /N° 6 Carpeta 3 / sección 2 /N° 10 Carpeta 3 / sección 3 /N° 16 Carpeta 3 / sección 4 /N° 21
• Han cumplido con sus obligaciones tributarias y de seguridad social.	Carpeta 1 / sección 1 / N°13 y 14 Carpeta 3 / sección 1 /N°5 Carpeta 3 / sección 3 /N°15 Carpeta 3 / sección 4 /N°20 Carpeta 4 / sección 5 /N°27
• Han cumplido con las demás condiciones de participación, establecidas de antemano en los avisos y el presente Pliego de Condiciones.	Carpeta 1 / sección 1 / N°13 y 14 Carpeta 3 / sección 1 /N°5 Carpeta 3 / sección 3 /N°15 Carpeta 3 / sección 4 /N°20 Carpeta 4 / sección 5 /N°27
• Se encuentran legalmente domiciliados y establecidos en el país de origen.	Carpeta 1 / sección 1 /N°5 Carpeta 3 / sección 1 /N°7 Carpeta 3 / sección 2 /N°11 Carpeta 3 / sección 3 /N°17 Carpeta 3 / sección 4 /N°22 Carpeta 4 / sección 5 /N°29

Página/Folio No.246 de 843

• Que los fines sociales sean compatibles con el objeto contractual; es decir que en los estatutos de la empresa esté consignado que la misma está facultada para realizar el tipo de trabajo requerido en la presente licitación.	Carpeta 1 / sección 1 /N°5 Carpeta 3 / sección 1 /N°7 Carpeta 3 / sección 2 /N°11 Carpeta 3 / sección 3 /N°17 Carpeta 3 / sección 4 /N°22 Carpeta 4 / sección 5 /N°29
• Que ni ellos ni su personal directivo hayan sido condenados por un delito relativo a su conducta profesional o por declaración falsa o fraudulenta acerca de su idoneidad para firmar un contrato adjudicado.	Carpeta 1 / sección 1 /N°15 Carpeta 3 / sección 1 /N°6 Carpeta 3 / sección 2 /N°10 Carpeta 3 / sección 3 /N°16 Carpeta 3 / sección 4 /N°21 Carpeta 4 / sección 5 /N°28
• Que no han incurrido o permitido faltas que, por su naturaleza, la Junta Central Electoral, se haya visto afectada en sus obligaciones institucionales.	Carpeta 1 / sección 1 /N°15 Carpeta 3 / sección 1 /N°6 Carpeta 3 / sección 2 /N°10 Carpeta 3 / sección 3 /N°16 Carpeta 3 / sección 4 /N°21 Carpeta 4 / sección 5 /N°28

1.22 Representante Legal

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Todos los documentos que presente el Oferente/Proponente dentro de la presente licitación, deberán estar firmados por él, o su Representante Legal, debidamente facultado al efecto.	Entendemos, aceptamos y cumplimos.

1.23Agente Autorizado

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Cada Oferente/Proponente, antes de realizar su primera consulta, podrá nombrar hasta dos (2) personas físicas, que puedan actuar indistinta y separadamente como sus Agentes Autorizados a los efectos de la licitación. La designación de los Agentes Autorizados deberá efectuarse mediante comunicación escrita de acuerdo con el modelo de "Carta de Designación o Sustitución de Agentes Autorizados" y el modelo de "Carta de Aceptación de Designación como Agentes Autorizados". Ambos modelos se anexan a este Pliego de Condiciones. (FL-03, FL-04).	Entendemos y aceptamos.

Página/Folio No.247 de 843

Los "Agentes Autorizados" serán las únicas personas facultadas por el Oferente/Proponente para efectuar consultas en relación con el proceso de licitación y recibir en nombre del Oferente/Proponente y con efecto obligatorio para éste, las Circulares y/o Enmiendas que formule el Comité de Compras y Contrataciones. El Oferente/Proponente podrá sustituir y revocar la designación de cualquiera de los Agentes Autorizados, o cambiar su domicilio, teléfono, fax, correo electrónico, mediante comunicación escrita de acuerdo con el modelo de Carta de Designación o Sustitución de Agentes Autorizados y el modelo de Carta de Aceptación de Designación como Agentes Autorizados. La sustitución de uno o más Agentes Autorizados o el cambio de domicilio, teléfono, fax, correo electrónico estarán vigentes desde la fecha de recepción por parte del Comité de Compras y Contrataciones, de las cartas antes indicadas. La sustitución de uno o más Agentes Autorizados no requerirá el consentimiento del o los Agente(s) Autorizado(s) sustituido(s).	

1.24 Subsanaciones

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
A los fines de la presente Licitación se considera que una oferta se ajusta sustancialmente al Pliego de Condiciones, cuando concuerda con los términos y especificaciones de dicho documento, sin desviaciones, reservas, omisiones o errores significativos. La ausencia de requisitos relativos a las credenciales de los Oferentes es siempre subsanable. La determinación de la Entidad Contratante de que una oferta se ajusta sustancialmente a los documentos de la licitación, se basará en el contenido de la propia oferta, sin que necesariamente tenga que recurrir a pruebas externas. Siempre que se trate de errores u omisiones de naturaleza subsanable, entendiendo por éstos, generalmente, aquellas cuestiones que no afecten el principio de que las ofertas deban ajustarse sustancialmente al Pliego de Condiciones, la Entidad Contratante podrá corregir el error o solicitar que, en un plazo breve, el Oferente/Proponente suministre la información faltante. El Comité de Compras y Contrataciones rechazará toda oferta que no se ajuste sustancialmente al Pliego de Condiciones. No se admitirán correcciones posteriores que permitan que cualquier oferta, que inicialmente no se ajustaba a dicho Pliego, posteriormente se ajuste al mismo.	Entendemos y aceptamos.

1.24.1 Excepciones

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"

Página/Folio No.248 de 843

A los fines de la presente Licitación se considera que una oferta se ajusta sustancialmente al Pliego de Condiciones, cuando concuerda con los términos y especificaciones de dicho documento, sin desviaciones, reservas, omisiones o errores significativos. La ausencia de requisitos relativos a las credenciales de los Oferentes es siempre subsanable. La determinación de la Entidad Contratante de que una oferta se ajusta sustancialmente a los documentos de la licitación, se basará en el contenido de la propia oferta, sin que necesariamente tenga que recurrir a pruebas externas. Siempre que se trate de errores u omisiones de naturaleza subsanable, entendiendo por éstos, generalmente, aquellas cuestiones que no afecten el principio de que las ofertas deban ajustarse sustancialmente al Pliego de Condiciones, la Entidad Contratante podrá corregir el error o solicitar que, en un plazo breve, el Oferente/Proponente suministre la información faltante. El Comité de Compras y Contrataciones rechazará toda oferta que no se ajuste sustancialmente al Pliego de Condiciones. No se admitirán correcciones posteriores que permitan que cualquier oferta, que inicialmente no se ajustaba a dicho Pliego, posteriormente se ajuste al mismo.	Entendemos y aceptamos.

1.24.2 Rectificaciones Aritméticas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Para fines de subsanaciones, los errores aritméticos serán corregidos de la siguiente manera: • Si existiere una discrepancia entre una cantidad parcial y la cantidad total obtenida multiplicando las cantidades parciales, prevalecerá la cantidad parcial y el total será corregido. • Si la discrepancia resulta de un error de suma o resta, se procederá de igual manera; esto es, prevaleciendo las cantidades parciales y corrigiendo los totales. • Si existiere una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras. • Si el Oferente no acepta la corrección de los errores, su oferta será rechazada. No se admitirán correcciones posteriores que permitan que cualquier oferta, que inicialmente no se ajustaba a dicho Pliego, posteriormente se ajuste al mismo.	Entendemos y aceptamos.

1.25Descripción de los bienes

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"

Página/Folio No.249 de 843

Las características de los bienes y servicios objeto de la presente licitación, están indicadas en la Ficha Técnica, la cual se encuentra en el presente documento como parte integral y vinculante del mismo (Ver numeral 1.7 del presente Pliego de Condiciones Específicas).	Entendemos, aceptamos y cumplimos.

1.26 Duración del servicio

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Por tratarse de un documento de seguridad y para mantener la homogeneidad o igualdad, tanto en la impresión, como en las características técnicas que habrán de emplearse en la elaboración de la nueva Cédula de Identidad y Electoral y la Cédula de Identidad, el contrato para la producción será por el período de vigencia de la nueva Cédula de Identidad y Electoral y Cédula de Identidad, diez (10) años, por lo que cada Oferente propondrá su mejor programa de producción o entrega y la Junta Central Electoral evaluará en función de su máximo interés. En todo caso, la Junta Central Electoral se reserva el derecho de rescindir el contrato, por causas atendibles, en cualquier etapa de su ejecución, siguiendo el procedimiento establecido en el contrato mismo y en el presente Pliego de Condiciones.	Entendemos y aceptamos.

1.27 Lugar y Programa de Suministros

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Los pedidos se librarán en el lugar designado por la Entidad Contratante dentro del ámbito territorial de la República Dominicana y conforme al cronograma de entrega que se establezca. En caso de no especificarse, se entenderá que el lugar de entrega será la sede principal de la Junta Central Electoral.	Entendemos y aceptamos.

1.27.1 Alcance

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
• Suministro de tarjetas de identidad: - Suministrar 7,200,000 de CIEs. - Suministrar 800,000 unidades de CIs emitidas a extranjeros, menores de 18, militares y policías, que no votan.	Entendemos y aceptamos.

Página/Folio No.250 de 843

- 900,000 CIEs anuales a partir del segundo año de operación y por 9 años adicionales. - 100,000 CIs anuales a partir del segundo año de operación y por 9 años adicionales. - Ambas tarjetas serán idénticas, salvo el color del fondo del policarbonato para poder diferenciarlas. Debe ofertarse un color diferente para cada una. • Suministro de equipos de impresión láser de tarjeta: - 214 máquinas de impresión, de las cuales 164 para la operación nacional en el país y 50 para el exterior de la República Dominicana. - Suministrar, Instalar y configurar los equipos de impresión en todos los centros. - Sistema de personalización (de la propia impresora). - Integración con el actual sistema de gestión con sede en la JCE. • PKI Infraestructura de clave pública (PKI). • El adjudicatario apoyará a la JCE en todos los aspectos relativos a la gestión de ser Autoridad Certificadora (CA). En cualquier caso, la responsabilidad de obtener la CA será de la JCE, de acuerdo con las leyes de la República Dominicana. • Tarjeta de Identidad Digital (CD) o Mobile ID • Servicios profesionales: - Instalación - Logística - Capacitación	

1.27.2 Etapas del contrato

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Habrá tres (3) etapas del contrato. • ETAPA 1: Implantación y puesta en marcha del proyecto. • ETAPA 2: Puesta en marcha y cedulación total de la población. • ETAPA 3: Operación anual y mantenimiento	Entendemos y aceptamos.

1.27.3 Etapa 1: Implantación y puesta en marcha del proyecto

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
En esta etapa, que durará máximo veintiséis (26) semanas a partir de la firma del contrato, el adjudicatario tendrá que realizar las siguientes actividades:	Entendemos y aceptamos.

1. Entregar el diseño de seguridad de las tarjetas a las cuatro (4) semanas después de la firma de contrato. 2. Suministrar dos impresoras de policarbonato a las dieciséis (16) semanas, así como 2,000 tarjetas genéricas de policarbonato con chip para pruebas. 3. Instalar la PKI y la CA, así como realizar la ceremonia de llaves a las dieciséis (16) semanas. 4. Ayudar a los técnicos de la JCE a adaptar el SDK de la impresora al sistema de la JCE. 5. Realizar pruebas unitarias, de integración, de pre-producción con las impresoras, las tarjetas, personalizando la tarjeta. 6. Realizar las pruebas piloto de la solución digital de la tarjeta CD (Mobile ID) antes de veintiséis (26) semanas, incluyendo el desarrollo de una app para la JCE. 7. Entrega de 300,000 tarjetas de policarbonato a las veintidós (22) semanas después de la firma de contrato. Esta entrega será acompañada con el reporte de laboratorio certificado e independiente, de los test de durabilidad de la tarjeta, así como el chip. 8. Capacitación al personal de la JCE de la operación y mantenimiento del equipo de impresión, PKI y solución digital.	

1.27.4 Etapa 2: Operación de la re-cedulación total de la población

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Todos los dominicanos iniciarán un periodo de reemplazo de su tarjeta actual a partir de esa fecha. En esta etapa, que durará máximo 12 meses a partir de la finalización de la etapa 1, el oferente adjudicado tendrá que realizar las siguientes actividades o entregar los siguientes elementos: 1. 500,000 tarjetas de policarbonato a las 26 semanas después de la firma de contrato. 2. 1,200,000 tarjetas de policarbonato a las 30 semanas después de la firma de contrato. 3. 1,000,000 tarjetas de policarbonato a las 34 semanas después de la firma de contrato. 4. 1,000,000 tarjetas de policarbonato a las 38 semanas después de la firma de contrato. 5. 1,000,000 tarjetas de policarbonato a las 42 semanas después de la firma de contrato. 6. 1,000,000 tarjetas de policarbonato a las 46 semanas después de la firma de contrato. 7. 1,000,000 tarjetas de policarbonato a las 50 semanas después de la firma de contrato.	Entendemos y aceptamos.

Página/Folio No.252 de 843

8. 1,000,000 tarjetas de policarbonato a las 54 semanas después de la firma de contrato. 9. Adquisición e instalación de los equipos de impresión y puesta en marcha en las sedes de la República Dominicana y en el exterior. Las fechas de las entregas y cantidades de dichos equipos serán acordados con el proveedor adjudicado y la JCE. 10. Puesta en marcha del mantenimiento de las impresoras en periodo de garantía. Para ello, el proveedor deberá de disponer de mínimo de dos (2) técnicos certificados en tecnología de impresión de tarjetas de identidad, y mínimo un total de diez (10) técnicos para soporte nacional de servicio para reparación de equipos en sitio durante el periodo de garantía. Para el exterior, el proveedor durante tiempo de garantía de las impresoras, deberá reparar en Nueva York (los equipos de Estados Unidos y Canadá) y en Madrid (los equipos de Europa), la JCE enviará las impresoras defectuosas a estos lugares según aplique. NOTA: La JCE podrá acordar con el adjudicatario el cambio de fechas o de cantidad, por problemas de almacenamiento o de consumo de las tarjetas.	

1.27.5 Etapa 3: Operación y mantenimiento

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Una vez terminada la etapa anterior, se inicia la fase de Operación y Mantenimiento, la cual durará doce (12) meses y podrán ser renovables hasta alcanzar los diez (10) años del contrato. Esta fase contemplará las siguientes actividades: 1. Suministrar tarjetas en la oficina Central de la JCE en base a la demanda que se requiera durante la vigencia del contrato que se estima en 1.000.000 de tarjetas al año, siempre un 10% CI. En todo momento la responsabilidad de poseer disponibilidad de CIs y CIEs es del proveedor. 2. Proveer mantenimiento de los equipos de impresión mientras los equipos estén en garantía. Cuando termine la garantía, los equipos deberán ser atendidos en las siguientes localidades: • Para los centros de cedulación ubicados en todo el territorio nacional, serán atendidos en la sede central de la JCE. • Para las oficinas OSE ubicadas en Estados Unidos de Norte América, serán atendidas en la OSE de New York. • Para las oficinas OSE ubicadas en Europa, serán atendidas en la OSE de Madrid.	Entendemos y aceptamos.

Página/Folio No.253 de 843

• Para las demás oficinas ubicadas en otras demarcaciones, serán atendidas en la Sede Central de la JCE. 3. Proveer mantenimiento de nivel 3 para el mantenimiento del sistema y equipos PKI, y sistemas y equipos para la tarjeta digital.	

Página/Folio No.254 de 843

1.27.6 Detalle del alcance de las etapas

<table>
<tr><th>Requerimiento</th><th>Respuesta Consorcio "Identidad 4.0 RD"</th></tr>
<tr><td>urante la etapa de Implementación y Puesta en Marcha el adjudicatario deberá suministrar bienes, insumos y servicios complementarios listados a continuación:

Etapa 1. Implantación y puesta en marcha del proyecto

Esta etapa durará como máximo veintiséis (26) semanas.

<table>
<tr><th>Ítem</th><th>Descripción</th></tr>
<tr><td>1. Diseño y tarjetas iniciales</td><td>Entregar el diseño de seguridad de las tarjetas a las cuatro (4) semanas después de la firma de contrato.
2,000 tarjetas de policarbonato genéricas con chip para pruebas a las dieciséis (16) semanas.
Entrega de 300,000 tarjetas de policarbonato a las veintidós (22) semanas después de la firma de contrato.</td></tr>
<tr><td>2. Instalación y puesta en marcha de 2 impresoras</td><td>Suministrar dos impresoras de policarbonato a las dieciséis (16) semanas.
Ayudar a los técnicos de la JCE a adaptar el SDK de la impresora al sistema de la JCE.
Realizar pruebas unitarias, de integración, de pre-producción con las impresoras, las tarjetas, personalizando la tarjeta.</td></tr>
<tr><td>3. Puesta en marcha de la CA y PKI</td><td>Instalación de la CA y la PKI, así como realizar la ceremonia de entrega de llaves a las dieciséis (16) semanas.</td></tr>
<tr><td>4. Desarrollo, implantación y despliegue de piloto de la Tarjeta de Identidad Digital (CD)</td><td>Realizar las pruebas piloto de la solución digital de la tarjeta CD (Mobile ID) antes de veintiséis (26) semanas, incluyendo el desarrollo de una app para la JCE.</td></tr>
<tr><td>5. Capacitación</td><td>Capacitación al personal de la JCE de la operación y</td></tr>
</table>
</td><td>Entendemos y aceptamos.</td></tr>
</table>

Página/Folio No.255 de 843

	mantenimiento del equipo de impresión, PKI y solución digital.

Etapa 2. Operación de la re-cedulación total de la población

Esta etapa durará máximo doce (12) meses a partir de la finalización de la etapa 1.

Item	Descripción
1. Suministro del inventario de tarjetas para la cedulación nacional. NOTA: La JCE podrá acordar con el adjudicatario el cambio de fechas o de cantidad, por problemas de almacenamiento o de consumo de las tarjetas.	500,000 tarjetas de Policarbonato a las 26 semanas después de la firma de contrato. 1,200,000 tarjetas de Policarbonato a las 30 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 34 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 38 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 42 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 46 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 50 semanas después de la firma de contrato. 1,000,000 tarjetas de Policarbonato a las 54 semanas después de la firma de contrato.
2. Adquisición e Instalación de los equipos de impresión y puesta en marcha en las sedes de la República Dominicana y en el exterior. NOTA: La JCE podrá acordar con el adjudicatario el cambio de fechas o de cantidad.	Instalación de maquinaria de personalización Integración con el sistema central de captura de datos y personalización. Las fechas de las entregas y cantidades de dichos equipos serán acordados con el proveedor adjudicado y la JCE.
3. Puesta en marcha del mantenimiento.	Puesta en marcha del mantenimiento de las impresoras en periodo de garantía. Para ello, el proveedor deberá de disponer de mínimo de dos (2) técnicos certificados en tecnología de impresión

Página/Folio No.256 de 843

	de tarjetas de identidad, y mínimo un total de diez (10) técnicos para soporte nacional de servicio para reparación de equipos en sitio durante el periodo de garantía. Para el exterior, el proveedor en el tiempo de garantía de las impresoras, deberá arreglarlas en Nueva York y Madrid, donde la JCE recogerá las impresoras defectuosas para su arreglo.

Etapa 3. Operación y mantenimiento

Una vez terminada la etapa 2, se inicia la fase de Operación y Mantenimiento, la cual durará doce(12) meses y podrán ser renovables hasta los diez (10) años de contrato

Ítem	Descripción
1. Suministro de tarjetas de identidad	Suministrar tarjetas en la oficina Central de la JCE en base a la demanda que se requiera durante la vigencia del contrato que se estima en 1,000,000 de tarjetas al año, siempre un 10% CI. En todo momento la responsabilidad de poseer disponibilidad de CIs y CIEs es del proveedor.
2. Mantenimiento del sistema de impresión en República Dominicana y en resto del Mundo	Proveer mantenimiento de los equipos de impresión en sitio mientras los equipos estén en garantía. Cuando la garantía se termine, el proveedor adjudicado deberá ir a las oficinas central de JCE para reparar los equipos que serán traídos de varias sucursales, solo cuando no han podido ser reparados por personal de la JCE (en el exterior a Nueva York y Madrid) entrenados por el proveedor. En dicho mantenimiento, deberá sustituir las piezas que estén defectuosas o rotas, siempre que sea por un uso normal de las impresoras.
3. Mantenimiento PKI, sistemas y CD	Proveer mantenimiento de nivel 3 para el mantenimiento del sistema y equipos PKI, y sistemas y equipos para la tarjeta digital.

Página/Folio No.257 de 843

1.27.7 Fases de producción y entregas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
1.27.7.1 Fases de diseño y puesta en marcha El proceso de elaboración del diseño gráfico será llevado en conjunto con personal de JCE, quienes aprobarán la versión final del diseño gráfico tras la propuesta del oferente. Para esta tarea, la JCE proporcionará con la firma de contrato, una serie de imágenes que deberán ser consideradas por la empresa ganadora en su diseño. La empresa ganadora del proceso de licitación deberá de entregar a la JCE el proyecto de arte final de la CI, por un lado, y de la CIE por otro, con un plazo no mayor de cuatro (4) semanas posteriores a la firma de la orden de inicio. Cada oferente en su oferta debe entregar una propuesta de diseño gráfico de las nuevas tarjetas de República Dominicana en formato impreso y electrónico. La Junta Central Electoral se reserva el derecho de asignar y desplazar a un equipo de técnicos para evaluar, in-situ, el proceso de producción en las instalaciones del proponente. El oferente suministrará dos impresoras de policarbonato a las dieciséis (16) semanas, así como 2,000 tarjetas de policarbonato con chip para pruebas. **1.27.7.2 Fase de producción masiva** El inicio de la producción de las tarjetas deberá contar con el visto bueno de la JCE una vez se haya revisado y aprobado el diseño e insumos de producción. En el primer año de ejecución del proyecto, a partir de la orden de inicio del contrato y aprobación de los diseños gráficos, el oferente deberá de entregar: • 300,000 tarjetas de policarbonato a las 22 semanas después de la firma de contrato. • 500,000 tarjetas de policarbonato a las 26 semanas después de la firma de contrato. • 1,200,000 tarjetas de policarbonato a las 30 semanas después de la firma de contrato. • 1,000,000 tarjetas de policarbonato a las 34 semanas después de la firma de contrato. • 1,000,000 tarjetas de policarbonato a las 38 semanas después de la firma de contrato.	Entendemos y aceptamos.

Página/Folio No.258 de 843

• 1,000,000 tarjetas de policarbonato a las 42 semanas después de la firma de contrato. • 1,000,000 tarjetas de policarbonato a las 46 semanas después de la firma de contrato. • 1,000,000 tarjetas de policarbonato a las 50 semanas después de la firma de contrato. • 1,000,000 tarjetas de policarbonato a las 54 semanas después de la firma de contrato. Las siguientes entregas serán acordadas con la JCE, estimando una entrega de 1,000,000 de tarjetas por año. **1.27.7.3 Cantidad total contratada** El contrato tendrá una duración diez (10) años. Se adquieren 8,000,000 de tarjetas electrónicas desde la firma del contrato y de acuerdo con el plan que se pacte. Adicionalmente, la JCE se compromete a la adquisición de al menos 1,000,000 de tarjetas adicionales al año durante los nueve años siguientes a la entrega de las primeras 8,000,000 de tarjetas. Se harán revisiones anuales para determinar las cantidades de tarjetas a entregar, hasta finalizar el contrato. Se firmará una Modificación/Respuesta o enmienda para incluir los costos de dichas entregas anuales. **1.27.7.4 Formas de entrega** La entrega de tarjetas se realizará en cajas que contendrá mil (1,000) unidades correlativas debidamente embaladas y selladas por la empresa ganadora, que garanticen el resguardo de condiciones ambientales y atmosféricas de los productos. La entrega se hará efectiva en el lugar que determine la JCE dentro de República Dominicana.	

1.27.8 Otras consideraciones

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
1.27.8.1 Derechos de propiedad La empresa adjudicataria deberá entregar a la JCE a más tardar dos (2) semanas después de la aprobación del diseño final:	Entendemos y aceptamos.

Página/Folio No.259 de 843

• Artes finales en formato digital (adobe, Corel Draw, u otro editable); • Artes finales de cada capa de diseño por separado; • Detalle de los elementos utilizados dentro de la producción de las CI y CIE; • Guía física del arte por separación de colores. • Protocolos de destrucción de tambores y planchas utilizadas en el proceso de producción de CI y CIE. **1.27.8.2 Control de calidad** Si se encontraren tarjetas dañadas, deterioradas, con desperfectos de fábrica, el adjudicatario deberá sustituirlas en un plazo no mayor a treinta (30) días calendarios, contados a partir de la fecha de notificación. Durante la recepción del suministro, la JCE hará pruebas al azar del producto para verificar las cantidades el número de ejemplares y comprobar el estado que deben de tener las tarjetas; reservándose el derecho de aceptar o rechazar total o parcialmente el producto. La empresa deberá entregar un manual impreso y otro en formato digital (Word y PDF) con las instrucciones de uso y recomendaciones para el manejo y resguardo de las tarjetas. El documento, entre otras cosas, deberá especificar las condiciones ambientales y de infraestructura recomendables del lugar en el cual serán almacenadas. Todo esto dirigido al Director de Cedulación de la JCE, Santo Domingo, República Dominicana.	

1.28Garantías

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Los Oferentes/Proponentes deberán presentar las garantías en la misma moneda de la oferta, y serán las siguientes: **1.28.1 Garantía de Seriedad de la Oferta** Para asegurar la seriedad de la Oferta, cada Oferente depositará una Póliza de Garantía a favor de la Junta Central Electoral por el equivalente al uno por ciento (1%) del monto total de la oferta, la cual deberá estar incluida dentro del sobre contentivo de la Propuesta Económica ("Sobre B"), al momento de presentarse las ofertas. La omisión de la Garantía de Seriedad de la Oferta; cuando la misma fuere insuficiente; cuando no esté en la misma moneda de la oferta; o cuando no fuere emitida a favor de la Junta Central Electoral,	Entendemos y aceptamos.

Página/Folio No.260 de 843

significará la desestimación de la oferta sin más trámite. La garantía debe tener una vigencia mínima de ciento cincuenta (150) días calendario. **1.28.2 Garantía de Fiel Cumplimiento** El adjudicatario cuyo contrato exceda el equivalente en Pesos Dominicanos de Diez Mil Dólares Estadounidenses con 00/100 (USD$10,000.00), está obligado a constituir una Póliza de Garantía en el plazo de cinco (5) días hábiles, contados a partir de la notificación de la adjudicación, por el importe del Cuatro Por Ciento (4%) del monto total del contrato a intervenir, a disposición de la Junta Central Electoral, cualquiera que haya sido el procedimiento y la forma de adjudicación del Contrato. La misma debe ser emitida por una entidad bancaria o compañía de seguros de reconocida solvencia en la República Dominicana y debe tener un tiempo de vigencia mínima de tres (3) meses posteriores al vencimiento del Contrato, deberá ser incondicional, irrevocable y renovable. **1.28.3 Garantía de Buen uso del Anticipo** En caso de que el adjudicatario requiera de la entrega de algún pago anticipado, estará obligado a constituir una garantía equivalente al monto recibido por adelanto, bajo el esquema de póliza de seguro. Esta garantía sirve para asegurar el buen uso del monto que reciba el adjudicatario por adelantado, y además, podrá responder, entre otras, a garantía por vicios ocultos (garantía calidad de bienes), por los gastos originados a la Junta Central Electoral por demora del Proveedor en el cumplimiento de sus obligaciones y de los daños y perjuicios ocasionados a la misma, con motivo de la ejecución del contrato o en el supuesto de incumplimiento del mismo.	

1.29 Devolución de las Garantías

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
a) **Garantía de Seriedad de la Oferta:** Le será devuelta al adjudicatario en un plazo no mayor de diez (10) días hábiles, contados a partir de la constitución de la Garantía de Fiel Cumplimiento del Contrato establecida en el numeral 1.28.2 y de haberse suscrito el Contrato correspondiente. A los demás Oferentes/Proponentes les será devuelta en un plazo no mayor de tres (3) días hábiles, contados a partir de la constitución de la Garantía de Fiel Cumplimiento por parte del Adjudicatario. b) **Garantía de Fiel Cumplimiento de Contrato:** Después de aprobada la liquidación del Contrato, si no resultaren responsabilidades que hayan de ejercerse sobre la garantía y transcurrido el plazo de la misma, se ordenará su devolución.	Entendemos y aceptamos.

Página/Folio No.261 de 843

c) **Garantía de Buen uso del Anticipo:** Esta fianza será liberada cuando todos los equipos, materiales o servicios requeridos, descansen en los almacenes de la Junta Central Electoral y fuesen recibidos satisfactoriamente.	

1.30 Devolución de las Garantías

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Todo litigio, controversia o reclamación resultante de este documento y/o del o los contratos a intervenir, sus incumplimientos, interpretaciones, resoluciones o nulidades, serán sometidos al Tribunal Superior Administrativo, conforme al procedimiento establecido en la Ley 13-07, de fecha cinco (5) de febrero del 2007, previo al agotamiento de los procedimientos administrativos establecidos en el Reglamento Interno de Compras, aprobado por la Junta Central Electoral. **Nota:** El (los) Proponente (s) reconoce (n) que no podrá (n) hacer uso de la facultad de someter algún reclamo al Tribunal Superior Administrativo, sin antes agotar el procedimiento correspondiente ante la Entidad Contratante, en las condiciones que se establece en el Capítulo VI, numeral 6.3 del presente Pliego de Condiciones Específicas.	Entendemos y aceptamos.

Página/Folio No.262 de 843

CAPITULO II
CONSULTAS, CIRCULARES Y ENMIENDAS

Página/Folio No.263 de 843

2.1 Consultas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Sólo los adquirientes de los Pliegos de Condiciones podrán efectuar consultas a través del Comité de Compras y Contrataciones, conforme al siguiente procedimiento:	Entendemos y aceptamos.

2.2 Procedimiento y Plazo

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Las consultas se formularán por escrito a través de uno de los representantes de los Oferentes/Proponentes dentro del plazo previsto en el Cronograma de la Licitación del numeral 1.14 del presente documento. Las Circulares o Enmiendas que emita el Comité de Compras y Contrataciones seguirán el procedimiento establecido en el Pliego de Condiciones y serán notificadas dentro del plazo establecido en el Cronograma de la Licitación fijado en el numeral 1.14 de este documento.	Entendemos y aceptamos.

2.3 Dirección

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Las consultas se remitirán a: JUNTA CENTRAL ELECTORAL Comité de Compras y Contrataciones Referencia: JCE-CCC-LPI-2024-0001 Dirección: Av. Gregorio Luperón esq. Av. 27 de Febrero, Edificio Administrativo, ala Este, 2do. nivel. Teléfono: (809) 537-0946 e-mail: licitaciones@jce.do	Entendemos y aceptamos.

2.4 Circulares

Página/Folio No.264 de 843

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Comité de Compras y Contrataciones podrá emitir circulares de oficio o para dar respuestas a las consultas planteadas por los Oferentes/Proponentes con relación al contenido del presente Pliego de Condiciones, formularios, anexos u otras circulares. Las circulares se hacen de conocimiento de todos los Oferentes/Proponentes.	Entendemos y aceptamos.

2.5 Enmiendas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
De considerarlo necesario, por iniciativa propia o como consecuencia de una consulta, el Comité de Compras y Contrataciones, podrá modificar, mediante enmiendas, el Pliego de Condiciones Específicas, formularios, anexos u otras enmiendas. Las enmiendas se hacen de conocimiento de todos los Oferentes/Proponentes. Tanto las enmiendas como las circulares emitidas por el Comité de Compras y Contrataciones, pasarán a constituir parte integral del presente Pliego de Condiciones y, en consecuencia, serán de cumplimiento obligatorio para todos los Oferentes/Proponentes.	Entendemos y aceptamos.

Página/Folio No.265 de 843

CAPITULO III

PRESENTACIÓN DE DOCUMENTOS DE ACREDITACIÓN Y DOCUMENTOS TÉCNICOS

Página/Folio No.266 de 843

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
3.1 Capacidad y Solvencia A los fines de ser evaluados sobre capacidad y solvencia, los Oferentes/Proponentes deberán depositar ante el Comité de Compras y Contrataciones de la Junta Central Electoral, los siguientes documentos: **3.1.2 Personas Físicas** En la presente licitación no se admitirán propuestas por parte de personas físicas, sólo se admitirán propuestas por parte de personas jurídicas (empresas). **3.1.3 Personas Jurídicas Nacionales** • Comprobante de pago para cubrir gastos administrativos.	Entendemos aceptamos y cumplimos. Ver carpeta 1 / sección 2 / N° 19
• Carta de presentación de la empresa oferente.	Ver carpeta 1 / Seccion 1
• Copia del Registro Nacional del Contribuyente (RNC).	Ver carpeta 1 / Seccion 1
• Registro Proveedores del Estado.	Ver carpeta 1 / Seccion 1
• Copia de Cédula de Identidad y Electoral de la (s) persona (s) con poderes otorgados para suscribir el contrato de adjudicación.	Ver carpeta 1 / Seccion 1
• Registro Mercantil (actualizado).	Ver carpeta 1 / Seccion 1
• Carta del concesionario, casa matriz o distribuidor principal, indicando que el proponente es un suplidor autorizado de la marca ofertada y certificando que en	Ver carpeta 1 / Seccion 1

caso de que el Proponente resulte adjudicatario, la firma asume el compromiso de suplir a éste; los materiales o servicios adjudicados.	
• Carta del concesionario, casa matriz, fabricante o distribuidor principal, en la que detalle las empresas o instituciones públicas del Estado para las cuales haya fabricado materiales similares a los requeridos mediante la presente licitación.	Ver carpeta 1 / Seccion 1
• Copia de los Estatutos Sociales, debidamente registrados en la Cámara de Comercio, certificados como conforme a su original por el secretario, el presidente y/o el gerente de la compañía o por la persona con calidad para hacerlo y sellado con el sello social de la compañía.	Ver carpeta 1 / Seccion 1
• Lista de la composición accionaria actualizada, debidamente registrada en la Cámara de Comercio, certificada como conforme a su original por el secretario, el Presidente y/o el gerente de la compañía y con el sello social.	Ver carpeta 1 / Seccion 1
• Estados Financieros de los últimos tres (3) períodos fiscales, certificados por un Contador Público Autorizado, avalado con copia del IR-2 de esos últimos tres (3) períodos fiscales, incluyendo la entrega certificada con el soporte correspondiente y/o el código de envío electrónico recibido. Las hojas financieras auditadas deben presentarse según la plantilla facilitada en el Anexo 9. Todos los datos financieros (en la plantilla) deben expresarse en Dólares Estadounidenses (USD).	Ver carpeta 1 / Seccion 1
• Poder de representación otorgado ante Notario Público, en caso de que proceda. Cuando la empresa oferente esté representada por su Presidente o por algún directivo, y siempre y cuando los Estatutos Sociales le otorguen el poder de representación de la sociedad, no será necesario este requerimiento.	Ver carpeta 1 / Seccion 1
• Certificación donde se haga constar que está al día en el pago de sus obligaciones fiscales (original).	Ver carpeta 1 / Seccion 1
• Certificación donde se haga constar que está al día en el pago de la Seguridad Social (original).	Ver carpeta 1 / Seccion 1
• Declaración Jurada del solicitante ante un notario público, debidamente legalizada en la Procuraduría General de la República Dominicana, en la que manifieste que no se encuentra dentro de las prohibiciones establecidas en el Artículo 14 de la Ley 340-06, sobre Compras y Contrataciones Públicas. Que no han incurrido o permitido faltas que, por su naturaleza, la Junta Central Electoral se haya visto afectada en sus obligaciones institucionales; que manifieste si tiene o no juicio con el Estado Dominicano o sus entidades del Gobierno Central, de las Instituciones Descentralizadas y Autónomas no Financieras, y de las Instituciones Públicas de la Seguridad Social. Que no están embargados, en estado de quiebra o en proceso de liquidación; sus negocios no han sido puestos bajo administración judicial, y sus actividades comerciales no han sido suspendidas ni se ha iniciado procedimiento judicial en su contra por cualquiera de los motivos precedentes. Que ni ellos ni su personal directivo ha sido condenado por un delito relativo a su conducta profesional o por declaración falsa o fraudulenta acerca de su idoneidad para firmar un contrato adjudicado. (Usar modelo denominado FL-06 que se encuentra anexo al Pliego).	Ver carpeta 1 / Seccion 1

Página/Folio No.268 de 843

• Cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee línea de crédito que pueda solventar al menos el monto de Dos Millones de Dólares Estadounidenses (USD$2,000,000.00), o su equivalente en pesos o euros.	Ver carpeta 1 / Seccion 1
• El oferente deberá proporcionar un mínimo de diez (10) muestras de las tarjetas junto con la propuesta técnica (estas muestras son adicionales a las requeridas para la prueba de concepto). Las muestras deben ser capaces de representar la personalización de las cédulas electrónicas y los detalles de las características que el proveedor propone, y éstas deben explicarse claramente. Junto con las muestras, el proveedor deberá presentar informes de pruebas independientes de acuerdo con la norma ISO 18745. La JCE se reserva el derecho de enviar estas muestras a laboratorios internacionales debidamente certificados, para validar sus características técnicas; en caso de no cumplir, su propuesta será descartada.	Sobre de seguridad "entrega de muestras"
NOTA: Las empresas nacionales que participen en el presente proceso deberán estar consorciadas con empresas nacionales o extranjeras fabricantes de los equipos y materiales objeto de la presente licitación, es decir, no se aceptarán empresas nacionales con cartas de distribuidores exclusivos autorizados si no están consorciados.	Entedemos, aceptamos y cumplimos Ver carpeta 1 / Seccion 2 / N°20
3.1.4 Personas Jurídicas Extranjeras • Comprobante de pago para cubrir gastos administrativos.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Carta de presentación de la empresa oferente.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Copia del pasaporte o documento de identificación válido de la persona con poderes otorgados para suscribir el contrato de adjudicación.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Carta del concesionario, casa matriz o distribuidor principal, indicando que el proponente es un suplidor autorizado de la marca ofertada y certificando que en caso de que el Proponente resulte adjudicatario, la firma asume el compromiso de suplir a éste; los materiales o servicios adjudicados.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Carta del concesionario, casa matriz, fabricante o distribuidor principal, en la que detalle las empresas o instituciones de gobiernos para las cuales haya fabricado materiales similares a los requeridos mediante la presente licitación.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Certificación de pago de la Tesorería de la Seguridad Social -TSS- (En el caso de una persona extranjera, este requisito sólo aplicará cuando dicha empresa se encuentre domiciliada y/o legalmente representada en la República Dominicana).	Carpeta 3 (GET) Carpeta 4 (SELP)
• Constancia de inscripción en el Registro de Proveedores del Estado (RPE). En el caso de una empresa extranjera, no necesitará estar registrada en el RPE, salvo el caso de que se encuentre domiciliada en la Rep. Dom. Sin embargo, si resulta adjudicataria, previa suscripción del contrato, deberá obtener y depositar el registro correspondiente.	Carpeta 3 (GET) Carpeta 4 (SELP)
• La empresa extranjera que resulte adjudicataria deberá solicitar su Registro de Proveedores del Estado (RPE) en un plazo no mayor de diez (10) días hábiles a	Carpeta 3 (GET) Carpeta 4 (SELP)

Página/Folio No.269 de 843

partir de la fecha de notificación de adjudicación. Pasado este plazo sin que se realice dicha inscripción quedará excluida del proceso sin más trámite.	
• Declaración Jurada ante Notario Público y debidamente legalizada por el organismo correspondiente en el país de origen, "donde el Oferente manifieste si tiene o no juicio con el Estado Dominicano o sus entidades del Gobierno Central, de las Instituciones Descentralizadas y Autónomas no Financieras, y de las Instituciones Públicas de la Seguridad Social". Que no han incurrido o permitido faltas que por su naturaleza, la Junta Central Electoral, se haya visto afectadas en sus obligaciones institucionales. La declaración será redactada conforme el formato suministrado en el anexo (FL-06) del presente Pliego.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Poder de representación otorgado ante Notario Público, en caso de que proceda. En caso de que la firma que otorgue el poder no esté establecida en el país, el Poder de Representación deberá ser certificado ante el consulado acreditado por el Estado Dominicano en el país de emisión y legalizado en el Ministerio de Relaciones Exteriores de la República Dominicana (MIREX).	Carpeta 3 (GET) Carpeta 4 (SELP)
• Todo poder que hubiese sido otorgado en un idioma que no sea el español; deberá de ser traducido por un intérprete judicial en la República Dominicana, en cuyo caso la firma de traducción deberá estar legalizada en la Procuraduría General de República. En caso de que la empresa Oferente esté representada por su Presidente o por uno de sus directivos, siempre y cuando los Estatutos Sociales le otorguen el Poder de Representación de la sociedad, no será necesario presentar este requerimiento.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Documentación pertinente que demuestre la legalidad de la constitución de la empresa en su país de origen. Deberán depositar junto a los documentos constitutivos exigidos por el país de origen, un certificado de "Good Standing", o su equivalente en el país del que se trate, que es el certificado de existencia de la compañía, expedido por la entidad gubernamental o Estatal respectiva. Dicho documento deberá contener las legalizaciones correspondientes.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Certificación actualizada y legible del organismo, que, en el país de origen de la empresa, sea el que determine que la misma se encuentra al día con sus obligaciones fiscales.	Carpeta 3 (GET) Carpeta 4 (SELP)
• Copia certificada del equivalente físico o electrónico al formulario IR-2 de la DGII (Dirección General de Impuestos Internos), o su equivalente, de los últimos tres (3) períodos fiscales, donde quede constancia oficial de la valoración efectiva de los aportes fiscales en su país de origen. Las hojas financieras auditadas deben presentarse según la plantilla facilitada en el Anexo 9. Todos los datos financieros (en la plantilla) deben expresarse en Dólares Estadounidenses (USD).	Carpeta 3 (GET) Carpeta 4 (SELP)
• Cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee línea de crédito que pueda solventar al menos el monto de USD$2.000.000.00 (o su equivalente en pesos o euros).	Carpeta 3 (GET) Carpeta 4 (SELP)
• El oferente deberá proporcionar un mínimo de diez (10) muestras originales de las tarjetas junto con la propuesta técnica. Las muestras deben ser capaces de representar la personalización de las cédulas electrónicas y los detalles de las características de seguridad que el proveedor propone, y éstas deben explicarse	Carpeta 3 (GET) Carpeta 4 (SELP)

Página/Folio No.270 de 843

claramente. Junto con las muestras, el proveedor deberá presentar informes de pruebas independientes de acuerdo con la norma ISO 18745.	
NOTA: Las empresas extranjeras que participen en el proceso deberán estar consorciadas con una empresa nacional relacionada con el objeto de la presente licitación.	Carpeta 3 (GET) Carpeta 4 (SELP)
Los documentos societarios, la Declaración Jurada, los poderes otorgados, así como cualquier otro documento que deba ser legalizado, deberán certificarse ante el consulado acreditado por el Estado Dominicano en el país de emisión y legalizado en el Ministerio de Relaciones Exteriores (MIREX).	Carpeta 3 (GET) Carpeta 4 (SELP)
Las legalizaciones de dichos documentos deben ser presentadas antes de la firma del Contrato con la empresa que resulte adjudicataria.	Carpeta 3 (GET) Carpeta 4 (SELP)
En caso de que la empresa Oferente sea originaria de un país miembro de la Convención de la Apostilla (Convención de la Haya, del 5 de octubre del 1961), podrá apostillar los documentos públicos que deban ser presentados, suprimiendo las legalizaciones diplomáticas necesarias.	Carpeta 3 (GET) Carpeta 4 (SELP)
Los documentos entregados en las propuestas deberán ser presentados en idioma español. La empresa oferente será la responsable de la exactitud y veracidad de las traducciones que sean necesarias.	Carpeta 3 (GET) Carpeta 4 (SELP)
Una vez completado este proceso, la Junta Central Electoral procederá a emitir la resolución correspondiente, declarando Oferente Habilitado o Inhabilitado para apertura de Oferta Económica en la licitación.	Carpeta 3 (GET) Carpeta 4 (SELP)
Con carácter previo a la fecha indicada para la apertura de la Propuesta Económica "Sobre B", se comprobará la documentación aportada por los Oferentes/Proponentes relativa a su capacidad, solvencia, propuesta técnica y muestras físicas de los formularios ofertados, descalificándose para participar en la presente licitación aquellos que no cumplan con los requisitos establecidos en el presente Pliego de Condiciones; y que, por tanto, no serán convocados ni podrán participar en las etapas restantes de la licitación.	Carpeta 3 (GET) Carpeta 4 (SELP)
NOTA: Los documentos de acreditación y solvencia, así como los documentos técnicos son subsanables (con excepción de los requisitos obligatorios), por lo cual su no presentación junto a la propuesta técnica no implica, necesariamente, el rechazo de la propuesta. Sin embargo, la no presentación de estos documentos junto a la propuesta técnica, o cuando siendo depositados junto a dicha propuesta estén incompletos o desactualizados, implicará la pérdida de la puntuación asignada para la evaluación, independientemente de que se incorporen o subsanen en los plazos otorgados a esos fines.	Carpeta 3 (GET) Carpeta 4 (SELP)
3.1.5 Personas Jurídicas Extranjeras Las empresas que actúen como Consorcio deben depositar un acuerdo bajo firma privada de constitución de consorcio, que haga a sus integrantes corresponsables de las acciones de este, incluyendo su objeto, las obligaciones de las partes, su porcentaje de participación y su relación con el órgano licitante. El documento debe ser debidamente notariado y legalizado.	Carpeta 1 / Seccion 2 / N°20

Página/Folio No.271 de 843

En el acuerdo deberá designarse un representante o gerente único. También, se acreditará la capacidad de ejercicio de cada miembro del consorcio, la solvencia económica y financiera y la idoneidad técnica y profesional; dicha solvencia e idoneidad se podrá acreditar mediante la consideración conjunta de las credenciales de cada uno de los miembros, depositando la documentación de cada una de las empresas que componen el Consorcio. De resultar adjudicatario, el contrato será suscrito por quienes ejerzan la representación legal de cada una de las empresas participantes, las cuales quedarán obligadas solidariamente ante la Entidad Contratante, sin perjuicio de la acreditación del representante o apoderado único previsto en el párrafo anterior. El consorcio durará como mínimo, el tiempo necesario para la ejecución del contrato, hasta su extinción y liquidación. NOTA: En los casos que el consorcio tenga intención de formalizar el mismo por medio de un RNC individual (en caso de resultar adjudicatario), deberá estipularlo en el acto de constitución, o en su defecto, mediante comunicación dirigida al Comité de Compras y Contrataciones en fecha anterior a la adjudicación.	
3.1.6 Documentos Técnicos **3.1.6.1 Resumen ejecutivo** a) Presentación de la empresa o consorcio. b) Visión del proyecto sugerencias y recomendaciones. c) Curriculum del líder del proyecto o jefe de proyecto, que debe tener como mínimo 5 años de experiencia en uno o varios proyectos de identificación de tarjetas de policarbonato en instituciones públicas, tener certificado PMP, PRINCE2 o similar, así como conocimientos ITIL. Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, así como detallar las experiencias de la persona propuesta en una de las empresas del consorcio. d) Curriculum del personal técnico certificado en tecnología de impresión de tarjetas de identidad localmente durante la vigencia del contrato para supervisión de la calidad de la impresión en todos los centros de impresión de cédulas. Se deben incluir las certificaciones correspondientes. Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, así como detallar las experiencias de la persona propuesta en una de las empresas del consorcio. e) Curriculum del personal técnico en campo (a nivel nacional) con experiencia en la producción de documentos de identidad nacionales mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a la infraestructura de impresión durante los años de garantía de los equipos. Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, así como detallar las experiencias de la persona propuesta en una de las empresas del consorcio.	Carpeta 2/ Seccion 1

Página/Folio No.272 de 843

3.1.6.2 Requisitos de experiencia (Obligatorios) a) Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo el suministro de impresoras de documentos de identidad de policarbonato electrónicos, incluyendo la instalación y el mantenimiento. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública. Para aceptar las experiencias, el oferente deberá presentar carta formulada a la JCE certificando la implementación del proyecto exclusiva para gobiernos mediante declaración jurada o carta emitida directamente por la entidad de gobierno, en la que se indiquen claramente los puntos aquí requeridos, en papel timbrado del gobierno del cliente, con nombre completo del firmante, cargo e institución, sellada y firmada, con teléfono de contacto y correo oficial para poder constatar la información. b) Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo un suministro de tarjetas de identidad electrónicas de policarbonato. Sólo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública. Para aceptar las experiencias, el oferente deberá presentar carta formulada a la JCE, en la que se indiquen claramente los puntos aquí requeridos, en papel timbrado, con nombre completo del firmante, cargo e institucion, sellada y firmada, con teléfono de contacto y correo oficial para poder constatar la información. c) Al menos una (1) experiencia, en el cual el oferente haya implementado un proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos. solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Para aceptar las experiencias, el oferente deberá presentar carta formulada a la JCE certificando la implementación del proyecto exclusiva para instituciones públicas mediante declaración jurada o carta emitida directamente por la entidad de gobierno, en la que se indiquen claramente los puntos aquí requeridos, en papel timbrado, con nombre completo del firmante, cargo e institución, sellada y firmada, con teléfono de contacto y correo oficial para poder constatar la información. d) Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Para aceptar las experiencias, el oferente deberá presentar carta formulada a la JCE certificando la implementación del proyecto de institución pública mediante declaración jurada o carta emitida directamente por la entidad de gobierno, en la que se indiquen claramente los puntos aquí requeridos, en papel timbrado,	Carpeta 2/ Seccion 1

Página/Folio No.273 de 843

	con nombre completo del firmante, cargo e institución, sellada y firmada, con teléfono de contacto y correo oficial para poder constatar la información.	
3.1.6.3	**Requisitos de experiencia (no obligatorios)** a) Más de una (1) experiencia, en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. La experiencia se podrá acreditar presentando cartas de referencias de clientes donde se muestre explícitamente la solicitud y deben ser dirigidas a la JCE. Al menos una de las referencias debe ser ISO 18013-5. b) Al menos una (1) experiencia de haber operado un proyecto de impresión de soluciones de identificación a nivel de gobierno con el suministro y mantenimiento de al menos doscientas (200) impresoras distribuidas nacional e internacional (fuera del país). c) Al menos una (1) experiencia en República Dominicana en proyectos de mantenimiento de tecnología en gobierno con al menos cinco (5) años de experiencia.	Carpeta 2/ Sección 1

Página/Folio No.274 de 843

CAPITULO IV

PRESENTACIÓN DE "SOBRE A" Y "SOBRE B"

Página/Folio No.275 de 843

4.1 Presentación de la Documentación Contenida en el "Sobre A"

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
4.1.1 Lugar, Fecha y Hora El acto para la presentación de documentos, credenciales y propuestas técnicas ("Sobre A"), así como la recepción de propuestas económicas ("Sobre B") de los oferentes, se efectuará ante el Comité de Compras y Contrataciones a las diez de la mañana (10:00 A.M.) del día 25 de junio del 2024, en el Salón de Sesiones del Comité de Compras y Contrataciones de la Junta Central Electoral, sito en el Edificio Administrativo, ala Este, 2do. nivel, al lado del almacén de la sede principal, ubicado en la Av. Gregorio Luperón, esq. Av. 27 de Febrero, Plaza de la Bandera. Sólo podrá postergarse por causas de fuerza mayor o caso fortuito definidos en el presente Pliego de Condiciones. El acto contará con la presencia de un Notario Público que certificará las incidencias del mismo. **4.1.2 Documentación a Presentar en el "Sobre A"** a. Documentos de Acreditación y Solvencia (Según lo requerido en el numeral 3.1.2 y 3.1.3 del Pliego, según corresponda). b. Documentos Técnicos (Según lo requerido en el numeral 3.1.6 del Pliego). c. Propuesta Técnica, la cual debe contener lo siguiente: • Propuesta técnica (Según lo requerido en el numeral 1.7 del Pliego). • Muestras de las tarjetas. • Cualquier otra información técnica que el oferente estime necesaria. **4.1.3 Forma para la Presentación del "Sobre A"** • Se requiere un (1) original, tres (3) copias impresas y una (1) copia en soporte electrónico legible de la propuesta técnica (Word o PDF) que será una copia idéntica a la impresa en papel, excepto las firmas manuscritas, documentos escaneados de	Entendemos y aceptamos.

Página/Folio No.276 de 843

Elegibilidad, Experiencias, o cualquier documentación que no sea generada por el oferente (podrán ser documentos escaneados), que se introducirán juntas en el sobre A denominado Oferta técnica. **Nota:** En el caso que no presente su propuesta técnica en el formato electrónico requerido, podrá hacerlo dentro del plazo de subsanación, y no se evaluará dicha propuesta hasta su depósito. Si pasado el plazo de subsanación, no se presentase dicho documento, la oferta quedaría descartada automáticamente. • El original y la copia deberán firmarse en todas las páginas por el Representante Legal. El Sobre deberá contener en su cubierta la siguiente identificación: NOMBRE DEL OFERENTE/PROPONENTE (Sello Social) COMITÉ DE COMPRAS Y CONTRATACIONES Dirección: Av. Gregorio Luperón esq. Av. 27 de Febrero, Edificio Administrativo, ala Este, 2do. nivel. Presentación de Documentos Referencia: JCE-CCC-LPI-2024-0001 Una vez que se haya realizado la revisión de lugar, verificando que los datos que figuran en el formulario se corresponden con las especificaciones técnicas solicitadas, se hará una marca de cotejo en cada renglón revisado. Se firmará y sellará como RECIBIDO el original y su copia.	

4.2 Presentación de la Documentación Contenida en el "Sobre B"

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
La presentación de las Propuestas Económicas se efectuará ante el Comité de Compras y Contrataciones de la Junta Central Electoral el día y hora señalados en el Cronograma de la Licitación y en el lugar que posteriormente les será comunicado. **4.2.1 Documentación a Presentar en el "Sobre B" (Oferta Económica)** a. Fianza o Póliza de Garantía de Seriedad de la Oferta. b. Oferta Económica, la cual deberá presentarse en el formulario FL-05, anexo al presente Pliego de Condiciones (no se aceptarán propuestas alternativas). c. La oferta deberá indicar el precio unitario, el subtotal, el ITBIS de manera segregada y el total general. d. Los precios no deberán presentar alteraciones ni correcciones, y deben ser expresados en dos decimales (0.00).	Entendemos y aceptamos.

Página/Folio No.277 de 843

e. La oferta de precio unitario debe presentarse en Pesos Oro Dominicanos (RD) o en Dólares Estadcunidenses (USD). Las ofertas presentadas en Dólares Estadounidenses (USD) serán evaluadas según el tipo de cambio para la venta del Banco de Reservas de la República Dominicana al día del acto de apertura de Propuestas Económicas. f. Los oferentes deben consignar que sus ofertas se mantendrán vigentes por el plazo mínimo de ciento cincuenta (150) días hábiles, contados a partir de la fecha de apertura. Si el Oferente no manifiesta información fehaciente de su voluntad de no renovar la oferta con una antelación de diez (10) días hábiles al plazo de vencimiento, aquella se considerará prorrogada automáticamente por el mismo plazo o el que fije la entidad contratante. **4.2.2 Forma para la Presentación del "Sobre B"** Los documentos deberán ser presentados en la forma siguiente: • Se requiere un (1) original, tres (3) copias impresas y una (1) copia en soporte electrónico legible de su oferta económica, que se introducirán juntas en el sobre titulado Oferta económica. • El original y la copia deberán estar firmados en todas las páginas por el Representante Legal. El Sobre deberá contener en su cubierta la siguiente identificación: NOMBRE DEL OFERENTE/PROPONENTE (Sello Social) COMITÉ DE COMPRAS Y CONTRATACIONES PRESENTACIÓN PROPUESTA ECONÓMICA REFERENCIA: JCE-CCC-LPI-2024-0001 NO ABRIR ANTES DE LAS 10:00 A.M. DEL DIA 6 DE AGOSTO, 2024	

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Las Ofertas deberán ser presentadas en el mismo orden de la solicitud, incluyendo el ITBIS de manera segregada del precio, conforme al formulario denominado FL-05. La oferta de precio unitario deberá presentarse en Pesos Dominicanos (RD) o en Dólares Estadounidenses (USD). Los precios deberán expresarse en dos (2) decimales (00.00) que tendrán que incluir todas las tasas (divisas), impuestos y gastos que correspondan, transparentados e implícitos.	Entendemos y aceptamos.

Página/Folio No.278 de 843

Es facultad de la Junta Central Electoral reconocer o no la factibilidad de aplicación de algún tipo de ajuste, por inflación o por cualquier otro motivo, en los precios y montos acordados.

En el caso de que el Oferente/Proponente adjudicatario solicitara un ajuste, la Junta Central Electoral (JCE) se compromete a dar respuesta dentro de los siguientes diez (10) días laborables, contados a partir de la fecha de acuse de recibo de la solicitud realizada.

La solicitud de ajuste no modifica el Cronograma de Entrega, por lo que, el Adjudicatario se compromete a no alterar la fecha programada para la entrega de los bienes o servicios correspondientes, bajo el alegato de esperar respuesta a su solicitud.

Los precios no deberán presentar alteraciones ni correcciones y deberán ser dados por la unidad de medida establecida en los listados.

Los Oferentes/Proponentes deben cotizar únicamente lo consignado en la ficha técnica. Será responsabilidad del Oferente/Proponente, la adecuación de los precios unitarios a las unidades de medidas solicitadas, considerando a los efectos de adjudicación, el precio consignado en la Propuesta Económica como el unitario y valorándolo como tal, respecto de otras ofertas. Se debe indicar el precio unitario (sin impuestos), así como el total, incluyendo exactamente las cantidades indicadas.

El precio de la Oferta incluirá los impuestos, derechos de aduana o gravámenes que hubiesen sido fijados por las autoridades municipales, estatales o gubernamentales, dentro y fuera de la República Dominicana, relacionados con los materiales y servicios conexos a ser suministrados.
Además, se deben transparentar los siguientes elementos:

- Monto de anticipo (si fuera requerido).
- Precio por cada unidad.
- Precio de cualquier otro elemento que forme parte de la oferta.

NOTAS:

1) Para fines de evaluación, las ofertas hechas en Dólares Estadounidenses (USD) serán consideradas en función del tipo de cambio para la venta, según la ventanilla del Banco de Reservas de la República Dominicana, a la fecha de apertura de las Propuestas Económicas.
2) Si por tratarse de un documento de interés nacional, la Junta Central Electoral lograra la exención de los aranceles, de los impuestos, derecho de aduana, o gravámenes que hubieren sido fijados por las autoridades gubernamentales o municipales de la República Dominicana, relacionados con los equipos y materiales, el adjudicatario deberá mostrar su disposición a importar a nombre de la Entidad Contratante, para que esta se encargue del proceso de retiro del puerto de que se trate.

Página/Folio No.279 de 843

CAPITULO V
APERTURA Y VALIDACIÓN DE OFERTAS

Página/Folio No.280 de 843

5.1 Procedimiento Apertura de Sobres

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
La apertura de sobres se realizará en acto público, en presencia del Comité de Compras y Contrataciones, el Notario Público actuante y todos los interesados.	Entendemos y aceptamos.

5.2 Apertura de "Sobres A", contentivos de Documentos de Acreditación, Solvencia y Propuestas Técnicas.

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
La recepción y apertura de sobres se realizará en presencia del Comité de Compras y Contrataciones, el Notario Público y los oferentes participantes en la fecha, lugar y hora que se establece en el cronograma de la licitación. El Comité de Compras y Contrataciones no recibirá sobres que no estén cerrados e identificados. Una vez pasada la hora establecida para la recepción de los sobres no se aceptará la presentación de nuevas propuestas, aunque el acto de apertura no se iniciare a la hora	Entendemos y aceptamos.

Página/Folio No.281 de 843

indicada, conforme lo establece el numeral siete (7) del artículo veinticinco (25) del Reglamento Interno para la Compra de Bienes y Contrataciones de Obras y Servicios de la Junta Central Electoral, el cual expresa lo siguiente: "Los o las licitantes que lleguen al acto de recepción y apertura de las propuestas del "Sobre A" pasada la hora de convocatoria, se les permitirá estar presentes en el mismo, pero sus ofertas no se tomarán en cuenta". Luego que el Presidente del Comité de Compras y Contrataciones da apertura a la licitación, el Notario Público preparará un registro de los participantes, según el orden de llegada de los oferentes y de inmediato se procederá a la recepción del "Sobre A" y "Sobre B" de las ofertas. Acto seguido se procederá con la apertura del "Sobre A", oferta técnica, presentadas según el orden de llegada de los oferentes, verificando que la documentación contenida en las mismas se corresponda con la indicada en el listado especificado en el presente Pliego de Condiciones. La revisión a detalle de los documentos contentivos en el "Sobre A" será realizada durante el proceso de evaluación de la oferta. En la fase de validación el Comité, siempre que se trate de errores u omisiones de naturaleza subsanable, puede requerir en un plazo breve que el oferente rectifique la información y/o suministre la faltante. En caso de que se trate de errores u omisiones de naturaleza no subsanable quedará descalificada la oferta. El Notario Público actuante levantará acta notarial de todas las incidencias del acto. Nota: Concluida la Fase I, se procederá en la Fase II a la apertura del "Sobre B" (oferta económica) en la fecha establecida en el cronograma de actividades. Sólo se dará apertura a las ofertas económicas de aquellos oferentes que hayan quedado habilitados en el proceso de verificación de los documentos contenidos en el "Sobre A".	

5.3 Validación, Verificación de Documentos y Evaluación Técnica

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Culminado el proceso de apertura de los "Sobres A", el Comité remite a los técnicos correspondientes las propuestas presentadas para su evaluación, si así lo amerita el objeto de la licitación, quienes verificarán que las mismas cumplan con los requisitos técnicos exigibles en el Pliego de Condiciones. El Comité de Compras y Contrataciones, si lo estima necesario y mientras dure el proceso de evaluación, podrá solicitar informes o requerimientos adicionales, exigir muestras y cualquier otro requerimiento adicional a los oferentes para el análisis de sus propuestas, siempre que no afecten materialmente la oferta.	Entendemos y aceptamos.

Página/Folio No.282 de 843

El Comité de Compras y Contrataciones, procederá a la verificación y validación de los documentos contenidos en el "Sobre A". Ante cualquier duda sobre la información presentada, dicho Comité podrá comprobar, por los medios que considere adecuados, la veracidad de la información recibida. Antes de proceder a la evaluación detallada del "Sobre A", el Comité de Compras y Contrataciones determinará si cada Oferta se ajusta sustancialmente al presente Pliego de Condiciones, o si existen desviaciones, reservas, omisiones o errores de naturaleza subsanables, de conformidad a lo establecido en el numeral 1.12 del presente documento. En los casos en que se presenten desviaciones, reservas, omisiones o errores de naturaleza subsanables, el Comité de Compras y Contrataciones procederá de conformidad con los procedimientos establecidos en el presente Pliego de Condiciones.	

5.4 Criterios de Evaluación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Las Propuestas deberán contener la documentación necesaria, suficiente y fehaciente, para demostrar los siguientes aspectos que serán verificados bajo la modalidad "cumple/no cumple" y mediante una ponderación por puntos (según aplique): **5.4.1 Elegibilidad:** • El consorcio debe licitar como una sola entidad. • Por lo tanto, los miembros del consorcio deben elegir al líder del consorcio para que lo represente. • Ningún oferente (de tarjetas, de impresoras, de cédula digital, de ABIS) podrá presentar más de una Oferta para el Proyecto. Un oferente que licite individualmente o como miembro de un consorcio no tendrá derecho a presentar otra oferta ni individualmente ni como miembro de ningún Consorcio. Esta restricción no se aplica a los proveedores de materiales o equipos tales como equipos de infraestructura, dispositivos o consumibles.	Entendemos y aceptamos.

Página/Folio No.283 de 843

- El oferente debe aceptar cumplir la sección de términos y condiciones adicionales de este documento.

- El oferente deberá presentar cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee línea de crédito que pueda solventar al menos el monto de USD$2,000,000.00 (o su equivalente en pesos o euros).

- El oferente deberá presentar los Estados Financieros de los últimos tres (3) períodos fiscales, certificados por un Contador Público Autorizado, avalado con copia del IR-2 de esos últimos tres (3) períodos fiscales, incluyendo la entrega certificada con el soporte correspondiente y/o el código de envío electrónico recibido.

- Las hojas financieras auditadas deben presentarse según la plantilla facilitada (Anexo 9).

- El plazo de validez de las ofertas será de ciento cincuenta (150) días a partir de la fecha límite de presentación de las ofertas.

- Las ofertas deben estar respaldadas por una Garantía de Seriedad de la Oferta. El oferente deberá depositar una Garantía de Seriedad de la Oferta por el 1% de su oferta.

- El oferente deberá proporcionar un mínimo de diez (10) muestras originales de las tarjetas junto con la propuesta técnica. Las muestras deben ser capaces de representar la personalización de las cédulas electrónicas y los detalles de las características de seguridad que el proveedor propone, y éstas deben explicarse claramente. Junto con las muestras, el proveedor deberá presentar informes de pruebas independientes de acuerdo con la norma ISO 18745.

- El fabricante de la tarjeta debe tener en vigor en el momento de la presentación de su oferta:

    - ISO 9001:2015.
    - ISO 27001:2013.
    - ISO 14001 o equivalente.
    - ISO 14928 INTERGRAF o equivalente nivel gobierno.

- Solvencia (Activo total / Pasivo total) del Consorcio debe ser mayor que >1
- Consorcio debe facturar (de media en los últimos 3 años) en su conjunto, al menos la totalidad del presupuesto de su propuesta total.
- Máximo tiempo de implementación: 26 semanas.

Página/Folio No.284 de 843

- Impresora pesa menos de 80kg.
- Impresora modular.
- Que el proponente esté legalmente autorizado para realizar sus actividades comerciales en el país.
- Que el oferente demuestre que tiene capacidad y experiencia para la entrega a tiempo y en las condiciones establecidas.

5.4.2 Situación Financiera

Que cuenta con la estabilidad financiera suficiente para ejecutar satisfactoriamente la eventual adjudicación. De las empresas nacionales, se evaluarán los estados financieros auditados de los últimos tres (3) períodos fiscales y el formulario IR-2 con sus respectivos anexos para determinar los Índices Financieros mínimos correspondientes. Para las empresas extranjeras, se evaluarán los estados financieros auditados de los últimos tres (3) períodos fiscales y un documento certificado que muestre su acreditación financiera.

5.4.3 Capacidad Técnica

Que cuenta con el aval necesario para suplir los materiales y servicios propuestos y que estos cumplan con las características indicadas en las Fichas Técnicas. El Comité de Compras y Contrataciones, auxiliado por la Comisión de Asesoría y Asistencia Técnica, ponderará las Propuestas Técnicas y las muestras presentadas por los licitantes, tomando en consideración cada una de las especificaciones indicadas en el Capítulo I, numeral 1.7 de este Pliego de Condiciones, para determinar la Capacidad Técnica. Es decir: Que los Proponentes cumplan con todas las condiciones y características especificadas para garantizar la calidad de los bienes y servicios ofertados y su correspondencia con los requerimientos.

En cuanto a la puntuación financiera, propuesta técnica, proyecto y experiencia, el oferente debe alcanzar al menos cincuenta (50) puntos de los setenta (70) asignados para este renglón. De no haber logrado este porcentaje, su propuesta no será considerada para la fase de apertura de propuestas económicas y automáticamente quedará descalificada.

5.4.4 Parámetros de Calificación de los Proponentes

Variables a evaluar	Puntos
Financiero	10
Propuesta técnica	30
Proyecto	15
Experiencia	15
Oferta Económica	30
Total	100

Matriz JCE Autoevaluación

Página/Folio No.285 de 843

5.4.5 Plantilla de Evaluación

Requisitos	Puntos	Criterios
Financiero	10	**· Solvencia: 5 puntos.** – *Solvencia total (Activo total/Pasivo total) >1,2:* ***2 puntos.*** – *Solidez crediticia: El oferente debe presentar cartas de referencias bancarias y/o entidades financieras, dirigidas a la Junta Central Electoral, que demuestren solvencia y respaldo económico y/o que certifiquen que posee líneas de crédito que puede solventar al menos el monto de USD$2,000,000.00 (o su equivalente en pesos o euros). Para acreditar la solidez, puede ser entre los miembros del consorcio en su conjunto o de forma individual:* ***3 puntos.***
		· Facturación: 5 puntos. – *Consorcio factura de media en los últimos 3 años en su conjunto al menos 2 veces más que la totalidad del presupuesto de su propuesta:* ***3 puntos.*** – *Oferente local factura de media en los 3 últimos años más de USD$5,000,000.00:* ***2 puntos.***
Propuesta técnica	30	**· Menor tiempo para iniciar el proyecto: 5 puntos.** – *Hasta 6 meses después de la firma del contrato:* ***0 puntos.*** – *Hasta 5 meses después de la firma del contrato:* ***2 puntos.*** *4,5 meses después de la firma del contrato:* ***5 puntos.***
		· Proveedor: 4 puntos. – *El oferente presta directamente (sin contratar a terceros) los servicios de desarrolladorde PKI, fabricante de tarjetas electrónicas y proveedor de servicios:* ***2 puntos.*** *El proveedor de las tarjetas y el proveedor de las impresoras, ambos están en laempresa conjunta:* ***2 puntos.***
		· Impresoras: 5 puntos. – *Pesa menos de 40 kg.:* ***3 puntos.*** – *Mide menos de 0,5 m² (largo x ancho):* ***1 punto.*** *Pueden incorporar un módulo adicional para personalizar la fotografía en color, sindependencia del policarbonato:* ***1 punto.***
		· Producción de tarjetas: 4 puntos. – *El oferente tiene al menos una instalación de producción de respaldo propia para la fabricación de tarjetas en una ubicación distinta de la fábrica principal propuesta de laempresa o la empresa conjunta:* ***1 punto.*** – *La construcción del cuerpo de la tarjeta está diseñada sin capas/materiales patentados que limitarían el abastecimiento de materiales de producción de tarjetas a proveedores dedicados:* ***1 punto.***

Página/Folio No.286 de 843

		El cuerpo de la tarjeta en blanco y el proceso de personalización de la misma en combinación no constituirán una solución dependiente o patentada que excluya a los proveedores de tarjetas y/o sistemas de personalización: **2 puntos**.
		· Prueba de concepto: 8 puntos. *– El proveedor ha realizado una prueba de concepto satisfactoria (realizar una captura de una persona, impresión en láser de la tarjeta de policarbonato, conforme a las especificaciones técnicas de la impresión, de la persona enrolada y luego una generación de una cédula electrónica a partir de esta cédula personalizada). Deberá incluir en dicha prueba, una aplicación móvil de verificación (mediante QR seguro generado desde la aplicación) y mostrar la funcionalidad de compartir un grupo de datos específicos seleccionados por el ciudadano.*
		· Diseño gráfico: 4 puntos. *– El oferente ha entregado un diseño de seguridad en tres lucas, de la tarjeta electrónicaconforme a las bases técnicas en formato imagen de alta resolución.*
Proyecto	15	*"El proveedor presenta la implementación, de por lo menos,* **un desarrollo de una solución, puesta en producción, de cédula digital, en una institución pública, de** *acuerdo a los requerimientos establecidos en el documento de especificaciones técnicas, y estar adheridas al estándar ISO 18013-5. Para comprobar dicha experiencia, el proveedor deberá presentar carta formulada a la JCE certificando la implementación del proyecto exclusiva para instituciones públicas mediante declaración jurada o carta emitida directamente por la entidad de gobierno, en la que se indiquen claramente los puntos aquí requeridos, en papel timbrado, con nombre completo del firmante, cargo e institución, sellada y firmada, con teléfono de contacto y correo oficial para poder constatar la información. También podrá presentar factura o contrato que detalle claramente el objeto de la contratación.* **· Personal: 6 puntos.** *– El oferente contará con un mínimo 2 técnicos certificados en tecnología de impresión de tarjetas de identidad localmente durante la vigencia del contrato para supervisión de la calidad de la impresión en todos los centros de impresión de cédulas: 3 puntos.* *– El oferente contará con un equipo de técnicos (al menos 10) en campo (a nivel nacional) con experiencia en la producción de documentos de identidad nacionales mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a le*

Página/Folio No.287 de 843

		infraestructura de impresión durante los años de garantía de los equipos: **3 puntos.**	

La Comisión de Asesoría y Asistencia Técnica valorará las Propuestas (documentos técnicos y Propuesta técnica) presentadas por los licitantes, tomando en consideración cada una de las especificaciones indicadas en el Objeto de la Licitación, para determinar la Capacidad Técnica, es decir, que los proponentes cumplan con las condiciones y características especificadas para cada propuesta evaluada, y así garantizar la calidad de la solución y su correspondencia con los requerimientos, de conformidad con la matriz arriba indicada.

Para la evaluación de las mejores ofertas económicas se le otorgarán 30 puntos a la propuesta que presente el menor precio (de las propuestas que califiquen). La puntuación de las demás ofertas económicas se determinará utilizando la siguiente fórmula:

POEi = Puntuación oferta económica individual.
POEi = 30 x menor oferta económica/oferta económica individual.

Determinación de la Mejor Oferta Evaluada.

Para determinar la mejor oferta, se utilizará la fórmula citada a continuación:

Puntuación Total Individual = PFi +PPTi + PPi + PEi + POEi PFi = Puntuación Financiera individual (solvencia).
PPTi = Puntuación Propuesta Técnica individual.

RNC 101038602
Santo Domingo, R.D.

PPi = Puntuación Proyecto individual. PEi = Puntuación Experiencia individual. POEi = Puntuación Oferta Económica individual. La mejor propuesta será aquella con la mayor Puntuación Total individual.	

5.5 Apertura de "Sobres B", contentivos de Propuestas Económicas

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Comité de Compras y Contrataciones dará inicio al acto de apertura de Propuestas Económicas "Sobre B", con la presencia del Notario Público y los oferentes habilitados que deseen estar presentes, el cual se desarrollará a las diez horas de la mañana (10:00 A.M.) del día 6 de agosto del 2024, en el Salón de Sesiones del Comité de Compras y Contrataciones de la Junta Central Electoral, sito en el Edificio Administrativo, ala Este, 2do. nivel, al lado del almacén de la sede principal, ubicado en la Av. Gregorio Luperón, esq. Av. 27 de Febrero, Plaza de la Bandera. Acto seguido, se procederá a la apertura de las Ofertas Económicas "Sobre B", el Comité de Compras y Contrataciones dará apertura a los "Sobres B" de los oferentes que hayan sido habilitados técnicamente, aun cuando sus proponentes no acudan al acto; en estos casos, primero se abrirán las propuestas de los oferentes presentes y luego aquellas cuyos proponentes no hayan asistido. Se procederá a la lectura de las Ofertas, certificando su contenido, rubricando y sellando cada página contenida en el "Sobre B". No se dará apertura ni serán tomadas en cuenta las Ofertas Económicas "Sobre B" presentadas por los Oferentes/Proponentes que no hayan resultado habilitados en la Fase I: Acreditación, Solvencia y Propuesta Técnica. Las observaciones referentes al renglón que se esté leyendo, deberán realizarse en ese mismo instante, levantando la mano para tomar la palabra. El Notario actuante procederá hacer constar todas las incidencias que se vayan presentando durante las lecturas. Finalizada la lectura de las Ofertas, el Presidente del Comité de Compras y Contrataciones procederá a invitar a los Representantes Legales o Agentes Autorizados de los Oferentes/Proponentes a hacer conocer sus observaciones; en caso de conformidad, se procederá a la clausura del acto. No se permitirá a ninguno de los presentes exteriorizar opiniones de tipo personal o calificativos peyorativos en contra de cualquiera de las empresas o personas participantes, ni entre los integrantes del Comité de Compras y Contrataciones.	Entendemos y aceptamos.

Página/Folio No.289 de 843

El Oferente/Proponente o su representante que durante el proceso de licitación tome la palabra sin ser autorizado o exteriorice opiniones despectivas sobre otro Oferente, será sancionado con el retiro de su presencia del salón.
En caso de discrepancia entre la Oferta presentada en el formulario correspondiente (FL-05), debidamente recibido por el Notario Público actuante y la lectura de la misma, prevalecerá el documento escrito.

El Notario Público actuante en el acto de apertura de los "Sobres B" certificará el acta correspondiente, incluyendo las observaciones realizadas en el desarrollo del acto de apertura, si las hubiere, por parte de los Representantes Legales o Agentes Autorizados de los Oferentes/ Proponentes. Copia del acta estará disponible para los Representantes Legales o Agentes Autorizados de los Oferentes/Proponentes.

5.5.1 Plazo de Mantenimiento de la Oferta

Los Oferentes/Proponentes deben consignar que sus Ofertas se mantendrán vigentes por el término de ciento cincuenta (150) días hábiles contados a partir de la fecha del acto de apertura. Si el Oferente no manifiesta en forma fehaciente su voluntad de no renovar la Oferta con una antelación mínima de diez (10) días hábiles al vencimiento del plazo, aquella se considerará prorrogada automáticamente por el mismo plazo original o el que fije la Entidad Contratante y así sucesivamente.

El Comité de Compras y Contrataciones, excepcionalmente podrá solicitar a los Oferentes/Proponentes una prórroga, antes del vencimiento del período de validez de sus Ofertas, con indicación del plazo. Los Oferentes/Proponentes podrán rechazar dicha solicitud, considerándose por tanto que han retirado sus Ofertas, por lo cual la Junta Central Electoral procederá a efectuar la devolución de la Garantía de Seriedad de la Oferta ya constituida. Aquellos que la consientan no podrán modificar sus Ofertas y deberán ampliar el plazo de la Garantía de Seriedad de Oferta oportunamente constituida.

5.5.2 Evaluación Oferta Económica

El Comité de Compras y Contrataciones evaluará y comparará únicamente las Ofertas que se ajustan sustancialmente al presente Pliego de Condiciones. Para la evaluación de las mejores ofertas económicas se le otorgarán treinta (30) puntos a la propuesta que presente el menor precio (de las propuestas que califiquen). La puntuación de las demás ofertas económicas se determinará utilizando el criterio indicado en el punto 5.4.5

CAPITULO VI
ADJUDICACIÓN

Página/Folio No.290 de 843

1.1 Criterios de Adjudicación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Comité de Compras y Contrataciones tomará en cuenta para la adjudicación al oferente cuya propuesta cumpla con los requerimientos y sea calificada como la más conveniente para los intereses de la Junta Central Electoral, teniendo en cuenta los requisitos que se	Entendemos y aceptamos.

Página/Folio No.291 de 843

establecen en el Pliego de Condiciones, considerando los resultados finales de la puntuación obtenida. El Comité de Compras y Contrataciones adjudicará dando cumplimiento a los principios de transparencia, objetividad, economía, celeridad y demás que regulan las contrataciones públicas. Se adjudicará un contrato administrativo por un período de diez (10) años, pudiendo ser renovado a través de un acuerdo entre las partes. Si se presentase una sola Oferta, esta deberá ser considerada y se procederá a la Adjudicación, si habiendo cumplido con lo exigido en el Pliego de Condiciones Específicas, se le considera conveniente a los intereses de la Institución. En caso de empate entre dos o más Oferentes/Proponentes, es decir igualdad de puntuación, se procederá mediante el método de sorteo entre los Oferentes/Proponentes empatados. De no ser aceptado por uno o más de los Oferentes/Proponentes empatados, el Comité de Compras y Contrataciones procederá con el sorteo entre los que acepten y si es solo uno, la adjudicación se hará a favor de este Oferente, siempre que la Oferta sea considerada válida y conveniente al máximo interés de la Junta Central Electoral. NOTA: Todos los oferentes que resultan adjudicatarios en cualquiera de los procesos de adquisición, serán evaluados en cuanto al cumplimiento de las condiciones establecidas dentro del proceso y las brindadas en su oferta, en virtud de los requisitos normativos y los estándares del Sistema de Gestión Integrada de Calidad de la institución.	

1.2 Acuerdo de Adjudicación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Comité de Compras y Contrataciones procederá a informar a todos los participantes el resultado de la licitación dentro de un plazo de cinco (5) días hábiles contados a partir de la expedición del Acta de Adjudicación. La notificación de adjudicación podrá entregarse de manera física o vía correo electrónico y se procederá a su publicación en el portal de la Junta Central Electoral y en el portal administrado por la Dirección General de Contrataciones Públicas.	Entendemos y aceptamos.

1.3 Reclamos, Impugnaciones y Controversias

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"

Página/Folio No.292 de 843

En caso de que algún o algunos Oferentes/Proponentes no estén conformes con las "Resoluciones de Habilitación o de Adjudicación", tendrán derecho a recurrir las mismas; dicha impugnación no tendrá efecto suspensivo del curso de la adjudicación, en virtud del artículo 32.2 del Reglamento interno para las Compras y Contrataciones de Obras y Servicio. El recurso contra las decisiones se hará por escrito y seguirá los siguientes pasos: • El recurrente presentará la impugnación ante la entidad contratante en un plazo no mayor de diez días (10) hábiles a partir de la fecha del hecho impugnado o de la fecha en que razonablemente el recurrente debió haber conocido el hecho. La entidad pondrá a disposición del recurrente los documentos relevantes correspondientes a la actuación en cuestión, con la excepción de aquellas informaciones declaradas como confidenciales por otros oferentes o adjudicatarios, salvo que medie su consentimiento. • En los casos de impugnación de adjudicaciones, para fundamentar el recurso, el mismo se regirá por las reglas de la impugnación establecidas en el presente Pliego de Condiciones y el Reglamento interno de Compras de la Junta Central Electoral. • Cada una de las partes deberá acompañar sus escritos de los documentos que hará valer en apoyo de sus pretensiones. • La entidad notificará la interposición del recurso a los terceros involucrados, dentro de un plazo de dos (2) días hábiles, contados a partir de la recepción del mismo. • Los terceros estarán obligados a contestar sobre el recurso dentro de cinco (5) días calendario, a partir de la recepción de notificación del recurso, de lo contrario quedarán excluidos de los debates. • La entidad estará obligada a resolver el conflicto, mediante resolución motivada, en un plazo no mayor de quince (15) días calendario, a partir de la contestación del recurso o del vencimiento del plazo para hacerlo. No será ponderada ninguna impugnación que incumpliere el procedimiento previsto en esta disposición. Las controversias no resueltas por los procedimientos indicados anteriormente se someterán al Tribunal Superior Administrativo, de conformidad con el Capítulo II, numeral 2.7 del presente documento. La información suministrada a la Entidad Contratante en el proceso de licitación, a la jurisdicción Contencioso-Administrativa, o en el proceso de impugnación de la Resolución Administrativa, que sea declarada como confidencial por el Oferente, no podrá ser divulgada si dicha divulgación pudiese perjudicar los intereses comerciales legítimos de quien la aporte o pudiese perjudicar la competencia leal entre los proveedores.	Entendemos y aceptamos.

Página/Folio No.293 de 843

1.4 Adjudicaciones Posteriores

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
En caso de incumplimiento del oferente adjudicatario, el Comité de Compras y Contrataciones procederá a adjudicar a la oferta que ocupe la siguiente posición, en el orden de mérito empleado para la adjudicación inicial, y así sucesivamente.	Entendemos y aceptamos.

1.5 Declaración de Desierto

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Comité de Compras y Contrataciones podrá declarar desierto el procedimiento, total o parcialmente, en los siguientes casos: a) Por no haberse presentado ofertas. b) Por haberse rechazado, descalificado o porque no son convenientes para los intereses de la Institución, la (s) oferta (s) presentadas. c) Por violación sustancial del procedimiento de Licitación Pública Internacional. d) Al evaluar las ofertas, ninguna cumple con los requerimientos y especificaciones de la presente licitación Si el proceso es declarado desierto, el Comité de Compras y Contrataciones podrá reabrirlo dando un plazo para la presentación de propuestas de hasta un cincuenta por ciento (50%) del plazo del proceso fallido.	Entendemos y aceptamos.

1.6 Cancelación de la Licitación

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Comité de Compras y Contrataciones se reserva el derecho de cancelar de manera justificada la Licitación o inhabilitar a cualquier oferente, ya sea antes o después de la apertura, siempre que existan razones justificadas y documentadas.	Entendemos y aceptamos.

Página/Folio No.294 de 843

CAPITULO VII
DISPOSICIONES SOBRE LOS CONTRATOS

Página/Folio No.295 de 843

7.1 Validez del Contrato

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Contrato será válido cuando se realice conforme al ordenamiento jurídico y cuando el acto definitivo de adjudicación y la constitución de la Garantía de Fiel Cumplimiento del Contrato sean cumplidos.	Entendemos y aceptamos.

7.2 Perfeccionamiento del Contrato

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
Para su perfeccionamiento deberán seguirse los procedimientos de contrataciones vigentes, cumpliendo con todas y cada una de sus disposiciones.	Entendemos y aceptamos.

RNC: 101038652
Santo Domingo, R.D.

El Contrato se perfeccionará con la recepción de la Orden de Compras o de Servicios por parte del proveedor.	

7.3 Formalización del Contrato

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
No se podrá proceder a la formalización del Contrato, mediante la emisión de la Orden de Compras o de Servicios, si no se ha comprobado previamente que el Oferente/ Proponente ha constituido y depositado la Garantía de Fiel Cumplimiento.	Entendemos y aceptamos.

7.4 Vigencia del Contrato

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
La vigencia del Contrato será por un periodo de diez (10) años, pudiendo ser prorrogado por acuerdo entre las partes.	Entendemos y aceptamos.

7.5 Incumplimientos y Finalización del Contrato

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El contrato finalizará por recepción de lo contratado, vencimiento de su plazo, de la última prórroga o por la concurrencia de alguna de las siguientes causas: 1. Incumplimiento del proveedor en las cláusulas contentivas del contrato. Se considerará incumplimiento del contrato, siendo enunciativas y no limitativas: • La mora del proveedor en la entrega. • Falta de calidad de los bienes y/o servicios adjudicados. • Si no se cumplen con las condiciones establecidas en el Pliego de Condiciones. • La no comparecencia del adjudicatario a constituir la Garantía de Fiel Cumplimiento de Contrato, en cuyo caso se entenderá que renuncia a la adjudicación y se procederá a la ejecución de la Garantía de Seriedad de la Oferta.	Entendemos y aceptamos.

Página/Folio No.297 de 843

- Cuando hubiese negativa a constituir la Garantía de Fiel Cumplimiento de Contrato, la Junta Central Electoral, como Órgano de Ejecución del Contrato, notificará la adjudicación al Oferente que hubiera obtenido la siguiente posición en el proceso de adjudicación. El nuevo adjudicatario depositará la Garantía de Fiel Cumplimiento del Contrato y firmará el mismo de acuerdo al plazo que le será otorgado por el Comité de Compras y Contrataciones, mediante comunicación formal.

- Incursión sobrevenida del Proveedor en alguna de las causas de prohibición de contratar con la Administración Pública que establezcan las normas vigentes

- Que incumpla cualquiera de las cláusulas del contrato resultante.

- Incursión sobrevenida del proveedor en alguna de las causas de prohibición de contratar que establezcan las normas vigentes.

7.5.1 Efectos del Incumplimiento

El incumplimiento del Contrato por parte del Proveedor determinará su finalización y supondrá para el Proveedor la ejecución de la Garantía de Fiel Cumplimiento del Contrato, además de pagar a la Junta Central Electoral el monto ascendente al veinte (20) por ciento (%) del valor total de la contratación a título de penalidad, procediéndose a contratar al siguiente Proveedor en el orden de mérito, en caso de que existiere.

Por incumplimiento a los tiempos de entrega acordados, se aplicará una penalidad del 0,5% por día del monto correspondiente a los artículos contratados para la entrega.

En adición a la penalidad mencionada anteriormente, el incumplimiento en los tiempos de entrega recurrente conllevará la Rescisión unilateral sin responsabilidad para la institución contratante, se procederá con la cancelación de las entregas pendientes, adjudicándole los restantes al proveedor siguiente de acuerdo al orden de evaluación.

Queda entendido que, si el incumplimiento del contrato ha sido provocado por Fuerza Mayor, las partes serán eximidas de toda responsabilidad respecto al mismo.

Queda entendido que, en caso de incumplimiento del cronograma de entrega, en cualquiera de sus fases, la Junta Central Electoral se reservará el derecho a rescindir el acuerdo de adjudicación sin hacerse responsable de ningún compromiso hecho por el proveedor en falta.

En los casos en que el incumplimiento del oferente constituya falta de calidad en los productos a suministrar o causare un daño o perjuicio a la institución o a terceros, la Junta Central Electoral podrá determinar su inhabilitación temporal o definitiva como suplidor, y dependiendo de la gravedad de la falta podrá realizar cualquier reclamo ante los tribunales correspondientes.

COPIA FIEL ... RNC: 131038652 ... Santo Domingo, R.D.

En el supuesto de que el incumplimiento del Contrato consistiera además en una conducta tipificada como infracción, falta o delito por las leyes y demás normas penales, se procederá a denunciar ante el Ministerio Público los hechos, a fin de que inicie las diligencias oportunas.	

7.6 Subcontratos

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Proveedor podrá subcontratar el suministro de algunos bienes o servicios conexos comprendidos en este Pliego, con la previa autorización de la entidad Contratante. El Oferente, en su propuesta, debe indicar los suministros que subcontrataría y las empresas que ejecutarían cada uno de ellas. Sin embargo, queda entendido que el Proveedor será el único responsable de todos los actos, omisiones, defectos, negligencias, descuidos o incumplimientos de los subcontratistas, de sus agentes, empleados o trabajadores. En ningún caso el contratista podrá ceder los derechos y obligaciones del Contrato a favor de un tercero, ni tampoco estará facultado para subcontratarlos sin la autorización previa y por escrito de la Junta Central Electoral.	Entedemos

CAPITULO VIII
ANEXOS

Página/Folio No.299 de 843

FORMULARIOS TIPO Y DOCUMENTOS

Requerimiento	Respuesta Consorcio "Identidad 4.0 RD"
El Oferente/Proponente deberá presentar sus Ofertas de conformidad con los Formularios y documentos determinados en el presente Pliego de Condiciones, los cuales se anexan como parte integral del mismo.	
Formularios:	
1. Inscripción de oferente (FL-01).	Carpeta 1 / sección 2
2. Presentación de oferta (FL-02).	
3. Modelo de carta de designación o sustitución de Agentes Autorizados (FL-03).	
4. Modelo de carta de aceptación de designación como Agentes Autorizados (FL-04).	
5. Presentación Oferta Económica (FL-05).	Sobre B Carpeta 1 (CSI) Carpeta 3 (GET) Carpeta 4 (SELP)
6. Declaración Jurada del Oferente/Proponente (FL-06).	
(ESTOS FORMULARIOS PODRAN PRESENTARSE EN PAPEL IDENTIFICADO O TIMBRADO DE LA EMPRESA, PERO MANTENIENDO EL FORMATO).	
Documentos:	
7. Doc 9303 de la OACI, octava (8ava.) edición, 2021.	
8. Plantilla financiera.	
9. Centros de impresión nacional.	
10. Estadísticas expediciones por centros de impresión nacional.	
11. Estadísticas sobre empadronados al 19-11-2023 y expediciones por localidad exterior en el año 2023.	
12. OSE y Satélite exterior.	

Página/Folio No.300 de 843

10 muestras de las tarjetas de Policarbonato

Ver "SOBRE DE SEGURIDAD NO.1 - Entrega de Muestra de las Tarjetas de PC"

Se ha entregado un sobre de seguridad contentiva de las muestras de Tarjeta Solicitadas en este proceso.

Diseño de la CIE y de la CI

Ver "SOBRE DE PROPUESTA DE DISEÑO DE LA CIE y CI de la Rep. Dom"

Se ha entregado un Sobre contentivo de la Propuesta de diseño de la CIE y CIE solicitadas en este proceso, listadas de la forma siguiente:

1. Carpeta de Propuesta de Diseño de la CIE y 3 copias.
2. Carpeta de Propuesta de Diseño de la CI y 3 copias.

Presentación del Equipo del Fabricante de las Impresoras, el PKI y Mobile ID.

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC 101838852
Santo Domingo, R.D.

The Commonwealth of Massachusetts
William Francis Galvin - Secretary of the Commonwealth

Apostille

(Convention de la Haye du 5 Octobre 1961)

1. Country: United States Of America

This Public Document

2. Has been signed by: Caitlyn E. Burns

3. Acting in the capacity of: Notary Public

4. Bears the seal/stamp of: Caitlyn E. Burns

Whose commission expires on: 12/29/2028

Certified

5. At: Boston, Massachusetts 6. The: February 21, 2025

7. By: The Secretary of Commonwealth

8. No.: 2680959

9. Seal/Stamp: *(Great Seal of the Commonwealth)*

10. Signature:

William Francis Galvin
Secretary of the Commo...

Prepared By: *NCorreia*

G.E.T. Secure ID Corp
230 Third Ave., Waltham, MA
T: +1 781 902 8700
F: +1 781 890 1801

CERTIFICACION - EQUIPO DE TRABAJO

El suscrito, **JOSHUA MOSES MARMOL**, con Pasaporte No. **566385611** de los **Estados Unidos d América**, Abogado de nacionalidad **Estadounidense**, con domicilio **230 Third Ave., Waltham, MA 02451 USA**, en mi condición de Presidente de la compañía **G.E.T. Secure ID Corp.** (junto con sus filiales en el grupo de empresas GET, "GET Group") una compañía debidamente incorporada y existente bajo las leyes de Estados Unidos, oferente de la solución de personalización "GET CLM600", el software PKI "GET Trust", y el software de identificación móvil "GET mID" (conjuntamente, los "Productos"), advertido de la trascendencia legal de este acto y de las penas previstas para los delitos de perjurio y falso testimonio, declaro bajo la fe de juramento que:

El equipo de trabajado presentado a continuación son empleados de GET Group y el currículo adjunto describe correctamente sus calificaciones y experiencias dentro de la compañía. Confirmo que se encuentran disponible para
desempeñar el rol indicado para cubrir los Productos ofrecidos de acuerdo con las disposiciones del proceso de la JUNTA CENTRAL ELECTORAL - REF.: JCE-CCC-LPI-2024-0001, DESTINADO A LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA NUEVA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI).

Ingeniero	Rol	Cargo / Funciones
Mauricio Moya	Lider Técnico	• Arquitecto jefe de soluciones • Entrenamiento certificado operativo y técnico. • Integración. • Soporte y Mantenimiento Impresoras - Tercer Nivel. [en sitio como de forma remota]
Camilo Motta	Ingeniero de hardware	• Ingeniero de Soporte • Entrenamiento certificado operativo y técnico. • Instalación. • Soporte y Mantenimiento Impresoras – Primer y Segundo Nivel. [en sitio como de forma remota]
Joel F. Perez	Gerente de Proyecto	• Líder del proyecto – Certificado PMP • Conocimientos ITIL • Gestión general del programa y diseño de la solución.

		• Dirección del equipo de trabajo: Arquitectos de Software y Equipo de desarrollo Integración, pruebas y Soporte al cliente.
Jon A. Donovan	Ingeniero de hardware	• Ingeniero de Soporte • Entrenamiento certificado operativo y técnico. • Instalación. • Soporte y Mantenimiento Impresoras – Primer y Segundo Nivel. [en sitio como de forma remota]
Oscar D. Reyes	Ingeniero de hardware	• Ingeniero de Soporte • Entrenamiento certificado operativo y técnico. • Instalación. • Soporte y Mantenimiento Impresoras – Primer y Segundo Nivel. [en sitio como de forma remota]
Arnie Pérez Rivera	Ingeniero de hardware	• Ingeniero de Soporte • Entrenamiento certificado operativo y técnico. • Instalación. • Soporte y Mantenimiento Impresoras – Primer y Segundo Nivel. [en sitio como de forma remota]
David Muñoz	Ingeniero de hardware	• Ingeniero de Soporte • Entrenamiento certificado operativo y técnico. • Instalación. • Soporte y Mantenimiento Impresoras – Primer y Segundo Nivel. [en sitio como de forma remota]

COPY & GRUPO INTERNACIONAL SA
CSI
RNC: 101036852
Santo Domingo, R.D.

Yo, **JOSHUA MOSES MARMOL** , hago constar que entiendo y conozco la responsabilidad y consecuencias que conlleva esta declaración y firmo en la ciudad de Waltham, MA USA el día [20] de febrero, del año 2025.

Firma,

Joshua M. Mármol
Presidente
G.E.T. SECURE ID CORP

GET GROUP
G.E.T. Secure ID Corp.
Established 2013; Delaware, USA

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 20 day of February, 2025 before me, the undersigned notary public, Joshua Mármol personally appeared, proved to me through satisfactory evidence of identification, which were USA passport, to be the person who signed the preceding or attached document in my presence and who swore or affirmed to me that the contents of the document are truthful and accurate to the best of (his) (her) knowledge and belief

Caitlyn E. Burns
Notary Public's Signature My Commission Expires December 29, 2028

CAITLYN E. BURNS
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
December 29, 2028

Curriculum del líder del proyecto o jefe de proyecto, que debe tener como mínimo 5 años de experiencia en uno o varios proyectos de identificación de tarjetas de policarbonato en instituciones públicas, tener certificado PMP, PRINCE2 o similar, así como conocimientos ITIL. Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, así como detallar las experiencias de la persona propuesta en una de las empresas del consorcio.

JOEL F. PEREZ, PMP

DIRECTOR DE PROGRAMAS Y PROYECTOS
Sr. MANAGER, PROGRAM AND PROJECT MANAGEMENT:

Arquitecto de soluciones, tecnología de la información, SDLC, servicios, entrega y soporte de CS

Alto directivo con un historial demostrado de racionalización de procesos, creación de relaciones y entrega de proyectos a tiempo, dentro del presupuesto y con alta calidad, siguiendo los principios y normas del PMI. Hábil negociador y priorizador de proyectos y tareas desarrollando sólidas relaciones de trabajo con organizaciones funcionales, clientes, proveedores externos y socios. Excelentes habilidades de comunicación a todos los niveles de gestión y con los miembros del equipo del proyecto. Amplia experiencia en organizaciones matriciales y gestión de equipos remotos. Siempre en busca de formas de mejorar los procesos para maximizar el tiempo y los recursos en proyectos de desarrollo e implantación de software y sistemas empresariales de TI y SI.

Desarrollo de soluciones - Entrega, implementación, interoperabilidad - Gestión de socios/clientes - Recopilación de requisitos empresariales y técnicos - Revisión de requisitos de control de calidad de SW y HW - Revisión de diseño detallada y de alto nivel - Desarrollo de SOW, NDA y CSA - Desarrollo de SW e ingeniería personalizada - Gestión del ciclo de vida de desarrollo de IT, IS y SW - Gestión de escalado - Recuperación de desastres y continuidad de negocio - NAS y SAN- Almacén de datos - Gestión de equipos remotos - Informes ETC, CAPEX - Criptografía - PKI - Herramientas de gestión de ID. - Conocimientos ITIL

EXPERIENCIA PROFESIONAL

Global Enterprise Technologies Corp., Waltham, MA - Ene/2016 - Presente
Soluciones y servicios de gestión de identidades

Director de Programas y Soluciones

En este puesto me centro en dos áreas: gestión de programas y diseño de soluciones. En el área de Gestión de Programas, soy responsable, junto con un equipo de Gestores de Programas y Proyectos, de la ejecución de Proyectos y Programas, estableciendo procesos y normas que estén en consonancia con los principios y directrices del PMBOK del PMI. Esto incluye la gestión de la entrega de proyectos internos y externos. Mi equipo se encuentra en los EE.UU. y algunos miembros del equipo se encuentran fuera de los EE.UU.. Mantengo la cartera de proyectos y las actualizaciones. En la función de diseño de soluciones, soy responsable de identificar nuevas tecnologías y diseñar nuevas soluciones, y trabajo con el equipo de desarrollo para transformar la solución en realidad. Los arquitectos y el equipo de desarrollo están bajo mi dirección. También soy responsable de un equipo de integradores y soporte. En este papel trabajo con empresas tecnológicas de todo el mundo para seleccionar la tecnología que mejor se adapte a nuestra solución. También participo en los grupos de trabajo de las normas ISO INCIT, WG10 y WG3 para identificaciones móviles y pasaportes.

Proyectos relacionados con el implementación de Soluciones emisión de documentos Físicos / Digitales de alta seguridad para gobierno:

a. Pasaporte electrónico de EE.UU. en Policarbonato, Enero 2018 - Presente
b. Permiso de conducir digital mDL [ISO mDL 18013-5] de Utha, USA, 2021 – Presente

MorphoTrust USA, una división estadounidense de Safran, Billerica, MA - Nov/2009 a Ene/2016
Empresa de servicios de seguridad y protección; componente de DOW, con más de 2000 empleados en todo el mundo.

Director de programa [Sr. Program Manager]
Organización PMO: Gestionar las operaciones y la entrega de aplicaciones de documentos seguros y programas de soluciones para el gobierno estatal y local, en un entorno funcional cruzado. Fui responsable de todos los recursos y el presupuesto operativo durante todo el ciclo de vida del programa, desde la recopilación de requisitos hasta la entrega de la solución completa. Trabajé en una organización interfuncional con equipos internos como ventas, gestión de productos, ingeniería de sistemas, desarrollo de software, compras, finanzas, control de calidad, gestión de la cadena de suministro, ingeniería de integración y alta dirección. Gestión y negociación con proveedores externos y clientes en la entrega de soluciones seguras. Gestión de equipos virtuales y miembros del equipo, así como de cara al cliente. Elaboración de informes de CAPEX, informes de desviaciones, estimación hasta la finalización (ETC), finalización real (AC), estimación/presupuesto a la finalización (EAC/BAC), gestión de cambios y desarrollo de planes de gestión de proyectos. Responsable de la ejecución general de programas generadores de ingresos. También contribuyo a los contratos RFP (Request for Proposal) durante el proceso de licitación. Contratación de personal y revisiones de Gate.

KENEXA CORPORATION - An IBM Company, Waltham, MA - Ene/2008 a Ene2009
Una empresa de desarrollo y soluciones de software de RRHH; componente del NasdaqGS, con más de 2500 empleados en todo el mundo.

Gestor de proyectos para clientes

Gestionó el desarrollo y el ciclo de vida de la entrega de proyectos de SW impulsados por los ingresos para clientes de la lista Fortune 500 como UBS, BP y PwC en la aplicación empresarial KRB de Kenexa, proporcionada como modelo SaaS. Gestión de varios jefes de equipo y directores funcionales en apoyo de proyectos de SI. Único punto de contacto para todos los proyectos de ingeniería y escalado. Gestionó equipos de proyecto de ingenieros de implementación en el Reino Unido, desarrolladores y miembros del equipo QE ubicados en la India. Entre sus responsabilidades se incluían el desarrollo de SOWs, contratos y la facilitación y presidencia de reuniones para la recopilación de requisitos, definición del alcance y firmas, actualizaciones de estado, presupuestos e informes de proyectos, presidencia de revisiones trimestrales de negocio.

EMC CORPORATION, Hopkinton, MA - Nov/1993 a Ene/2008

Diversos puestos en el Servicio de Atención al Cliente y Organizaciones de Apoyo

Gestionó el desarrollo y la entrega de proyectos impulsados por los ingresos, superiores a 750 000, para socios y clientes importantes. Gestión de varios jefes de equipo y gestores de proyectos.
Gestionó el ciclo de vida de desarrollo de la entrega, la evaluación y las soluciones de EMC para la implantación sobre el terreno, especializándose en continuidad del negocio y copias de seguridad y recuperación. Gestión de relaciones con socios. Cualificación de la interoperabilidad con servidores NCR y sus sistemas operativos MPRAS (Unix) y Windows, que ejecutan su buque insignia.
Producto de base de datos Data Warehouse Teradata con matrices de almacenamiento empresarial de EMC.
Asistencia sobre el terreno y configuración de matrices de almacenamiento Symmetrix empresariales en entornos heterogéneos, con múltiples hosts y sistemas operativos, incluida la recuperación ante desastres (SRDF y TimeFinder).

Instalación y mantenimiento de las principales matrices de almacenamiento de EMC (Symmetrix), así como de productos de gama media como la serie Harmonix. Algunos de los sistemas operativos implicados fueron el mainframe MVS, AS400, UNIX y Windows NT.

FORMACIÓN Y CERTIFICACIONES

Máster en Gestión de Ingeniería
Northeastern University - Boston, MA
Máster en Gestión de Tecnologías de la Información
Universidad Brandeis - Waltham, MA
Certificado de Posgrado en Ingeniería de Software
Universidad Brandeis - Waltham, MA
Licenciatura en Informática
Boston College - Chestnut Hill, MA
Certificado Unix C/C++
WPI - Worcester, MA
Certificado PMP #1497957

Formación y desarrollo
Criptografía y gestión de identidades; Six Sigma Green Belt; Cursos de gestión y liderazgo empresarial; Cursos de TI; Agile; SCRUM; Waterfall

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC

Project Management Institute.

THIS IS TO CERTIFY THAT

Joel F Perez

HAS BEEN FORMALLY EVALUATED FOR DEMONSTRATED EXPERIENCE, KNOWLEDGE AND PERFORMANCE IN ACHIEVING AN ORGANIZATIONAL OBJECTIVE THROUGH DEFINING AND OVERSEEING PROJECTS AND RESOURCES AND IS HEREBY BESTOWED THE GLOBAL CREDENTIAL

Project Management Professional (PMP)®

IN TESTIMONY WHEREOF, WE HAVE SUBSCRIBED OUR SIGNATURES UNDER THE SEAL OF THE INSTITUTE

LuAnn Placard, PMP | Chair, Board of Directors

Project Management Institute Corporate Seal Pennsylvania

Pierre Le Manh | President & CEO

Certification Number: 1497567

Original Grant Date: 16 April 2012

Expiration Date: 16 April 2027

COPY SOLUTIONS INTERNATIONAL S.A.
RNC 101

TRADUCCIÓN OFICIAL: Curriculum del Lider del Proyecto.

Yo, **LIC.SANTO C SIERRA.** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en Inglés, y cuya versión al Español, según mi mejor conocimiento, es el siguiente:

JOEL F. PEREZ, PMP

DIRECTOR DE PROGRAMAS Y PROYECTOS
Sr. MANAGER, PROGRAM AND PROJECT MANAGEMENT:

Arquitecto de soluciones, tecnología de la información, SDLC, servicios, entrega y soporte de CS.

Alto directivo con un historial demostrado de racionalización de procesos, creación de relaciones y entrega de proyectos a tiempo, dentro del presupuesto y con alta calidad, siguiendo los principios y normas del PMI. Hábil negociador y priorizador de proyectos y tareas desarrollando sólidas relaciones de trabajo con organizaciones funcionales, clientes, proveedores externos y socios. Excelentes habilidades de comunicación a todos los niveles de gestión y con los miembros del equipo del proyecto. Amplia experiencia en organizaciones matriciales y gestión de equipos remotos. Siempre en busca de formas de mejorar los procesos para maximizar el tiempo y los recursos en proyectos de desarrollo e implantación de software y sistemas empresariales de TI y SI.

Desarrollo de soluciones - Entrega, implementación, interoperabilidad - Gestión de socios/clientes - Recopilación de requisitos empresariales y técnicos - Revisión de requisitos de control de calidad de SW y HW - Revisión de diseño detallada y de alto nivel - Desarrollo de SOW, NDA y CSA - Desarrollo de SW e ingeniería personalizada - Gestión del ciclo de vida de desarrollo de IT, IS y SW - Gestión de escalado - Recuperación de desastres y continuidad de negocio - NAS y SAN- Almacén de datos - Gestión de equipos remotos - Informes ETC, CAPEX - Criptografía - PKI - Herramientas de gestión de ID. - Conocimientos ITIL

EXPERIENCIA PROFESIONAL

Global Enterprise Technologies Corp., Waltham, MA - Ene/2016 - Presente
Soluciones y servicios de gestión de identidades

Director de Programas y Soluciones

En este puesto me centro en dos áreas: gestión de programas y diseño de soluciones. En el área de Gestión de Programas, soy responsable, junto con un equipo de Gestores de Programas y Proyectos, de la ejecución de Proyectos y Programas, estableciendo procesos y normas que estén en consonancia con los principios y directrices del PMBOK del PMI. Esto incluye la gestión de la entrega de proyectos internos y externos. Mi equipo se encuentra en los EE.UU. y algunos miembros del equipo se encuentran fuera de los EE.UU. Mantengo la cartera de proyectos y las actualizaciones. En la función de diseño de soluciones, soy responsable de identificar nuevas tecnologías y diseñar nuevas soluciones, y trabajo con el equipo de desarrollo para transformar la solución en realidad. Los arquitectos y el equipo de desarrollo están bajo mi dirección. También soy responsable de un equipo de integradores y soporte. En este papel trabajo con empresas tecnológicas de todo el mundo para seleccionar la tecnología que mejor se adapte a nuestra solución. También participo en los grupos de trabajo de las normas ISO INCITS, WG10 y WG3 para identificaciones móviles y pasaportes.

Proyectos relacionados con el implementación de Soluciones emisión de documentos Físicos / Digitales de alta seguridad para gobierno:

a. Pasaporte electrónico de EE.UU. en Policarbonato, Enero 2018 - Presente
b. Permiso de conducir digital mDL [ISO mDL 18013-5] de Utha, USA, 2021 – Presente

MorphoTrust USA, una división estadounidense de Safran, Billerica, MA - Nov/2009 a En[illegible]

Empresa de servicios de seguridad y protección; componente de DOW, con más de 2000 empleados en todo el mundo.

Director de programa [Sr. Program Manager]

Organización PMO: Gestionar las operaciones y la entrega de aplicaciones de documentos seguros y programas de soluciones para el gobierno estatal y local, en un entorno funcional cruzado. Fui responsable de todos los recursos y el presupuesto operativo durante todo el ciclo de vida del programa, desde la recopilación de requisitos hasta la entrega de la solución completa. Trabajé en una organización interfuncional con equipos internos como ventas, gestión de productos, ingeniería de sistemas, desarrollo de software, compras, finanzas, control de calidad, gestión de la cadena de suministro, ingeniería de integración y alta dirección. Gestión y negociación con proveedores externos y clientes en la entrega de soluciones seguras. Gestión de equipos virtuales y miembros del equipo, así como de cara al cliente. Elaboración de informes de CAPEX, informes de desviaciones, estimación hasta la finalización (ETC), finalización real (AC), estimación/presupuesto a la finalización (EAC/BAC), gestión de cambios y desarrollo de planes de gestión de proyectos. Responsable de la ejecución general de programas generadores de ingresos. También contribuyo a los contratos RFP (Request for Proposal) durante el proceso de licitación. Contratación de personal y revisiones de Gate.

KENEXA CORPORATION - An IBM Company, Waltham, MA - Ene/2008 a Ene2009
Una empresa de desarrollo y soluciones de software de RRHH; componente del NasdaqGS, con más de 2500 empleados en todo el mundo.

Gestor de proyectos para clientes

Gestionó el desarrollo y el ciclo de vida de la entrega de proyectos de SW impulsados por los ingresos para clientes de la lista Fortune 500 como UBS, BP y PwC en la aplicación empresarial KRB de Kenexa, proporcionada como modelo SaaS. Gestión de varios jefes de equipo y directores funcionales en apoyo de proyectos de SI. Único punto de contacto para todos los proyectos de ingeniería y escalado. Gestionó equipos de proyecto de ingenieros de implementación en el Reino Unido, desarrolladores y miembros del equipo QE ubicados en la India. Entre sus responsabilidades se incluían el desarrollo de SOWs, contratos y la facilitación y presidencia de reuniones para la recopilación de requisitos, definición del alcance y firmas, actualizaciones de estado, presupuestos e informes de proyectos, presidencia de revisiones trimestrales de negocio.

EMC CORPORATION, Hopkinton, MA - Nov/1993 a Ene/2008

Diversos puestos en el Servicio de Atención al Cliente y Organizaciones de Apoyo

Gestionó el desarrollo y la entrega de proyectos impulsados por los ingresos, superiores a 750 000, para socios y clientes importantes. Gestión de varios jefes de equipo y gestores de proyectos.
Gestionó el ciclo de vida de desarrollo de la entrega, la evaluación y las soluciones de EMC para la implantación sobre el terreno, especializándose en continuidad del negocio y copias de seguridad y recuperación. Gestión de relaciones con socios. Cualificación de la interoperabilidad con servidores NCR y sus sistemas operativos MPRAS (Unix) y Windows, que ejecutan su buque insignia.
Producto de base de datos Data Warehouse Teradata con matrices de almacenamiento empresarial de EMC.
Asistencia sobre el terreno y configuración de matrices de almacenamiento Symmetrix empresariales en entornos heterogéneos, con múltiples hosts y sistemas operativos, incluida la recuperación ante desastres (SRDF y TimeFinder).

Instalación y mantenimiento de las principales matrices de almacenamiento de EMC (Symmetrix), así como de productos de gama media como la serie Harmonix. Algunos de los sistemas operativos implicados fueron el mainframe MVS, AS400, UNIX y Windows NT.

LIC. SANTO C. SIERRA
Suprema Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

Máster en Gestión de Ingeniería
Northeastern University - Boston, MA
Máster en Gestión de Tecnologías de la Información
Universidad Brandeis - Waltham, MA
Certificado de Posgrado en Ingeniería de Software
Universidad Brandeis - Waltham, MA
Licenciatura en Informática
Boston College - Chestnut Hill, MA
Certificado Unix C/C++
WPI - Worcester, MA
Certificado PMP #1497957
Formación y desarrollo
Criptografía y gestión de identidades; Six Sigma Green Belt; Cursos de gestión y liderazgo empresarial; Cursos de TI; Agile; SCRUM; Waterfall

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

Project Management Institute

Este certificado certifica que

Joel F Perez

Ha sido formalmente evaluado por su experiencia demostrada, conocimiento y desempeño en el logro de un objetivo organizacional a través de la definición y supervisión de proyectos y recursos, y por lo tanto, se le otorga la credencial global de

Profesional en Dirección de Proyectos (PMP)

En testimonio de lo cual, hemos suscrito nuestras firmas bajo el sello del Instituto.

LuAnn Piccard, PMP | Presidenta, Junta Directiva

Pierre Le Manh | Presidente y CEO

Número de certificación: 1497957 Fecha de concesión original: 16 de abril de 2012 Fecha de expiración: 16 de abril de 2027

LIC. SANTO C. SIERRA
Juez 1ra Instancia D.N.
SANTO DOMINGO, R.D.

Inicio» Certificaciones» Recursos de Certificación

Registro de Certificación

Registro de Certificación

Nombre	Apellido	Certificación	*País / Región*
Joel	Pérez	Todas las certificaciones	Estados Unidos

[Buscar de nuevo]

*Campo obligatorio

Los titulares de certificaciones pueden optar por no aparecer en el registro y no se mostrarán en la búsqueda

3 resultados para Joel Pérez, Estados Unidos

Nombre	Ubicación	Certificación
Joel F. Pérez MA,	Estados Unidos	![PMP] Activo desde abril de 2012

Traducido a solicitud del interesado e inscrito en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, hoy Diez (10) del mes de Julio del año Dos Mil Veinticuatro (2024).

PROCURADURÍA GENERAL DE LA REPÚBLICA
MINISTERIO PÚBLICO
CENTRO DE ATENCIÓN AL CIUDADANO

Código CIS: 001-5202-4757115-5

5184-12-8-96

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

LIC. SANTO C. SIERRA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

Curriculum del personal técnico certificado en tecnología de impresión de tarjetas de identidad localmente durante la vigencia del contrato para supervisión de la calidad de la impresión en todos los centros de impresión de cédulas. Se deben incluir las certificaciones correspondientes.Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, así como detallar las experiencias de la persona propuesta en una de las empresas del consorcio.

MAURICIO MOYA PAEZ

Bogotá, Colombia
Cel: 314 353 1992
mamoro77@gmail.com

PERFIL PROFESIONAL

Ingeniero de Sistemas, especialista en Gerencia de Proyectos, con alto nivel de inglés. Amplia experiencia en desarrollo e implementación de proyectos de software, en el sector Industria, Gobierno y Financiero, liderando equipos técnicos. Alta capacidad para aprender rápidamente. Habilidades de liderazgo, orientado a resultados, innovador. Excelentes relaciones interpersonales.

EXPERIENCIA LABORAL

GET GROUP LATAM **2018 - Presente**
Arquitecto de Soluciones

Responsable de propuestas técnicas de proyectos de Preventa y Postventa de Software y Hardware, trabajando como SME (Subject Matter Expert) en productos del Grupo GET Group y posibles alianzas técnicas para cumplir con los requerimientos de los clientes de Gobierno.

- ✓ Trabaje como arquitecto de soluciones para la implementación del producto de Identificación y verificación biométrica digital Biometric ID, desde la conceptualización del producto hasta la implementación completa, incluido el soporte de ventas y licitaciones, el esfuerzo de gestión de proyectos y la entrega de desarrollo de software. Trabajar con 4 equipos técnicos para implementar el proyecto.
- ✓ Trabajo en el diseño de una suite de productos digitales que involucra biometría y servicios digitales, para una plataforma SaaS.
- ✓ Encargado y certificado en la Implementación de 4 proyectos de impresión de documentos de identificación haciendo uso de tecnologías de impresión en Re-Transferencia Térmica indirecta.
- ✓ Participación en la construcción de propuestas Técnico - Comerciales, obteniendo tres proyectos exitosos (USD$ 5,1 M).

CITIBANK COLOMBIA S.A. **2017 - 2018**
Technology Business Representative

Responsable de los productos de Software de Pagos y Tarjetas Comerciales de Citibank para clientes Corporativos en Colombia, realizando el Análisis de Negocio de los requisitos Regulatorios, Comerciales y Tecnológicos, y gestionando la implementación de nuevas iniciativas, en colaboración con fábricas y proveedores de software internos.

3M COLOMBIA S.A. **2016 – 2017**
Ingeniero Líder de Aplicaciones Técnicas

Responsable por la preventa, implementación y soporte de proyectos del portafolio de Identity Management, ALPR y Electronic Monitoring en Colombia, trabajando con clientes directos de Gobierno como integradores y distribuidores.

- ✓ Participé en la construcción de propuestas técnico – comerciales, obteniendo un proyecto exitoso, ocho licitaciones públicas y tres propuestas comerciales privadas.
- ✓ Contribuí con el soporte técnico de cuenta para lograr la meta de facturación en 102% para Electronic Monitoring en 2016 y 2017.
- ✓ Contribuí en el lanzamiento de nuevos productos, con la generación de demostraciones de Reconocimiento facial y Lectores de documentos seguros, dentro de la campaña de nuevos integradores de tecnología, ampliando los conocimientos técnicos de los ingenieros que permitieron aumentar la venta.

MIGRACION COLOMBIA **2013 - 2016**
Profesional Especializado, Coordinador del Grupo de Desarrollo de Software

Responsable por los proyectos de desarrollo e implementación del software misional de la Entidad, coordinando grupos técnicos internos y externos, gestionando los requerimientos de la Entidad.

- ✓ Coordiné la consolidación de los sistemas de información desarrollados por la Entidad para el control migratorio.
- ✓ Lideré la implementación de la metodología de SaaS en la Entidad para soportar la integración de los diferentes sistemas que intervienen en el paso migratorio.
- ✓ Lideré la implementación de nuevos sistemas tales como APIS (Advance Passanger Information System), SIRE (Sistema para la reporte de información de personas extrajeras en Colombia) y Verificación Biométrica de Ciudadanos Extranjeros.

COMISION DE REGULACION DE COMUNICACIONES **2012 - 2013**
Profesional Especializado

Responsable de la administración del software de información regulatoria de la Comisión, dando soporte directo a los usuarios regulados, y la implementación de nuevos requerimientos de información, gestionando proveedores.

- ✓ Administré el software misional SIUST de la Comisión y el MinTic.
- ✓ Coordine la implementación del sistema de Homologación de Terminales Móviles.
- ✓ Implementé sistemas de soporte a la gestión, como Qlikview y OnBase.

DYNATECH MOBILE **2012**
Supervisor de Desarrollo IT

Responsable por el soporte técnico al sistema de Fulfillment de la compañía, dando soporte técnico al software, desarrollando nuevos requerimientos y pruebas unitarias.

TECNOIMAGENES **2010 - 2011**
Ingeniero de Implementación

Responsable por la implementación del software de Gestión de Contenido Empresarial OnBase para los clientes asignados, gestionando los requerimientos solicitados e implementando los flujos de trabajo requeridos, brindando el soporte necesario.

- ✓ Implemente la Gestión de Reclamaciones de seguros SOAT haciendo uso de los flujos de trabajo del software OnBase.

CITYNETWORKS, INC. **2008 - 2010**
Especialista de Producto

Responsable por la preventa de los productos de software de la compañía, realizando presentaciones técnicas y desarrollando demostraciones y pilotos para el sector bancario, especializado en aplicaciones para conciliaciones de cuentas bancarias, registros de sistemas y operaciones SWIFT.

NETTING SOLUTIONS LTDA. **2006 - 2008**
Director de Producción de Software

Responsable por el desarrollo e implementación de software web para E-Learning, siguiendo el ciclo de vida de los proyectos de software.

- ✓ Participe en la Certificación ISO 9000 para el proceso de producción de software.
- ✓ Lideré la implementación de procedimientos de control de calidad para el desarrollo de software.
- ✓ Coordine el equipo interdisciplinario para la atención de los requerimientos de desarrollo de software dentro del sistema E-learning.

BRIGHTPOINT DE COLOMBIA INC. **2005 - 2006**
Asistente de desarrollo

SCRIPTA SOFTWARE **2004 - 2005**
Ingeniero desarrollador

FORMACIÓN ACADÉMICA

Especialista en Gerencia de Proyectos de Sistemas - Universidad del Rosario - Bogotá, Colombia - 2009

Ingeniero de Sistemas - Universidad EAN – Bogotá, Colombia - 2004

FORMACIÓN COMPLEMENTARIA

- Programa de Liderazgo y Comunicación. INALDE Business School – Universidad de la Sabana
- Curso de Gestión de Proyectos PMI. Universidad del Rosario
- Scrum Master. IT Service. En curso.
- Programming a Microsoft SQL Server 2000 Database. CTT Corporation
- Querying Microsoft SQL Server 2000 with Transact-SQL. CTT Corporation
- Formación de Auditores Internos de Calidad. ICONTEC
- Microsoft Certified Application Developer (MCAD). Curso. Aptech
- Programas manejados: Ofimática, Herramientas de desarrollo de software (.Net, Java, SQL, PL-SQL), Microsoft Project.

REFERENCIAS LABORALES

RODRIGO AMORTEGUI
Líder de Grupo Calidad de la Factura - **Empresa de Telecomunicaciones de Bogotá, ETB.**
Celular 300 218 2896

JOSÉ VELEZ
Coordinador de Desarrollo - **DYNATECH MOBILE**
Teléfono 439 5237

ANDRES FELIPE RAMIREZ
Regional Sales Manager – **GET GROUP**
Celular 320 232 6191

Camilo Ernesto Motta Zambrano

Ingeniero Electrónico

ca-motta@uniandes.edu.co, camermo@gmail.com
Dirección: Av Cra 86# 22F 19, Apto 101. Bogotá,
Celular: +57 300 5707126, +57 300 1244032

COPY SOLUTIONS INTERNATIONAL, S.A. RNC: 101 Santo Domingo R.D.

PERFIL PROFESIONAL:

Ingeniero Electrónico Bilingüe, con amplio conocimiento en lenguajes de programación, lo que me ha permitido hacer desarrollos en distintas áreas de la ingeniería donde he trabajado, tales como: Machine Learning, Análisis de espectro radioeléctrico, ventas de servicios - productos, aplicaciones para inventarios, personalización de tarjetas inteligentes, entreotros. Con 8 años de experiencia en manejo de grupos de trabajo para dar soluciones técnicas o soporte en las mismas. Autodidacta y hábil para el aprendizaje continuo, diario, no solo de lenguajes de programación, sinotambién de herramientas complementarias en audio, video, diseño, estructuración de proyectos, que hacen mi trabajo más fácil, y de calidad.

ESTUDIOS:

- **Pregrado en Ingeniería Electrónica:** Universidad de los Andes, Bogotá, Colombia 2010.
  - **Tesis Remarcable**: Aplicación de algoritmos de **Machine Learning** e **Inteligencia Artificial** (usando Python,Java y c++) a bases de datos con información extraída de audios de voz cantada, para identificar patrones que permitan decidir cuando se están aplicando correctamente 5 lineamientos concretos de la técnica vocal lirica. Link de publicación: dhttps://repositorio.uniandes.edu.co/handle/1992/25276?show=full
  - **Directora de Tesis**: Alba Graciela Ávila Bernal, phD Cambridge University, profesora asociada en la Facultad de Ingeniería Eléctrica y Electrónica de la Universidad de los Andes. Bogotá – Colombia.
- **Grado Opcional (al grado de Ingeniero electrónico) en Música: "Técnicas de Grabación":** Universidad de los Andes, Bogotá, Colombia 2010.
- **Estudiante de intercambio:** Institución "Warren Central High School". Bowling Green, Kentucky, Estados Unidos. Septiembre de 2001 a septiembre de 2002. ***Manejo 100% de idioma ingles hablado y escrito.***
- **Diplomado en Gerencia de Mercadeo y ventas:** Universidad Sergio Arboleda, Bogotá, Colombia, 2014.
- **Certificación en Desarrollo Web Full Stack en Html, CSS3 , Bootstrap, and JavaScript:** Johns Hopkins University, Baltimore USA, Julio a septiembre de 2020.
- **Programa en desarrollo de software:** MinTic Colombia 2022. 8 meses, Especialización Virtual de 4 ciclos: C1-Fundamentos en lenguaje Python. C2-Fundamentos en lenguaje Java, GitHub, and SQL. S3- Desarrollo de apps utilizando Java, Springboot framework, HTML, CSS3, and JavaScript. C4- Desarrollo de aplicaciones Móviles.

EXPERIENCIA PROFESIONAL:

Compañía: **G.E.T SECURE ID CORP (GET GROUP LATAM)**
Período: Enero 10 de 2023 – Trabajando Actualmente aquí
Cargo: Hardware Engineer
Labores:

- Ingeniero certificado en el manejo y mantenimiento de máquinas de impresión por re-

trasferencia térmica marca Toppan. G.E.T GROUP Dubai UAE.
- Capacitador certificado en manejo y mantenimiento de máquinas de impresión por re-trasferencia térmica, marca Toppan. G.E.T GROUP, Dubai UAE.
- Soporte ingenieril en procesos de venta y posventa, de acuerdo a condiciones técnico-comerciales pactadas con clientes de la región andina.
- Capacitar a clientes de la región con las ultimas actualizaciones y versiones de los productos que obtienen con la compañia.
- Inclusión e instalación de SDKs (Java, Kotlin) de soluciones de terceros en productos actuales de la compañía, en pro de expandir las oportunidades de negocio en la región.
- Revisión de condiciones Técnico-contractuales de NDAs, business contracts, etc, que se acuerdan con otras compañías, con el objetivo de trabajar conjuntamente en soluciones que signifiquen posibles oportunidades de negocio.
- Reportes de desempeño al cliente, utilizando manipulación SQL de bases de datos, que se generan por una plataforma de mesa de ayuda basada en tickets, al gestionar el trabajo de un socio técnico, que brinda soporte técnico durante la operación oficial nacional de emisión de licencias de conducir en Ecuador.
- Administrar partners de soporte técnico, con el objetivo de lograr la mejor percepción posible que los clientes tienen de los productos obtenidos con la compañía.
- Soportar al departamento de ventas, sosteniendo la mejor relación posible con los clientes en términos de posventa y solución de inquietudes de ingenieria que puedan llevar a posibles negocios futuros.
- Adaptación e inclusión en Python de modelos de AI previamente entrenados, para hacer aplicaciones de escritorio que faciliten tareas diarias de la compañía.
- Desarrollo y alojamiento de API REST y DB en instancias de AZURE y AWS, hechas en c# .NET CORE, con el fin de conectarlas, y generar bases de datos con información vital en la elaboración de reportes para proyectos de clientes.
- Levantamiento de requerimientos de clientes para estructurar demos de productos de software, que son expuestos en gestiones de preventa.
- Instalación, despliegue y administración en ambientes cloud y on-premise, de aplicaciones web (ZABBIX y otros) de monitoreo de calidad de servicios y productos software tanto de la compañía como de terceros.
- Diseño de mockups en **FIGMA** y **Adobe Ilustrator** de aplicativos web y aplicativos móviles, utilizados en presentaciones internas y a clientes.
- **CERTIFICACIONES:**
  1. Manejo y mantenimiento de máquinas de impresión por re-trasferencia térmica marca Toppan. 1er semestre de 2023. G.E.T GROUP Dubai UAE.
  2. Capacitador en manejo y mantenimiento de máquinas de impresión por re-trasferencia térmica, marca Toppan. 2do semestre de 2023. G.E.T GROUP, Dubai UAE.

Compañía: **BARBARIAN S.A.S (Nit 901045886-0)**
Periodo: **Diciembre de 2017 – Diciembre de 2022**
Cargo: **CDO(Chief Digital Officer).**
Labores:

- Desarrollo de sitio web de la marca en tecnologías HTML5, CSS3, y JavaScript.
- Seguimiento continuo al desempeño de la página para optimizar tiempos en consultas y errores presentados en las mismas.
- Atención exclusiva para clientes angloparlantes.
- Programación de todo el motor generador de la base de datos de clientes e interesados en franquicias de la marca, para llevar a cabo gestiones de remarketing principalmente.

- Desarrollo de micro webs conectados con bases de datos de la empresa, mediante los cuales se hace el levantamiento de datos de clientes en puntos de venta, durante su acceso a wifi y otros servicios.
- Representación de la empresa en rueda de negocios con inversionistas de **Shark Tank Colombia** en su tercera temporada, logrando un levantamiento de capital y socio estratégico, significativos. Link de la presentación:https://www.youtube.com/watch?v=3FNLwkquAcY&t=58s

Compañía: Zamhi Inversiones Inmobiliaria
Periodo: Enero 2015 a Diciembre 2017
Cargo: Director E-commerce
Labores:

- Estructurar y liderar reuniones de acercamiento y cierre de venta, toda vez que un vendedor y comprador manifieste interés en llevar a cabo un negocio.
- Actualización, seguimiento, y publicación de campañas de ecommerce de inmuebles en redes sociales y medios electrónicos relacionados con la finca raíz, que permitan obtener un feedback diario del tipo de propiedades, compradores, y zonas de mayor interés en el mercado inmobiliario.
- Permanente elaboración y depuración del sitio web de la compañía que permita un rápido acceso de clientes con posibles oportunidades de negocio.
- Elaboración de una plataforma electrónica de recursos para la propia empresa y para clientes, de generación automática de documentos y certificaciones.
- Posicionamiento del sitio web y marca en principales buscadores de internet, a través de manejo de analítica de datos, herramientas de ads management, estrategias de SEO, entre otras.
- Elaboración y sincronización de aplicaciones móviles con bases de datos de la empresa, para sistematizar procesos operativos importantes en la captación de inmuebles, y nuevos clientes.

Compañía: IDEMIA
Periodo: Noviembre 21 de 2012 – Octubre 17 de 2014
Cargo: Consultor Técnico Local para la Región Andina
Labores:

- Programación de SIMcards y USIMcards, en cuanto a sus contenidos, sus aplicaciones, siguiendo estándares técnicos de las comunicaciones en telefonía celular de instituciones mundiales como ETSI, GSMA, etc, y de acuerdo con las necesidades de los clientes.
- Investigación y preparación de productos demo de tecnologías contactless como NFC para aplicaciones en industrias de la telefonía móvil, la identificación, y payment.
- Desarrollar aplicativos de escritorio útiles para el ingreso de la información en códigos hexadecimales a las tarjetas inteligentes, de acuerdo con estándares USIM.
- Impulso al departamento de ventas, a través de presentaciones de productos a clientes, con workshops técnico-comerciales.

Compañía: Cine Colombia S.A
Periodo: Marzo de 2011 – Noviembre 19 de 2012,
Cargo: Ingeniero de Telecomunicaciones
Labores:

- Diseño y elaboración de aplicaciones web enlazadas con bases de datos, para control y supervisión de consumo de servicios públicos en todos los multiplex a nivel nacional.
- **Logros importantes:** Implementación a nivel nacional de una red de recepción satelital de TV en HD en 7 puntos distintos, para recibir contenidos alternativos y proyectarlos en salas de cine, todo, con una infraestructura inhouse.
- Encargado de las comunicaciones en idioma inglés hechas por la gerencia técnica. Capacitación de personal en Manejo de equipos de medición satelital.

Compañía: Agencia Nacional del Espectro (ANE), Ministerio de Comunicaciones
Periodo: Febrero 2011 - Marzo 2011
Cargo: Ingeniero de soporte técnico y administrativo
Labores:

- **Operativo**: Operación de equipos para toma de datos de espectro radioeléctrico durante visitas técnicas y trabajo de campo.
- **Administrativo**: Elaboración de informes técnicos de sesiones de toma de datos realizados en distintos lugares del país, para supervisión del buen uso del espectro radioeléctrico, de acuerdo ala ley Colombiana.
- **Logros importantes:** Ofrecimiento de ascenso por excelente desempeño y conocimiento teórico-práctico de equipos de medición de alto nivel.

Compañía: **Universidad de los Andes. Facultad de Matemática Pura**
Periodo: Semestres: 2009-1, 2009-2, 2010-1, 2010-2
Cargo: Tutor de
MatemáticasLabores:

- Orientación académica y tutoria en: Calculo Diferencial, Calculo Integral, Calculo Multivariado, Ecuaciones Diferenciales, Algebra Lineal, Estadística y Probabilidad.
- **Logros importantes:** Escogido entre estudiantes de ingeniería para este cargo por obtener excelentes calificaciones en todas las asignaturas de matemática cursadas durante el pregrado.

Compañía: Universidad de los Andes.
Periodo: Primer semestre de 2007.
Labores:

- Desarrollo en PHP y HTML del sitio web "Mapa Sonoro de la Universidad de losAndes".
- Web master del sitio:
- **URL del sitio: (http://mapasonoro.uniandes.edu.co) (ver creditos).**

Compañía: SOMMEILL LTDA - TRACFONE WIRELESS.
Periodo: June 2004 - June
2005.Cargo: Agente internacional.

Labores:

- Soporte a clientes, basado en aéreas de cobertura, tecnologías de telefonía celular, carriers asociados, etc.
- Aplicación de servicios OTA para llevar a cabo procesos como actualización de teléfonos, redención de tarjetas prepago, activación de servicios, restablecimiento de señal, entre otros.
- Presentación de productos a clientes de acuerdo a sus necesidades y ubicaciones.
- Identificación y localización de usuarios en bases de datos a través de IMEI's, IMSI's, y pruebasde validación en tarjetas SIM.
- **Logros importantes:** Ascenso al "Departamento de Activación de Líneas" por excelente uso delenguaje técnico, manejo de clientes y fluidez al hablar, todo esto, en idioma inglés.

PROYECTOS PROFESIONALES REMARCABLES:

Trabajo Realizado: Implementación de una red CISCO de conectividad vía internet inalámbrico, hecha en Instituciones educativas de bajos recursos en Quimbaya-Quindio, En compañía de estudiantes de la Universidad Politécnica de Cataluña-España.

Periodo: Intersemestral de 2009.

Labores:

Programación y acondicionamiento de antenas, routers, y demás elementos de la red siguiendo diseños basados en **protocolo Cisco de redes inalámbricas unificadas**. Trabajo de campo paralevantamiento de torres y estructuras de soporte.

CONOCIMIENTOS EN SOFTWARE Y PROGRAMACION

- Desarrollo de frontend y backend de sitios web en **Html5**, **CSS**, y **javaScript**.
- Diseño y gestión de Bases de Datos utilizando **SQL**, **Python** y **PostgreSQL**.
- Diseño de APIs Rest en **Spring Boot**, **C#**, y **javaScript**.
- Desarrollo de aplicaciones de escritorio en frameworks de **python**, **C#**.
- Diseño de **mockups** y **layouts** en **FIGMA**, **Adobe Ilustrator**, y **Android Studio.**
- Diseño y Edición de video en **Adobe Premiere**.
- Edición profesional de audio en **Protools**, **Logic Pro.**

CURSOS Y ESTUDIOS IMPORTANTES:

- Capacitación en telefonía móvil y nuevos modelos de negocio de esta tecnología. Paris – Francia. Verano del 2013, en instalaciones de la empresa Oberthur Technologies.
- Certificación nivel 1 en programación y operación de proyectores Digitales marca "Barco". Sao Paulo Brasil , Abril de 2011. Patrocinado por Cine Colombia S.A.
- Curso de edición y creación de video con Abode Premiere. Plataforma virtual Udemy. Septiembre de 2022. Certificado: https://www.udemy.com/certificate/UC-7385b6d5-b1ec-4aed-ad9a-88bb672c3a33/

IDIOMAS:

- Español (100% hablado y escrito)
- Inglés (100% Hablado y escrito)
- Francés (En estudio intensivo del lenguaje).

JOHAN DAVID MUÑOZ BONILLA

+57 3057696405

johan_munoz@hotmail.es

Carrera 8 # 170 – 52. Bogotá. Colombia

COPY SOLUTIONS INTERNATIONAL SA
RNC 101858652
Santo Domingo, R.D.

Resumen Profesional

Ingeniero Electrónico con amplia experiencia y conocimientos prácticos en soporte tecnológico en diversas áreas de tecnologías de la información tanto en software como en hardware con especial enfoque en optimizar procesos para solución de incidencias. Cuento con amplias habilidades de comunicación y relaciones interpersonales. Mis características son mi rápida adaptación, proactividad y entusiasmo además de una excelente actitud para trabajar en equipo o de forma independiente.

Aptitudes

Habilidades Sociales:

- Excelentes relaciones interpersonales
- Rápido aprendizaje
- Fácil Adaptación
- Habilidad para trabajar bajo presión

IT:

Herramientas de Administración:

- Oracle SOA, Developer, Toad, Tortoise SVN, Tortoise CVS, IntelliJ, Eclipse
- Team Foundation Server, Microsoft Visual Studio, Kactus HCM, Seven ERP
- Mantenimiento de Equipos de Computo
- Desarrollo y Automatización:
- Java, Selenium, TestNG, Serenity, Cucumber

Desarrollo:

- Aplicaciones Android -Kotlin, java
- Aplicaciones Web - JS, React
- Aplicaciones de Escritorio - C#

Diplomas

- ITIL Foundation 4
- Fundamentos de seguridad en tecnologías de la información- Fundación de Egresados Universidad Distrital Colombia
- Conexión y colaboración NFC Objetivo Fiber Connect
- Oracle Service Bus 11g: Administración del sistema Intl

HISTORIAL LABORAL

07/2024 – Actual
DET Group Latin America S.A.S | Bogotá. DC. Colombia
Technical Business Analyst & Software Lead

- Diseño de proyectos técnicos e implementación de soluciones de acuerdo a las necesidades de los clientes
- Liderar el proceso de desarrollo de software en colaboración con los equipos internos y externos
- Proveer capacitación y soporte a cada uno de los proyectos a fin de asegurar la calidad y el buen servicio.

11/2022 – 07/2024
GMI Software S.A.S | Bogotá. DC. Colombia
Test Automator Senior

- Desarrollo y mantenimiento de la suite de automatización destinada a regresiones y smoke test del cliente
- Soporte y apoyo al equipo de QA en la ejecución de tareas de regresión y smoke test
- Trabajar mano a mano con los equipos de otras regionales a fin de mantener los estándares, lineamientos y políticas que rigen los desarrollos dentro de la entidad

04/2019 – 11/2022
DET Group Latin America S.A.S | Bogotá. DC. Colombia
Hardware Technician

- Preparación de herramientas y útiles para Tradeshows
- Pruebas de Producto y Control de calidad
- Formación de nuevos Clientes en referencia a los productos ofrecidos por la compañía
- Mantenimiento preventivo y correctivo
- Detección y resolución de incidencias de acuerdo a los protocolos establecidos.
- Apoyo en el desarrollo de nuevas herramientas de software.
- Respuesta a problemas/consultas de los clientes.

07/2018 – 04/2019
Migración Colombia | Bogotá. DC. Colombia
Técnico Administrativo

- Administración de servidores (Windows Server 2008, Server 2012
- Linux: Oracle Linux, RedHat)
- Gestión del Código y administración del Repositorio (Tortoise SVN, Microsoft Team Foundation Server)
- Control y Publicación de Aplicaciones Jboss
- Administración de Bases de Datos ORACLE y SQL
- Atención al Cliente
- Guía y orientación al Extranjero

FORMACIÓN

01/2009 – 12/2013
Universidad Cooperativa de Colombia | Bogotá. DC. Colombia
Ingeniero Electrónico

01/2003 – 12/2008
I.E.D Aquileo Parra | Bogotá. DC. Colombia
Bachiller Académico

IDIOMAS

Español: Idioma Nativo
Inglés: IELTS Band 8.5

Curriculum del personal técnico en campo (a nivel nacional) con experiencia en la producción de documentos de identidad nacionales mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a la infraestructura de impresión durante los años de garantia de los equipos. Para acreditar dicha experiencia, el oferente debe aportar el Curriculum Vitae del candidato, asi como detallar las experiencias de la persona propuesta en una de las empresas del consorcio.

The Commonwealth of Massachusetts

William Francis Galvin
Secretary of the Commonwealth

COPY SOLUTIONS INTERNATIONAL SA
CSI
RNC 401898852
Santo Domingo, R.D.

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *Country:* United States of America

This public document

2. *has been signed by:* Wilfredo Martinez
3. *acting in the capacity of:* Notary Public
4. *bears the seal/stamp of:* Wilfredo Martinez

whose commission expires on: October 18, 2030

Certified

5. *at:* Boston, Massachusetts
6. *the:* 25 June, 2024
7. *by:* the Secretary of the Commonwealth
8. *No.:* 2605554
9. *Seal/stamp:* ***Great Seal of the Commonwealth***

10. *Signature:*

William Francis Galvin
Secretary of the Commonwealth

prepared by NCorreia

G.E.T. Secure ID
230 Third Avenu
Waltham, MA 02
T: +1 (781) 902-
F: +1 (781) 890-
www.getgroup.

[21] de junio 2024

Para: Junta Central Electoral de la República Dominicana.
Referencia: JCE-CCC-LPI-2024-0001
Asunto: Carta de Certificación de Experiencia Personal Técnico a Nivel Nacional.

Estimados Sres.,

NOSOTROS, G.E.T. Secure ID Corp, (junto con sus filiales en el grupo de empresas GET, "GET Group") una compañía debidamente incorporada y existente bajo las leyes de Estados Unidos, oferente de la solución de personalización "GET CLM600", el software PKI "GET Trust", y el software de identificación móvil "GET mID" (conjuntamente, los "Productos),

POR LA PRESENTE CERTIFICAMOS que el SR. HARRY WILLIAM REYES FERNANDEZ portador de la cédula de Identidad y Electoral No. 001-1807174-5 cuenta con vasta experiencia en nuestras soluciones para la producción de documentos de Identidad Nacional mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a la infraestructura de impresión de la República Dominicana.

Firmado:

Nombre: Joshua M. Mármol
Posición: PRESIDENTE

G.E.T. Secure ID Corp.
Established 2013; Delaware, USA

Debidamente autorizado para firmar esta Autorización en nombre de: G.E.T. Secure ID Corp

Fecha de fecha: [21] de Junio, del año 2024

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 21 day of June, 2024, before me, the undersigned notary public, Joshua Marmol personally appeared, proved to me through satisfactory evidence of identification, which were USA passport, to be the person whose name is signed on the preceding or attached document in my presence.

Notary Public's Signature
My Commission Expires October 18, 2030

WILFREDO MARTINEZ
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
October 18, 2030

Calle Doctor Delgado
Esq. San Juan Bosco Edif.
DD-I APT 302, Gazcue

809-443-1667

reyes_harry@hotmail.com

HARRY WILLIAM REYES FERNANDEZ

FORMACION ACADEMICA

Licenciado en Informática
Universidad del Caribe Rep.
Dominicana

Técnico en Electrónica Mención Microprocesadores
Instituto Técnico Salesiano (ITESA) Rep.
Dominicana

Estudios Primarios
Colegio Don Bosco Rep.
Dominicana

FORMACIÓN COMPLEMENTARIA:

- **A+ It Essentials**, Instituto Tecnológico las Américas (ITLA)
- **Server+**, Instituto Tecnológico las Américas (ITLA)
- **CCNA**, Instituto Tecnológico las Américas (ITLA)
- **Security+**, Instituto Tecnológico las Américas (ITLA)
- **Color Theory 101**, Kyocera Corp.
- **Core Basic V3**, Ricoh learning Institute
- **Core Basic V5**, Ricoh learning Institute
- **Digital Color Basic CBT**, Ricoh learning Institute
- **Series Blended Learning**, Ricoh learning Institute
- **Fabricación y diseño de inversores**, ICTEC Fibras Ópticas
- **Seminario de Redes WAN**, Inforedes
- **Diseño de circuito impresos**, fundación dominico Japonesa
- **Especialist alphard**, Kyocera Corp.
- **M022 Series Self Pace Color MFP**, Ricoh learning Institute
- **D127 Series Self Pace**, Ricoh learning Institute
- **Digital Troubleshooting Concept**, Ricoh learning Institute
- **D124 color wide Format MFP**, Ricoh learning Institute
- **Printing Technologies V1.5**, Ricoh learning Institute
- **PRO C5100S/C5110S**, Ricoh learning Institute New Jersey
- **SP4510 Series Self Pace**, Ricoh learning Institute
- **D146 Series**, Ricoh learning Institute Orlando
- **PRO 8100S**, Ricoh learning Institute Puerto Rico

- **TOPPAN CP500,** GET GROUP
- **TOPPAN CL40,** GET GROUP

EXPERIENCIA PROFESIONAL

2004 - 2006	Soporte Técnico PC Factory & Services
2006 - 2007	Representante de Servicios Copy Solutions International
2007 - 2011	Supervisor de Servicios Copy Solutions International
2011 - 2011	Gerente de Servicios Kyodom
2011- 2015	Sub Gerente de Servicios Copy Solutions International
2016- Actual	Gerente de Servicio Tecnico Copy Solutions International

INFORMÁTICA:

- Ofimática nivel avanzado.
- Linux Nivel Intermedio.
- Mac OS Nivel Avanzado.

IDIOMAS:

Español: Nativo
Inglés: Hablado Avanzado,
Escrito Avanzado

OTROS DATOS DE INTERÉS:

Licencia de Conducir 02.

Vehículo propio. Disponibilidad para viajar.

The Commonwealth of Massachusetts

William Francis Galvin
Secretary of the Commonwealth

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC 101898852
Santo Domingo, R.D.

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *Country:* United States of America

This public document

2. *has been signed by:* Wilfredo Martinez
3. *acting in the capacity of:* Notary Public
4. *bears the seal/stamp of:* Wilfredo Martinez

whose commission expires on: October 18, 2030

Certified

5. *at:* Boston, Massachusetts
6. *the:* 25 June, 2024
7. *by:* the Secretary of the Commonwealth
8. *No.:* 2605555
9. *Seal/stamp:* ***Great Seal of the Commonwealth***

10. *Signature:*

William Francis Galvin
Secretary of the Commonwealth

prepared by NCorreia

G.E.T. Secure ID C
230 Third Avenue
Waltham, MA 0245
T: +1 (781) 902-8
F: +1 (781) 890-1
www.getgroup.c

GET GROUP

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101893152 Santo Domingo R.D.

21] de junio 2024

Para: Junta Central Electoral de la República Dominicana.
Referencia: JCE-CCC-LPI-2024-0001
Asunto: Carta de Certificación de Experiencia Personal Técnico a Nivel Nacional.

Estimados Sres.,

NOSOTROS, G.E.T. Secure ID Corp, (junto con sus filiales en el grupo de empresas GET, "GET Group") una compañía debidamente incorporada y existente bajo las leyes de Estados Unidos, oferente de la solución de personalización "GET CLM600", el software PKI "GET Trust", y el software de identificación móvil "GET mID" (conjuntamente, los "Productos),

POR LA PRESENTE CERTIFICAMOS que el SR. MARCOS NEFTALI TAVAREZ POLONIA portador de la cédula de Identidad y Electoral No. 223-0007382-6 cuenta con vasta experiencia en nuestras soluciones para la producción de documentos de Identidad Nacional mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a la infraestructura de impresión de la República Dominicana.

GET GROUP
G.E.T. Secure ID Corp.
Established 2013; Delaware, USA

Firmado:

Nombre: Joshua M. Mármol
Posición: PRESIDENTE

Debidamente autorizado para firmar esta Autorización en nombre de: G.E.T. Secure ID Corp

Fecha de fecha: [21] de Junio, del año 2024

WILFREDO MARTINEZ
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
October 18, 2030

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 21 day of June, 2024 before me, the undersigned notary public, Joshua Marmol personally appeared, proved to me through satisfactory evidence of identification, which were USA passport, to be the person whose name is signed on the preceding or attached document in my presence.

Notary Public's Signature
My Commission Expires October 18, 2030

MARCOS NEFTALI TAVAREZ POLONIA

CALLE 8 #24, EDIF JGS • TELS.:809-315-2791 • 809-414-6637

TEC. EN COMPUTADORA Y SISTEMAS

DATOS PERSONALES:

COPY SOLUTIONS INTERNATIONAL S.A. RNC: 101[illegible]052 Santo Domingo, R.D.

Nombres:
- Marcos Neftali.

Apellidos:
- Tavárez Polonia.

Cédula:
- 223-0007382-6

Fecha de Nacimiento:
- 19/Sept/1984

Estado Civil:
- Casado

Teléfonos:
- 809-315-2791; 809-414-6637.

OBJETIVO:

Desallorar e implementar mis conocimientos, para el buen desempeño en mis tareas o actividades. Llenar todas mis expectativas y las de la empresa, con la cual conseguiré un paso importante en mi superación personal, junto con el orgullo de ser parte de su equipo de trabajo.

FORMACION ACADEMICA:

Politecnico Fabio A. Mota • 3er y 4to de Bachiller.
- Técnico en Electrónica Básica y Digital.

Universidad Dominicana O&M•Octavo Cuatrimestre.
- Ingeniero en Sistemas.

Inst Dominico Americano • Cuarto Nivel.
- Inglés Básico.

Inst CENTU.
- Reparación de Computadora
- Digitación.

Direccion General de Aduanas.
- Proceso de despacho de importación en el sistema integral de Gestión Aduanera (SIGA).

OTROS CONOCIMIENTOS BASICOS:

Programación Básica.

- VB.NET
- Visual Basic.
- PHP/MySQL

Diseño Web Básico .

- XHTML.
- HTML

Diseño Gráfico.

- Corel Draw.
- Photoshop.
- Freehand.

EXPERIENCIA LABORAL:

POWER ONE

Técnico de Máquina Industrial • 2005 – 2007

- Reparación .
- Mantenimiento.
- Soporte Técnico.

IMPRESORA JUANA

Técnico de Computos • 2008 – 2011

- Soporte Técnico y Mantenimiento de Computadoras.

GRUPO RODRIGUEZ FERNANDEZ

Asistente de Cómputos • 2013-2014

- Digitación, Soporte Técnico y Mantenimiento de Computadoras.

GRUPO CSI

Servicio Técnico • 2014

- Técnico de Máquinas TOPPAN.
- Técnico de Impresoras M. RICOH

REFERENCIA PERSONAL:

- Ing Miguel Angel Ramos. Tel.: 809-918-4484
- Dr Dolores Linares. Tel.: 809-781-9759

The Commonwealth of Massachusetts

William Francis Galvin
Secretary of the Commonwealth

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 01898852
Santo Domingo, R.D.

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *Country:* United States of America

This public document

2. *has been signed by:* Wilfredo Martinez
3. *acting in the capacity of:* Notary Public
4. *bears the seal/stamp of:* Wilfredo Martinez

whose commission expires on: October 18, 2030

Certified

5. *at:* Boston, Massachusetts
6. *the:* 25 June, 2024
7. *by:* the Secretary of the Commonwealth
8. *No.:* 2605556
9. *Seal/stamp:* ***Great Seal of the Commonwealth***

10. *Signature:*

William Francis Galvin

William Francis Ga
Secretary of the Co

prepared by NCorreia

G.E.T. Secure
230 Third Ave
Waltham, MA
T: +1 (781) 90
F: +1 (781) 89
www.getgrou

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo, R.D.

[21] de junio 202

Para: Junta Central Electoral de la República Dominicana.
Referencia: JCE-CCC-LPI-2024-0001
Asunto: Carta de Certificación de Experiencia Personal Técnico a Nivel Nacional.

Estimados Sres.,

NOSOTROS, G.E.T. Secure ID Corp. (junto con sus filiales en el grupo de empresas GET, "GET Group") una compañía debidamente incorporada y existente bajo las leyes de Estados Unidos, oferente de la solución de personalización "GET CLM600", el software PKI "GET Trust", y el software de identificación móvil "GET mID" (conjuntamente, los "Productos),

POR LA PRESENTE CERTIFICAMOS que el SR. ESTANLIN ORTIZ NUÑEZ portador de la cédula de Identidad y Electoral No. 402-2436333-9 cuenta con vasta experiencia en nuestras soluciones para la producción de documentos de Identidad Nacional mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a la infraestructura de impresión de la República Dominicana.

Firmado:

GET GROUP
G.E.T. Secure ID Corp.
Established 2013; Delaware, USA

Nombre: Joshua M. Mármol
Posición: PRESIDENTE

Debidamente autorizado para firmar esta Autorización en nombre de: G.E.T. Secure ID Corp

Fecha de fecha: [21] de Junio, del año 2024

WILFREDO MARTINEZ
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
October 18, 2030

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 21 day of June, 2024 before me, the undersigned notary public, Joshua Marmol personally appeared, proved to me through satisfactory evidence of identification, which were USA passport, to be the person whose name is signed on the preceding or attached document in my presence.

Notary Public's Signature
My Commission Expires October 18, 2030

Estanlin Ortiz Núñez

Ingeniero de Sistemas y computación

DIRECCIÓN:
Vista Catalina, Calle 9, casa #10. La Romana

E-MAIL:
estanlin12@mail.com

TELÉFONO:
849-208-8726

EXPERIENCIA

Abril 2024 – Actualidad
Instructor técnico certificado – Copy Solutions International S.A.

Me desempeño como instructor técnico, siendo responsable de capacitar y certificar a todo el personal técnico de la empresa, y de supervisar específicamente al personal técnico de la zona este.

Octubre 2019 – Abril 2023
Técnico – Copy Solutions International S.A.

Desempeñé el puesto como técnico de servicio en las multifuncionales Ricoh en la zona este, con constante capacitación para brindar un mejor servicio.

Junio 2019 - Octubre 2019
Asistente de Monitoreo y Evaluación
Clínica de Familia La Romana

Realizando la recopilación de datos para general reportes para el Proyecto HS3.

Julio 2015 - Junio 2019
Administrador de bases de datos – Clínica de Familia La Romana

Monitoreando, editando y creando las bases de datos de la institución, realizando mantenimiento y encargado del área de digitación, digitando el historial clínico de cada

EDUCACIÓN

Universidad Dominicana O&M
INGENIERO DE SISTEMAS Y COMPUTACION

Ricoh Learning Institute (Programa Spire)
INSTRUCTOR TÉCNICO

Infotep
ELECTRICISTA INSTALADOR RESIDENCIAL

OBJETIVO

Mi objetivo es desempeñar y desarrollar de manera óptima mis capacidades aplicando los conocimientos adquiridos en mi formación académica y prácticas profesionales, para seguir desarrollándome profesionalmente para el buen desempeño de las funciones asignadas y así contribuir a los logros de los objetivos de la empresa.

HABILIDADES

- Trabajo en equipo
- Manejo de Office
- Buena comunicación
- Puntualidad y responsabilidad
- Capacidad de organización
- Adaptabilidad
- Ingles

REFERENCIAS

Dra. Adriana Tiburcio (Encargada de SAI)
Teléfono: 809-479-0001
Email: dra.tiburcioj@hotmail.com

Lic. Bernardo Rosario (Contralor General)
Teléfono:809-217-7217 y
809-875-7217
Email: bernardormartinez@hotmail.com

Harry Reyes (Gerente de servicios)
Teléfono:809-443-1667
Email: h.reyes@grupocsi.com.do

The Commonwealth of Massachusetts

William Francis Galvin
Secretary of the Commonwealth

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *Country:* United States of America

This public document

2. *has been signed by:* Wilfredo Martinez
3. *acting in the capacity of:* Notary Public
4. *bears the seal/stamp of:* Wilfredo Martinez

whose commission expires on: October 18, 2030

Certified

5. *at:* Boston, Massachusetts
6. *the:* 25 June, 2024
7. *by:* the Secretary of the Commonwealth
8. *No.:* 2605559
9. *Seal/stamp:* ***Great Seal of the Commonwealth***

10. *Signature:*

William Francis Galvin
Secretary of the C

prepared by MLam

G.E.T. Secure ID
230 Third Avenu
Waltham, MA 02
T: +1 (781) 902
F: +1 (781) 890
www.getgroup

21] de junio 202

Para: Junta Central Electoral de la República Dominicana.
Referencia: JCE-CCC-LPI-2024-0001
Asunto: Carta de Certificación de Experiencia Personal Técnico a Nivel Nacional.

Estimados Sres..

NOSOTROS, G.E.T. Secure ID Corp, (junto con sus filiales en el grupo de empresas GET, "GET Group") una compañía debidamente incorporada y existente bajo las leyes de Estados Unidos, oferente de la solución de personalización "GET CLM600", el software PKI "GET Trust", y el software de identificación móvil "GET mID" (conjuntamente, los "Productos),

POR LA PRESENTE CERTIFICAMOS que el SR. CRISTHIAN EZEQUIEL TINEO MARTINEZ portador de la cédula de Identidad y Electoral No. 031-0479653-1 cuenta con vasta experiencia en nuestras soluciones para la producción de documentos de Identidad Nacional mediante modelo descentralizado de impresión, ofreciendo servicios de instalación, soporte y mantenimiento a la infraestructura de impresión de la República Dominicana.

Firmado:

Nombre: Joshua M. Mármol
Posición: PRESIDENTE

G.E.T. Secure ID Corp.
Established 2013; Delaware, USA

Debidamente autorizado para firmar esta Autorización en nombre de: G.E.T. Secure ID Corp

Fecha de fecha: [21] de Junio, del año 2024

WILFREDO MARTINEZ
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
October 18, 2030

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 21 day of June, 2024 before me, the undersigned notary public, Joshua Marmol personally appeared, proved to me through satisfactory evidence of identification, which were USA passport, to be the person whose name is signed on the preceding or attached document in my presence.

Notary Public's Signature
My Commission Expires October 18, 2030

CRISTHIAN EZEQUIEL TINEO MARTINEZ

PERFIL

Técnico con 11 años de experiencia en reparación de equipos de impresión, con amplia trayectoria en servicios técnicos y sólida formación en electrónica. Certificado en AUTOCAD, MS PROTEC y en Equipo de impresión RICOH, actualmente en proceso de obtener título en Administración de Empresas.

Ademas me considero proactivo, responsable, respetuoso y con capacidad de autogestión, trabajo en equipo, así como facilidad de aprender de forma autodidacta.

CONTACTO

809-430-0489

Dirección: Calle Duarte, no.43,
El Higuerito, Moca.

Cristhian.tineo@hotmail.es

Licencia de Conducir:
Categoría 02.

ACTIVIDADES E INTERESES

Botanica
Cine
Carpintería
Viajes
Gastronomía

REFERENCIAS PERSONALES

-Carlos Santana
cel.: 829-883-5518
-Sonnia de león chalas
cel.: 809-902-7998

EXPERIENCIA LABORAL

C.S.I. | Técnico Nivel III
Noviembre 2013 - Actualidad (11 años 5 meses).
- Especialista en reparación y mantenimiento de equipos de impresión.
- Diagnóstico y solución de problemas técnicos complejos.
- Implementación de protocolos de servicio y mejora continua.

FORMACIÓN ACADÉMICA

- Estudiante de Administración de Empresas, Universidad Abierta Para Adultos (UAPA), En curso
-Técnico en Mecánica Automotriz, INFOTEP Centro Regional Norte
- Estudiante de Ingeniería Electrónica, UTESA
- Técnico en Electrónica Industrial, INFOTEP Centro Regional Norte
- Bachiller, Colegio UTESIANO

EXPERIENCIAS ANTERIORES

- Taller El Rubio | Mecánico (3 años)
- Tienda de Telefonía | Servicio al Cliente y Técnico de Reparación (2 años)

CARACTERÍSTICAS Y COMPETENCIAS CLAVE

- Reparación de equipos de impresión
- Servicio al cliente
- Diagnóstico técnico
- Manejo de herramientas especializadas
- Conocimientos en AUTOCAD
- Gestión de proyectos técnicos

CERTIFICACIONES

- AUTOCAD
- MS PROJET
-Seminario -Taller: Técnicas de relajación y manejo del estrés.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101828852 Santo Domingo, R.D.

Jon A. Donovan

Teléfono: 617-893-2470 (celular) Correo electrónico: jdonovan@getgroupna.com

OBJETIVO: Convertirse en una parte integral de una empresa de tecnología moderna que sea gratificante tanto personal como profesionalmente

EXPERIENCIA:

2016-2025 ***Gerente de Servicio al Cliente*** GETNA
(9 años)

- 6 años de experiencia como Gerente de Servicio al Cliente en el contrato actual del Proyecto de Pasaporte de Próxima Generación (NGPP)
- 9 años de experiencia en sistemas de impresión de pasaportes de la serie IAI Book Master
- Miembro contribuyente de 6 años del equipo de licitación GETNA NGPP RFP de 2013 a 2018
- Responsable de la supervisión y capacitación de los ingenieros de servicio para el Proyecto de Pasaporte de Próxima Generación (NGPP)
- Responsable de la coordinación de la implementación y el servicio posterior requerido por las agencias y centros de NGPP con un gran enfoque en el cumplimiento de los acuerdos de nivel de servicio (SLA) de NGPP
- Responsable de las notificaciones adecuadas a nuestro socio principal de NGPP y a los PM de GETNA
- Responsable de mantener las piezas/herramientas y suministros adecuados para los equipos de servicio de NGPP • Proporcionó cobertura del sitio NGPP y capacitación del operador en las implementaciones
- Responsable del establecimiento y la supervisión del servicio de asistencia de GETNA, la selección del software del portal y sus actividades
- Responsable de la contratación de nuevos ingenieros de servicio de GETNA
- Responsable de la coordinación de los ingenieros de servicio de GETNA en respuesta a las solicitudes de servicio de los clientes

2014-2016 ***Gerente de Servicios Técnicos/Ing. de Servicios*** GETGROUP (2 años)

- Responsable de establecer nuevas instalaciones del R&D y miembros del equipo
- Responsable como enlace entre la empresa matriz y los proveedores para el desarrollo de nuevos productos
- Garantizar el soporte de las solicitudes de servicio al cliente de GET y la correspondiente Administración de servicios del Proveedor
- Responsable de la contratación de ingenieros de laboratorio de GET para el desarrollo de nuevos productos

COPY SOLUTIONS INTERNATIONAL SA
RNC 101898852
Santo Domingo, R.D.

2012-2014 ***Técnico de investigación y desarrollo*** GETGROUP(2.5 años)

- Introducción a la serie IAI Book Master de impresoras de pasaportes
- Completamente capacitado en impresoras de tarjetas y pasaportes de identificación seguras de GET Group • Responsable de todo tipo de pruebas de impresión de tarjetas, pasaportes y los materiales, tintas y películas seguros utilizados en el proceso de impresión
- Responsable de crear, diseñar, probar e implementar nuevas características en las líneas de productos de la empresa para obtener ventajas de participación de mercado sobre los competidores
- Interactúa diariamente con los proveedores, la gestión de desarrollo de productos y las ventas para respaldar las nuevas características del producto y capacitar cuando sea necesario
- Viaje hasta el 25% para visitar proveedores y socios (extranjeros y nacionales) • Asistir, organizar y apoyar ferias comerciales que exhiban nuestras líneas de productos
- Soporte a la línea directa de la mesa de servicio interna en un rol de respaldo para el Departamento de Servicios Técnicos.

2009-2012 ***Técnico de servicio de campo*** NBM Inc.
(3 años)

- Capacitado en una amplia gama de impresoras, faxes y escáneres Sharp y HP • Enlace de servicio/ventas para el equipo de Servicios Gestionados de Impresión de la Cuenta Principal
- Realizar todas las tareas asociadas con 20+ años de experiencia en Field Service

2006-2009 ***Servicio de Atención al Cliente/Técnico de Atención al Cliente*** EMC Corp.
(3 años)

- Proporciona soporte no técnico de front-end para clientes internos y externos de EMC mientras crea, investiga y actualiza las solicitudes de servicio
- Implemente procedimientos de escalamiento e interactúe con los equipos de EMC global

2007-2008 ***Asociado de Xerox DocuCare en el lugar*** EMC Corp.
(2 años)

- Técnico in situ responsable de la resolución de problemas y el mantenimiento preventivo de todos los equipos de impresión en los centros de fabricación de EMC
- Responsable de los problemas de conectividad, instalaciones, mudanzas, reposición de suministros y capacitación al cliente de toda la línea de productos

2004-2007 ***Inversionista Inmobiliario Independiente***
(3 años)

1992-2004 ***Ingeniero Sr. de Servicio al Cliente III*** Xerox Corp.
(12 años)

- Técnico de campo para impresoras láser a color de alto volumen/conectadas a la red de Xerox ubicadas en entornos de producción de ritmo rápido
- Valioso miembro del equipo que asumió problemas complejos de campo, como el gasto de piezas y los excesos de uso, utilizando técnicas de resolución de problemas con miembros del grupo de trabajo y soporte de ingeniería
- Mentoría y capacitación de nuevos CSE de campo para que se asimilen a las prácticas y técnicas de campo de Xerox

1985-1992 ***Ingeniero de Servicio al Cliente I y II*** Xerox Corp.
(7 años)

- Capacitado en una amplia gama de impresoras de escritorio, faxes y escáneres Xerox • Entrenado en computadoras de escritorio y portátiles fabricadas por Dell, Compaq y HP
- Gestión de grandes territorios de equipos en pequeños grupos de trabajo en MA&NH • Responsable de los inventarios de piezas de la máquina, administración del coche de la empresa, suministros y ventas por contrato, mantenimiento de computadoras portátiles e ingreso de datos de facturación con un fuerte enfoque en la satisfacción del cliente

EDUCACIÓN:

- 27 años de formación corporativa continua en los campos de reparación de impresoras (tanto monocromáticas como en color) y PC, instalación y resolución de problemas de software, resolución de problemas de red de dispositivos conectados, productos MS-DOS, MS Windows y MS Office, así como innumerables paquetes de software propietarios.
- 2 años de cursos en UNH, Durham NH en Ciencias Físicas y Bio
- Graduado de 4 años (los más altos honores) de Burlington HS, Burlington, MA

REFERENCIAS: Amueblada según sea necesario

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101036852
Santo Domingo, R.D.

Arnie Pérez Rivera

Teléfono: (787) 450-3939
arnie_perez@yahoo.com

Objetivo: Ser miembro de una organización donde pueda aportar mis habilidades y experiencia en cualquier puesto disponible para contribuir a las metas y objetivos de la empresa.

Educación Profesional:

1998 – 2001 Universidad Interamericana de Puerto Rico Aguadilla, P.R. BS en Tecnología de Ingeniería Electrónica, Cum Laude

1994 - 1997 Universidad de Puerto Rico Aguadilla, P.R.
Grado Asociado en Tecnología Electrónica

Habilidades:
Liderazgo fuerte y habilidades interpersonales con experiencia práctica sustancial en el conocimiento de las leyes federales, estatales, y extranjeras, reglamentos, reglas, procesos y prácticas comerciales. Capacidad para comunicarse eficazmente con todos los niveles y el personal. Fuertes habilidades electromecánicas y de automatización. Capacidad para leer y comprender diagramas esquemáticos y ser competente en el desmontaje y montaje de dispositivos electromecánicos complejos. Experiencia de viajar fuera del país para trabajos de servicio en el sitio. Realizar reparaciones, calibraciones, instalaciones, resolución de problemas y mantenimiento preventivo de equipos electrónicos. Buenas habilidades escritas, orales y de presentación, incluida la documentación en un entorno regulado. Conocimientos en Dispositivos Médicos, FDA, OSHA, LOTO, SOP, GMP y normas ISO. Dominio firme de los siguientes sistemas operativos Microsoft: Windows, Excel, Word, Power Point, Oracle, SAGE, Maximo, SAP, Midas y sistemas SCADA. Experiencia con instrumentos analíticos y herramientas de mejora de procesos. Conocimientos en el diagnóstico, aislamiento, corrección de fallos de funcionamiento y realización de mantenimiento a nivel organizativo de los equipos electrónicos. Experiencia en mantenimiento de equipos electrónicos, sistemas informáticos y sistemas de seguridad. Actualmente ocupa un puesto con autorización del gobierno de los EE. UU.

Idiomas: Bilingüe (español e inglés)

Experiencia Profesional:

2022 - Actualidad GET Group North America - Global Enterprise Technologies Corp.
Ingenieros de Servicio de Campo (FSE) - Oficina de San Juan

- Instalar, mantener y respaldar todos los esfuerzos de mantenimiento del sistema, de conformidad con los requisitos del Acuerdo de Nivel de Servicio (SLA) del cliente.

- Responder de manera oportuna a todas las llamadas de mantenimiento. Documentar cada acción de mantenimiento con el tiempo, la mano de obra, los medidores, las notas de resolución y las piezas utilizadas.
- Mantener un inventario preciso de servicios in situ en las instalaciones asignadas.
- Ayudar a los operadores y administradores del sistema a solucionar los problemas que encuentren al usar nuestros sistemas y proporcionar pasos prácticos para resolver problemas.
- Maximizar el uso de hardware y software mediante la capacitación de los usuarios; interpretación instrucciones; responder preguntas; Proporcionar retroalimentación.
- Aportar ideas para mejorar las instrucciones de funcionamiento que deben utilizar los usuarios finales, colaborando en un entorno de grupo de trabajo.
- Mantienee el conocimiento profesional y técnico asistiendo a talleres educativos; revisión de publicaciones profesionales; el establecimiento de redes personales; Participación en sociedades profesionales.
- Realizar la resolución de problemas, el mantenimiento preventivo, la reparación, la modificación y instalación de equipos electromecánicos del Departamento de Estado de los EE. UU.
- Otras asignaciones solicitadas por la Dirección.

2018 - 2021 AM Técnico

Ingeniero de servicio de campo

- Realizar la resolución de problemas del servicio en el sitio, el mantenimiento preventivo, la reparación y la instalación de unidades de liofilizadores, equipos analíticos y de dispositivos médicos.
- Realizar reparación y mantenimiento de equipos electrónicos y electromecánicos.
- Realizar reparación y mantenimiento de sistemas hidráulicos, enfriadores, compresores de refrigeración, válvulas, bombas, calentadores, cámaras térmicas, sensores, sistemas de visión.
- Capacidad para trabajar por mi cuenta con supervisión mínima con electrónica Esquemas, equipos de prueba, herramientas para equipos electrónicos y electromecánicos.
- Realizar viajes complementarios a otros territorios.
- Mantener y administrar todos los activos asignados de la empresa: herramientas, automóviles de la empresa, inventario de piezas, teléfono celular, tarjeta de crédito, computadora y accesorios.

2007- 2018 Integra CI, Inc. P.R.

Técnico de E&I

- Coordine el trabajo con los compañeros de trabajo para realizar las tareas de instalación, mantenimiento y reparación. Desarrollar soluciones que identifiquen el equipo o el método para hacer frente a los problemas del producto o de la producción en el día a día.

- A cargo del inventario de repuestos, equipos automatizados para dispositivos médicos
preparación. Solicitud de cotizaciones de repuestos y buscador de nuevos proveedores, que permiten a Integra ser más competitivos en los precios de nuestros proveedores.
- Ser responsable de programar y realizar el mantenimiento periódico, la instalación, la reparación de dispositivos médicos y equipos de laboratorio analíticos.
- Realizar reparación y mantenimiento de Unidades de Liofilizadores, sistemas hidráulicos, enfriadores, compresores de refrigeración, compresores de aire, válvulas, bombas, calentadores, cámaras térmicas, generadores de vapor, sistemas de tratamiento de agua purificada (Millipore/Meco), máquinas selladoras (Multivac), sensores, sistemas de visión, etc.
- Experiencia en automatización de sistemas de control y procesos de moldeo por inyección.
- Mantener y administrar todos los activos asignados de la compañía que pueden incluir, pero no se limitan a: herramientas, automóviles de la compañía, inventario de piezas, computadora y accesorios.
- Buen conocimiento de trabajo en PLC, máquinas de embalaje, escáneres, transportadores, servomotores, VFD, AC / DC y equipos de CA trifásicos.
- Experiencia con instrumentos analíticos: Multimetro digital, Osciloscopio, etc.
- Llevar a cabo análisis de causa raiz que conduzcan a una resolución eficaz de problemas.

1996 - 2007 Hewlett Packard, P.R.
Técnico de Mantenimiento y Reparación

- Equipos de montaje, resolución de problemas, sistemas de visión y dispensación, configuración/calibración. Actividades realizadas de reparación y mantenimiento asociadas con el equipo y el cartucho y las líneas de fabricación. Experiencia de sala limpia.
- Ayudar a los ingenieros en el personal, incluida la toma de proyectos de mejora,
el apoyo a los proyectos existentes, y la recopilación y el análisis de datos.
- Interactuar con los proveedores de Compras, Ingeniería, Producción, Instalaciones y Mantenimiento para coordinar reparaciones, mejoras e instalaciones en equipos críticos y especializados.
- Experiencia en el área de reparación y análisis de piezas. Análisis de piezas realizado para
Mejore la calidad, la producción, la reducción de costos y el rendimiento.
- Realiza y documenta pruebas funcionales operativas, resolución de problemas y depuración de componentes, subconjuntos, materiales y sistemas de fabricación para aislar fallas y determinar el remedio para el mal funcionamiento.

- Realiza pruebas y auditorias de procesos/productos para verificar la conformidad con la calidad y/o requisitos reglamentarios.
- Experiencia en la modernización de capacidades de máquinas para mejorar el rendimiento y aumentar la productividad, proyectos de ingenieria, compra e instalación de equipos de automatización y nuevas lineas de productos de fabricación.

Mayores logros:

- Instalación, SAT y Puesta en Marcha de Equipos del Cliente en las instalaciones del cliente.
- Instalación y puesta en marcha del sistema de producción de agua Millipore y MECO.
- Instalación y puesta en marcha de la máquina de cámara térmica de reticulación.
- Unidad de liofilizadores de casco FAT en las instalaciones de SP Industries en las instalaciones del cliente.
- Compra, instalación y puesta en marcha de la unidad de liofilizadores de casco en la ubicación del cliente,
- Instalación y puesta en marcha en la ubicación de múltiples clientes
- Instalación y puesta en marcha de la máquina de envasado Multivac R240 en las instalaciones del cliente.

Referencias disponibles bajo petición

OSCAR D. REYES

5744 Camino de Saplin
El Paso, Texas 79932

Celular: (915) 256-4678
oscrey_1@yahoo.com

RESUMEN DE CALIFICACIONES

Ingeniero eléctrico proactivo y centrado en la calidad con experiencia en diseño, pruebas, análisis y coordinación de proyectos. Experto en ingeniería de software, diseño de sistemas digitales, circuitos eléctricos, programación y documentación. Posee habilidades de calidad para la resolución de problemas, analítica y de toma de decisiones para lograr soluciones desafiantes, prácticas y rentables.

IDIOMAS

Español
Inglés

COMPETENCIAS BÁSICAS

- ☑ Ingeniería eléctrica
- ☑ Ingeniería de Software
- ☑ Gestión de proyectos
- ☑ Diseño de sistemas digitales
- ☑ Mejora de la calidad
- ☑ Circuitos eléctricos
- ☑ Desarrollo de programas
- ☑ Documentación
- ☑ Relaciones con los clientes

DESCRIPCIÓN GENERAL DEL CONJUNTO DE HABILIDADES TÉCNICAS

Programación: Jes, C, Java, Python, Assembly
Software: MATLAB, Quartus II, Xilinx, Cadence, SimuAid, Microsoft Office, Multisim, FracPro, Ecostruxure, Maintenance Connection.

EDUCACIÓN

Licenciatura en Ciencias en Ingeniería Eléctrica
Enfoque en Ingeniería Informática Universidad
de Texas en El Paso, El Paso, Texas

EXPERIENCIA PROFESIONAL

GLOBAL ENTERPRISE TECHNOLOGIES (GET GROUP NA) **07/2022-**
Actualidad
SERVICE ENGINEER I **El Paso, Texas**

- Instalación, mantenimiento, servicio, reparación y supervisión la funcionalidad de la maquinaria y la producción en el sitio.
- Asistencia a operadores de máquinas y administradores de sistemas respondiendo a los problemas encontrados durante la producción de manera oportuna para cumplir con los acuerdos de nivel de servicio.
- Mantenimiento de rutina realizado para garantizar condiciones de trabajo eficientes y duraderas de la máquina.
- Contribuciones:
  - Creación de informes detallados a través de la conexión de mantenimiento para registrar problemas, realizar un seguimiento de las piezas y los tiempos de finalización.
  - Análisis de causa raíz realizado para restaurar la funcionalidad y maximizar la productividad.
  - Se comunicó y colaboró con los miembros del equipo y los clientes para mantener una satisfacción excepcional del servicio al cliente.

SCHNEIDER ELECTRIC 09/2020 – 07/2022
QUALITY TESTER II El Paso, Texas

- Solución de incidentes, reparaciones, y pruebas en el tablero de distribución eléctrica de alta tensión y en el equipo de conmutación
- Interpretación de diagramas eléctricos, planos complejos, diagramas de cableado, diagramas unifilares, y lista de materiales.
- Aplicación de carros de inyección de voltaje y corriente, probadores dieléctricos de alta potencia y multímetros para probar la funcionalidad de transformadores, fallas a tierra, dispositivos de protección contra sobretensiones, unidades UPS y unidades de tierra de alta resistencia.

Contribuciones:

- Se utilizaron programas como Ecostruxure para configurar los protocolos Modbus y TCP/IP para los módulos de comunicación.
- Se comunicó y colaboró frecuentemente con los miembros del equipo de diferentes departamentos para resolver problemas de manera rápida y eficaz para cumplir con las metas mensuales de la planta.

CUDD ENERGY SERVICES 05/2019 – 04/2020
FIELD ENGINEER I Odessa, Texas

- Preparación de documentos y hojas de cálculo para trabajos individuales de fracking según las necesidades del cliente.
- Supervisión de todas las operaciones calculando y rastreando la arena y las cantidades de químicos utilizadas.
- Desarrollo de habilidades sólidas de priorización y multitarea al manejar con eficacia numerosas tareas requeridas por operaciones de ritmo rápido.

Contribuciones:

- Creación de informes detallados y facturas tanto para el cliente como para CUDD a través del análisis de FracPro y las aplicaciones de Microsoft Office.
- Comunicación con los proveedores, los compañeros de equipo, la gerencia, y el cliente para cumplir con los plazos y minimizar el NPT.

CUDD ENERGY SERVICES 03/2017 – 03/2019
ELECTRONIC TECHNICIAN Odessa, Texas

- Responsable de pruebas, solución de incidentes, reparación, y del mantenimiento de todo el equipo utilizado en el sitio de trabajo.
- Planificación y diseño de materiales basados en las necesidades específicas del cliente.
- Conocimiento y cumplimiento de las reglas y procedimientos de seguridad basados en la política de CUDD.

Contribuciones:

- Conocimiento obtenido de las operaciones del campo petrolífero mediante el mantenimiento de los sistemas de control para el equipo de fracturación.
- Sistemas de cómputo gestionados en todos los equipos de fracturación para garantizar la funcionalidad adecuada.

NATIONAL INSTITUTE FOR OCCUPATIONAL SAFETY AND HEALTHOCUPACIONAL (NIOSH)
08/2011 ELECTRICAL ENGINEER SUMMER INTERN 06/2011 – Pittsburgh, PA

- Asistir Ingenieros profesionales a experimentar métodos prácticos en la resolución de problemas.
- Investigación de componentes electrónicos para su uso posterior en la construcción de prototipos para lámparas de gorra de minero.

Contribuciones:

- Colaboración a equipos de ingenieros dentro de una mina de investigación para investigar

métodos para la mejora de las líneas de transmisión subterráneas.

- Preparación y conducción de experimentos tanto la trituración como la perforación de las baterías, las pruebas para la seguridad contra incendios.
- Asistir en el diseño de un experimento controlado que trata con la visibilidad dentro de una mina llena de humo; realización de pruebas de funcionamiento, recopilación de resultados y prepatración datos para su análisis.

CONSOLIDADO DE LAS EXPERIENCIAS DEL CONSORCIO

I. **Suministro de impresoras de documentos de identidad de policarbonato electrónicos, instalación y mantenimiento.**

Experiencia 1 (Requerimiento):
G.E.T ENTERPRISE TECHNOLOGIES CORP.
Proyecto de Pasaporte de los Estados Unidos de Norteamérica.

Experiencia 2 (Criterio para obtención de 3 puntos):
G.E.T INTERNATIONAL FZCO.
Proyecto de Documento Nacional de Identidad Surinam.

II. **Suministro de tarjetas de identidad electrónicas de policarbonato.**

Experiencia 1 (Requerimiento):
SELP S.A.S
Proyecto de Suministro de Tarjetas de Identificación Republica de Chad.

Experiencia 2 (Criterio para obtención de 3 puntos):
SELP S.A.S
Proyecto de Suministro de Tarjetas Inteligentes con Chip de Republica de Pakistán.

Experiencia 3 (Criterio para obtención de 3 puntos):
SELP S.A.S
Proyecto de Suministro de Licencias de Conducir Electrónicas del Gobierno de Nepal.

III. **Proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos.**

Experiencia 1 (Requerimiento):
G.E.T INTERNATIONAL FZCO
Proyecto de Identificación Fronteriza en China.

Experiencia 2 (Criterio para obtención de 2 puntos):
G.E.T INTERNATIONAL FZCO.
Proyecto de Licencias de Conducir en Egipto.

Experiencia 3 (Criterio para obtención de 3 puntos):
SELP S.A.S
Proyecto de Transición de las Naciones Unidas para el desarrollo de Malawi.

IV. Proyecto de Integración de sistemas en un proyecto de identificación electrónica.

Experiencia 1 (Requerimiento):
G.E.T INTERNATIONAL FZCO.
Proyecto de Identificación Fronteriza en China.

Experiencia 2:
G.E.T INTERNATIONAL FZCO.
Proyecto de Licencias de Conducir en Egipto.

Acreditación de las Experiencias Obligatorias

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101038652
Santo Domingo, R.D.

The Commonwealth of Massachusetts
William Francis Galvin - Secretary of the Commonwealth

Apostille

(Convention de la Haye du 5 Octobre 1961)

1. Country: United States Of America

This Public Document

2. Has been signed by: Caitlyn E. Burns

3. Acting in the capacity of: Notary Public

4. Bears the seal/stamp of: Caitlyn E. Burns

Whose commission expires on: 12/29/2028

Certified

5. At: Boston, Massachusetts 6. The: February 21, 2025

7. By: The Secretary of Commonwealth

8. No.: 2680964

9. Seal/Stamp: *(Great Seal of the Com*

10. Signature:

William Francis Galvin
Secretary of the Commonwealth

Prepared By: **DCooper**

Global Enterprise Tech
230 Second Ave., Waltham,
T: +1 781 890 6700
www.getgroupna.com

Junta Electoral Central ("JCE")

Whosoever undersigned, **Mr. Alexander Kambanis**, of the USA, of legal age, married, bearer of USA Passport No. 570930520, domiciled and resident in Waltham, MA USA, acting in the name and representation of **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**, a commercial company organized and existing in accordance with the laws of the State of Delaware, USA, with Tax Identification Number 04-3254957, and registered office in 230 Second Avenue, Waltham, MA 02451 USA, in accordance with the Powers granted to me by the Board of Directors of the company, in my capacity as PRESIDENT of the same,

Quien suscribe, **Sr. Alexander Kambanis**, de EE.UU., mayor de edad, casado, titular del Pasaporte de EE.UU. nº 570930520, domiciliado y residente en Waltham, MA EE.UU., actuando en nombre y representación de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**, sociedad mercantil constituida y existente de conformidad con las leyes del Estado de Delaware, EE.UU., con Identificación Fiscal Número 04-3254957, y domicilio social en 230 Second Avenue, Waltham, MA 02451 EE.UU., en virtud de los Poderes que me han sido otorgados por la Junta Directiva de la compañía, en mi calidad de PRESIDENTE de la misma,

On **January 17, 2025**, by means of this document, and in response to the requirements of the International Public Bidding, Ref.: **JCE-CCC-LPI-2024- 0001**, I DECLARE **UNDER THE MOST SOLEMN FAITH OF THE OATH,** the following:

En fecha 17 de enero de 2025, por medio del presente documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024- 0001**, declaro **BAJO LA MAS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

A. That **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**'s experience with the passport project of the United States of America satisfies the following requirements for the tender, as modified by the Questions and Answers provided by the JCE and summarized in the Matrix:

   Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** en el proyecto de pasaportes de los Estados Unidos de América satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

3.1.6.2 (a) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.1

Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo el suministro de impresoras de documentos de identidad de policarbonato electrónicos, incluyendo la instalación y el mantenimiento. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública.

Y

5.4.5 Plantilla para Evaluación – Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

Al menos dos (2) experiencias en dos proyectos, de clientes y países distintos, en el cual el oferente haya llevado a cabo el suministro de impresoras, la instalación, las pruebas, la puesta en servicio y el mantenimiento de un sistema de documentos de identidad electrónicas de policarbonato distribuidas, con impresoras láser en los últimos cinco (5) años, a nivel de gobierno: 3 puntos.

B. That **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**'s experience with the passport project in the United States of America can be validated using the following data:

Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de pasaporte en los Estados Unidos de América puede ser validada utilizando los siguientes datos:

Name of Public Institution / Agencia Gubernamental: United States Department of State
Physical address / Dirección física: 2201 C Street N.W., Washington D.C. 20520 USA
Electronic address / Dirección electrónica: https://www.state.gov/
Name of the contact / Nombre de contacto: Michelle Wilson
Title of the contact / Cargo de contacto: Counselor – TSA
Telephone number / Teléfono: +1 (571) 227-5705
Email address / Correo electrónico: michelle.wilson@tsa.dhs.gov

C. That **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**'s experience with the mobile driver's license project in the State of Utah, USA satisfies the following requirements for the tender, as modified by the Questions and Answers provided by the JCE and summarized in the Matrix:

Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de licencia de conducir móvil en el Estado de Utah, EE.UU. satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

3.1.6.3 (a)- Requisitos de experiencia (no obligatorios)
MATRIZ 3.3.1

Más de una (1) experiencia, en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Al menos una de las referencias debe ser ISO 18013-5.

Y

5.4.5-Plantilla para Evaluación
MATRIZ SECCIÓN AUTO-EVALUACIÓN

(i) "Plan del proyecto" -El proveedor presenta la implementación, de por lo menos, un desarrollo de una solución, puesta en producción, de cédula digital, en una institución pública, de acuerdo a los requerimientos establecidos en el documento de especificaciones técnicas, y estar adheridas al estándar ISO 18013-5: 4 puntos.

(ii) "Experiencia" (acreditable con contratos celebrados con empresas miembros de un mismo grupo económico (empresas con accionistas en común) de los consorciados en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

- 1 contratos: 1 punto.
- 2 contratos: 2 puntos.
- Más de 2 contratos: 3 puntos.

D. That **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**'s experience with the mobile driver's license project in the State of Utah, USA can be validated using the following data:

3.1.6.2 (a) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.1

Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo el suministro de impresoras de documentos de identidad de policarbonato electrónicos, incluyendo la instalación y el mantenimiento. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública.

Y

5.4.5 Plantilla para Evaluación – Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

Al menos dos (2) experiencias en dos proyectos, de clientes y países distintos, en el cual el oferente haya llevado a cabo el suministro de impresoras, la instalación, las pruebas, la puesta en servicio y el mantenimiento de un sistema de documentos de identidad electrónicas de policarbonato distribuidas, con impresoras láser en los últimos cinco (5) años, a nivel de gobierno: 3 puntos.

B. That **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**'s experience with the passport project in the United States of America can be validated using the following data:

Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de pasaporte en los Estados Unidos de América puede ser validada utilizando los siguientes datos:

Name of Public Institution / Agencia Gubernamental: United States Department of State
Physical address / Dirección fisica: 2201 C Street N.W., Washington D.C. 20520 USA
Electronic address / Dirección electrónica: https://www.state.gov/
Name of the contact / Nombre de contacto: Michelle Wilson
Title of the contact / Cargo de contacto: Counselor – TSA
Telephone number / Teléfono: +1 (571) 227-5705
Email address / Correo electrónico: michelle.wilson@tsa.dhs.gov

C. That **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**'s experience with the mobile driver's license project in the State of Utah, USA satisfies the following requirements for the tender, as modified by the Questions and Answers provided by the JCE and summarized in the Matrix:

Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de licencia de conducir móvil en el Estado de Utah, EE.UU. satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

3.1.6.3 (a)- Requisitos de experiencia (no obligatorios)
MATRIZ 3.3.1

Más de una (1) experiencia, en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Al menos una de las referencias debe ser ISO 18013-5.

Y

5.4.5-Plantilla para Evaluación
MATRIZ SECCIÓN AUTO-EVALUACIÓN

(i) "Plan del proyecto" -El proveedor presenta la implementación, de por lo menos, un desarrollo de una solución, puesta en producción, de cédula digital, en una institución pública, de acuerdo a los requerimientos establecidos en el documento de especificaciones técnicas, y estar adheridas al estándar ISO 18013-5: 4 puntos.

(ii) "Experiencia" (acreditable con contratos celebrados con empresas miembros de un mismo grupo económico (empresas con accionistas en común) de los consorciados en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

- 1 contratos: 1 punto.
- 2 contratos: 2 puntos.
- Más de 2 contratos: 3 puntos.

D. That **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**'s experience with the mobile driver's license project in the State of Utah, USA can be validated using the following data:

Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de licencia de conducir móvil en el Estado de Utah, EE.UU. puede ser validada con los siguientes datos:

Name of Public Institution / Agencia Gubernamental: State of Utah Department of Public Safety – Driver License Division
Physical address / Dirección física: Driver's License Division, P.O. Box 144501, Salt Lake City, Utah, 84114-4501 USA
Electronic address / Dirección Electronica: https://dld.utah.gov/
Name of the contact / Nombre de contacto: Christopher Caras
Title of the contact / Cargo de contacto: Director
Telephone number / Teléfono: +1 801 965 4793
Email address / Correo electrónico: ccaras@utah.gov

[signature page to follow / firma en la página que continúa]

This Affidavit has been made in the City of Waltham, MA USA, on the 17th day of the month of January of the year 2025.

Esta Declaración Jurada ha sido hecha en la Ciudad de Waltham, MA USA, el día 17 del mes de enero del año 2025.

Alexander Kambanis

GLOBAL ENTERPRISE TECHNOLOGIES CORP.

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 17 day of January, 2025 before me, the undersigned notary public, Alexander Kambanis personally appeared, proved to me through satisfactory evidence of identification, which were USA passport, to be the person who signed the preceding or attached document in my presence and who swore or affirmed to me that the contents of the document are truthful and accurate to the best of (his) (her) knowledge and belief.

Caitlyn E. Burns
Notary Public's Signature My Commission Expires December 29, 2028

CAITLYN E. BURNS
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
December 29, 2028

TRADUCCIÓN OFICIAL: Experiencias aportadas por G.E.T ENTERPRISE TECHNOLOGIES CORP.

Yo, Licenciado Luis Eduardo Aquino Rivero, Intérprete Judicial debidamente investido para este fin en virtud de la Resolución No. 13/2014 del Consejo del Poder Judicial, de fecha ocho (8) del mes de diciembre del año dos mil catorce (2014), CERTIFICO que lo presente es una traducción fiel y conforme al documento originalmente instrumentado en idioma inglés y cuya versión en español de conformidad con mi mejor entendimiento se lee como sigue: I, Luis Eduardo Aquino Rivero, licensed Judicial Interpreter duly invested for this purpose by virtue of Resolution No. 13/2014 of the Council of the Judicial Power, dated December eight (8) of the year two thousand fourteen (2014), CERTIFY that this is a faithful translation and in accordance with the document originally instrumented in the English language and whose version in Spanish, according to my best understanding, reads as follows:

Global Enterprises Technologies Corp.
230 Second Ave. Waltham, MA 02451 USA
T: +1 781 810 4200
www.getgroup.com

CORPORACIONES GLOBALES, S.A.
RNC: 101038652
Santo Domingo, R.D.

[Seal GET GROUP]

Junta Electoral Central ("JCE")

Quien suscribe, **Sr. Alexander Kambanis**, de los EE.UU., mayor de edad, casado, portador del Pasaporte de los EE.UU. No. 570930520, domiciliado y residente en Waltham, MA USA, actuando en nombre y representación de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.**, una sociedad comercial organizada y existente de conformidad con las leyes del Estado de Delaware, EE.UU., con Número de Identificación Fiscal 04-3254957, y oficina registrada en 230 Second Avenue, Waltham, MA 02451 EE.UU., de conformidad con los Poderes que me otorga la Junta Directiva de la compañía, en mi calidad de PRESIDENTE de la misma,

El **17 de enero de 2025**, por medio de este documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024-001**, DECLARO **BAJO LA MÁS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

A. Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de pasaporte de los Estados Unidos de América satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por la JCE y resumidas en la Matriz:

3.1.6.2 (a) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.1

Al menos una (1) experiencia en un proyecto, en el cual el diferente haya llevado a cabo el suministro de impresoras de documentos de identidad de policarbonato electrónicos, incluyendo la instalación y el mantenimiento. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública.

Y

5.4.5 Plantilla para Evaluación – Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

Al menos dos (2) experiencias en dos proyectos, de clientes y países distintos, en el cual el oferente haya llevado a cabo el suministro de impresoras, la instalación, las pruebas, la puesta en servicio y el mantenimiento de un sistema de documentos de identidad electrónicos de policarbonato distribuidos, con impresoras láser en los últimos cinco (5) años, a nivel de gobierno: 3 puntos.

B. Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de pasaporte en los Estados Unidos de América puede ser validada utilizando los siguientes datos:

Nombre de Institución Pública: Departamento de Estado de los Estados Unidos
Dirección física: 2201 Calle C N.W., Washington D.C. 20520 USA
Dirección electrónica: https://www.state.gov/
Nombre del contacto: Michelle Wilson
Cargo del contacto: Asesor – TSA
Número de teléfono: +1 (571) 227-5705
Dirección de correo electrónico: michelle.wilson@tsa.dhs.gov

C. Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de licencia de conducir móvil en el Estado de Utah, EE. UU. satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por la JCE y resumidas en la Matriz:

INTÉRPRETE JUDICIAL
PODER JUDICIAL
REPÚBLICA DOMINICANA
LUIS EDUARDO AQUINO RIVERO
Código: 27950

3.1.6.3 (a)- Requisitos de experiencia (no obligatorios)
MATRIZ 3.3.1

Más de una (1) experiencia, en distintos clientes y países, en cédulas digitales o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Al menos una de las referencias debe ser ISO 18013-5.

Y

5.4.5-Plantilla para Evaluación
MATRIZ SECCIÓN AUTO-EVALUACIÓN

(i) "Plan del proyecto" -El proveedor presenta la implementación, de por lo menos, un desarrollo de una solución, puesta en producción, de cédula digital, en una institución pública, de acuerdo a los requerimientos establecidos en el documento de especificaciones técnicas, y estar adheridas al estándar ISO 18013-5: 4 puntos.

(ii) "Experiencia" (acreditable con contratos celebrados con empresas miembros de un mismo grupo económico (empresas con accionistas en común) de los consorciados en distintos clientes y países, en cédulas digitales o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de la presentación.

- 1 contrato: 1 punto.
- 2 contratos: 2 puntos: 3 puntos.
- Más de 2 contratos: 3 puntos.

D. Que la experiencia de **GLOBAL ENTERPRISE TECHNOLOGIES CORP.** con el proyecto de licencia de conducir móvil en el Estado de Utah, EE.UU. se puede validar utilizando los siguientes datos:

Nombre de Institución Pública: Estado de Utah Departamento de Seguridad Pública – División de Licencia de Conducir
Dirección física: División de Licencia de Conducir, P.O> Box 144501, Salt Lake City, Utah, 84114-4501 EE.UU.
Dirección electrónica: https://dld.utah.gov/
Nombre del contacto: Christopher Caras
Cargo del contacto: Director
Número de teléfono: +1 801 965 4793
Dirección de correo electrónico: ccaras@utah.gov

[firma en la página siguiente]

INTERPRETE JUDICIAL
PODER JUDICIAL
LUIS EDUARDO AQUINO RIVERO
Código: 27959

Esta Declaración Jurada ha sido realizada en la Ciudad de Waltham, MA EE.UU., el día 17 del mes de enero del año 2025.

[Firma ilegible]
Alexander Kambanis

GLOBAL ENTERPRISE TECHNOLOGIES CORP. [Sello Corporativo Global Enterprises Technologies Corp.]

MANCOMUNIDAD DE MASSACHUSETTS
CONDADO DE Middlesex

En este día 17 de enero, 2025 ante mí, el infrascrito
el notario público, [Firma ilegible] compareció personalmente, me demostró
a través de pruebas satisfactorias de identificación, que eran
pasaporte de EE.UU., ser la persona que firmó el documento precedente
o adjunto en mi presencia y que me juró o afirmó
que el contenido del documento es veraz y preciso
al mejor de [su] conocimiento y creencia.

Caitlyn E. Burns
Firma del Notario Público Mi Comisión Expira 29 de diciembre, 2028

CAITLYN E. BURNS
Notario Público
MANCOMUNIDAD DE MASSACHUSETTS
Mi Comisión Expira
29 de diciembre, 2028

Copia fiel y exacta al documento en inglés, en fe de lo cual he sellado y rubricado cada una de sus fojas. Traducción hecha a instancias de la parte interesada, en Santo Domingo de Guzmán, Distrito Nacional, República Dominicana, el día veintiuno (21) del mes de febrero del año dos mil veinticinco (2025), inscrita en mis registros habilitados para este fin bajo el número 11/2025.

This is a true and exact copy of the document in English; in witness thereof, I have sealed and initialed each of its pages. Translation made at the request of the interested party, in Santo Domingo de Guzmán, National District, Dominican Republic, on the Twenty-First (21st) day of February of the year Two Thousand Twenty-Five (2025), registered in my records enabled for this purpose under the number 11/2025.

Lic. Luis Eduardo Aquino Rivero
Intérprete Judicial–Judicial Interpreter

LUIS EDUARDO AQUINO RIVERO
Código: 27950

COPY SOLUTIONS INTERNATIONAL S.A.I.
CSI
RNC: 101[illegible]52
Santo Domingo, R.D.

The Commonwealth of Massachusetts
William Francis Galvin - Secretary of the Commonwealth

Apostille

(Convention de la Haye du 5 Octobre 1961)

1. Country: United States Of America

This Public Document

2. Has been signed by: Caitlyn E. Burns

3. Acting in the capacity of: Notary Public

4. Bears the seal/stamp of: Caitlyn E. Burns

Whose commission expires on: 12/29/2028

Certified

5. At: Boston, Massachusetts 6. The: February 21, 2025

7. By: The Secretary of Commonwealth

8. No.: 2680962

9. Seal/Stamp: *(Great Seal of the Commonwe*

10. Signature:

William Francis Galvin
Secretary of the Commonwealth

Prepared By: **DCooper**

GET Internet
P.O. Box: 95700
T: +971 (4) 299
F: +971 (4) 299
www.getg

Junta Electoral Central ("JCE")

Whosoever undersigned, **Ms. Maysoon F. Jamal**, of Lebanon, of legal age, married, bearer of Lebanese Passport No. LR3118926, domiciled and resident in Dubai, UAE, acting in the name and representation of **GET INTERNATIONAL FZCO**, a commercial company organized and existing in accordance with the laws of Dubai, UAE, with Tax Registration Number 104335821500001, and registered office in K18, Dubai Airport Free Zone (DAFZA), Dubai, UAE, in accordance with the powers granted to me by the Board of Directors of the company, in my capacity as MANAGER of the same,

Quien suscribe, **Sra. Maysoon F. Jamal**, de Líbano, mayor de edad, casada, portadora del Pasaporte Libanés nº LR3118926, domiciliada y residente en Dubái, EAU, actuando en nombre y representación de **GET INTERNATIONAL FZCO,** sociedad mercantil constituida y existente de acuerdo con las leyes de Dubái, EAU, con Número de Registro Fiscal 104335821500001, y domicilio social en K18, Dubai Airport Free Zone (DAFZA), Dubai, EAU, de acuerdo con los poderes que me han sido otorgados por la Junta Directiva de la sociedad, en mi calidad de GERENTE de la misma,

On **January 17, 2025**, by means of this document, and in response to the requirements of the International Public Bidding, Ref.: **JCE-CCC-LPI-2024- 0001**, I DECLARE **UNDER THE MOST SOLEMN FAITH OF THE OATH,** the following:

En fecha **17 de enero de 2025**, por medio del presente documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024- 0001**, DECLARO **BAJO LA MAS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

A. That **GET INTERNATIONAL FZCO**'s experience with the national ID project of Suriname satisfies the following requirements for the tender, as modified by the Questions and Answers provided by the JCE and summarized in the Matrix:

   Que la experiencia de **GET INTERNATIONAL FZCO** en el proyecto de identificación nacional de Surinam satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

   3.1.6.2 (a) Requisitos de experiencia (Obligatorios)
   MATRIZ 3.2.1

   Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo el suministro de impresoras de documentos de identidad de policarbonato electrónicos, incluyendo la instalación y el mantenimiento. Solo serán válidos contratos (en vigor o

terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública.

Y

5.4.5 Plantilla para Evaluación – Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

Al menos dos (2) experiencias en dos proyectos, de clientes y países distintos, en el cual el oferente haya llevado a cabo el suministro de impresoras, la instalación, las pruebas, la puesta en servicio y el mantenimiento de un sistema de documentos de identidad electrónicas de policarbonato distribuidas, con impresoras láser en los últimos cinco (5) años, a nivel de gobierno: 3 puntos.

B. That **GET INTERNATIONAL FZCO**'s experience with the national ID project of Suriname can be validated using the following data:

Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de documento nacional de identidad de Surinam puede validarse utilizando los siguientes datos:

Name of Public Institution/Agencia Gubernamental: Suriname Ministry of the Interior
Physical address/ Dirección física: Wilhelminastraat #3 Paramaribo, Suriname
Electronic address/ Dirección electronica: https://gov.sr/ministeries/ministerie-van-binnenlandse-zaken/
Name of the contact/Nombre de contacto: Valery Finsy
Title of the contact/ Cargo de contacto: Head of Printing House
Telephone number/ Teléfono: +597 8567111
Email address/ Correo electronica: valery.finsy@yahoo.com (to ensure prompt communication protocol, please copy Bosko Bozilovic, bosko@vlatacom.com) (para garantizar un protocolo de comunicación ágil, sírvase copiar a Bosko Bozilovic, bosko@vlatacom.com)

C. That **GET INTERNATIONAL FZCO**'s experience with the border ID project in China satisfies the following requirements for the tender, as modified by the Questions and Answers provided by the JCE and summarized in the Matrix:

Que la experiencia **de GET INTERNATIONAL FZCO** en el proyecto de identificación fronteriza en China satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

3.1.6.2 (c) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.3
Al menos una (1) experiencia, en el cual el oferente haya implementado un proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

Y

5.4.5 Plantilla para Evaluación – Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

Más de una (1) experiencia, en distintos clientes y países en proyectos de transición de documentos de identificación sin electrónica a documentos de identificación electrónica. Solo serán válidos contratos de al menos proyectos de 1,000,000 de documentos de identificación al año, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta:

- 2 contratos: 2 puntos.
- Más de 2 contratos: 3 puntos

Y

3.1.6.2 (d) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.4

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

D. That **GET INTERNATIONAL FZCO**'s experience with the border ID project in China can be validated using the following data:

Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de identificación fronteriza en China puede validarse utilizando los siguientes datos:

Name of Public Institution/Agencia Gubernamental: Aisino Corporation – government owned company working in coordination with the Ministry of Public Security

(Aisino Corporation- empresa estatal que trabaja en coordinación con el Ministerio de Seguridad Pública)
Physical address/ Dirección física: Aisino Science Park, 18, Xingshikou Road, Haidian District, Beijing, China
Electronic address/ Dirección electronica: www.aisino.com
Name of the contact/Nombre de contacto: Ms. Gu Shuxia
Title of the contact/ Cargo de contacto: Operational Director
Telephone number/ Teléfono: 0086-10-8889 6837 (office); 0086-135 2272 0052 (mobile)
Email address/ Correo electronica: gushuxia@aisino.com

E. That **GET INTERNATIONAL FZCO**'s experience with the driver's license project in Egypt satisfies the following requirements for the tender, as modified by the Questions and Answers provided by the JCE and summarized in the Matrix:

Que la experiencia de **GET INTERNATIONAL FZCO** en el proyecto de licencias de conducir en Egipto satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

3.1.6.2 (c) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.3

Al menos una (1) experiencia, en el cual el oferente haya implementado un proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

Y

5.4.5 Plantilla para Evaluación – Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

Más de una (1) experiencia, en distintos clientes y países en proyectos de transición de documentos de identificación sin electrónica a documentos de identificación electrónica. Solo serán válidos contratos de al menos proyectos de 1,000,000 de documentos de identificación al año, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta:

- 2 contratos: 2 puntos.
- Más de 2 contratos: 3 puntos

Y

3.1.6.2 (d) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.4

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

F. That **GET INTERNATIONAL FZCO**'s experience with the driver's license project in Egypt can be validated using the following data:

Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de permiso de conducir en Egipto puede validarse con los siguientes datos:

Name of Public Institution / Agencia Gubernamental: Traffic Administration Department under the Ministry of Interior
Physical address / Dirección física: km 4.5 - Cairo Suez Road, Near National Gas Station, Cairo, Egypt
Electronic address / Dirección electronica:
https://traffic.moi.gov.eg/English/Pages/default.aspx
Name of the contact / Nombre de contacto: Mohamed Ameen
Title of the contact / Cargo de contacto: Police Lieutenant
Telephone number / Teléfono: +2 01272274444
Email address / Correo electrónico: ameen.m@gmail.com (to ensure prompt communication protocol, please copy Sally Mamdouh at sally.mamdouh@amangroup-eg.com) (para garantizar un protocolo de comunicación ágil, sírvase copiar a Sally Mamdouh at sally.mamdouh@amangroup-eg.com)

G. That **GET INTERNATIONAL FZCO**'s experience with the digital health passport project in Egypt satisfies the following requirements for the tender, as modified by the Questions and Answers provided by the JCE and summarized in the Matrix:

Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de pasaporte sanitario digital en Egipto satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

3.1.6.3 (a)- Requisitos de experiencia (no obligatorios)
MATRIZ 3.3.1

Más de una (1) experiencia, en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Al menos una de las referencias debe ser ISO 18013-5.

Y

5.4.5-Plantilla para Evaluación
MATRIZ SECCIÓN AUTO-EVALUACIÓN

(i) "Plan del proyecto" -El proveedor presenta la implementación, de por lo menos, un desarrollo de una solución, puesta en producción, de cédula digital, en una institución pública, de acuerdo a los requerimientos establecidos en el documento de especificaciones técnicas, y estar adheridas al estándar ISO 18013-5: 4 puntos.

(ii) "Experiencia" (acreditable con contratos celebrados con empresas miembros de un mismo grupo económico (empresas con accionistas en común) de los consorciados en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

- 1 contratos: 1 punto.
- 2 contratos: 2 puntos.
- Más de 2 contratos: 3 puntos.

H. That **GET INTERNATIONAL FZCO**'s experience with the digital health passport in Egypt can be validated using the following data:

Que la experiencia de **GET INTERNATIONAL FZCO** con el pasaporte sanitario digital en Egipto puede validarse con los siguientes datos:

Name of Public Institution / Agencia Gubernamental: Ministry of Health & Population
Physical address / Dirección física: 3 Magles El Shaab Street, Lazoghli, Cairo, Egypt
Electronic address / Dirección Electronica: https://www.mohp.gov.eg/
Name of the contact / Nombre de contacto: Ahmed Mesbah
Title of the contact / Cargo de contacto: Director of Projects

Telephone number / Teléfono: +201007570338
Email address / Correo electrónico: ahmed.mesbah@mohp.gov.eg (to ensure prompt communication protocol, please copy Wael Talaat, wael.talaat@tazkarti.com) (para garantizar un protocolo de comunicación ágil, sírvase copiar a Wael Talaat, wael.talaat@tazkarti.com)

I. That, in addition to meeting the reference requirements requested in the process, **GET INTERNATIONAL FZCO** has proven experience in PKI – CA infrastructure for government projects, such as the Malawi e-passport - according to **ÍTEM VI, ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO** - VI.1 Especificaciones técnicas del mantenimiento, "For PKI maintenance, proven expertise support shall be provided."

Que, además de cumplir con los requisitos de referencia solicitados en el proceso, GET INTERNATIONAL FZCO tiene experiencia probada en infraestructura PKI - CA para proyectos gubernamentales, como el pasaporte electrónico de Malawi -de acuerdo con **ÍTEM VI, ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO** - VI.1 Especificaciones técnicas del mantenimiento "Para dar mantenimiento a la PKI, se deberá proveer soporte de experiencia comprobada."

[signature page to follow / firma en la página que continúa]

This Affidavit has been made in the City of Waltham, MA USA, on the 17th day of the month of January of the year 2025.

Esta Declaración Jurada ha sido hecha en la Ciudad de Waltham, MA USA, el día 17 del mes de enero del año 2025.

Maysoon F. Jamal
GET INTERNATIONAL FZCO

جي إي تي انترناشيونال ش م ح
GET INTERNATIONAL FZCO
P.O. Box 95703, Dubai - UAE No.: 1782

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 17 day of January 2025 before me, the undersigned notary public, Maysoon Jamal personally appeared, proved to me through satisfactory evidence of identification, which were Lebanese passport, to be the person who signed the preceding or attached document in my presence and who swore or affirmed to me that the contents of the document are truthful and accurate to the best of (his) (her) knowledge and belief.

Caitlyn E. Burns
Notary Public's Signature My Commission Expires December 29, 2028

CAITLYN E. BURNS
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
December 29, 2028

TRADUCCIÓN OFICIAL: Experiencias aportadas por G.E.T INTERNATIONAL FZCO.

Yo, Licenciado Luis Eduardo Aquino Rivero, Intérprete Judicial debidamente investido para este fin en virtud de la Resolución No. 13/2014 del Consejo del Poder Judicial, de fecha ocho (8) del mes de diciembre del año dos mil catorce (2014), CERTIFICO que la presente es una traducción fiel y completa del documento originalmente instrumentado en idioma inglés y cuya versión en español de conformidad con mi mejor entendimiento se lee como sigue: Yo, Licenciado Aquino Rivero, licensed Judicial Interpreter duly invested for this purpose by virtue of Resolution No. 13/2014 of the Council of the Judicial Branch, dated December 8th of the year two thousand fourteen (2014), CERTIFY that this is a faithful translation and in accordance with the document originally instrumented in the English language and whose version in Spanish, according to my best understanding, reads as follows:

GET International FZCO
P.O. Box 66703, Dubai, UAE
T. +971 (4) 299 06 86
F. +971 (4) 299 06 87
www.getgroup.com

[Seal GET GROUP] Constituida de acuerdo con la Ley No.2 de 1996 con Responsabilidad Limitada Licencia Comercial No. 1782

Junta Electoral Central ("JCE")

Quien suscribe, **Sra. Maysoon F. Jamal**, del Líbano, mayor de edad, casada, portadora del Pasaporte Libanés No. LR3118926, domiciliada y residente en Dubai, UAE, actuando en nombre y representación de **GET INTERNATIONAL FZCO**, una sociedad comercial organizada y existente de conformidad con las leyes de Dubai, UAE, con Número de Identificación Fiscal 104335821500001, y oficina registrada en K18, Zona Franca del Aeropuerto de Dubai (DAFZA), Dubai, UAE, de acuerdo con los poderes otorgados a mí por la Junta Directiva de la compañía, en mi calidad de GERENTE de la misma,

El **17 de enero de 2025**, por medio de este documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024-001**, DECLARO **BAJO LA MÁS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

A. Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de Documento Nacional de Identidad de Surinam satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por la JCE y resumidas en la Matriz:

3.1.6.2 (a) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.1

Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo el suministro de impresoras de documentos de identidad de policarbonato electrónicos, incluyendo la instalación y el mantenimiento. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública.

Y

5.4.5 Plantilla para Evaluación - Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

Al menos dos (2) experiencias en dos proyectos, de clientes y países distintos, en el cual el oferente haya llevado a cabo el suministro de impresoras, la instalación, las pruebas, la puesta en servicio y el mantenimiento de un sistema de documentos de identidad electrónicas de policarbonato distribuidas, con impresoras láser en los últimos cinco (5) años, a nivel de gobierno: 3 puntos.

B. Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de Documento Nacional de Identidad de Surinam puede validarse utilizando los siguientes datos:

Nombre de Institución Pública: Ministerio del Interior de Surinam
Dirección física: Wilhelminastraat #3 Paramaribo, Surinam
Dirección electrónica: https://gov.sr/ministeries/ministerie-va-binnenlandse-zaken
Nombre del contacto: Valery Finsy
Cargo del contacto: Jefe de Imprenta
Número de teléfono: +597 8567111
Dirección de correo electrónico: valery.finsy@yahoo.com (para asegurar un protocolo de comunicación ágil, sírvase copiar a Bosko Bozilovic, bosko@vlatacom.com)

C. Que la experiencia de **GET INTERNATIONAL FZCO** en el proyecto de Documento de Identificación Fronteriza en China satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por la JCE y resumidas en la Matriz:

INTÉRPRETE JUDICIAL
PODER JUDICIAL
LUIS EDUARDO AQUINO RIVERO
Código: 27559

COPY SOLUTIONS INTERNATIONAL SA
CSI
RNC. 101888852
Santo Domingo, RD

3.1.6.2 (c) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.3
Al menos una (1) experiencia, en el cual el oferente haya implementado un proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

Y

5.4.5 Plantilla para Evaluación - Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

Más de una (1) experiencia, en distintos clientes y países en proyectos de transición de documentos de identificación sin electrónica a documentos de identificación electrónica.
Solo serán válidos contratos de al menos proyectos de 1,000,000 de documentos de identificación al año, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta:

- 2 contratos: 2 puntos.
- Más de 2 contratos: 3 puntos

Y

3.1.6.2 (d) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.4

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

D. Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de Documento de Identificación Fronteriza en China puede validarse utilizando los siguientes datos:

Nombre de Institución Pública: Aisino Corporation – compañía estatal que trabaja en coordinación con el Ministerio de Seguridad Pública
Dirección física: Aisino Science Park, 18, Xingshikou Road, Distrito Haidian, Beijing, China
Dirección electrónica: www.aisino.com
Nombre del contacto: Sra. Gu Shuxia
Cargo del contacto: Director Operacional
Número de teléfono: 0086-10-8889 6837 (oficina); 0086-135 2272 0052 (móvil)
Dirección de correo electrónico: gushuxia@aisino.com

E. Que la experiencia de **GET INTERNATIONAL FZCO** en el proyecto de licencias de conducir en Egipto satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

3.1.6.2 (c) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.3

Al menos una (1) experiencia, en el cual el oferente haya implementado un proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

Y

5.4.5 Plantilla para Evaluación - Experiencia
MATRIZ SECCIÓN AUTO-EVALUACIÓN

PODER JUDICIAL
LUIS EDUARDO AQUINO RIVERO
Código: 27950

Más de una (1) experiencia, en distintos clientes y países en proyectos de transición de documentos de identificación sin electrónica a documentos de identificación electrónica.
Solo serán válidos contratos de al menos proyectos de 1,000,000 de documentos de identificación al año, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta:

- 2 contratos: 2 puntos.
- Más de 2 contratos: 3 puntos

Y

3.1.6.2 (d) Requisitos de experiencia (Obligatorios)
MATRIZ 3.2.4

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Solo serán válidos contratos (en vigor o terminados) dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

F. Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de permiso de conducir en Egipto puede validarse con los siguientes datos:

Nombre de Institución Pública: Departamento de Administración del Tránsito bajo el Ministerio de Interior
Dirección física: km 4.5 – Cairo Suez Road, Cerca de la Estación de Gas, Ciro, Egipto
Dirección electrónica: https://traffic.moi.gov.eg/English/Pages/default.aspx
Nombre del contacto: Mohamed Ameen
Cargo del contacto: Teniente de la Policía
Número de teléfono: +2 0127227444
Dirección de correo electrónico: ameen.m@gmail.com (para asegurar un protocolo de comunicación ágil, sírvase copiar a Sally Mamdouh at sally.mamdouh@amangroup-eg.com)

G. Que la experiencia de **GET INTERNATIONAL FZCO** con el proyecto de pasaporte sanitario digital en Egipto satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por el JCE y resumidas en la Matriz:

3.1.6.3 (a)- Requisitos de experiencia (no obligatorios)
MATRIZ 3.3.1

Más de una (1) experiencia, en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Al menos una de las referencias debe ser ISO 18013-5.

Y

5.4.5-Plantilla para Evaluación
MATRIZ SECCIÓN AUTO-EVALUACIÓN

(i) "Plan del proyecto" -El proveedor presenta la implementación, de por lo menos, un desarrollo de una solución, puesta en producción, de cédula digital, en una institución pública, de acuerdo a los requerimientos establecidos en el documento de especificaciones técnicas, y estar adheridas al estándar ISO
18013-5: 4 puntos.

(ii) "Experiencia" (acreditable con contratos celebrados con empresas miembros de un mismo grupo económico (empresas con accionistas en común) de los consorciados en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

- 1 contratos: 1 punto.
- 2 contratos: 2 puntos.

PODER JUDICIAL
LUIS EDUARDO AQUINO RIVERO
Código: 27950

- Más de 2 contratos: 3 puntos.

H. Que la experiencia de **GET INTERNATIONAL FZCO** con el pasaporte sanitario digital en Egipto puede validarse con los siguientes datos:

Nombre de Institución Pública: Ministerio de Salud & Población
Dirección física: 3 Magles Calle El Shaab, Lazoghli, Cairo, Egipto
Dirección electrónica: https://www.mohp.gov.eg/
Nombre del contacto: Ahmed Mesbah
Cargo del contacto: Director de Proyectos
Número de teléfono: +201007570338
Dirección de correo electrónico: ahmed.mesbah@mohp.gov.eg (para asegurar un protocolo de comunicación ágil, sírvase copiar a Wael Talaat, wael.talaat@tazkarti.com)

I. Que, además de cumplir con los requisitos de referencia solicitados en el proceso, **GET INTERNATIONAL FZCO** tiene experiencia probada en infraestructura PKI - CA para proyectos gubernamentales, como el pasaporte electrónico de Malawi -de acuerdo con **ÍTEM VI, ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO** - VI.1
Especificaciones técnicas del mantenimiento "Para dar mantenimiento a PKI, se deberá proveer soporte de experiancia comprobada."

[firma en la página siguiente]

INTÉRPRETE JUDICIAL
PODER JUDICIAL
LUIS EDUARDO AQUINO RIVERO
Código: 27950

Esta Declaración Jurada ha sido realizada en la Ciudad de Waltham, MA EE.UU., el día 17 del mes de enero del año 2025.

[Firma ilegible]
Maysoon F. Jamal
GET INTERNATIONAL FZCO [Sello GET INTERNATIONAL FZCO]

MANCOMUNIDAD DE MASSACHUSETTS
CONDADO DE Middlesex

En este día 17 de enero, 2025 ante mí, el infrascrito
al notario público, [Firma ilegible] compareció personalmente, me demostró
a través de pruebas satisfactorias de identificación, que era
pasaporte Ubanés, ser la persona que firmó el documento precedente
o adjunto en mi presencia y que me juró o afirmó
que el contenido del documento es veraz y preciso
al mejor de (su) conocimiento y creencia.

Caitlyn E. Burns
Firma del Notario Público Mi Comisión Expira 29 de diciembre, 2028

CAITLYN E. BURNS
Notario Público
MANCOMUNIDAD DE MASSACHUSETTS
Mi Comisión Expira
29 de diciembre, 2028

Copia fiel y exacta al documento en inglés, en fe de lo cual he sellado y rubricado cada una de sus fojas. Traducción hecha a instancias de la parte interesada, en Santo Domingo de Guzmán, Distrito Nacional, República Dominicana, el día veintiuno (21) del mes de febrero del año dos mil veinticinco (2025), inscrita en mis registros habilitados para este fin bajo el número 12/2025.

This is a true and exact copy of the document in English; in witness thereof, I have sealed and initialed each of its pages. Translation made at the request of the interested party, in Santo Domingo de Guzmán, National District, Dominican Republic, on the Twenty-First (21st) day of February of the year Two Thousand Twenty-Five (2025), registered in my records enabled for this purpose under the number 12/2025.

Lic. Luis Eduardo Aquino Rivero
Intérprete Judicial–Judicial Interpreter

INTÉRPRETE JUDICIAL
PODER JUDICIAL
LUIS EDUARDO AQUINO RIVERO
Código: 27901

MINISTERIO PÚBLICO
CENTRO DE ATENCIÓN AL CIUDADANO
DISTRITO NACIONAL

TRADUCCIÓN OFICIAL: Experiencias aportada por SELP para proyecto NEPAL.

CSI CPV SOLUTIONS INTERNATIONAL, SA RNC 104693852 Santo Domingo, R.D.

REFERENCE LETTER

Carta de Referencia / Lettre de Référence

N'Djaména, 18th February 2022

We, undersigned **ANATS**,

Certify that SELP SAS is the supplier of the following contract:

Supply of 1.7 million polycarbonate ID cards with JavaCard OS chip with logo on the contact plate and including ICAO LDS applets, PKI electronic signature and Match on Card.

Implementation period: 2019 – still ongoing

SELP SAS has successfully fulfilled the obligations of the contract.

N'Djaména, el 18 de febrero de 2022

Los abajos firmantes **ANATS**.

Certificamos que SELP SAS es el proveedor del contrato siguiente :

Suministro de 1,7 millones de tarjetas de identificación de policarbonato con el chip JavaCard OS con el logotipo en la placa de contacto y que incluye ICAO LDS applets, firma electrónica PKI y Match on Card.

Implementación: **2019 – Todavía en curso**

SELP SAS ha realizado con éxito las obligaciones del contrato.

N'Djaména, le 18 février 2022

Nous soussignés ANATS,

Certifions que SELP SAS est le fournisseur du contrat suivant :

Fourniture de 1,7 millions de cartes d'identité en polycarbonate avec une puce avec OS Javacard et logo présent sur le module contact et incluant les applets LDS ICAO, signature électronique PKI et Match On Card.

Implémentation : **2019 – Toujours en cours**

SELP SAS a rempli avec succès ses obligations pour ce contrat.

Name	Appellido	Nom	:	**Mahamat Oumar Kessou**
Position	Función	Poste	:	**Directeur Général**
Company	Sociedad	Société	:	**ANATS**
Address	Dirección	Adresse	:	**BP 5558, N'Djaména - Tchad**
Phone	Teléfono	Téléphone	:	**+235 225 24030 / +235 662 38389**
E-mail			:	**mhtokessou@gmail.com**
Signature	Firma	Signature	:	.....
Stamp	Tampón	Tampon	:	

SELP

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC: 101899652 Santo Domingo, R.D.

Declaración Jurada

Quien suscribe, Señor Bastien Blanc, francés, mayor de edad, portador del Pasaporte No. 23EE65071, domiciliado y residente en 1 rue Saint Charles, 75015 Paris, Francia, actuando en nombre y representación de SELP S.A.S., sociedad de comercio organizada y existente de conformidad con las leyes francesas, con RSC de Périgueux No 351 667 928, y domicilio social en 187 Allées des Plagnes, 24340 Mareuil en Périgord, conforme a los poderes que me fueran otorgados por el Consejo de Administración de la compañía, en mi condición de Director General de Roland Holding, a su vez presidente de SELP S.A.S, en fecha 14 de febrero de 2024, por medio del presente documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024-0001**, declaro **BAJO LA MAS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

La empresa SELP S.A.S. proporcionó desde el año 2019 hasta el 2022, 1,7 millones de tarjetas de identificación en policarbonato con chip JavaCard OS, y que incluyen ICAO LDS applets, firma electrónica PKI y Match on Card, a la "Agencia Nacional de Títulos de Identidad de Alta Seguridad" (ANATS, por sus siglas en francés) del Gobierno de Chad.

El contrato se ejecutó a satisfacción de la Agencia Nacional de Títulos de Identidad de Alta Seguridad de la República de Chad.

Indica el país:	República de Chad
Entidad contratante: (ANATS)	Agencia Nacional de Títulos de Identidad de Alta Seguridad
Detalles de contacto:	Mahamat Oumar Kessou Director General de ANATS BP 5558, N'Djaména - Chad +235 225 24030/ +235 662 38389 mhtokessou@gmail.com

Número de tarjetas de identidad: 1,7 millones
Nivel de satisfacción del proyecto: El proyecto ha sido realizado por SELP con éxito en las obligaciones del contrato.

La presente Declaración Jurada ha sido realizada en la Ciudad de Paris, a los 14 días del mes de febrero del año 2025.

Atentamente,

Bastien Blanc
Representante
SELP S.A.S.

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tél.: 05 53 60 84 44 - Fax : 05 53 60 84 45
SIRET : 351 667 928 00011

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC
apposée ci-contre

Notario Público

SELP

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC. 101899852 Santo Domingo, R.D.

Declaración Jurada

Quien suscribe, Señor Bastien Blanc, francés, mayor de edad, portador del Pasaporte No. 23EE65071, domiciliado y residente en 1 rue Saint Charles, 75015 Paris, Francia, actuando en nombre y representación de SELP S.A.S., sociedad de comercio organizada y existente de conformidad con las leyes francesas, con RSC de Périgueux No 351 667 928, y domicilio social en 187 Allées des Plagnes, 24340 Mareuil en Périgord, conforme a los poderes que me fueran otorgados por el Consejo de Administración de la compañía, en mi condición de Director General de Roland Holding, a su vez presidente de SELP S.A.S, en fecha 14 de febrero de 2024, por medio del presente documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024-0001**, declaro **BAJO LA MAS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

La empresa SELP S.A.S. proporcionó desde el año 2020 hasta el 7 de diciembre del 2023, 30 millones de tarjetas inteligentes con chip, en policarbonato, como tarjetas de identidad para la "Autoridad Nacional de Bases de Datos y Registro" (NADRA, por sus siglas en inglés) del Gobierno de Pakistán por un importe de $20.400.000,00 dólares.

El contrato se ejecutó a satisfacción de la Autoridad Nacional de Bases de Datos y Registro de la República de Pakistán.

Indica el país:	República de Pakistán
Entidad contratante:	National Database and Registration Authority (NADRA)
Detalles del contacto Actual:	Kamran Latif Responsable de Producción Oficinas centrales de NADRA, G-10/4, Mauve Area, Islamabad +92 300 5013086 Kamran.Latif@nadra.gov.pk

Fecha del contrato: 16 octubre, 2020
Número de tarjetas de identidad: 30 millones
Nivel de satisfacción del proyecto: El contrato concluyó dentro del plazo indicado, cumpliendo con todos los bienes solicitados, en los tiempos acordados y calificando el servicio como satisfactorio, sin tener penalización alguna.
Plazo de entrega: 2020-2023
Monto del proyecto: $20 400 000,00 USD

La presente Declaración Jurada ha sido realizada en la Ciudad de Paris, a los 14 días del mes de febrero del año 2025.

Atentamente,

Bastien Blanc
Representante
SELP S.A.S.

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tél. : 05 53 60 84 44 - Fax : 05 53 60 84 45
SIRET : 351 667 928 00011

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC
apposée ci-contre

Notario Público

COPY SOLUTIONS INTERNATIONAL, S.A.
RNC: 101899
Santo Domingo, R.D.

MINUTE SHEET
PROCUREMENT DEPARTMENT
ADMIN DIRECTORATE, NADRA HQ
G-10/4, Mauve Area, Islamabad

CERTIFICATE OF COMPLETION/CONFORMITY

To Whom it may concern

On the 07th day of December 2023, the delivered good is approved, corresponding to service contract (Purchase order) No NADRA/proc/CNIC/6285, dated October 16th, 2020 and amount of USD $20,400,000 (twenty million four hundred thousand US dollars), provided by the company SELP S.A.S., 187 allée des Plagnes, 24340 Mareuil en Périgord, France, with Business Registration Number (RCS) 351 667 928, which the manufacture of the smart cards as identity documents, was carried out in accordance with the requested Terms of References and concluded within the indicated term, complying with all the requested goods, in the agreed times and qualifying the service as: SATISFACTORY, without having any penalty.

It is worth mentioning that the service provided by SELP S.A.S corresponds to the delivery of 30,000,000 Smart Cards as an identity document with chip in Polycarbonate material.

We proceed to give consent to the service provided and attest to which we sign the respective minutes.

Signature

Rehman Mehmood Butt
Deputy Director (Procurement)
NADRA Headquarters, Islamabad
Contact: 0092 51 90392829

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101[illegible]52
Santo Domingo, R.D.

COUR D'APPEL DE PARIS

COUR D'APPEL DE PARIS

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *République française* REPUBLIQUE DOMINICAINE

Le présent acte public

2. a été signé par Me Tillier

3. agissant en qualité de Notaire

4. est revêtu du sceau timbre de... Son étude

Arrêté FEV. 2025

5. à Paris

6. le

7. par le Procureur général près la Cour d'appel de Paris

8. sous n° 1136

9. Sceau Sylvie SCHLANGER Avocat général 10. Signature

"L'Apostille confirme seulement l'authenticité de la signature, du sceau ou timbre sur le document. Elle ne signifie pas que le contenu du document est correct ou que la République française approuve son contenu"

COUR D'APPEL DE PARIS

Government of Nepal
Ministry of Physical Infrastructure and Transport
Department of Transport Management
(Minbhawan, Kathmandu)

Phone 4474767
4474768
4474921
Fax 4474922
Email: trans@dotm.gov.np
Website
www.dotm.gov.np

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC 101898852
Santo Domingo, R.D.

REFERENCE LETTER

Carta de Referencia / Lettre de Référence

Addressed to the Central Electoral Board
Purchasing and Contracting Committee
Reference: JCE-CCC-LPI-2024-0001

Kathmandu – Nepal, 11th June, 2024,

We, undersigned **Department of Transport Management under the government of Nepal,**

Certify that SELP SAS is the supplier of the following contract:

Supply of more than 1.4 Million polycarbonate electronic driving licences including manufacturing of preprinted smartcards with security features and Java Card Operating System for a minimum global value of USD 1 200 000.

Implementation period: **2021**

SELP SAS has successfully fulfilled the obligations of the contract.

Last Name /Name	:	**BARAL BODHARAJ**
Position	:	**COMPUTER ENGINEER**
Company	:	**DEPARTMENT OF TRANSPORT MANAGEMENT**
Address	:	**MINBHAWAN, KATHMANDU**
Phone	:	**+977- 01 447467, 4474768**
E-mail	:	**Bodharajbaral.gulmi@gmail.com**

Signature : .....

Stamp :

Government of Nepal
Ministry of Physical Infrastructure and Transport
Department of Transport Management
Minbhawan, Kathmandu

Scanned with CamScanner

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO haber procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membrete del Ministerio de Infraestructura Física y Transporte del Gobierno de Nepal • Teléfono 4474767 – 4474768 – 4474921 • Fax: [illegible] • correo: trans@dotm.gov.np • sitio web: www.dotm.gov.np

Gobierno de Nepal
Ministerio de Infraestructura Física y Transporte

Departamento de Administración de Transporte

CARTA DE REFERENCIA

Dirgida a la Junta Central Electoral
Comité de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001

Kathmandu – Nepal, 11 de junio de 2024

Nosotros, los suscritos del Departamento de Administración de Transporte, bajo el gobierno de Nepal, certificamos que SELP SAS es el proveedor del siguiente contrato:

Suministro de más de 1,4 millones de licencias de conducir electrónicas de policarbonato, incluyendo la fabricación de tarjetas inteligentes pre-impresas, con características de seguridad y el Sistema Operativo de la Tarjeta Java por un valor mínimo global de USD 1 200 000.

Período de Implementación: 2021

SELP SAS ha complido satisfactoriamente las obligaciones del contrato.

Apellido /Nombre : BARAL BODHARAJ
Posición : INGENIERO INFORMATIVO
Compañía : DEPARTAMENTO DE ADMINISTRACION DE TRANSPORTE
Dirección : MINBHAWAN, KATHMANDU
Teléfono : +977-01 447467, 4474768
Correo : Bodharajbaral.gulmi@gmail.com

Firma : ilegible
Timbre : Impreso el sello del Ministerio de Infraestructura Física y Transporte del Gobierno de Nepal

EN FE DE LO CUAL, firmo y sello la presente **Certificación,** a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los veinticuatro (24) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 274/25.

Ana María Feria

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO: Que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membrete del Ministerio de Infraestructura Física y Transporte del Gobierno de Nepal • Teléfono 4474767 – 4474768 – 4474921 • Fax 4474762
• correo: juans@dotm.go.np • sitio web: www.dotm.gov.np

Gobierno de Nepal
Ministerio de Infraestructura Física y Transporte

Departamento de Administración de Transporte

CARTA DE REFERENCIA

Dirgida a la Junta Central Electoral
Comité de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001

Kathmandu – Nepal, 11 de junio de 2024

Nosotros, los suscritos del Departamento de Administración de Transporte, bajo el gobierno de Nepal, certificamos que SELP SAS es el proveedor del siguiente contrato:

Suministro de más de 1,4 millones de licencias de conducir electrónicas de policarbonato, incluyendo la fabricación de tarjetas inteligentes pre-impresas, con características de seguridad y el Sistema Operativo de la Tarjeta Java por un valor mínimo global de USD 1 200 000.

Periodo de Implementación: 2021

SELP SAS ha complido satisfactoriamente las obligaciones del contrato.

Apellido /Nombre : BARAL BODHARAJ
Posición : INGENIERO INFORMATIVO
Compañía : DEPARTAMENTO DE ADMINISTRACION DE TRANSPORTE
Dirección : MINBHAWAN, KATHMANDU
Teléfono : +977-01 447467, 4474768
Correo : Bodharajbaral.gulmi@gmail.com

Firma : ilegible
Timbre : Impreso el sello del Ministerio de Infraestructura Fisica y Transporte del Gobierno de Nepal

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los veinticuatro (24) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 274/25.

Ana María Feria

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO haber procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membrete del Ministerio de Infraestructura Física y Transporte del Gobierno de Nepal • Teléfono 4474787 – 4474768 – 4474821 • Fax: [illegible] • correo: trans@dotm.gov.np • sitio web: www.dotm.gov.np

Gobierno de Nepal
Ministerio de Infraestructura Física y Transporte

Departamento de Administración de Transporte

CARTA DE REFERENCIA

Dirgida a la Junta Central Electoral
Comité de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001

Kathmandu – Nepal, 11 de junio de 2024

Nosotros, los suscritos del Departamento de Administración de Transporte, bajo el gobierno de Nepal, certificamos que SELP SAS es el proveedor del siguiente contrato:

Suministro de más de 1,4 millones de licencias de conducir electrónicas de policarbonato, incluyendo la fabricación de tarjetas inteligentes pre-impresas, con caracteristicas de seguridad y el Sistema Operativo de la Tarjeta Java por un valor mínimo global de USD 1 200 000.

Periodo de Implementación: 2021

SELP SAS ha complido satisfactoriamente las obligaciones del contrato.

Apellido /Nombre : BARAL BODHARAJ
Posición : INGENIERO INFORMATIVO
Compañía : DEPARTAMENTO DE ADMINISTRACION DE TRANSPORTE
Dirección : MINBHAWAN, KATHMANDU
Teléfono : +977-01 447467, 4474768
Correo : Bodharajbaral.gulmi@gmail.com

Firma : ilegible
Timbre : Impreso el sello del Ministerio de Infraestructura Física y Transporte del Gobierno de Nepal

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los veinticuatro (24) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 274/25.

Ana María Feria

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO haber procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membrete del Ministerio de Infraestructura Física y Transporte del Gobierno de Nepal • Teléfono 4474767 – 4474768 – 4474921 • Fax: 4474624
• correo: trans@dotm.gov.np • sitio web: www.dotm.gov.np

Gobierno de Nepal
Ministerio de Infraestructura Física y Transporte

Departamento de Administración de Transporte

CARTA DE REFERENCIA

Dirgida a la Junta Central Electoral
Comité de Compras y Contrataciones
Referencia: JCE-CCC-LPI-2024-0001

Kathmandu – Nepal, 11 de junio de 2024

Nosotros, los suscritos del Departamento de Administración de Transporte, bajo el gobierno de Nepal, certificamos que SELP SAS es el proveedor del siguiente contrato:

Suministro de más de 1,4 millones de licencias de conducir electrónicas de policarbonato, incluyendo la fabricación de tarjetas inteligentes pre-impresas, con caracteristicas de seguridad y el Sistema Operativo de la Tarjeta Java por un valor mínimo global de USD 1 200 000.

Período de Implementación: 2021

SELP SAS ha complido satisfactoriamente las obligaciones del contrato.

Apellido /Nombre : BARAL BODHARAJ
Posición : INGENIERO INFORMATIVO
Compañía : DEPARTAMENTO DE ADMINISTRACION DE TRANSPORTE
Dirección : MINBHAWAN, KATHMANDU
Teléfono : +977-01 447467, 4474768
Correo : Bodharajbaral.gulmi@gmail.com

Firma : ilegible
Timbre : Impreso el sello del Ministerio de Infraestructura Física y Transporte del Gobierno de Nepal

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los veinticuatro (24) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 274/25.

Ana María Feria

SELP

CSI SOLUTIONS INTERNATIONAL S.A. RNC 101898852 Santo Domingo, R.D.

Declaración Jurada

Quien suscribe, Señor Bastien Blanc, francés, mayor de edad, portador del Pasaporte No. 23EE65071, domiciliado y residente en 1 rue Saint Charles, 75015 Paris, Francia, actuando en nombre y representación de SELP S.A.S., sociedad de comercio organizada y existente de conformidad con las leyes francesas, con RSC de Périgueux No 351 667 928, y domicilio social en 187 Allées des Plagnes, 24340 Mareuil en Périgord, conforme a los poderes que me fueran otorgados por el Consejo de Administración de la compañía, en mi condición de Director General de Roland Holding, a su vez presidente de SELP S.A.S, en fecha 14 de febrero de 2024, por medio del presente documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024-0001**, declaro **BAJO LA MAS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

La empresa SELP S.A.S. proporcionó desde el año 2017 hasta el 23 de marzo del 2020, más de 12 millones de tarjetas inteligentes con chip & PKI Middleware, como documento nacional de identidad para el "UNDP Office in Malawi" (Programa De Las Naciones Unidas Para El Desarrollo en español en la Republica de Malawi).

El contrato se ejecutó satisfactoriamente para el Programa de las Naciones Unidas para el Desarrollo en Malawi, siendo SELP el encargado de llevar a cabo la implementación del proyecto de transición, permitiendo el paso de un sistema sin documentos de identidad a la emisión directa de documentos electrónicos con chip.

Indica el país:	República de Malawi
Entidad contratante:	UNDP Office in Malawi Plot 7 Area 40 P.O. Box 30135 LILONGWE 3 MALAWI
Detalles del contacto Actual:	Victor Margall von Hegyeshalmy Electoral/ID Procurement Lead - Bureau of Management Services Tel: (+45) 4533 6066 Email: victor.margall@undp.org

Fecha del contrato: 24 abril, 2017 hasta marzo 2020.
Número de tarjetas de identidad: 12.18 millones
Ultima entrega: 23 marzo, 2020 para 1 millón de tarjetas de identidad.
Nivel de satisfacción del proyecto: El contrato concluyó dentro del plazo indicado, cumpliendo con todos los bienes solicitados, en los tiempos acordados y calificando el servicio como satisfactorio, sin tener penalización alguna.
Plazo de entrega: 2017-2020

La presente Declaración Jurada ha sido realizada en la Ciudad de Paris, a los 14 días del mes de febrero del año 2025.

Atentamente,

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tél. : 05 53 60 84 44 - Fax : 05 53 60 84 45
SIRET : 351 667 928 00011

Bastien Blanc
Representante
SELP S.A.S.

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC
apposée ci-contre

Notario Público

CSI SOLUTIONS INTERNATIONAL S.A.
CSI
RNC. 101[illegible]852
Santo Domingo R.D.

COUR D'APPEL DE PARIS

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *République française* REPUBLIQUE DOMINICAINE

Le présent acte public

2. a été signé par Me Tillier

3. agissant en qualité de Notaire

4. est revêtu du sceau timbre de Son étude

Attesté

5. à Paris 17 FEV. 2025

6. le

7. *par le Procureur général près la Cour d'appel de Paris*

8. sous n° AJ134

9. Sceau N2 Sylvie SCHLANGER Avocat général 10. Signature :

"L'Apostille confirme seulement l'authenticité de la signature, du sceau ou timbre sur le document. Elle ne signifie pas que le contenu du document est correct ou que la République française approuve son contenu"

COUR D'APPEL DE PARIS

eGovernment Unit
Cayman Islands Government

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

REFERENCE LETTER

9th of February 2024

We, undersigned **The Cayman Islands Government represented by the e-Government Unit,**

Certify that SELP SAS is the supplier of a full end-to-end, turn-key solution to deliver the ability for the Cayman Islands government (CIG) to issue a National eID to Caymanians, permanent residents and any other person who is legally and ordinarily resident in the Cayman Islands.

As part of this contract, SELP SAS has supplied:

- Dual-Interface eID cards with Javacard OS containing, ICAO, eIDAS compliant QSCD applet, supporting certificates for authentication and qualified electronic signatures
- A full implemented structure for the enrolment, personalization, issuance, authentication, stock management, document management, quality control and lifecycle management of the National eID cards to residents of the Cayman Islands.
    - Fix Office Solution and Mobile Solution hardware
    - EIPS Software License including:
        - Enrolment Software Module
        - Personalization Software Module
        - Issuance Software Module
        - Configuration & System Administration Module
    - API to allow access to specific data by government's entities
    - Integration with X-ROAD *(trademarked to Estonia)* interoperability solution
    - PKI solution to issue Digital Signature Certificates and Digital Authentication Certificates
    - Credential Management System – Managing Cards and Certificates lifecycle
    - Digital Identity solution including:
        - eID Middleware software for National eID card holders to support functionality of PIN and PUK changes, digital identity verification, digital signature creation, digital signature validation and digital authentication to eServices platform.
            - Desktop APP for Windows, MacOS and Linux
            - Mobile APP (iOS & Android) for digital signature,
- USB & Bluetooth eID card readers compatible with computer and Mobile.

As part of this contract, SELP SAS is providing the following services:
- Specification and development of the end-to-end solution
- Integration of the end-to-end solution within CIG Infrastructure (X-Road based Solution)
- Project management, UI/UX design, delivery, installation & training

Implementation period: July 2021 – December 2023
Minimum value of the contract: 1 M USD
Contract period: July 2021 – July 2026 (+ 5 additional years optional)

The end-to-end National eID solution Implementation has been successfully realized by SELP in December 2023.

The global scope of the contract includes the following modules and services:
- Online enrolment solution
    - Web based/web responsive solution

Ian Tibbetts
Director
D. +1 (345) 244 3614
E. Ian.Tibbetts@gov.ky

89 Nexus Way| Suite 8210
Grand Cayman
KY1-9000

gov.ky

eGovernment Unit
Cayman Islands Government

- Biometric Identity verification (facial dynamic control)
- Integration with CIG Payment Service Provider
- ID Document authentication verification

  - Helpdesk to support end user
  - Maintenance services of the end-to-end solution

Name	:	Ian Tibbetts
Position	:	Director
Company	:	eGovernment
Address	:	89 Nexus Way| Suite 8210| Grand Cayman
Phone	:	1 (345)244-3614
Phone	:	1 (345) 925-8021
E-mail	:	Ian.Tibbetts@gov.ky

Signature :

Stamp :

Ian Tibbetts
Director
D. +1 (345) 244 3614
E. Ian.Tibbetts@gov.ky

89 Nexus Way| Suite 8210
Grand Cayman
KY1-9000

gov.ky

Yo **LIC. SANTO C. SIERRA**, intérprete judicial, debidamente juramentada para el ejercicio de mis funciones **CERTIFICO** que he procedido a traducir las partes centrales de un documento escrito originalmente en Ingles, cuya versión en idioma Español de acuerdo a mi mejor el conocimiento es el siguiente:

Unidad de Gobierno Electrónico Gobierno de las Islas Caimán

CARTA DE REFERENCIA

9 de febrero de 2024

Nosotros, los abajo firmantes, el Gobierno de las Islas Caimán representado por la Unidad de Gobierno Electrónico,

Certifique que SELP SAS es el proveedor de una solución integral, llave en mano, para ofrecer al gobierno de las Islas Caimán (CIG) la posibilidad de emitir una identificación electrónica nacional a caimaneses, residentes permanentes y cualquier otra persona que sea legal y residente habitual en las Islas Caimán.

Como parte de este contrato, SELP SAS ha suministrado:

Tarjetas de identificación electrónica de interfaz dual con sistema operativo Javacard que contiene el subprograma QSCD compatible con eIDAS de la OACI, certificados compatibles para autenticación y firmas electrónicas calificadas

Una estructura completamente implementada para la inscripción, personalización, emisión, autenticación, gestión de existencias, gestión de documentos, control de calidad y gestión del ciclo de vida de las tarjetas de identificación electrónicas nacionales para residentes de

Las Islas Caimán.

Reparar el hardware de la solución Office y la solución móvil

Licencia de software EIPS que incluye:

- Módulo de software de inscripción
- Módulo de software de personalización
- Módulo de software de emisión
- Módulo de configuración y administración del sistema
  - API para permitir el acceso a datos específicos por parte de entidades gubernamentales

- Integración con la solución de interoperabilidad X-ROAD (marca registrada en Estonia)
- Solución PKI para emisión de Certificados de Firma Digital y Certificados de Autenticación Digital
- Sistema de gestión de credenciales: gestión del ciclo de vida de tarjetas y certificados
- Solución de identidad digital que incluye:
- Software eID Middleware para titulares de tarjetas de identificación electrónicas nacionales para admitir la funcionalidad de cambios de PIN y PUK, verificación de identidad digital, creación de firmas digitales, validación de firmas digitales y autenticación digital en la plataforma de servicios electrónicos.
- APLICACIÓN de escritorio para Windows, MacOS y Linux
- APLICACIÓN móvil (iOS y Android) para firma digital,

Lectores de tarjetas de identificación electrónica USB y Bluetooth compatibles con computadora y móvil.

Como parte de este contrato, SELP SAS proporciona los siguientes servicios:

Especificación y desarrollo de la solución extremo a extremo.

Integración de la solución de extremo a extremo dentro de CIG Infrastructure (solución basada en X-Road) Gestión de proyectos, diseño, entrega, instalación y capacitación de UI/UX

Período de implementación: julio de 2021 - diciembre de 2023

Valor mínimo del contrato: 1 M USD

Período de contratación: julio 2021 - julio 2026 (+ 5 años adicionales opcionales)

SELP realizó con éxito la implementación de la solución nacional de identificación electrónica de extremo a extremo en diciembre de 2023.

El alcance global del contrato incluye los siguientes módulos y servicios:

- Solución de inscripción en línea
- Solución web responsiva/basada en web

Ian Tibbetts
Director

89 Nexus Way Suite 8210

+1 (345) 244 3614 Gran Caimán KY1-9000

E.Ian. Tibbetts@gov.ky

Unidad de Gobierno Electrónico

Gobierno de las Islas Caimán

- Verificación de Identidad Biométrica (control dinámico facial)
- Integración con el proveedor de servicios de pago CIG
- Verificación de autenticación de documento de identidad

  - Mesa de ayuda para apoyar al usuario final
  - Servicios de mantenimiento de la solución extremo a extremo.

Nombre: Ian Tibbetts

Posición :Director

Empresa: administración electrónica

DIRECCIÓN: 89 Nexus Way Suite 8210 | Gran Caimán

Teléfono: 1 (345)244-3614

Teléfono: 1 (345) 925-8021

Correo electrónico: Ian. Tibbetts@gov.ky

Firma :

Estampilla:

Traducido a petición de la parte interesada y registrada en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Veintitrés (23) días del mes de Octubre del año Dos Mil Veinticuatro (2024).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

S.C.S / DPE
5184-12-8-96

LIC. SANTO C. SIERRA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, D.N.

Acreditación de Experiencias No Obligatorias.

CONSOLIDADO DE LAS EXPERIENCIAS DEL CONSORCIO

I. **Experiencia en distintos clientes y paises, en cédulas digital o identidades móviles (Mobile ID).**

Experiencia 1 (Criterio para obtención de 1 puntos):
G.E.T ENTERPRISE TECHNOLOGIES CORP.
Proyecto de Licencia de Conducir Móvil en el Estado de Utah.

Experiencia 2 (Criterio para obtención de 2 puntos):
G.E.T INTERNATIONAL FZCO.
Proyecto de Pasaporte Sanitario Digital en Egipto.

Experiencia 3 (Criterio para obtención de 3 puntos):
G.E.T SECURE ID CORP.
Proyecto de Licencia de Conducir Móvil en Ecuador.

II. **Experiencia de haber operado un proyecto de impresión de soluciones de identificación a nivel de gobierno con el suministro y mantenimiento de al menos doscientas (200) impresoras distribuidas nacional e internacional (fuera del pais).**

Experiencia 1 (Requerimiento):
Copy Solutions International S.A.
Proyecto de Cédula de Identidad de República Dominicana.

III. **Experiencia en República Dominicana en proyectos de mantenimiento de tecnologia en gobierno con al menos cinco (5) años de experiencia.**

Experiencia 1 (Requerimiento):
Copy Solutions International S.A.
Mantenimiento de tecnología para EDENORTE.

Experiencia 2:
Copy Solutions International S.A.
Mantenimiento de tecnología para Cámara de Diputados.

Experiencia 3:
Copy Solutions International S.A.
Mantenimiento de tecnología para Ayuntamiento del Distrito Nacional.

Experiencia 4:
Copy Solutions International S.A.
Mantenimiento de tecnología para Banco Popular Dominicano.

COPY SOLUTIONS INTERNATIONAL SA
RNC: 101098652
Santo Domingo, R.D.

The Commonwealth of Massachusetts
William Francis Galvin - Secretary of the Commonwealth

Apostille

(Convention de la Haye du 5 Octobre 1961)

1. Country: United States Of America

This Public Document

2. Has been signed by: Caitlyn E. Burns

3. Acting in the capacity of: Notary Public

4. Bears the seal/stamp of: Caitlyn E. Burns

Whose commission expires on: 12/29/2028

Certified

5. At: Boston, Massachusetts 6. The: February 21, 2025

7. By: The Secretary of Commonwealth

8. No.: 2680963

9. Seal/Stamp: *(Great Seal of the [illegible])*

10. Signature:

William Francis Galvin
Secretary of the Commonwealth

Prepared By: **DCooper**

G.E.T. Secure ID Corp
230 Third Ave., Waltham MA 02451
T: +1 781 902 8700
F: +1 781 890 1901
www.getgroup.com

Junta Electoral Central ("JCE")

Quien suscribe, **Sr. Joshua M. Mármol**, de EE.UU., mayor de edad, casado, titular del Pasaporte de EE. UU. nº 566385611, domiciliado y residente en Waltham, MA EE. UU, actuando en nombre y representación de **G.E.T. SECURE ID CORP.**, sociedad mercantil constituida y existente de acuerdo con las leyes del Estado de Delaware, EE.UU., con Identificación Fiscal Número 46-5107943, y domicilio social en 230 Third Avenue, Waltham, MA 02451 EE.UU., en virtud de los Poderes que me han sido otorgados por la Junta Directiva de la compañía, en mi calidad de PRESIDENTE de la misma, en fecha 21 de febrero de 2025, por medio del presente documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024- 0001**, declaro **BAJO LA MAS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

A. Que la experiencia de **G.E.T. SECURE ID CORP.** en el proyecto de licencias de conducir móviles en Ecuador satisface los siguientes requisitos para la licitación, modificados por las Preguntas y Respuestas proporcionadas por la JCE y resumidas en la MATRIZ:

3.1.6.3 (a)- Requisitos de experiencia (no obligatorios)
MATRIZ 3.3.1

Más de una (1) experiencia, en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta. Al menos una de las referencias debe ser ISO 18013-5.

Y

5.4.5-Plantilla para Evaluación
MATRIZ SECCIÓN AUTO-EVALUACIÓN

(i) "Plan del proyecto" -El proveedor presenta la implementación, de por lo menos, un desarrollo de una solución, puesta en producción, de cédula digital, en una institución pública, de acuerdo a los requerimientos establecidos en el documento de especificaciones técnicas, y estar adheridas al estándar ISO 18013-5: 4 puntos.

(ii) "Experiencia" (acreditable con contratos celebrados con empresas miembros de un mismo grupo económico (empresas con accionistas en común) de los consorciados en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo serán válidos contratos de al menos proyectos de 100,000 cédulas en total, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

- 1 contratos: 1 punto.
- 2 contratos: 2 puntos.
- Más de 2 contratos: 3 puntos.

B. Que la experiencia de **G.E.T. SECURE ID CORP.** con el proyecto de licencia de conducir móvil en Ecuador puede ser validada con los siguientes datos:

Agencia Gubernamental: Ministerio de Telecomunicaciones y de la Sociedad de la Información ("MINTEL")
Dirección física: Av. 6 de Diciembre N25-75 y Av. Colón Edif. MINTEL, Planta Baja
Dirección electrónica: https://www.telecomunicaciones.gob.ec/
Nombre de contacto: Carlos Saavedra
Cargo de contacto: Subsecretario MINTEL
Teléfono: +(593) 986766257
Correo electrónico: carlos.saavedra@mintel.gob.ec

[firma en la página que continúa]

Esta Declaración Jurada ha sido hecha en la Ciudad de Waltham, MA USA, el día 21 del mes de febrero del año 2025.

Joshua M. Mármol

G.E.T. SECURE ID CORP.

G.E.T. Secure ID Corp.
Established 2013; Delaware, USA

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 21 day of February, 2025, before me, the undersigned notary public, Joshua Mármol personally appeared, proved to me through satisfactory evidence of identification, which were USA passport, to be the person who signed the preceding or attached document in my presence and who swore or affirmed to me that the contents of the document are truthful and accurate to the best of (his) (her) knowledge and belief.

Caitlyn E. Burns
Notary Public's Signature My Commission Expires December 29, 2028

CAITLYN E. BURNS
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
December 29, 2028

Señor:

José Manuel Infante R.
Presidente
Copy Solutions International, S. A.

Asunto: **Carta de referencia.**

Distinguido señor Infante:

Por medio de la presente, certificamos que la empresa **Copy Solutions International, S. A. (CSI)**, ha prestado servicios en la **JUNTA CENTRAL ELECTRORAL** desde el **26 de diciembre 2013** hasta el **26 de diciembre 2024**.

Durante este periodo, **Copy Solutions International, S. A.** ha demostrado un alto nivel de profesionalismo, responsabilidad y compromiso en la ejecución de sus labores. Sus servicios en:

- Suministro de más de 14MM de tarjetas PVCPET para la impresión de la cédula.
- Suministro, instalación y mantenimiento de más de 300 equipos de solución de impresión Toppan, incluyendo suministros.
- Equipos periféricos para la captura y procesamiento biométrico.
- Entrenamiento a usuarios y formación técnica básica a soporte técnico de la JCE.

Estos servicios han sido de gran calidad, cumpliendo con los estándares exigidos y contribuyendo significativamente al buen funcionamiento de nuestra institución.

Destacamos especialmente su cumplimiento con los plazos establecidos, la eficiencia en la resolución de problemas y la disposición para atender cualquier requerimiento adicional.

Atentamente,

Américo Rodríguez
Director Nacional de Cedulación

edenorte
Edenorte Dominicana, S.A.

Santiago, R.D.
12 de febrero de 2025

Dirigido a: JUNTA CENTRAL ELECTORAL

Distinguidos señores:

Por medio de la presente, certificamos que la compañía **Copy Solutions International, S.A.**, identificada con el Registro Nacional de Contribuyentes (RNC) No. 1-01-89885-2, ha prestado servicios a EDENORTE Dominicana, S.A. desde el año 2013, desempeñándose como proveedor de alquiler de impresoras y soluciones tecnológicas.

Durante este tiempo, Copy Solutions International ha demostrado un alto nivel de profesionalismo, cumpliendo con los estándares de calidad requeridos y brindando un servicio eficiente y confiable. Sus responsabilidades han incluido la provisión, mantenimiento y gestión de soluciones de impresión y documentación, garantizando un soporte técnico oportuno y adecuado.

Dado su historial de cumplimiento y desempeño satisfactorio en la ejecución de sus servicios, emitimos esta carta como referencia para su participación en el proceso de licitación **JCE-CCC-LPI-2024-0001 de la Junta Central Electoral.**

Para cualquier consulta adicional, quedamos a su disposición.

Esta solicitud se expide a favor de la parte interesada, en Santiago de los Caballeros, República Dominicana, a los 12 días del mes de febrero de 2025.

Muy atentamente,

EDENORTE DOMINICANA, S.A.
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

Luduing Rodríguez
Director TI
EDENORTE DOMINICANA, S.A.

Cámara de Diputados de la República Dominicana

SECRETARIA GENERAL ADMINISTRATIVA

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo, R.D.

Santo Domingo, D. N.
12 de febrero del 2025.

Señores:
Junta Central Electoral
Ciudad.-

Atención: Proceso con número de referencia
JCE-CCC-LPI-2024-0001

Distinguidos señores:

Cortésmente hacemos constar que esta institución mantiene excelentes relaciones comerciales con la compañía **Copy Solutions International, S.A.**

La compañía **Copy Solutions International, S.A.**, ha participado en varios procesos de compras y servicios, en estos momentos tiene el suministro de equipos de impresión en diversas áreas de la institución, con un tiempo aproximado de más de 10 años, ofreciendo productos y servicios de excelente calidad.

Esta certificación se expide a solicitud de la parte interesada, cualquier información adicional comunicarse a los números 809-535-2626 Ext. 3048/3050/3051.

Muy cortésmente,

CAMARA DE DIPUTADOS

Lic. Elvira Méndez Medina
Secretaria General Administrativa

EM/YJ-

Ayuntamiento del Distrito Nacional
República Dominicana
DIRECCION DE TECNOLOGIA DE LA INFORMACION

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo, R.D.

Santo Domingo, D. N.
17 de febrero de 2025

A quien pueda Interesar

Por medio de la presente, certificamos que la empresa Copy Solutions International identificada con el Registro Nacional de Contribuyentes (RNC) 101-89885-2 ha prestado servicios al Ayuntamiento del Distrito Nacional desde año 2019, desempeñándose como proveedor de alquiler de impresoras y soluciones tecnológicas.

Durante la ejecución de dicho contrato, la empresa ha cumplido conforme lo contratado, demostrando profesionalismo, eficiencia y compromiso con los estándares requeridos.

Emitimos esta carta como constancia de su desempeño y como referencia para el proceso de licitación No. JCE-CCC-LPI-2024-0001 de la Junta Central Electoral.

Gracias al esfuerzo y buen trabajo desarrollado por la empresa **Copy Solutions International** se encuentra dentro de nuestra lista de proveedores.

Atentamente,

AYUNTAMIENTO DEL DISTRITO NACIONAL DIRECCION DE TECNOLOGIA DE LA INFORMACION

Francisco Faña Martinez, ISC, MBA, PFC
Director de tecnología de la información
Email: Francisco.fana@adn.gob.do
Tel Ofic: 809-535-1181 ext. 1440
Flota: 809-272-4556

BANCO POPULAR DOMINICANO S.A. - BANCO MÚLTIPLE
AV. JOHN F. KENNEDY #20, APARTADO 1441 - ZONA POSTAL 1
SANTO DOMINGO, REPÚBLICA DOMINICANA

TEL: 809-544-5000
www.popularenlinea.com
RNC 101010632

Filial del Grupo Popular, S.A.

POPULAR®

13 de febrero de 2025

Santo Domingo, Rep. Dom.

COPY SOLUTIONS INTERNATIONAL, S.A. RNC 101836852 Santo Domingo, R.D.

Señores: JUNTA CENTRAL ELECTORAL

Sus manos

Estimados señores:

Mediante esta carta, hacemos constar que **COPY SOLUTIONS INTERNATIONAL** sociedad comercial organizada y existente de conformidad con las leyes de la República Dominicana, con el número de RNC: 1-01-89885-2 y Registro Mercantil No. 20849SD con su domicilio y asiento principal ubicado en la Calle José Andrés Aybar Castellanos, No 153, Santo Domingo, República Dominicana, ofrecen sus **servicios especializados de Onbase para gestión de procesos y documentación ECM a BANCO POPULAR DOMINICANO, S.A., BANCO MÚLTIPLE** desde el año dos mil catorce (2014).

Esta carta se expide a solicitud de la parte interesada y de manera confidencial para fin único de utilizarla como referencia, a los trece (13) días del mes de febrero del año dos mil veinticinco (2025).

Sin más por el momento, se despide,

Atentamente,

Ayeisa De los Santos Figueroa

Digitally signed by Ayeisa De los Santos Figueroa
Date: 2025.02.13 10:29:00 -04'00'

Ayeisa De Los Santos
Vicepresidente
Área Gestión de Abastecimiento

Este documento fue firmado de manera electrónica, por lo que su entrega debe permanecer en formato digital.

Carta de Certificación de Propiedad y Manufactura de Impresoras, PKI y Mobile ID

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 1-30-98852 Santo Domingo, R.D.

The Commonwealth of Massachusetts
William Francis Galvin - Secretary of the Commonwealth

Apostille

(Convention de la Haye du 5 Octobre 1961)

1. Country: United States Of America

This Public Document

2. Has been signed by: Caitlyn E. Burns

3. Acting in the capacity of: Notary Public

4. Bears the seal/stamp of: Caitlyn E. Burns

Whose commission expires on: 12/29/2028

Certified

5. At: Boston, Massachusetts 6. The: January 27, 2025

7. By: The Secretary of Commonwealth

8. No.: 2670496

9. Seal/Stamp: *(Great Seal of the Commonwealth)*

10. Signature:

William Francis Galvin
Secretary of the Commonwealth

Prepared By: EPanico

Whosoever undersigned, **Ms. Maysoon F. Jamal**, of Lebanon, of legal age, married, bearer of Lebanese Passport No. LR3118926, domiciled and resident in Dubai, UAE, acting in the name and representation of **GET INTERNATIONAL FZCO**, a commercial company organized and existing in accordance with the laws of Dubai, UAE, with Tax Registration Number 104335821500001, and registered office in K18, Dubai Airport Free Zone (DAFZA), Dubai, UAE, in accordance with the powers granted to me by the Board of Directors of the company, in my capacity as MANAGER of the same,

Quien suscribe, **Sra. Maysoon F. Jamal**, de Líbano, mayor de edad, casada, portadora del Pasaporte Libanés nº LR3118926, domiciliada y residente en Dubái, EAU, actuando en nombre y representación de **GET INTERNATIONAL FZCO,** sociedad mercantil constituida y existente de acuerdo con las leyes de Dubái, EAU, con Número de Registro Fiscal 104335821500001, y domicilio social en K18, Dubai Airport Free Zone (DAFZA), Dubai, EAU, de acuerdo con los poderes que me han sido otorgados por la Junta Directiva de la sociedad, en mi calidad de GERENTE de la misma,

And/Y

Mr. Joshua M. Mármol, of the USA, of legal age, married, bearer of USA Passport No. 566385611, domiciled and resident in Waltham, MA USA, acting in the name and representation of **G.E.T. SECURE ID CORP.**, a commercial company organized and existing in accordance with the laws of the State of Delaware, USA, with Tax Identification Number 46-5107943, and registered office in 230 Third Avenue, Waltham, MA 02451 USA, in accordance with the powers granted to me by the Board of Directors of the company, in my capacity as PRESIDENT of the same,

Sr. Joshua M. Mármol, de EE.UU., mayor de edad, casado, titular del Pasaporte de EE. UU. nº 566385611, domiciliado y residente en Waltham, MA EE. UU, actuando en nombre y representación de **G.E.T. SECURE ID CORP.,** sociedad mercantil constituida y existente de acuerdo con las leyes del Estado de Delaware, EE.UU., con Identificación Fiscal Número 46-5107943, y domicilio social en 230 Third Avenue, Waltham, MA 02451 EE.UU., en virtud de los Poderes que me han sido otorgados por la Junta Directiva de la compañía, en mi calidad de PRESIDENTE de la misma,

On **January 17, 2025**, by means of this document, and in response to the requirements of the International Public Bidding, Ref.: **JCE-CCC-LPI-2024- 0001**, WE DECLARE **UNDER THE MOST SOLEMN FAITH OF THE OATH,** the following:

En fecha 17 de enero de 2025, por medio del presente documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024- 0001**, DECLARAMOS **BAJO LA MAS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

1) That we are jointly the official manufacturers of the personalization solution "GET CLM600". / Que somos conjuntamente los fabricantes oficiales de la solución de personalización «GET CLM600».

2) That we are the jointly the developers and owners of the PKI software "GET Trust" and its copyrights. / Que somos conjuntamente los desarrolladores y propietarios del software PKI «GET Trust» y sus derechos de autor.

3) That we are jointly the developers and owners of the mobile identification software solution "GET mID" and its copyrights. / Que somos conjuntamente los desarrolladores y propietarios de la solución de software de identificación móvil "GET mID" y de sus derechos de autor.

4) That we are offering the GET CLM600, the GET Trust and GET mID through the consortium in which we are participating for the above-referenced tender. / Que estamos ofreciendo GET CLM600, GET Trust y GET mID a través del consorcio en el que participamos para la licitación arriba mencionada.

5) That either of **GET INTERNATIONAL FZCO** or **G.E.T. SECURE ID CORP.** are authorized to sign any documents required of the manufacturer/developer/owner of the GET CLM600, the GET Trust and GET mID that are required for the above-referenced tender. / Que tanto **GET INTERNATIONAL FZCO** como **G.E.T. SECURE ID CORP.** están autorizados a firmar cualquier documento requerido del fabricante/desarrollador/propietario de GET CLM600, GET Trust y GET mID que se requieran para la licitación arriba mencionada.

[signature page to follow / firma en la página que continúa]

This Affidavit has been made in the City of Waltham, MA USA, on the 17th day of the month of January of the year 2025.

Esta Declaración Jurada ha sido hecha en la Ciudad de Waltham, MA USA, el día 17 del mes de enero del año 2025.

Maysoon F. Jamal
GET INTERNATIONAL FZCO

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 17 day of January 2025 before me, the undersigned notary public, Maysoon Jamal personally appeared, proved to me through satisfactory evidence of identification, which were Lebanese passport, to be the person who signed the preceding or attached document in my presence and who swore or affirmed to me that the contents of the document are truthful and accurate to the best of (his) (her) knowledge and belief.

Caitlyn E. Burns
Notary Public's Signature My Commission Expires December 29, 2028

CAITLYN E. BURNS
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
December 29, 2028

Joshua M. Mármol
G.E.T. SECURE ID CORP.

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 17 day of January 2025 before me, the undersigned notary public, Joshua Marmol personally appeared, proved to me through satisfactory evidence of identification, which were USA passport, to be the person who signed the preceding or attached document in my presence and who swore or affirmed to me that the contents of the document are truthful and accurate to the best of (his) (her) knowledge and belief.

Caitlyn E. Burns
Notary Public's Signature My Commission Expires December 29, 2028

CAITLYN E. BURNS
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
December 29, 2028

TRADUCCIÓN OFICIAL: Carta de Certificación de Propiedad y Manufactura de Impresoras, PKI y Mobile ID

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

La Comunidad de Massachusetts

William Francis Galvin - Secretario de la Comunidad

APOSTILLE
(Convention de La Haye du 5 octobre 1961)

1. País: Estados Unidos de América

Este documento público

2. Ha sido firmado por: Caitlyn E. Burns
3. Actuando en su calidad de: Notario Público
4. Llevando el sello/timbre de: Caitlyn E. Burns
cuya comisión expira el: 29/12/2028

Certificado

5. En: Boston, Massachusetts
6. Este: 27 de enero de 2025
7. Por: El Secretario de la Comunidad
8. Número: **2670496**
9. Sello/Timbre: el Gran Sello de la Comunidad
10. Firma: Ilegible, William Francis Galvin, Secretario de la Comunidad

Lleva el sello dorado de la Comunidad lacrado con cintas azules

Preparado por **EPanico**

Quien suscribe, **Sra. Maysoon F. Jamal**, del Líbano, mayor de edad, casada, portadora del Pasaporte Libanés Nº LR3118926, domiciliada y residente en Dubái, Emiratos Árabes Unidos, actuando en nombre y representación de **GET INTERNATIONAL FZCO**, sociedad comercial organizada y existente en conformidad con las leyes de Dubái, Emiratos Árabes Unidos, con Número de Registro Fiscal 104335821500001, y domicilio social en K18, Dubai Airport Free Zone (DAFZA), Dubai, Emiratos Árabes Unidos, de acuerdo con los poderes que me han sido otorgados por la Junta Directiva de la compañía, en mi calidad de GERENTE de la misma,

Y

Sr. Joshua M. Mármol, estadounidense, mayor de edad, casado, titular del Pasaporte de estadounidense Nº 566385611, domiciliado y residente en Waltham, MA, Estados Unidos de América, actuando en nombre y representación de **G.E.T. SECURE ID CORP.**, sociedad comercial organizada y existente en conformidad con las leyes del Estado de Delaware, Estados Unidos de América, con Identificación Fiscal Número 46-5107943, y domicilio social en 230 Third Avenue, Waltham, MA 02451, Estados Unidos de América, en virtud de los Poderes que me han sido otorgados por la Junta Directiva de la compañía, en mi calidad de PRESIDENTE de la misma,

En fecha **17 de enero de 2025**, por medio del presente documento, y en respuesta a los requerimientos de la Licitación Pública Internacional, Ref.: **JCE-CCC-LPI-2024- 0001**, DECLARAMOS **BAJO LA MAS SOLEMNE FE DEL JURAMENTO**, lo siguiente:

1) Que somos conjuntamente los fabricantes oficiales de la solución de personalización «GET CLM600».
2) Que somos conjuntamente los desarrolladores y propietarios del software PKI «GET Trust» y sus derechos de autor.
3) Que somos conjuntamente los desarrolladores y propietarios de la solución de software de identificación móvil "GET mID" y de sus derechos de autor.
4) Que estamos ofreciendo GET CLM600, GET Trust y GET mID a través del consorcio en el que participamos para la licitación arriba mencionada.

5) Que tanto **GET INTERNATIONAL FZCO como G.E.T. SECURE ID CORP.** están autorizados a firmar cualquier documento requerido del fabricante/desarrollador/propietario de GET CLM600, GET Trust y GET mID que se requieran para la licitación arriba mencionada.

Esta Declaración Jurada ha sido hecha en la Ciudad de Waltham, MA, Estados Unidos de América, el día 17 del mes de enero del año 2025.

Sinceramente,
Firma ilegible
Maysoon Jamal
GET INTERNATIONAL FZCO

COMUNIDAD DE MASSACHUSETTS
CONDADO DE MIDDLESEX

A los 17 días de enero de 2025, compareció ante mí, notario público que suscribe, el Sr. Maysoon Jamal, a quien conozco personalmente, y quien probó ante mí mediante evidencia de identificación satisfactoria, que era el pasaporte libanés, ser la persona cuyo nombre firma el documento precedente o anexado en el mismo ante mi presencia.

Firma de Caitlyn E. Burns
Notario Público
Mi comisión expira el 29 de diciembre de 2028

CAITLYN E. BURNS
Notario Público
COMUNIDAD DE MASSACHUSETSS
Mi comisión expira el
29 de diciembre de 2028

Sinceramente,
Firma ilegible
Joshua M. Mármol
G.E.T. SECURE ID CORP.

COMUNIDAD DE MASSACHUSETTS
CONDADO DE MIDDLESEX

A los 17 días de enero de 2025, compareció ante mí, notario público que suscribe, el Sr. Joshua M. Mármol, a quien conozco personalmente, y quien probó ante mí mediante evidencia de identificación satisfactoria, que era el pasaporte estadounidense, ser la persona cuyo nombre firma el documento precedente o anexado en el mismo ante mi presencia.

Firma de Caitlyn E. Burns
Notario Público
Mi comisión expira el 29 de diciembre de 2028

CAITLYN E. BURNS
Notario Público
COMUNIDAD DE MASSACHUSETSS
Mi comisión expira el
29 de diciembre de 2028

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los cuatro (4) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 144/25.

Ana María Feria

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Apostille
(Convention de La Haye, du 5 octobre 1961)

1. País: Estados Unidos de América
   Este documento público
2. Ha sido firmado por Jeffrey W. Bullock
3. Actuando en su calidad de Secretario de Estado del Estado de Delaware
4. Llevando el sello/timbre de la Secretaría de Estado

Certificado

5. En: Dover, Delaware
6. Este 13 de mayo del Año del Señor 2024
7. Por: Secretario de Estado; Departamento de Estado de Delaware
8. No. 203453718
9. Sello/Timbre: Sello del Estado de Delaware

10.Firma Illegible
Jeffrey W. Bullock, Secretario de Estado

Lleva estampado el sello dorado del Estado de Delaware

DELAWARE
El Primer Estado

Yo, Jeffrey W. Bullock, Secretario de Estado del Estado de Delaware, por este medio certifico que el anexo es una copia fiel y exacta del Certificado de Incorporación de "G.E.T. SECURE ID CORP.", depositado en estas Oficinas el dieciocho de diciembre del Año del Señor 2013, a las 04:22 horas de la tarde.

Firmado por Jeffrey W. Bullock, Secretario de Estado. Contiene el sello de la Oficina de la Secretaría del Estado

5452065 8100
SR# 20242051934

Autenticación: 203453717
Fecha: 13-05-14

Usted puede verificar este certificado en línea en corp.delaware.gov/authver.shtml

Estado de Delaware
Secretaría de Estado
División de Corporaciones
Entregado 04:38 pm 18/12/2013
DEPOSITADO a las 04:22 pm 18/12/2013
SRV 131446339 – Número Expediente 5452065

CERTIFICADO DE INCORPORACION

PRIMERO: El nombre de esta corporación será **G.E.T. SECURE ID CORP.**

SEGUNDO: La oficina registrada de esta Corporación en el Estado de Delaware estará ubicada en el 2711 Centerville Road, Suite 400, Wilmington, Condado de New Castle, Delaware 19808 y el nombre del agente registrado de la corporación en el Estado de Delaware, en esa dirección es The Company Corporation.

TERCERO: El propósito de la Corporación será:

comprometerse en cualquier acto o actividad legal para las cuales se puedan organizar las corporaciones bajo la Ley General de Corporaciones de Delaware.

CUARTO: El número total de acciones del capital que la Corporación tiene autorización para emitir es de Mil (1.000) acciones comunes, sin valor par.

QUINTO: El nombre y la dirección del fundador es como sigue:

The Company Corporation
2711 Centerville Road
Suite 400
Wilmington, Delaware 19808

SEXTO: La Junta de Directores tendrá todo el poder para adoptar, enmendar o revocar los estatutos.

SÉPTIMO: Ningún director actual o anterior de la Corporación será personalmente responsable ante la Corporación o ante sus accionistas por daños monetarios causados por cualquier violación al deber fiduciario de ese director, como director. Sin tomar en consideración la oración que antecede, un director será responsable como previsto en la ley aplicable, (i) por violación como Director a su deber de lealtad a la Corporación o a sus accionistas; (ii) por actos u omisiones que no sean de buena fe o que incluyan mala conducta intencional o conocimiento de violación a la ley; (iii) en conformidad con la Sección 174 de la Ley General de Corporaciones de Delaware, o (iv) cualquier transacción de la que el director derive un beneficio personal indebido. Ninguna enmienda o derogación a este Artículo Séptimo aplicará o tendrá efecto sobre la obligación o presunta responsabilidad del director actual o anterior de la Corporación por, o, con respecto a algún acto u omisión de ese director que ocurra antes de la fecha de esa enmienda.

EN FE DE LO CUAL, el suscrito, siendo el fundador antes mencionado, ha ejecutado, firmado y reconocido este certificado de incorporación, este dia 18 de diciembre de 2013.

The Company Corporation, Fundador

Por: Firma ilegible
Nombre: William Bartz
Secretario Adjunto

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los diez (10) días del mes de junio del año dos mil veinticuatro (2024), habiéndola inscrito en el registro a mi cargo, bajo el No. 912/24.

Ana María Feria

MINISTERIO PÚBLICO
CENTRO DE ATENCIÓN AL CIUDADANO DISTRITO NACIONAL

INTERPRETE JUDICIAL DE JUZGADO DE 1ra INSTANCIA
LICDA. ANA MARIA FERIA
DEL DIST. NAC. SANTO DOMINGO, D.N.

Declaración Jurada de no utilización de Materiales patentados en la Tarjeta de Policarbonato con chip sin contacto

SELP

Paris, 26 de junio, 2024

CSI CONSOLUTIONS INTERNATIONAL S.A. RNC 101898852 Santo Domingo, R.D.

DECLARACION JURADA
CERTIFICADO DE CUMPLIMIENTO DE ESPECIFICACIONES

A QUIEN INTERESE:

El abajo firmante, **Bastien BLANC,** actuando en mi carácter de representante de la empresa SELP SAS., una empresa constituida bajo las leyes de Francia en el registro mercantil de Périgueux, bajo el No. 351 667 928, que tiene su sede social en 187 Allées des Plagnes, 24340 Mareuil en Périgord, Francia, en virtud de las facultades que me confiere certifico que:

Las tarjetas de identidad en policarbonato con chip sin contacto para el **"Pliego de Condiciones especificas destinado a la contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)"**, con número de procedimiento JCE-CCC-LPI-2024-0001, **cumplen con los requisitos solicitados, mostrados a continuación:**

- La construcción del cuerpo de la tarjeta está diseñada sin capas/materiales patentados que limitarían el abastecimiento de materiales de producción de tarjetas a proveedores dedicados.
- El cuerpo de la tarjeta en blanco y el proceso de personalización de la misma en combinación no constituirán una solución dependiente o patentada que excluya a los proveedores de tarjetas y/o sistemas de personalización.

EN NOMBRE DE SELP

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tél. : 05 53 60 84 44 - Fax : 05 53 60 84 45
SIRET : 351 667 928 00011

Bastien BLANC
Representante
SELP SAS

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC
apposée ci-contre

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC 101859852
Santo Domingo, R.D.

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *République française* REPUBLIQUE DOMINICAINE

Le présent acte public

2. a été signé par Me MILLER

3. agissant en qualité de Notaire

4. est revêtu du sceau timbre de Son étude

Atteste

5. à Paris 10 JUIL. 2024

6. le

7. par le Procureur général près la Cour d'appel de Paris

8. sous n° 1287

9. Sceau SYLVIE SCHLANGER 10. Signature

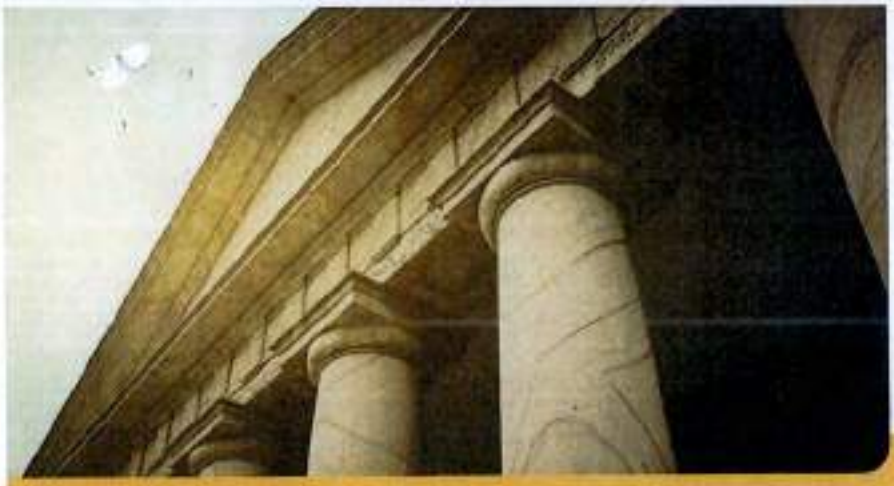
PROCUREUR GÉNÉRAL

L'Apostille confirme uniquement l'authenticité de la signature, du sceau ou timbre apposé sur le document. Elle ne signifie pas que le contenu du document est approuvé par la République française ou ses autorités.

COUR D'APPEL DE PARIS

COUR D'APPEL DE PARIS

Ficha Técnica del Chip sin contacto



NXP® JCOP® Java Card™ OS for SmartMX2 Secure Microcontrollers

SOLUTIONS INTERNATIONAL S.A.
RNC
Santo Domingo, R.D.

JCOP 4: The Most Advanced Java Card OS for Secure Identity Applications

JCOP 4 is a secure, field-proven, vendor-independent OS for secure identity chip-card applications. It provides multi-application support for contact, contactless, and dual communication interfaces, and delivers benchmark transaction performance for security documents.

KEY FEATURES

- >1 billion devices powered by JCOP already deployed in the field
- Best-in-class in terms of performances with an e-Passport SAC transaction in less than 2s
- Java Card v3.0.5 Classic Edition
- GlobalPlatform®
  - GP v2.2 ID Configuration
  - GP v2.2 Mapping Guidelines configuration v1.0.1
  - GP v2.3 Common Implementation Configuration v2.0
- ISO 7816-3 T=0, T=1
- ISO 14443 (up to 848kbps)
- Dual-interface support
- Support of DES, 3DES, AES, RSA, ECC and SHA via dedicated hardware-based coprocessors
- Operating System located in ROM boosting execution performance
- Available Non-Volatile Memory (NVM) for applications and personalization data up to 180kB
- Highly flexible feature and Applet selection for FLASH preloading for customer-specific products
- MIFARE Plus® / MIFARE Classic® EV1 or MIFARE® DESFire® EV2 contactless IC implementations
- Support (optional)
  - Korean SEED support (optional)
  - Match-on-Card (optional)
- Common Criteria EAL 6+ certified
- EMVCo™ approved
- FIPS certified

KEY BENEFITS

- Unique platform supports convergence of secure identity, payment and transport, increasing flexibility while reducing cost and complexity
- Easy implementation with full range of certified applets available for loading to FLASH, improving time-to-market, offering highest customization capabilities
- Optimized for high performance OS initialization and personalization for excellent machine utilization and throughput
- JCOP best-in-class transaction speed – from border control gates to contactless payment terminals, and automatic fare/collection schemes – enabling a unique and differentiated customer experience
- Trusted Java Card OS Open Platform based on current and future NXP secure ICs with highest certification security level, ensuring reliable project deployment

APPLICATIONS

- National eID
- Electronic Passport
- Electronic Driver's License Card
- Electronic Health and Social Benefits Cards
- ePKI / eServices / Digital Signature Card
- Payment and Micro Payment
- Public Transport
- Logical and Physical Access

Common Criteria EAL 6+ certified and EMVCo approved, JCOP 4 is optimized for use with NXP's SmartMX3 family, a line of secure microcontrollers with hardware accelerators.

JCOP 4 supports every SmartMX3 crypto-algorithm and delivers best-in-class transaction performance and personalization time (with ~50% reduced perso time compared to JCOP 3).

Customers can develop their own Java Card applets based on JCOP and have them loaded to FLASH memory, or get a head start on design by using NXP's available applets.

The NXP offering for JCOP includes cost-effective solutions based on the first advanced CMOS040 technologies available on the market with more than >1B FLASH secure ICs sold.

COPY SOLUTIONS INTERNATIONAL S.A. RNC: 101 [illegible] 852 Santo Domingo

PRODUCT FEATURES

ITEM	JCOP 4
Specifications and Features	
Java Card Version	3.0.5 Classic Edition
GlobalPlatform Version	2.3
Secure Channel Protocol (SCP)	SCP 01, 02 and 03
Delegated Management	Yes
Secure Box	Yes
Physical Unclonable Function (PUF)	Yes
Available Memory and Technology	
FLASH (available before loading MIFARE, Applets, OS Addons)	up to 180kB
CMOS Technology	CMOS040
MIFARE IC	
MIFARE Classic / Plus Implementation	EV1 – up to 4kB (optional)
MIFARE DESFire Implementation	EV2 – up to 8kB (optional)
Transaction Performance	
SAC Electronic Passport	< 2s
MasterCard Transaction Time	< 200ms
Cryptography	
DES/TDES	56b, 112b and 168b
AES	256b
RSA	4096b
ECC GF(p)	521b
SHA	128b, 224b, 256b, 384b and 512b
Certifications and Approvals	
EMVCo Platform Approval	Yes
VISA Approvals	Yes
MasterCard PIC (TAS & CAST)	Yes
EMVCo CPA	Yes
Common Criteria for OS	EAL 6+ (AVA_VAN.5, ALC_FLR.1 and ASE_TSS.2)
Federal Information Processing Standard (FIPS)	140-2 level 3

APPLETS

Name	Specification & Features
Secure Identity Application Suite	• ICAO BAC (CC EAL4+) • ICAO SAC / EAC (PACEv2) (CC EAL5+) • Secure Signature Creation Device – SSCD (CC EAL5+) • National eID • European Citizen Card • PKI / Digital Signature • eIDAS • International Driving License • European Health Insurance Card • Fingerprint Match-On-Card • One Time Password
VISA	VSDC2.9, VSDC2.8.1G1
MasterCard M/Chip Advance	M/Chip Advance v1.2 Specification including Data Storage and MMAR
EMVCo CPA	• EMV Common Payment • Application Specification v1 Dec 2005

www.nxp.com

© 2018 NXP Semiconductors N.V. Date of release: July 2018. Document order number: JCOP4SECDAPPM REV.0
All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent – or other industrial or intellectual property rights.

TRADUCCIÓN OFICIAL: Ficha Técnica del Chip Sin Contacto

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

NXP® JCOP® Java Card™ OS para Microcontroladores Seguros SmartMX3®

JCOP 4: Java Card OS la tarjeta más avanzada para aplicaciones de identidad segura

JCOP 4 es un sistema operativo seguro, probado en campo e independiente del proveedor para aplicaciones de tarjetas de identificación con chip seguras. Proporciona soporte para múltiples aplicaciones de interfaces de comunicación con contacto, sin contacto y duales y ofrece rendimiento en las transacciones de referencia en los documentos de seguridad.

CARACTERISTICAS CLAVES

- >Mil millones de dispositivos alimentados por JCOP ya implementados sobre el terreno
- El mejor en su clase en términos de rendimiento con una transacción SAC para pasaporte electrónico en menos de 2 segundos
- Tarjeta Java v3.0.5 Edición Clásica
- Plataforma Global®
  - Configuración de identificación de GP v2.2
  - Pautas de mapeo de GP v2.2, configuración v1.0.1
  - Configuración de implementación común GP v2.3 v2.0
- ISO 7816-3 T=0, T=1
- ISO 14443 (hasta 848 kbps)
- Soporte de interfaz dual
- Compatibilidad con DES, 3DES, AES, RSA, ECC y SHA a través de coprocesadores dedicados basados en hardware
- Sistema operativo ubicado en ROM, mejorando el rendimiento de ejecución
- Memoria no volátil (NVM) disponible para aplicaciones y datos de personalización de hasta 180 kB
- Selección de funciones y subprogramas altamente flexibles para la precarga FLASH para productos específicos del cliente
- Implementaciones de circuitos integrados sin contacto MIFARE Plus® / MIFARE Classic® EV1 o MIFARE® DESFire® EV2
- Soporte (opcional)
  - Soporte para SEED en coreano (opcional)
  - Coincidencia en tarjeta (opcional)
- Certificación Common Criteria EAL 6+
- Aprobado por EMVCo™
- Certificado FIPS

BENEFICIOS CLAVES

- Convergencia de soportes de plataforma únicos para seguridad de la identidad, pago y transporte, aumentando la flexibilidad mientras reduce el costo y la complejidad.
- Fácil implementación en todos los rangos de las aplicaciones FLASH certificadas disponibles para cargar, aumentando el tiempo en el mercado, ofreciendo las más altas capacidades de normalización,
- Optimizando el más alto rendimiento para la inicialización y la personalización del sistema operativo para un excelente uso y rendimiento de la máquina.
- La mejor velocidad en transacciones de su clase, según JCOP (desde controles fronterizos hasta terminales de pago sin contacto y esquemas automáticos de tarifas y cobros), lo que permite una experiencia diferente y única al cliente.

- Confiable Plataforma Abierta del Sistema Operativo Java Card, basada en circuitos integrados NXP seguros, actuales y futuros, con el nivel de seguridad de certificación más alto, lo que garantiza una implementación confiable del proyecto

APLICACIONES

- DNI Electrónico Nacional
- Pasaporte Electrónico
- Licencia de Conducir Electrónica
- Tarjetas Electrónicas de Prestaciones Sociales y Sanitarias
- ePKI / eServices / Tarjeta de Firma Digital
- Pagos y Micropagos
- Transporte Público
- Acceso Lógico y Físico

JCOP4, que cuenta con la certificación Common Criteria EAL 6+ y la aprobación de EMVCo, está optimizado para su uso con la familia SmartMX3 de NXP, una línea de microcontroladores seguros con aceleradores de hardware.

JCOP4 es compatible con todos los algoritmos criptográficos SmartMX3 y ofrece el mejor rendimiento de transacciones y tiempo de personalización de su clase (con un 50 % menos de tiempo empleado por persona en comparación con JCOP 3).

Los clientes pueden desarrollar sus propios applets de Java Card basados en JCOP y cargarlos en la memoria FLASH, o empezar con ventaja en el diseño utilizando los applets disponibles de NXP.

La oferta de NXP para JCOP incluía soluciones rentables basadas en las primeras tecnologías avanzadas CMOS040 disponibles en el mercado, con más de 1.000.000 circuitos integrados seguros FLASH vendidos.

CARACTERISTICAS DEL PRODUCTO

ARTICULO	JCOP 4
Especificaciones y Caracteristicas	
Versión Java Card	Edición Clásica 3.0.5
Versión GlobalPlatform	2.3
Protocolo Canal Seguridad (SCP)	SCP 01, 02 y 03
Gestión Delegada	Sí
Caja Seguridad	Sí
Función Física no Clonable (PUF)	Sí
Memoria y Tecnología Disponible	
FLASH (disponible antes de cargar MIFARE, Applets, OS Addons)	Hasta 180kB
Tecnología CMOS	CMOS040
MIFARE IC	
MIFARE Clàsico / Implementación Plus	EV1-hasta 4kB (opcional)
MIFARE DESFire Implementación	EV2-hasta 8kB (opcional=
Rendimiento Transacción	
SAC Pasaporte Electrónico	< 2s
MasterCard Tiempo Transacción	< 200 ms
Criptografía	
DES/TDES	56b, 112b Y 168b
AES	256b
RSA	4096b

ECC GF(p)	521b
SHA	128b, 224b, 256b, 384b y 512b
Certificaciones y Aprobaciones	
Aprobación Plataforma EMVCo	Si
Aprobaciones VISA	Si
MasterCard PIC (TAS & CAST)	Si
EMVCo CPA	Si
Criterio Común del Sistema Operativo	EAL 6+ (AVA_VAN.5, ALC_FLR.1 y ASE_TSS.2)
Normativas Procedimientos Información Federal (FIPS)	140-2 Nivel 3

APPLETS

Nombre	Especificaciones & Características	
Conjunto Aplicaciones Identidad Segura	• ICAO BAC (CC EAL4+) • ICAO SAC / EAC (PACEV2) (CC EAL5+) • Dispositivo Creación Firma Digital – SSCD (CC EAL5+) • eID Nacional • Tarejta Ciudadanía Europea	• PKI / Firma Digital • eIDAS • Licencia Conducir Internacional • Tarjeta Seguro Salud Europeo • Tarjeta Coincidencias Huellas • Contraseña un solo Uso
VISA	VSDC2.9, VSDC2.8.1G1	
MasterCar M/Chip Advance	M/Chip Advance Especificación v 1.2, incluyendo Almacenaje de Datos y MMAR	
EMVCo CPA	• EMV Pago Común	• Especifiación Aplicación v1 Dic 2025

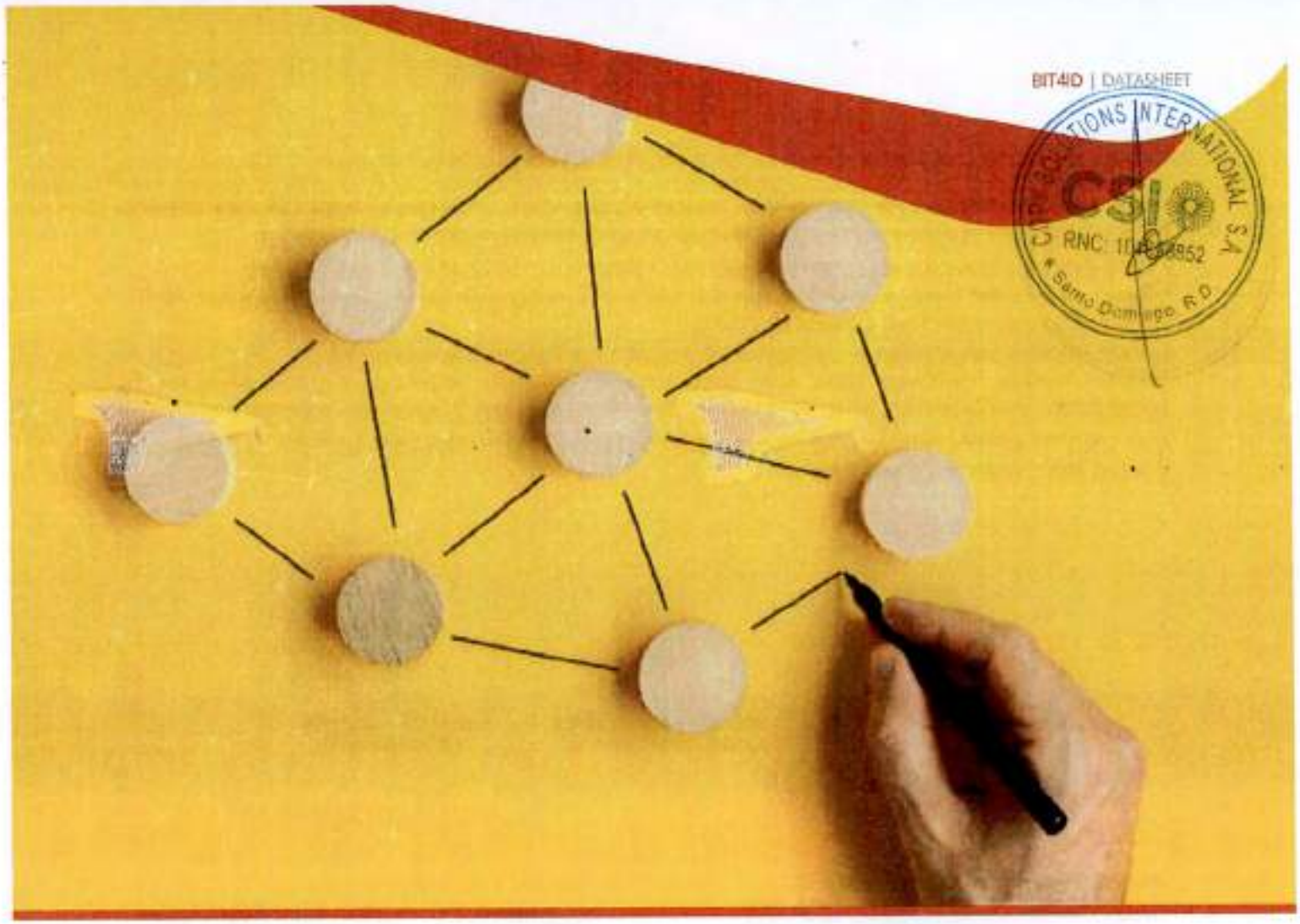
www.nxp.com

©2018 NXP Semiconductores N.V. Fecha Liberación: julio 2018, Número orden del documento: JCOP4SECIDPPA4 REV 0
Todos los derechos reservados. La reproducción en todo o en parte está prohibida sin el consentimiento escrito y previo del propietario de los derechos de autor. La información presentada en este documento no es parte de ninguna licitación ni contrato, creemos es correcta y confiable y puede ser cambiada sin notificación. El publicista no aceptará responsabilidad alguna por las consecuencias de su uso. La publicación no otorga ni implica ninguna licencia bajo patente – u otros derechos de propiedad industrial o intelectual.

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los doce (12) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 223/25.

Ana María Feria

Ficha Técnica del MiddleWare



Universal Middleware.

Strong authentication with cryptographic devices

The tool which provides the broadest support for different functionalities, such as: PKI, Strong authentication, smartcard logon, Single Sign-on, network access, VPN and remote access.

bit4id.com

bit4id

SECURITY FEATURES IN THIRD PARTY APPLICATIONS

The Universal Middleware for cryptographic devices is a strategic product that includes **software libraries to interface several smart cards and USB cryptographic tokens.** In particular, it includes:

- library module that exposes an API that supports PKCS#11 v2.11 / v2.40 / v3.0 specification;
- system module that exposes an API that supports Microsoft Cryptographic Service Provider (CryptoSPI/2006) and Cryptography API: Next Generation (CNG);
- Library module that exposes an API that supports MacOS X TokenD/CryptoTokenKit;
- system module "certificate store" that implements an automatic import of the credentials on the cryptographic device into the store "Personal" of the user (in Microsoft Windows environments).

Such modules provide various **programming interfaces**, enabling in third party applications the usage of cryptographic smart cards and tokens.

Reliability
Used by million of users in Europe for daily work

Portability
USB tokens can work without installation on the host pc

Compliancy
Support of all international reference standards

Main features

- Security features in third party applications
- Strong authentication/smart card logon to workstations, networks and applications using cryptographic smartcards/USB tokens
- Single sign-on to commercial/proprietary applications
- Creation and management of keypairs/credentials/certificates on cryptographic devices
- File and email encryption/decryption
- File and email digital signature

Standards:

PKCS#11
MS CryptoAPI / CSP / KSP-NG
MacOS X TokenD / CryptoTokenKit
X.509 v3
PC/SC
Java Card
SSL/TLS v1.2 and v1.3 with PSS IPsec

Almost all applications working with cryptographic cards in Italy and Spain use Bit4id Universal Middleware: a single software allows to work with a wide range of cryptographic cards and applications. The development of this package has been possible thanks to the Bit4id's extensive experience and know-how in the field of cryptographic cards.

Technical features

Supported Smartcards	
Idemia/Oberthur	ID-One COSMO 64K v.5, Cosmo V5 RSA 64K, Cosmo v7 64k, Cosmo v8.1 IAS and PIV, Cosmo V9, Cosmo V9.1
ST/Incard	Incrypto 34, T&S 2048, ~~jSIGN 2, jSIGN 3, jSIGN 4~~
NXP	JCOP 3, JCOP 4 ChipDoc
Others	Italian CNS | Italian CIE 3.0 | Spanish/Peruvian DNI
Applet (based on card)	CNS, ChipDoc, IDentity Applet (ID&Trust Ltd)
Interfaces	PKCS#1, 5, 7, 8, 10, 11, 12, 15 Microsoft CryptoSPI (CSP) Cryptography API Next Generation (CNG) MacOS X TokenD/CryptoTokenKit
Supported readers	PC/SC compliant smart card readers (Bit4id, Gemalto, OMNIKEY, SCM, etc.)
Operating Systems	Win 8, Win 8.1, Win 10, Win 11, Windows Server 2008 (+); MacOS 10.12 (+); Ubuntu 18.04 (+); RedHat E. 7.0 (+); Centos 7.0 (+), Fedora 28 (+), Debian 8.0 (+)

Some technical features may be subject to evolution/changes without prior notice

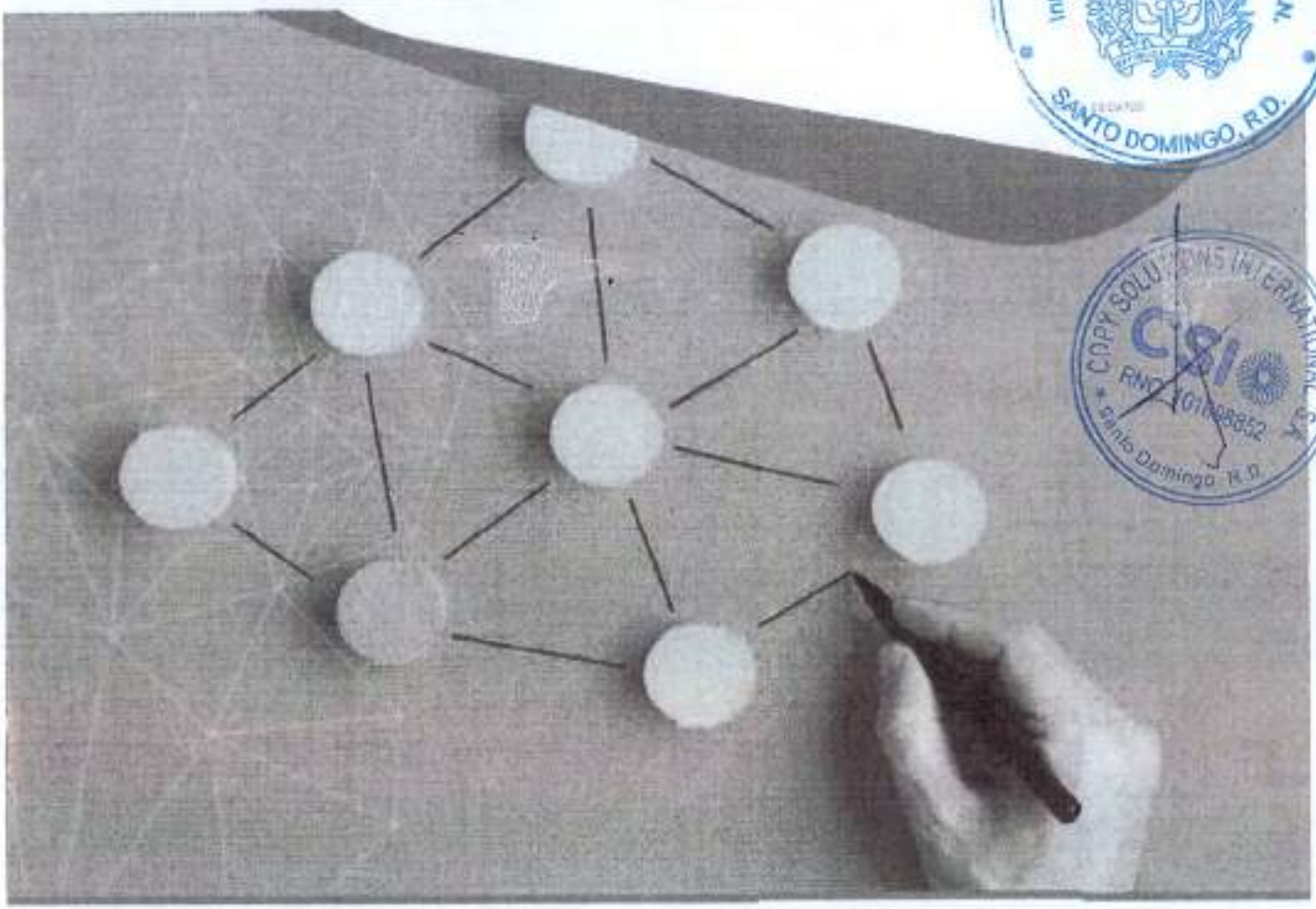
Página/Folio No.439 de 843

TRADUCCIÓN OFICIAL: Ficha Técnica del MiddleWare

Yo **LIC. SANTO C. SIERRA,** intérprete judicial, debidamente juramentada para el ejercicio de mis funciones **CERTIFICO** que he procedido a traducir las partes centrales de un documento escrito originalmente en Ingles, cuya versión en idioma Español de acuerdo a mi mejor el conocimiento es el siguiente:

LIC. SANTO C. SIERRA Intérprete Judicial 1ra Instancia D.N. SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL SRL RNC 101008852 Santo Domingo R.D.



Middleware universal.

Autenticación sólida

con dispositivos criptográficos

La herramienta que proporciona el soporte más amplio para diferentes funcionalidades, tales como: PKI, autenticación fuerte, inicio de sesión con tarjeta inteligente, inicio de sesión único, acceso a red, VPN y acceso remoto.

FUNCIONES DE SEGURIDAD EN APLICACIONES DE TERCEROS

El middleware universal para dispositivos criptográficos es un producto estratégico que incluye bibliotecas de software para interconectar varias tarjetas inteligentes y tokens criptográficos USB. En particular, incluye:

- Módulo de biblioteca que expone una API que admite la especificación PKCS#11 v2.11/v2.40/v3.0;
- Módulo de sistema que expone una API compatible con Microsoft Cryptographic Service Provider (CryptoSPI/2006) y Cryptography API: Next Generation (CNG);
- Módulo de biblioteca que expone una API compatible con MacOS X TokenD/CryptoTokenKit;
- Módulo de sistema "almacén de certificados" que implementa una importación automática de las credenciales del dispositivo criptográfico al almacén "Personal" del usuario (en entornos Microsoft Windows).

Estos módulos proporcionan varias interfaces de programación, permitiendo el uso de tarjetas inteligentes y tokens criptográficos en aplicaciones de terceros.

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC 101898852 Santo Domingo, R.D.

Flexibilidad

Portabilidad
Los tokens USB pueden funcionar sin instalación en la PC host.

Cumplimiento

Características principales

- Funciones de seguridad en aplicaciones de terceros

Redes y aplicaciones que utilizan criptografía.

- Inicio de sesión único en aplicaciones comerciales/propietarias
- Creación y gestión de pares de claves/solicitudes/certificados en dispositivos criptográficos

Estándares:

PKCS#11
MS CryptoAPI / CSP / KSP-NG
MacOS X TokenD / CryptoTokenKit
X.509 v3
PC/SC
Tarjeta Java
SSL/TLS v1.2 y v1.3 con PSS IPsec

Casi todas las aplicaciones que trabajan con tarjetas criptográficas en Italia y España utilizan Universal Middleware, un único software permite trabajar con una amplia gama de tarjetas criptográficas y aplicaciones. El desarrollo de este paquete ha sido posible gracias a la amplia experiencia y al know-how en el campo de las tarjetas criptográficas.

Características técnicas

Idemia/Oberthur	G-One COSMO 64K versión 5, Cosmo V5 RSA 64K, Cosmo v7 64k, Cosmo v8.1 IAS y PIV, Cosmo V9, Cosmo V9.1
S7/Incard	Incrypto 34, T&S 2048, JSIGN 2, JSIGN 3, JSIGN 4
NXP	
Otros	SNC italiano) CIE 3.0 italiano) Dnie español/peruano
Applet (cosido en tarjeta)	Subprograma de identidad (Identity Unit)
Interfaces	PKCS n.° 1, 5, 7, 8, 10, 11, 12, 15 Microsoft CryptoSPI (CSP) API de criptografía de próxima generación (CNG) MacOS X TokenD/CryptoTokenKit
Lectores compatibles	Lectores de tarjetas inteligentes compatibles con PC/SC (Bit4id, Gemalto, OMNIKEY, SCM, etc.)
Sistemas operativos	Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server 2008 (+); MacOS 10.12 (+); Ubuntu 18.04 (+); RedHat E. 7.0 (+); Centos 7.0 (+), Fedora 28 (+), Debian 8.0 (+)

Traducido a petición de la parte interesada y registrada en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Once (11) días del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

LIC. SANTO C. SIERRA Intérprete Judicial Cámara Penal Corte de Apelación D.N. SANTO DOMINGO, R.D.

PROCURADURÍA GENERAL DE LA REPÚBLICA DEPARTAMENTO DE ATENCIÓN AL CIUDADANO DISTRITO NACIONAL

Procuraduría General de la República
Confirme la validez de este documento ingresando el código QR en portal.servicios.pgr.gob.do
Código QR: 001-5202-3215274-3

Certificaciones ISO del Fabricante de las Tarjetas

ISO INTERGRAF Nivel Gobierno

INTERGRAF Certificate for Management of Security Printing Processes

Intergraf hereby certifies that, based on the results of the audit conducted by SQS, Swiss Association for Quality and Management Systems, Switzerland,

SELP SECURE (SELP SAS)

Rue Louis Pergaud, 16000 Angoulême, France

complies with ISO 14298:2021 "Management of Security Printing Processes" and with the relevant Intergraf requirements for this standard.

Certification Level: Governmental Level

Markets of Operation: National, International, Governmental, Non-Governmental organisations

Scope: Manufacturing and personalization of banking, identity and smart cards.

Reference Number of the Certificate: 202403693
Expiration Date: 13 April 2027

Brussels, 16 April 2024

For Intergraf

INTERGRAF

Beatrice Klose
Secretary General

For SQS

SQS

Felix Müller
CEO

CERTIFIÉ CONFORME À L'ORIGINAL
Bastien BLANC, CEO
15/05/2024

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC
apposée ci-contre

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tel. 05 53 60 84 44 - Fax. 05 53 60 84 45
SIRET 351 667 928 00011

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

COUR D'APPEL DE PARIS

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *République française* REPUBLIQUE DOMINICAINE

Le présent acte public

2. a été signé par Me Millier

3. agissant en qualité de Notaire

4. est revêtu du sceau/timbre de Son étude

Attesté

5. à Paris 23 MAI 2024

6. le

7. *par le Procureur général près la Cour d'appel de Paris*

8. sous n° 052

9. Sceau N2

10. Signature :

"L'Apostille confirme seulement l'authenticité de la signature, du sceau ou timbre sur le document. Elle ne certifie pas le contenu du document est correct ou que la République française approuve son contenu"

SYLVIE SCHLANGER
AVOCAT GÉNÉRAL

COUR D'APPEL DE PARIS

CERTIFIÉ CONFORME A L'ORIGINAL

TRADUCCIÓN OFICIAL: ISO INTERGRAF Nivel Gobierno

Yo, **LIC. SANTO C. SIERRA,** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en francés y cuya versión al español, según mi mejor conocimiento, es el siguiente:

LIC. SANTO C. SIERRA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

INTERGRAF Certificado para la Gestión de Procesos de Impresión de Seguridad

CSI CSV SOLUTIONS INTERNATIONAL S.A. PNC. 10-6852 Santo Domingo, R.D.

Intergraf certifica que, en base a los resultados de la auditoría realizada por SQS, Asociación Suiza de Sistemas de Gestión y Calidad, Suiza,

SELP SECURE (SELPSAS)

Rué Louis Pergaud, 16000 Angulema, Francia

Cumple con la norma ISO 14298:2021 "Gestión de procesos de impresión de seguridad" y con los requisitos de Intergraf pertinentes para esta norma.

Nivel de certificación:	Nivel Gubernamental
Mercados de Operación	Nacional, Internacional, Organizaciones gubernamentales, no gubernamentales
Alcance	Fabricación y personalización de tarjetas bancarias, de identidad y inteligentes.

Número de Referencia del Certificado: 202403693
Fecha de vencimiento: 13 de abril de 2027

Bruselas, 16 de abril de 2024

Firma ilegible, **INTERGRAF**

Beatriz Klose
Secretaria General

Para SQS

Firma ilegible, **SQS**

Félix Müller
Director General

Sr. Francois MILLIER
Notario de París, abajo firmante
Certifica la firma de
Señor BLANC
Adjunto aquí

CERTIFICADO
EN EL ORIGINAL
Bastien BLANC,
director ejecutivo
15/05/2024

SELP SAS
187 Avenida de las Plagnes
24340 MAREUIL-EN-PERIGORD
Tel: 05 53 69 84 44 – Fax: 05 53 60 84 45
SIRET: 351 667 928 00011

APOSTILLA
(Convención de la Haya del 5 de octubre de 1961)

1- País : **República Dominicana**

Este documento público

2- ha sido firmado por **Millier**

3- Actuar en Calidad **Notarial**

4- lleva el sello/timbre **Su estudio**

Certificado

5- en París 6- El día 23 de mayo de 2024

7- por E fiscal general del Tribunal de Apelación de París

8- Número: 652

9- Sello/sello 10- Firma

Firma ilegible

Este Apóstol certifica de manera única la autenticidad de la empresa, la calidad de la firma del documento que se ha actualizado y, en su caso, la identidad del vendedor o sello con que se cubre el documento público.

Firmado y Sellado
Sylvie SCHLANGER
Avocat General

Traducción a petición de la parte interesada y registrada en mí protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Catorce (14) días del mes de Junio del año Dos Mil Veinticuatro (2024).

LIC. SANTO E. SIERRA
INTERPRETE JUDICIAL
HELP

ISO 27001:2022

Bureau Veritas Certification

Bastien BLANC, Représentant légal le 17/01/2025

Tel. : 05 53 60 04 44 - Fax : 05 53 60 04 45 Notaire à Paris, soussigné
SIRET : 351 667 928 00011
Certifie la signature de M. BLANC apposée ci-contre

SELP ANGOULEME

RUE LOUIS PERGAUD 16000 ANGOULEME - France

Bureau Veritas Certification Holding SAS - UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2022

Scope of certification

SECURE ARTWORK DESIGN, EMBEDDING AND INITIALIZATTION OF SMART CARDS

CONCEPTION DE VISUELS SECURITAIRES, ENCARTAGE ET PERSONNALISATION DE CARTES A PUCES

Original cycle start date:	12 November 2015
Expiry date of previous cycle:	11 November 2024
Certification / Recertification Audit date:	18 December 2024
Certification / Recertification cycle start date:	12 November 2024
Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on:	11 November 2027

Certificate No.: FR094191 Version: 1 Issue date: 17 January 2025

Contrat number: 23090509

UKAS MANAGEMENT SYSTEMS 0008

Samuel DUPRIEU - President
Signed on behalf of BVCH SAS UK Branch

Certification Body Address: 5th Floor, 100 Lower Thames Street, London, EC3R 6DL, United Kingdom

Local Office: 1 place Zaha Hadid - 92400 Courbevoie

Further clarifications regarding the scope of this certificate the applicability of the management system requirements may be obtained by consulting the organization.
To check this certificate validity, please use the QR Code.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

COUR D'APPEL DE PARIS

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *République française* REPUBLIQUE DOMINICAINE

Le présent acte public

2. a été signé par Me NILLIER

3. agissant en qualité de Notaire

4. est revêtu du sceau timbre de Son étude

Attesté

5. à Paris

6. le 31 JAN 2025

7. par le Procureur général près la Cour d'appel de Paris

8. sous n° 2084

9. Sceau

Sylvie SCHLANGER
Avocat général

10. Signature

"L'Apostille confirme seulement l'authenticité de la signature, du sceau ou timbre sur le document. Elle ne signifie pas que le contenu du document est correct ou que la République française approuve son contenu"

COUR D'APPEL DE PARIS

TRADUCCIÓN OFICIAL: 27001:2022

Yo LIC. SANTO C. SIERRA, intérprete judicial, debidamente juramentada para el ejercicio de mis funciones **CERTIFICO** que he procedido a traducir las partes centrales de un documento escrito originalmente en francés, cuya versión en idioma Español de acuerdo a mí mejor el conocimiento es el siguiente:

CERTIFICADO DE CONFORMIDAD CON EL ORIGINAL Bastien BLANC, Representante Le legal 17/01/2025

SELP SAS
Callejón Placries 187
24340 MAREUIL-EN-PERIGORD
Teléfono: 05 53 60 84 44 - Fax: 05

SELP ANGULEME

CALLE LOUIS PERGAUD 16000 ANGOULEME Francia

El señor [illegible] Notario en Paris [illegible] Certifica la firma de Bastien BLANC Adjunto al presente

Certificación Bureau Veritas

Bureau Veritas Certification Holding SAS - Succursal del Reino Unido certifica que el sistema de gestión de la organización antes mencionada ha sido auditado y se ha determinado que cumple con los requisitos de las normas del sistema de gestión que se detallan a continuación.

ISO/IEC 27001:2022

Alcance de la certificación

DISEÑO DE ILUSTRACIONES SEGURAS, INCORPORACIÓN E INICIALIZACIÓN DE TARJETAS INTELIGENTES

DISEÑO DE VISUALES DE SEGURIDAD, INCRUSTACIONES Y PERSONALIZACIÓN DE TARJETAS INTELIGENTES

Fecha de inicio del ciclo original:	12 de noviembre de 2018
Fecha de caducidad del ciclo anterior:	11 de noviembre de 2024
Fecha de auditoría de certificación/recertificación:	18 de diciembre de 2024
Fecha de inicio del ciclo de certificación/recertificación:	12 de noviembre de 2024
Sujeto al funcionamiento satisfactorio continuo del Sistema de Gestión de la organización, este certificado caduca el:	11 de noviembre de 2027

Número de certificado: FR014031 Versión: 1 Fecha de emisión: 7 de enero de 2025

Número de contrato: 23090509

SISTEMAS 0008

Bureau Veritas Holdings Limited
en nombre de la sucursal británica de BVCH SAS

Dirección del organismo de certificación: 5th Floor, 100 Leman Square Street, London, EC1R 6DL, Reino Unido

Oficina local: 1 place Zaha Hadid 92400 Courbevoie

Para obtener más información sobre el alcance de este certificado y la aplicabilidad de los requisitos del sistema de gestión, consulte a la organización. Para comprobar la validez de este certificado, utilice el código QR.

Traducido a petición de la parte interesada y registrada en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Once (11) días del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

SANTO C. SIERRA Judicial Jurg 1ra [illegible] D.N. SANTO DOMINGO, R.D.

ISO 14001:2015

Bureau Veritas Certification

SELP

RUE LOUIS PERGAUD
16000 ANGOULEME
FRANCE

Bureau Veritas Certification France certifie que le système de management de l'organisme susmentionné a été audité et jugé conforme aux exigences de la norme :

ISO 14001:2015

Domaine d'activité

FABRICATION, IMPRESSION & PERSONNALISATION DE CARTES BANCAIRES, CARTES A PUCES ET DOCUMENTS D'IDENTITE.

DESIGN, MANUFACTURING & PERSONALIZATION OF BANKING, IDENTITY & SMART CARDS.

CERTIFIÉ CONFORME À L'ORIGINAL
Bastien BLANC, CEO
10/04/2024

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tél. : 05 53 60 84 44 - Fax : 05 53 60 84 45
SIRET : 351 667 928 00011

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC ci-dessus

Date de début du cycle de certification : **16 septembre 2023**

Sous réserve du respect des dispositions contractuelles et des résultats positifs des surveillances réalisées, ce certificat est valable jusqu'au : **15 septembre 2026**

Date d'expiration du cycle précédent : **07 juin 2023**

Date d'audit de certification/recertification : **26 mai 2023**

Date de certification originale : **16 septembre 2020**

par un autre organisme de certification avant le 02/03/23)

Certificat n° : **FR082609-1**

Affaire n° : **18363737**

Date de révision : **01 août 2023**

Samuel DUPRIEU - Président

Adresse de l'organisme certificateur : Bureau Veritas Certification France
1 Place Zaha Hadid - 92400 Courbevoie

Des informations supplémentaires concernant le périmètre de ce certificat ainsi que l'applicabilité des exigences du référentiel peuvent être obtenues en consultant l'organisme.
Pour vérifier la validité de ce certificat, veuillez utiliser le QR Code.

cofrac
CERTIFICATION DE SYSTEMES DE MANAGEMENT
ACCREDITATION n°4-0002
Liste des sites et portées disponibles sur www.cofrac.fr

Página/Folio No.456 de 843

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101088852
Santo Domingo

COUR D'APPEL DE PARIS

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *République française*

Le présent acte RÉPUBLIQUE DOMINICAINE

2. a été signé par Me Tillier

3. agissant en qualité de Notaire

4. est revêtu du sceau/timbre de Son étude

5. à Paris — Attesté 23 MAI 2024

6. le

7. *par le Procureur général près la Cour d'appel de Paris*

8. sous n° 649

9. Sceau : — 10. Signature :

"L'Apostille confirme seulement l'authenticité de la signature, du sceau ou timbre sur le document. Elle ne signifie pas que le contenu du document est correct ou que la République française approuve son contenu"

COUR D'APPEL

SYLVIE SCHLANGER
AVOCAT GENERAL

TRADUCCIÓN OFICIAL: ISO 14001:2015

Yo, **LIC. SANTO C. SIERRA,** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en francés y cuya versión al español, según mi mejor conocimiento, es el siguiente:

LIC. SANTO C. SIERRA Intérprete Judicial Primera Instancia D.N. SANTO DOMINGO, R.D.

Certificación Bureau Veritas

SELP

CALLE LOUIS PERGAUD
16000 ANGULEMA
FRANCIA

Bureau Ventas Certification France certifica que el sistema de gestión de la organización antes mencionada ha sido auditado y cumple con los requisitos de la norma:

ISO 14001:2015

Esfera de actividad

FABRICACIÓN, IMPRESIÓN Y PERSONALIZACIÓN DE TARJETAS BANCARIAS, TARJETAS CHIP Y DOCUMENTOS DE IDENTIDAD.

DISEÑO, FABRICACIÓN Y PERSONALIZACIÓN DE TARJETAS BANCARIAS, DE IDENTIDAD Y INTELIGENTES.

CSI COPY SOLUTIONS INTERNATIONAL S.A. FIN 1898852 Santo Domingo R.D.

CERTIFICADO
ORIGINAL
Bastien BLANC, director ejecutivo
10/04/2024

SELP SAS

187 Altée des Plagnes
24340 MAREUIL-EN-PERIGORD
Semejante. : 05 53 60 84 44 - Fax: 05 53 60 84 45
SIRET: 351 667 928 00011

Sr. Frangcis MILLIER
Notario de Paris, abajo firmante,
Certifica la firma de
Señor Blanc
Fijado arriba

Fecha de inicio del ciclo de certificación: **16 de septiembre de 2023**

Sujeto al cumplimiento de las disposiciones contractuales y de los resultados del seguimiento realizado anteriormente, este certificado es válido hasta: **15 de septiembre de 2026**

Fecha de vencimiento del ciclo anterior: **7 de junio de 2023**

Fecha de auditoría de certificación/recertificación: **26 de mayo de 2023**

Fecha de certificación original: **16 de septiembre de 2020**

por otro organismo de certificación antes del 03/02/23)

Número de certificado: FR082609-1

Número de caso: 18363737 ***Fecha de revisión:*** 1 de agosto de 2023

Samuel DUPRIEU – Presidente ***Firma ilegible***

Dirección del organismo de certificación: Bureau Veritas Certification Francia
1 plaza Zaha Hadid - 92400 Courbevoie

Se puede obtener información adicional sobre el alcance de este certificado, así como la aplicabilidad de los requisitos de la norma, consultando a la organización.

APOSTILLA
(Convención de la Haya del 5 de octubre de 1961)

16- País : **República Dominicana**

Este documento público

17- ha sido firmado por **Millier**

18- Actuar en Calidad **Notarial**

19- lleva el sello/timbre **Su estudio**

Certificado

20- en París 6- El día 23 de Mayo, 2024

16- por E fiscal general del Tribunal de Apelación de París

17- Número: 650

18- Sello/sello 10- Firma

Firma ilegible

Este Apóstol certifica de manera única la autenticidad de la empresa, la calidad de la firma del documento que se ha actualizado y, en su caso, la identidad del vendedor o sello con que se cubre el documento público.

Firmado y Sellado
Sylvie SCHLANGER
Avocat General

Traducido a petición de la parte interesada y registrada en mí protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Catorce (14) días del mes de Junio del año Dos Mil Veinticuatro (2024).

S.C.S / DPE
5184-12-8-96

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

LIC. SANTO C. SIERRA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

ISO 9001:2015

Bureau Veritas Certification

SELP

RUE LOUIS PERGAUD
16000 ANGOULEME
FRANCE

Bureau Veritas Certification France certifie que le système de management de l'organisme susmentionné a été audité et jugé conforme aux exigences de la norme :

ISO 9001:2015

Domaine d'activité

FABRICATION, IMPRESSION & PERSONNALISATION DE CARTES BANCAIRES, CARTES A PUCES ET DOCUMENTS D'IDENTITE.

DESIGN, MANUFACTURING & PERSONALIZATION OF BANKING, IDENTITY & SMART CARDS.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 1 01898852 Santo Domingo R.D.

CERTIFIÉ CONFORME À L'ORIGINAL
Bastien BLANC, CEO
10/04/2024

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tél. : 05 53 60 84 44 - Fax : 05 53 60 84 45
SIRET : 351 667 928 00011

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC
apposée ci-dessus

Date de début du cycle de certification : **16 septembre 2023**

Sous réserve du respect des dispositions contractuelles et des résultats positifs des surveillances réalisées, ce certificat est valable jusqu'au : **15 septembre 2026**

Date d'expiration du cycle précédent : **07 juin 2023**

Date d'audit de certification/recertification : **26 mai 2023**

Date de certification originale : **16 septembre 2020**

(Organisme certifié par un autre organisme de certification avant le 02/03/23)

Certificat n° : FR082608-1

Affaire n° : 18363737

Date de révision : 01 août 2023

Samuel DUPRIEU - Président

Adresse de l'organisme certificateur : Bureau Veritas Certification France
1 Place Zaha Hadid - 92400 Courbevoie

Des informations supplémentaires concernant le périmètre de ce certificat ainsi que l'applicabilité des exigences du référentiel peuvent être obtenues en consultant l'organisme.
Pour vérifier la validité de ce certificat, veuillez utiliser le QR Code.

cofrac
CERTIFICATION DE SYSTEMES DE MANAGEMENT
ACCREDITATION

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC. 101898852
Santo Domingo R.D.

COUR D'APPEL DE PARIS

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *République française*

Le présent acte public REPUBLIQUE DOMINICAINE

2. a été signé par... Me .....

3. agissant en qualité de... Notaire .....

4. est revêtu du sceau/timbre de... Son étude .....

.....

Attesté

5. à Paris

6. le..... 23 MAI 2024 .....

7. *par le Procureur général près la Cour d'appel de Paris*

.....

8. sous n° ..... 650 .....

9. Sceau : 10. Signature :

.....

"L'Apostille confirme seulement l'authenticité de la signature, du sceau ou timbre sur le document. Elle ne signifie pas que le contenu du document est correct ou que la République française approuve son contenu"

SYLVIE SCHLANGER
AVOCAT GENERAL

COUR D'APPEL DE PARIS

TRADUCCIÓN OFICIAL: ISO 14001:2015

Yo, **LIC. SANTO C. SIERRA,** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en francés y cuya versión al español, según mi mejor conocimiento, es el siguiente:

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

SELP

CALLE LOUIS PERGAUD
16000 ANGOULEME
FRANCIA

Bureau Veritas Certification France certifica que el sistema de gestión de la organización antes mencionada ha sido auditado y cumple con los requisitos de la norma:

Norma ISO 9001:2015

Esfera de actividad

FABRICACIÓN, IMPRESIÓN Y PERSONALIZACIÓN DE TARJETAS BANCARIAS, TARJETAS CON CHIP Y DOCUMENTOS DE IDENTIDAD.

DISEÑO, FABRICACIÓN Y PERSONALIZACIÓN DE TARJETAS BANCARIAS, DE IDENTIDAD Y SAAART.

CSI SOLUTIONS INTERNATIONAL S.A. RNC 101898852 Santo Domingo, R.D.

Certificación Bureau Veritas

CERTIFICADO
ORIGINAL
Bastien BLANC, director ejecutivo
10/04/2024
Firma ilegible

SELP SAS
187 Altée des Plagnes
24340 MAREUIL-EN-PERIGORD
Semejante. : 05 53 60 84 44 - Fax: 05 53 60 84 45
SIRET: 351 667 928 00011

Sr. Frangois MILLIER
Notario de Paris, abajo firmante,
Certifica la firma de
Señor Blanc
Fijado arriba

Fecha de inicio del ciclo de certificación: **16 de septiembre de 2023**

Sujeto al cumplimiento de las disposiciones contractuales y a los resultados positivos del seguimiento realizado, este certificado es válido hasta: **15 de septiembre de 2026**

Fecha de vencimiento del ciclo anterior: **7 de junio de 2023**

Fecha de auditoría de certificación/recertificación: **26 de mayo de 2023**

Fecha de certificación original: **16 de septiembre de 2020**

(Organización certificada por otro organismo de certificación antes del 23/03/23)

Número de certificado:
FR082608-1
Número de caso: 18363737

Fecha de revisión: 1 de agosto de 2023

Samuel DUPRIEU - Presidente

Firma ilegible

Dirección del organismo de certificación: Bureau Veritas Certification Francia

Se puede obtener información adicional sobre el alcance de este certificado, así como la aplicabilidad de los requisitos de la norma, consultando a la organización.

APOSTILLA
(Convención de la Haya del 5 de octubre de 1961)

11- País : **República Dominicana**

Este documento público

12- ha sido firmado por Millier

13- Actuar en Calidad **Notarial**

14- lleva el sello/timbre **Su estudio**

Certificado

15- en París 6- El día 23 de Mayo, 2024

13- por E fiscal general del Tribunal de Apelación de París

14- Número: 650

15- Sello/sello 10- Firma

Firma ilegible

Este Apóstol certifica de manera única la autenticidad de la empresa, la calidad de la firma del documento que se ha actualizado y, en su caso, la identidad del vendedor o sello con que se cubre el documento público.

Firmado y Sellado
Sylvie SCHLANGER
Avocat General

Traducido a petición de la parte interesada y registrada en mí protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Catorce (14) días del mes de Junio del año Dos Mil Veinticuatro (2024).

S.C.S / DPE
5184-12-8-96

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

LIC. SANTO C. SIERRA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

Common Criteria EAL4+ Superior / ISO 15408.

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 Parts 1, 2 & 3 (ISO/IEC 15408-1, ISO/IEC 15408-2 & ISO/IEC 15408-3)
Certificate number	**CC-22-180212/2**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors Germany GmbH** **Troplowitzstrasse 20, 22529 Hamburg, Germany**
Product and assurance level	**JCOP 4 P71** Assurance Package: ▪ EAL6 augmented with ASE_TSS.2 and ALC_FLR.1 Protection Profile Conformance ▪ Java Card System - Open Configuration Protection Profile, December 2017, Version 3.0.5, registered under the reference BSI-CC-PP-0099-2017
Project number	**180212_5**
Evaluation facility	**SGS Brightsight located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2 and ALC_FLR.3

SOGIS Mutual Recognition Agreement for components up to EAL 7 and ALC_FLR.3

Validity	
Date of 1st issue	: **23-07-2019**
Date of 2nd issue	: **20-03-2020**
Date of 3rd issue	: **01-03-2021**
Date of 4th issue	: **05-07-2022**
Date of 5th issue	: **19-09-2022**
Certificate expiry	: **19-09-2027**

PRODUCTS RvA C078 Accredited by the Dutch Council for Accreditation

R.L. Kruit, LFM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

TÜVRheinland®
Precisely Right.

www.tuv.com

COPY SOLUTIONS INTERNATIONAL SA CSI RNC: 101898852 Sto Domingo, R.D.

Version 2021-01

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Bundesamt
für Sicherheit in der
Informationstechnik

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC. 101898852
Santo Domingo, R.D.

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1136-V4-2024 (*)

Smartcard Controller

NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4)

from	NXP Semiconductors Germany GmbH
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ASE_TSS.2, ALC_FLR.1
valid until:	04 March 2029

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 5 March 2024

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Sandro Amendola
Director-General

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

TRADUCCIÓN OFICIAL: Common Criteria EAL4+ Superior / ISO 15408.

Yo **LIC. SANTO C. SIERRA,** intérprete judicial, debidamente juramentada para el ejercicio de mis funciones **CERTIFICO** que he procedido a traducir las partes centrales de un documento escrito originalmente en Ingles, cuya versión en idioma Español de acuerdo a mi mejor el conocimiento es el siguiente:

Certificado

Estándar
Criterios comunes para la evaluación de la seguridad de las tecnologías de la información (CC), versión 3.1, revisión 5, partes 1, 2 y 3 (ISO/IEC 15408-1, ISO/IEC 15408-2 e ISO/IEC 15408-3)

Número de certificado
CC-22-180212/2

TÜV Rheinland Nederland B.V. certifica:

Titular del certificado y desarrollador
NXP Semiconductors Alemania GmbH

Troplowitzstrasse 20, 22529 Hamburgo, Alemania

Nivel de producto y garantía

Paquete de garantía:
- EAL5 ampliado con ASE_TSS.2 y ALC_FLR.1

Conformidad del perfil de protección
- Java Card System - Perfil de protección de configuración abierta, diciembre de 2017, versión 3.0.5, registrado con la referencia BSI-CC-PP-0099-2017

Número de proyecto
180212_5

Instalación de evaluación
SGS Brightsight se encuentra en Delft, Países Bajos

Aplicación de la metodología común para la evaluación de la seguridad de las tecnologías de la información (CEM), versión 3.1, revisión 5 (ISO/IEC 18045)

El producto de TI identificado en este certificado ha sido evaluado en un centro de evaluación acreditado y certificado utilizando la Norma para la evaluación de la seguridad de TI, versión 3.1 Revisión 5. Esta evaluación se llevó a cabo de conformidad con las disposiciones del esquema de los Países Bajos para la certificación en el área de seguridad de TI [NSCIB] y las conclusiones del informe de certificación completa. La evaluación se ha llevado a cabo de conformidad con las disposiciones del esquema de los Países Bajos para la certificación en el área de seguridad de TI [NSCIB] y las conclusiones del centro de evaluación en el informe técnico de evaluación son técnicamente sólidas. Este certificado no constituye una aprobación del producto de TI por parte de TÜV Rheinland Nederland B.V. ni de ninguna otra organización que reconozca o haga efectivo este certificado, y no se expresa ni implica ninguna garantía del producto de TI por parte de TÜV Rheinland Nederland B.V. ni de ninguna otra organización que reconozca o haga efectivo este certificado.

Validez
Fecha de la primera emisión: 23-07-2019
Fecha de la 2ª edición: 20-03-2020
Fecha de la 3ª edición: 01-03-2021
Fecha de la 4ª edición: 05-07-2022
Fecha de la 5ª edición: 19-09-2022
Fecha de caducidad del certificado: 19-09-2027

Firma

[illegible]
Certificado de calidad TÜVRheinland
Nederland B.V. Apartado Postal Westervoortsedijk 73
6827 AV Arnhem Apartado Postal 2220, NL-6802 CE
Arnhem Países Bajos

www.tuv.com

TÜVRheinland®

Traducido a petición de la parte interesada y registrada en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Once (11) días del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
REI

Yo LIC. SANTO C. SIERRA, intérprete judicial, debidamente juramentada para el ejercicio de mis funciones **CERTIFICO** que he procedido a traducir las partes centrales de un documento escrito originalmente en Ingles, cuya versión en idioma Español de acuerdo a mí mejor el conocimiento es el siguiente:

Oficina
Federal de Seguridad de
la Información

Alemán — Certificado de seguridad informática

expedido por — Oficina Federal de Seguridad de la Información

BSI-DSZ-CC-1136-V4-2024 (*)

Controlador de tarjeta inteligente

Controlador de tarjeta inteligente segura NXP N7121 con software dedicado de IC y bibliotecs de cifrado (R1/R2/R3/R4)

de	NXP Semiconductors Alemania GmbH
Conformidad de PP:	Perfil de protección de la plataforma Security IC con paquetes de ampliación Versión 1.0, 13 de enero de 2014, BSI-CC-PP-0084-2014
Funcionalidad:	Conforme a PP más extensiones específicas del producto Criterios comunes Parte 2 ampliada
Garantía:	Criterios comunes Parte 3 conforme EAL 6 ampliado por ASE_TSS.2, ALC_FLR.1
válido hasta:	04 de marzo de 2029

El producto de TI identificado en este certificado ha sido evaluado en un centro de evaluación aprobado utilizando la Metodología común para la evaluación de la seguridad de TI (CEM), versión 3.1, ampliada con interpretaciones del esquema por recomendación del organismo de certificación para los componentes que van más allá de EAL 5 y los documentos de respaldo de CC que se enumeran en el informe de certificación para la conformidad con los criterios comunes para la evaluación de la seguridad de TI (CC), versión 3.1. CC y CEM también se publican como ISO/IEC 15408 e ISO/IEC 18045.

(*) Este certificado se aplica únicamente a la versión y el lanzamiento específicos del producto en su configuración evaluada y en conjunto con el Informe de certificación y la notificación completos. Para obtener más información sobre la validez, consulte el capítulo 5 de la parte A del Informe de certificación.

La evaluación se ha llevado a cabo de conformidad con las disposiciones del sistema de certificación de la Oficina Federal Alemana de Seguridad de la Información (BSI) y las conclusiones del centro de evaluación en el informe técnico de evaluación son consistentes con las pruebas aportadas.

Este certificado no constituye una aprobación del producto de TI por parte de la Oficina Federal de Seguridad de la Información o cualquier otra organización que reconozca o dé efecto a este certificado, y no se expresa ni implica ninguna garantía del producto de TI por parte de la Oficina Federal de Seguridad de la Información o cualquier otra organización que reconozca o dé efecto a este certificado.

Bonn, 5 de marzo de 2024
Para la Oficina Federal de Seguridad de la Información

Sandro Amendola
Director General

L.S.

Oficina Federal de Seguridad de la Información
Godesberger Allee 185 - 189 - D-53175 Bonn - Apartado Postal 20003 63 - D-53133 Bonn - Teléfono +49
(0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infobox +49 (0)228 99 9582

Traducido a petición de la parte interesada y registrada en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Once (11)días del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

Procuraduría General de la República
Confirme la validez de este documento ingresando el código CIB en portal.servicios.pgr.gob.do
Código CIB: 001-5202-422500I-7
Vence automáticamente dentro de 6 meses

PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT ANSSI-CC-2021/18v2

Ce certificat est associé au rapport de certification ANSSI-CC-2021/18v2

ChipDoc v3.1 on JCOP 4 P71 in ICAO BAC configuration

version 3.1.6.52

Développeur : NXP SEMICONDUCTORS
Commanditaire : NXP SEMICONDUCTORS
Centre d'évaluation : THALES/CNES

Critères Communs version 3.1, révision 5

EAL4 Augmenté

(ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3)

conforme au profil de protection :

Machine Readable Travel Document with « ICAO Application », Basic Access Control, version 1.10, certifié BSI-CC-PP-0055-2009

Date de validité : 3 juin 2026

Paris, le 28 septembre 2022

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti

Dans le cadre du CCRA, ce certificat est reconnu au niveau EAL2.

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information.

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Página/Folio No.473 de 843

Le produit, objet de cette certification, a été évalué par THALES/CNES sis en France en appliquant la *Common Methodology for Information Technology Security Evaluation*, version 3.1, révision 5, conforme aux Critères communs, version 3.1, révision 5.

Ce certificat s'applique uniquement à cette version spécifique de produit dans sa configuration évaluée. Il ne peut être dissocié de son rapport de certification complet. L'évaluation a été menée conformément aux dispositions du SOG-IS, du CCRA et du schéma français. Les conclusions du centre d'évaluation, formulées dans le rapport technique d'évaluation, sont cohérentes avec les preuves fournies.

Ce certificat ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Página/Folio No.474 de 843

Yo, **LICDA. MARIA TERESA PUIGBO**, Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en francés, y cuya versión al español, según mi mejor conocimiento, es el siguiente:

PRIMERO
MINISTRO

Libertad
Igualdad
Fraternidad

Sistema francés de evaluación y certificación de la seguridad de los Tecnologías de la información

CERTIFICADO ANSSI-CC-2021/18v2
Este certificado está asociado al informe de certificación ANSSI-CC-2021/18v2

ChipDoc v3.1 en JCOP 4 P71 en configuración BAC

Versión 3.1.6.52 de la OACI

Desarrollador: NXP SEMICONDUCTORS
Patrocinador: NXP SEMICONDUCTORS
Centro de evaluación: THALES/CNES

Criterios comunes versión 3.1, revisión 5

EAL4 Aumentado
(ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3)

Cumple con el perfil de protección:
Documento de viaje legible por máquina con "Aplicación ICAO", Control de Acceso Básico, versión 1.10, certificado BSI-CC-PP-0055-2009

Fecha de validez: 3 de junio de 2026

París, 28 de septiembre de 2022

El Director General de la Agencia Nacional
De seguridad de los sistemas de información

Guillermo POUPARD

[FIRMA ORIGINAL]

En el marco de la CCRA, este certificado está reconocido en el nivel EAL2.

Este certificado se emite de conformidad con el Decreto 2002-535 del 18 de abril de 2002, modificado, relativo a la evaluación y certificación de la seguridad ofrecida por los productos y sistemas de tecnología de la información.

Secretaría General de Defensa y Seguridad Nacional, Agencia Nacional de Seguridad de los Sistemas de Información
51, bulevar de La Tour-Maubourg, 75700 PARÍS 07 SP

El producto, objeto de esta certificación, fue evaluado por THALES/CNES con sede en Francia aplicando la Metodología Común para la Evaluación de la Seguridad de las Tecnologías de la Información, versión 3.1, revisión 5, de conformidad con los Criterios Comunes, versión 3.1, revisión 5.

Este certificado se aplica únicamente a esta versión específica del producto en su configuración evaluada. No puede separarse de su informe de certificación completo. La evaluación se llevó a cabo de conformidad con las disposiciones de la SOG-IS, la CCRA y el régimen francés. Las conclusiones del centro de evaluación, tal y como se establecen en el informe de evaluación técnica, son coherentes con la evidencia aportada.

Esta certificación no constituye en sí misma una recomendación del producto por parte de la Agencia Nacional de Seguridad de los Sistemas de Información y no garantiza que el producto certificado esté completamente libre de vulnerabilidades explotables.

Traducción a petición de la parte interesada el día y registrada en mi protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los dieciocho (18) días del mes de febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de maintenance
ANSSI-CC-2021/18v2-M01

ChipDoc v3.2 on JCOP 4 P71 in ICAO BAC configuration

(Version 3.2.0.52)

Certificat de référence : ANSSI-CC-2021/18v2

Paris, le 28 septembre 2022

Le directeur général de l'Agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Página/Folio No.478 de 843

1 Références

[CER]	Rapport de certification ANSSI-CC-2021/18v2, ChipDoc v3.1 on JCOP 4 P71 in ICAO BAC configuration (version 3.1.6.52).
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IAR]	*ChipDoc v3.2 on JCOP 4 P71 v3.2.0.52 Impact Analysis Report, rev 1.0*, 3 juin 2021.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.*
[CCRA]	*Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.*

2 *Identification* du produit maintenu

Le produit objet de la présente maintenance est « ChipDoc v3.2 on JCOP 4 P71 in ICAO BAC configuration, (Version 3.2.0.52) » développé par la société NXP SEMICONDUCTORS.

Le produit a été certifié avec réduction de portée sous la référence ANSSI-CC-2021/18v2 (référence [CER]).

La version maintenue du produit est identifiable par les éléments suivants :

- l'*applet* est identifiée en réponse à la commande GET_DATA par les valeurs suivantes :
  - Nom : 0x43686970446F63 ;
  - Version : 0x03020052 ;
  - *Card capabilities* : 0x00036FEF ;
- la plateforme est identifiée en réponse à la commande GET_DATA(IDENTIFY) par les valeurs suivantes :
  - Patch ID : 0x0000000000000001 ;
  - ROM ID : 2E5AD88409C9BADB ;
  - *Platform ID* : 4A335233353130314641394530343030DD0984593B0048EF ou 4A335233353130323336333130343030DCE5C19CFE6D0DCF ;
- la configuration limitée à BAC est reconnue par l'absence des fichiers EF.CardAccess et EF.DG14.

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- la correction de *bugs* ;
- l'ajout d'une option de configuration ;
- le retrait d'une commande inutile en phase opérationnelle.

Página/Folio No.479 de 843

4 Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	*ChipDoc 3.2, User Guide Manual, ref 678510*, 22 avril 2021	[R-M01]
	ChipDoc 3.2, ICAO Personalization Guide, ref 678610, 23 avril 2021	[R-M01]
	ChipDoc 3.2, Crypto Guide, révision 1.0, 29 avril 2021	[R-M01]
	ChipDoc V3 Application Note, révision 1.4, 20 juin 2022	[CER]
[ST]	Cibles de sécurité de référence: ChipDoc v3.2 on JCOP 4 P71 in ICAO BAC configuration – Security Target, revision 1.2, 13 juillet 2022, NXP. Version publique : ChipDoc v3.2 on JCOP 4 P71 in ICAO BAC configuration – Security Target Lite, revision 1.2, 13 juillet 2022, NXP.	[R-M01]
[CONF]	*Configuration Item List, CDv3.2_1_04920_ALC_CIL_v2.0*, 19 juillet 2022	[R-M01]

5 Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur.

Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.

6 Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

Página/Folio No.480 de 843

Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs.

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org

Página/Folio No.481 de 843

Yo, **LIC. SANTO C. SIERRA,** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en francés, y cuya versión al español, según mi mejor conocimiento, es el siguiente:

PRIMERA MINISTRO

Secretaría General de Defensa y Seguridad Nacional

Libertad
Igualdad
Fraternidad

Agencia de Seguridad Nacional
Sistemas de información

Informe de mantenimiento
ANSSI-CC-2021/18v2-M01

ChipDoc v3.2 en JCOP 4 P71 en configuración
Base de datos de la OACI

(Versión 3.2.0.52)

Certificado de referencia: ANSSI-CC-2021/18v2

París, 28 de septiembre de 2022

El Director General de la Agencia Nacional
de seguridad de los sistemas de información

Guillermo POUPARD

[FIRMA ORIGINAL]

ADVERTENCIA

El nivel de resistencia de un producto certificado se degrada con el tiempo. Como parte de este mantenimiento no se realizó un análisis de vulnerabilidad de esta versión del producto con respecto a nuevos ataques que han aparecido desde que se emitió el certificado. Sólo una reevaluación o seguimiento de esta nueva versión del producto permitiría mantener el nivel de confianza en el tiempo.

Toda correspondencia relacionada con este informe deberá dirigirse a:

Secretaría General de Defensa y Seguridad Nacional

Agencia Nacional para la Seguridad de los Sistemas de Información

Centro de Certificación

51, bulevar de la Torre Maubourg
75700 París cedex 07 SP

certificación@ssi.gouv.fr

Se autoriza la reproducción de este documento sin alteración ni corte.

1 Referencias

[CER]	Informe de certificación ANSSI-CC-2021/18v2, ChipDoc v3.1 sobre JCOP 4 P71 en configuración ICAO BAC (versión 3.1.6.52).
[MAI]	Procedimiento: Continuidad del seguro, referencia ANSSI-CC-MAI-P-01.
[IAR]	Informe de análisis de impacto de ChipDoc v3.2 sobre JCOP 4 P71 v3.2.0.52, revisión 1.0, 3 de junio de 2021.
[SOG-IS]	Acuerdo de Reconocimiento Mutuo de Certificados de Evaluación de Seguridad de Tecnologías de la Información, versión 3.0, 8 de enero de 2010, Comité Directivo.
[CCRA]	Acuerdo sobre el reconocimiento de certificados de Criterios Comunes en el ámbito de la seguridad de las tecnologías de la información, 2 de julio de 2014.

2 Identificación del producto mantenido

El producto sujeto a este mantenimiento es << ChipDoc v3.2 en JCOP 4 P71 en configuración ICAO BAC, (Versión 3.2.0.52) » desarrollado por la empresa NXP SEMICONDUCTORS.

El producto ha sido certificado con reducción de rango bajo la referencia ANSSI-CC-2021/18v2 (referencia [CER]).

La versión mantenida del producto se identifica mediante los siguientes elementos:

El subprograma se identifica en respuesta al comando GET_DATA mediante los siguientes valores:

Nombre: 0x43686970446F63;

Versión: 0x03020052;

Capacidades de la tarjeta: 0x00036FEF;

La plataforma se identifica en respuesta al comando GET_DATA(IDENTIFY) mediante los siguientes valores:

ID del parche: 0x0000000000000001;

Identificación de ROM: 2E5AD88409C9BADB;

ID de plataforma: 4A335233353130314641394530343030DD098459380048EF 4A335233353130323336333130343030DCE5C19CFE6D0DCF;

La configuración limitada de BAC se reconoce por la ausencia de los archivos EF.CardAccess y EF.DG14.

3 Descripción de los desarrollos

El Informe de Análisis de Impacto de Seguridad (referencia [IAR]) menciona que se realizaron las siguientes modificaciones:

Corrección de errores;

Añadiendo una opción de configuración;

La retirada de un pedido innecesario en la fase operativa.

4 Suministros aplicables

En la siguiente tabla se enumeran los suministros, incluidas las guías aplicables al producto al que se le realiza el mantenimiento. La última columna identifica el origen de la consideración por parte de ANSSI del documento correspondiente. En particular , [R-M01] hace referencia al presente mantenimiento .

[GUIAS]	de ChipDoc 3.2, n.º de pieza 678510, 22 de abril de 2021	[R-M01]
	ChipDoc 3.2, Guía de personalización de la OACI, ref. 678610, 23 de abril de 2021	[R-M01]
	ChipDoc 3.2, Guía de criptografía, revisión 1.0, 29 de abril de 2021	[R-M01]
	de ChipDoc V3, revisión 1.4, 20 de junio de 2022	[CER]
[ST]	Objetivos de seguridad de referencia: ChipDoc v3.2 sobre JCOP 4 P71 en configuración ICAO BAC - Objetivo de seguridad, revisión 1.2, 13 de julio de 2022, NO . Versión pública: ChipDoc v3.2 sobre JCOP 4 P71 en configuración ICAO BAC - Security Target Lite, revisión 1.2, 13 de julio de 2022, NXP	[R-M01]
[CONF.]	Lista de elementos de configuración, CDv3.2_1_04920_ALC_CIL_v2.0, 19 de julio de 2022	[R-M01]

5 Conclusiones

Se considera que los desarrollos enumerados anteriormente tienen un impacto menor.

Por tanto, el nivel de confianza en esta nueva versión del producto es idéntico al de la versión certificada.

6 Reconocimiento del certificado

Reconocimiento europeo (SOG-IS)

Este certificado se emite bajo los términos del Acuerdo SOG-IS [SOG-IS].

El Acuerdo de Reconocimiento Europeo SOG-IS 2010 permite el reconocimiento, por parte de los países firmantes del acuerdo, de los certificados ITSEC y Common Criteria. El reconocimiento europeo se aplica, para tarjetas inteligentes y dispositivos similares, hasta el nivel ITSEC E6 High y CC EAL7 cuando se cumplen las dependencias CC. Los certificados reconocidos bajo este acuerdo se emiten con la siguiente marca:

Reconocimiento internacional de criterios comunes (CCRA)

Este certificado se emite bajo los términos del Acuerdo CCRA [CCRA].

El acuerdo « Acuerdo de reconocimiento de criterios comunes » permite el reconocimiento, por parte de los países firmantes, de los certificados Criterios comunes.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: J01698852 Santo Domingo, R.D.

==========

Traducido a petición de la parte interesada y registrada en mi protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los dieciocho (18) del mes de Febrero del año Dos Mil Veinticinco (2025).

PROCURADURÍA GENERAL DE LA REPÚBLICA MINISTERIO PÚBLICO CENTRO DE ATENCIÓN AL CIUDADANO DISTRITO NACIONAL Santo Domingo, R.D.

República Dominicana Procuraduría General de la República Confirme la validez de este documento ingresando el código CSE en portal.servicios.pgr.gob.do Código CSE: 0001-5202-020414-4

S.C.S / DPE 5184-12-8-96

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

LIC. SANTO C. SIERRA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

Common Criteria EAL5+ o Superior

PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

COPY SOLUTIONS INTERNATIONAL SA
RNC 101-00802
Santo Domingo, R.D.

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT ANSSI-CC-2021/19v2

Ce certificat est associé au rapport de certification ANSSI-CC-2021/19v2

ChipDoc v3.1 on JCOP 4 P71 in ICAO EAC (1&2) with PACE configuration

version 3.1.6.52

Développeur : NXP SEMICONDUCTORS
Commanditaire : NXP SEMICONDUCTORS
Centre d'évaluation : THALES/CNES

Critères Communs version 3.1, révision 5

EAL5 Augmenté
(ALC_DVS.2, AVA_VAN.5)

conforme aux profils de protection :

Machine Readable Travel Document with « ICAO Application », Extended Access Control with PACE, version 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02

Machine Readable Travel Document using Standard Inspection Procedure with PACE, version 1.0.1, BSI-CC-PP-0068-V2-2011-MA-01

Date de validité : 3 juin 2026

Paris, le 28 septembre 2022

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

Dans le cadre du CCRA, ce certificat est reconnu au niveau EAL2.

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information.

COPY CONTROLLED
CSI
RNC: 101038852
Santo Domingo, RD

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Le produit, objet de cette certification, a été évalué par THALES/CNES sis en France en appliquant la *Common Methodology for Information Technology Security Evaluation*, version 3.1, révision 5, conforme aux Critères communs, version 3.1, révision 5.

Ce certificat s'applique uniquement à cette version spécifique de produit dans sa configuration évaluée. Il ne peut être dissocié de son rapport de certification complet. L'évaluation a été menée conformément aux dispositions du SOG-IS, du CCRA et du schéma français. Les conclusions du centre d'évaluation, formulées dans le rapport technique d'évaluation, sont cohérentes avec les preuves fournies.

Ce certificat ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de maintenance
ANSSI-CC-2021/19v2-M01

ChipDoc v3.2 on JCOP 4 P71 in ICAO EAC (1&2) with PACE configuration

(Version 3.2.0.52)

Certificat de référence : ANSSI-CC-2021/19v2

Paris, le 28 septembre 2022

Le directeur général de l'Agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

Página/Folio No.490 de 843

COPY SOLUTIONS INTERNATIONAL SA
RNC 101898652
Santo Domingo, R.D.

AVERTISSEMENT

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Página/Folio No.491 de 843

1 Références

[CER]	Rapport de certification ANSSI-CC-2021/19v2, ChipDoc v3.1 on JCOP 4 P71 in ICAO EAC (1&2) with PACE configuration (version 3.1.6.52).
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IAR]	*ChipDoc v3.2 on jCOP 4 P71 v3.2.0.52 Impact Analysis Report, rev 1.0*, 3 juin 2021.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.*
[CCRA]	*Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.*

2 Identification du produit maintenu

Le produit objet de la présente maintenance est « ChipDoc v3.2 on JCOP 4 P71 in ICAO EAC (1&2) with PACE configuration, (Version 3.2.0.52) » développé par la société NXP SEMICONDUCTORS.

Le produit a été certifié avec réduction de portée sous la référence ANSSI-CC-2021/19v2 (référence [CER]).

La version maintenue du produit est identifiable par les éléments suivants :

- L'*applet* est identifiée en réponse à la commande GET_DATA par les valeurs suivantes :
  - Nom : 0x43686970446F63 ;
  - Version : 0x03020052 ;
  - *Card capabilities* : 0x00036FEF ;
- La plateforme est identifiée en réponse à la commande GET_DATA(IDENTIFY) par les valeurs suivantes :
  - Patch ID : 0x0000000000000001 ;
  - ROM ID : 2E5AD88409C9BADB ;
  - *Platform* ID : 4A335233353130314641394530343030DD098459380048EF ou 4A3352333531303233363331303430 30DCE5C19CFE6D0DCF ;
- La configuration EAC avec PACE est reconnue par la présence du fichier EF.CardAccess.

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- Correction de *bugs* ;
- Ajout d'une option de configuration ;
- Retrait d'une commande inutile en phase opérationnelle.

Página/Folio No.492 de 843

COPY SOLUTIONS

4 Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	*ChipDoc 3.2, User Guide Manual*, ref 678510, 22 avril 2021	[R-M01]
	ChipDoc 3.2, ICAO Personalization Guide, ref 678610, 23 avril 2021	[R-M01]
	ChipDoc 3.2, Crypto Guide, révision 1.0, 29 avril 2021	[R-M01]
	ChipDoc V3 Application Note, révision 1.4, 20 juin 2022	[CER]
[ST]	Cibles de sécurité de référence: *ChipDoc v3.2 on JCOP 4 P71 in ICAO EAC(1&2) with PACE configuration – Security Target, revision 1.2*, 13 juillet 2022, NXP. Version publique : *ChipDoc v3.2 on JCOP 4 P71 in ICAO EAC(1&2) with PACE configuration – Security Target Lite, revision 1.2*, 13 juillet 2022, NXP.	[R-M01]
[CONF]	*Configuration Item List, CDv3.2_1_04920_ALC_CIL_v2.0*, 19 juillet 2022	[R-M01]

5 Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur.

Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.

6 Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

Página/Folio No.493 de 843

Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs.

[1] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Página/Folio No.494 de 843

TRADUCCIÓN OFICIAL: Common Criteria EAL5+ o Superior

Yo, **LIC. SANTO C. SIERRA,** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento escrito originalmente en Francés, y cuya versión al Español, según mi mejor conocimiento, es el siguiente:

PRIMERA MINISTRO

Secretaría General de Defensa y Seguridad Nacional

Libertad
Igualdad
Fraternidad

Agencia de Seguridad Nacional
Sistemas de información

Informe de mantenimiento
ANSSI-CC-2021/19v2-M01

ChipDoc v3.2 sobre JCOP 4 P71 en ICAO EAC (1 y 2) con Configuración de PACE
(Versión 3.2.0.52)

Certificado de referencia: ANSSI-CC-2021/19v2

París, 28 de septiembre de 2022

El Director General de la Agencia Nacional
de seguridad de los sistemas de información

Guillermo POUPARD

[FIRMA ORIGINAL]

ADVERTENCIA

El nivel de resistencia de un producto certificado se degrada con el tiempo. Como parte de este mantenimiento no se realizó un análisis de vulnerabilidad de esta versión del producto con respecto a nuevos ataques que han aparecido desde que se emitió el certificado. Sólo una reevaluación o seguimiento de esta nueva versión del producto permitiría mantener el nivel de confianza en el tiempo.

LIC. SANTO C. SIERRA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC 101898852
Santo Domingo, R.D.

Toda correspondencia relacionada con este informe deberá dirigirse a:

Secretaría General de Defensa y Seguridad Nacional Agencia Nacional de Seguridad de los Sistemas de Información Centro de Certificación 51, boulevard de la Tour Maubourg 75700 París cedex 07 SP

certificación@ssi.gouv.fr

Se autoriza la reproducción de este documento sin alteración ni corte.

1 Referencias

[CER]	Informe de certificación ANSSI-CC-2021/19v2, ChipDoc v3.1 sobre JCOP 4 P71 en ICAO EAC (1 y 2) con configuración PACE (versión 3.1.6.52).
[MAI]	Procedimiento: Continuidad del seguro, referencia ANSSI-CC-MAI-P-01.
[IAR]	Informe de análisis de impacto de ChipDoc v3.2 sobre JCOP 4 P71 v3.2.0.52, revisión 1.0, 3 de junio de 2021.
[SOG-IS]	Acuerdo de Reconocimiento Mutuo de Certificados de Evaluación de Seguridad de Tecnologías de la Información, versión 3.0, 8 de enero de 2010, Comité Directivo.
[CCRA]	Acuerdo sobre el reconocimiento de certificados de Criterios Comunes en el ámbito de la seguridad de las tecnologías de la información, 2 de julio de 2014.

2 Identificación del producto mantenido

El producto sujeto a este mantenimiento es << ChipDoc v3.2 en JCOP 4 P71 en ICAO EAC (1&2) con configuración PACE, (Versión 3.2.0.52) » desarrollado por la empresa NXP SEMICONDUCTORS.

El producto ha sido certificado con reducción de rango bajo la referencia ANSSI-CC-2021/19v2 (referencia [CER]).
La versión mantenida del producto se identifica mediante los siguientes elementos:

El subprograma se identifica en respuesta al comando GET_DATA mediante los siguientes valores:

Nombre: 0x43686970446F63;
Versión: 0x03020052;
Capacidades de la tarjeta: 0x00036FEF;

La plataforma se identifica en respuesta al comando GET_DATA(IDENTIFY) mediante los siguientes valores:

ID de parche: 0x0000000000000001;
Identificación de ROM: 2E5AD88409C9BADB;
ID de plataforma: 4A335233353130314641394530343030DD098459380048EF
O 4A3352333531303233363331303430 30DCE5C19CFE6D0DCF;

La configuración de EAC con PACE se reconoce por la presencia del archivo EF.CardAccess .

3 Descripción de los desarrollos

El Informe de Análisis de Impacto de Seguridad (referencia [IAR]) menciona que se realizaron las siguientes modificaciones:

Corrección de errores;

Opción de configuración agregada;

Retirada de un pedido innecesario en la fase operativa.

4 Suministros aplicables

En la siguiente tabla se enumeran los suministros, incluidas las guías aplicables al producto al que se le realiza el mantenimiento. La última columna identifica el origen de la consideración por parte de ANSSI del documento correspondiente. En particular , [R-M01] hace referencia al presente mantenimiento .

[GUIAS]	ChipDoc 3.2, n.º de pieza 678510, 22 de abril de 2021	[R-M01]
	ChipDoc 3.2, Guía de personalización de la OACI, ref. 678610, 23 de abril de 2021	[R-M01]
	ChipDoc 3.2, Guía de criptografía, revisión 1.0, 29 de abril de 2021	[R-M01]
	de ChipDoc V3, revisión 1.4, 20 de junio de 2022	[CER]
[ST]	Objetivos de seguridad de referencia: ChipDoc v3.2 sobre JCOP 4 P71 en ICAO EAC (1 y 2) con configuración PACE Objetivo de seguridad, revisión 1.2, 13 de julio de 2022, NO . Versión pública: ChipDoc v3.2 sobre JCOP 4 P71 en ICAO EAC (1 y 2) con configuración PACE Security Target Lite, revisión 1.2, 13 de julio de 2022, NO .	[R-M01]
[CONF.]	Lista de elementos de configuración, CDv3.2_1_04920_ALC_CIL_v2.0, 19 de julio de 2022	[R-M01]

5 Conclusiones

Se considera que los desarrollos enumerados anteriormente tienen un impacto menor. Por tanto, el nivel de confianza en esta nueva versión del producto es idéntico al de la versión certificada.

6 Reconocimiento del certificado

Reconocimiento europeo (SOG-IS)

Este certificado se emite bajo los términos del Acuerdo SOG-IS [SOG-IS].

El Acuerdo de Reconocimiento Europeo SOG-IS 2010 permite el reconocimiento, por parte de los países firmantes del acuerdo, de los certificados ITSEC y Common Criteria. El reconocimiento europeo se aplica, para tarjetas inteligentes y dispositivos similares, hasta el nivel ITSEC E6 High y CC EAL7 cuando se cumplen las dependencias CC. Los certificados reconocidos bajo este acuerdo se emiten con la siguiente marca:

Reconocimiento internacional de criterios comunes (CCRA)

Este certificado se emite bajo los términos del Acuerdo CCRA [CCRA].

El acuerdo « Acuerdo de reconocimiento de criterios comunes » permite el reconocimiento, por parte de los países firmantes², de los certificados Criterios comunes.

Traducido a petición de la parte interesada y registrada en mi protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los dieciocho (18) del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

Yo, **LICDA. MARIA TERESA PUIGBO,** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en francés, y cuya versión al español, según mi mejor conocimiento, es el siguiente:

PRIMERO
MINISTRO

Libertad
Igualdad
Fraternidad

Sistema francés de evaluación y certificación de la seguridad de los Tecnologías de la información

CERTIFICADO ANSSI-CC-2021/19v2
Este certificado está asociado al informe de certificación ANSSI-CC-2021/19v2

ChipDoc v3.1 sobre JCOP 4 P71 en ICAO EAC (1 y 2) con versión de configuración
RITMO 3.1.6.52

Desarrollador: NXP SEMICONDUCTORS
Patrocinador: NXP SEMICONDUCTORS
Centro de evaluación: THALES/CNES

Criterios comunes versión 3.1, revisión 5

EAL5 Aumentado
(ALC_DVS.2, AVA_VAN.5)

Cumple con los perfiles de protección:

Documento de viaje legible por máquina con <<Aplicación ICAO> »,

Control de acceso extendido con PACE, versión 1.3.2, BSI-CC-PP-0056-V2-2012-MA-02

Documento de viaje legible por máquina que utiliza el procedimiento de inspección estándar con PACE, versión 1.0.1, BSI-CC-PP-0068-V2-2011-MA-01

Fecha de validez: 3 de junio de 2026

París, 28 de septiembre de 2022

El Director General de la Agencia Nacional de seguridad de los sistemas de información

Guillermo POUPARD

[FIRMA ORIGINAL]

En el marco de la CCRA, este certificado está reconocido en el nivel EAL2.

Este certificado se emite de conformidad con el Decreto 2002-535 del 18 de abril de 2002, modificado, relativo a la evaluación y certificación de la seguridad ofrecida por los productos y sistemas de tecnología de la información.

Secretaría General de Defensa y Seguridad Nacional, Agencia Nacional de Seguridad de los Sistemas de Información
51, bulevar de La Tour-Maubourg, 75700 PARÍS 07 SP

El producto, objeto de esta certificación, fue evaluado por THALES/CNES con sede en Francia aplicando la Metodología Común para la Evaluación de la Seguridad de las Tecnologías de la Información, versión 3.1, revisión 5, de conformidad con los Criterios Comunes, versión 3.1, revisión 5.

Este certificado se aplica únicamente a esta versión específica del producto en su configuración evaluada. No puede separarse de su informe de certificación completo. La evaluación se llevó a cabo de conformidad con las disposiciones de la SOG-IS, la CCRA y el régimen francés. Las conclusiones del centro de evaluación, tal y como se establecen en el informe de evaluación técnica, son coherentes con la evidencia aportada.

Este certificado no constituye en sí mismo una recomendación del producto por parte de la Agencia Nacional de Seguridad de los Sistemas de Información y no garantiza que el producto certificado esté completamente libre de vulnerabilidades explotables.

Traducido a petición de la parte interesada y registrada en mí protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Dieciocho (18) del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT ANSSI-CC-2021/20v2

Ce certificat est associé au rapport de certification ANSSI-CC-2021/20v2

ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration

version 3.1.6.52

Développeur : NXP SEMICONDUCTORS
Commanditaire : NXP SEMICONDUCTORS
Centre d'évaluation : THALES/CNES

Critères Communs version 3.1, révision 5

EAL5 Augmenté

(ALC_DVS.2, AVA_VAN.5)

conforme aux profils de protection :

Protection profiles for secure signature creation device
Part 2 : Device with key generation, v2.0.1, certifié BSI-CC-PP-0059-2009-MA-01
Part 3 : Device with key import, v1.0.2, certifié BSI-CC-PP-0075-2012
Part 4 : Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, certifié BSI-CC-PP-0071-2012
Part 5 : Extension for device with key generation and trusted communication with signature creation application, v1.0.1, certifié BSI-CC-PP-0072-2012
Part 6 : Extension for device with key import and trusted communication with signature creation application, v1.0.4, certifié BSI-CC-PP-0076-2013

Date de validité : 3 juin 2026

Paris, le 28 septembre 2022

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

Dans le cadre du CCRA, ce certificat est reconnu au niveau EAL2.

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information.

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Página/Folio No.503 de 843

Le produit, objet de cette certification, a été évalué par THALES/CNES sis en France en appliquant la *Common Methodology for Information Technology Security Evaluation*, version 3.1, révision 5, conforme aux Critères communs, version 3.1, révision 5.

Ce certificat s'applique uniquement à cette version spécifique de produit dans sa configuration évaluée. Il ne peut être dissocié de son rapport de certification complet. L'évaluation a été menée conformément aux dispositions du SOG-IS, du CCRA et du schéma français. Les conclusions du centre d'évaluation, formulées dans le rapport technique d'évaluation, sont cohérentes avec les preuves fournies.

Ce certificat ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Página/Folio No.504 de 843

Yo, **LICDA. SANTO C. SIERRA**, Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en Francés, y cuya versión al Español, según mi mejor conocimiento, es el siguiente:

PRIMER
MINISTRO

Libertad
Igualdad
Fraternidad

Sistema francés de evaluación y certificación de la seguridad de los Tecnologías de la información

CERTIFICADO ANSSI-CC-2021/20v2
Este certificado está asociado al informe de certificación ANSSI-CC-2021/20v2

ChipDoc v3.1 en JCOP 4 P71 en configuración SSCD
Versión 3.1.6.52

Desarrollador: NXP SEMICONDUCTORS
Patrocinador: NXP SEMICONDUCTORS
Centro de evaluación: THALES/CNES

Criterios comunes versión 3.1, revisión 5
EAL5 Aumentado
(ALC_DVS.2, AVA_VAN.5)

Cumple con los perfiles de protección:
Perfiles de protección para dispositivos de creación de firma segura
Parte 2: Dispositivo con generación de claves, v2.0.1, certificado BSI-CC-PP-0059-2009-MA-01
Parte 3: Dispositivo con importación de claves, v1.0.2, certificado BSI-CC-PP-0075-2012
Parte 4: Extensión para dispositivo con generación de claves y comunicación segura con aplicación de generación de certificados, v1.0.1, certificada BSI-CC-PP-0071-2012
Parte 5: Extensión para dispositivo con generación de claves y comunicación segura con aplicación de creación de firma, v1.0.1, certificada BSI-CC-PP-0072-2012
Parte 6: Extensión de dispositivo con importación de claves y comunicación segura con aplicación de creación de firmas, v1.0.4, certificado BSI-CC-PP-0076-2013

Fecha de validez: 3 de junio de 2026

París, 28 de septiembre de 2022

El Director General de la Agencia Nacional de seguridad de los sistemas de información

Guillermo POUPARD

[FIRMA ORIGINAL]

En el marco de la CCRA, este certificado está reconocido en el nivel EAL2

Este certificado se emite de conformidad con el Decreto 2002-535 del 18 de abril de 2002, modificado, relativo a la evaluación y certificación de la seguridad ofrecida por los productos y sistemas de tecnología de la información.

Secretaría General de Defensa y Seguridad Nacional, Agencia Nacional de Seguridad de los Sistemas de Información
51, bulevar de La Tour-Maubourg, 75700 PARÍS 07 SP

El producto, objeto de esta certificación, fue evaluado por THALES/CNES con sede en Francia aplicando la Metodología Común para la Evaluación de la Seguridad de las Tecnologías de la Información, versión 3.1, revisión 5, de conformidad con los Criterios Comunes, versión 3.1, revisión 5.

Este certificado se aplica únicamente a esta versión especifica del producto en su configuración evaluada. No puede separarse de su informe de certificación completo. La evaluación se llevó a cabo de conformidad con las disposiciones de la SOG-IS, la CCRA y el régimen francés. Las conclusiones del centro de evaluación, tal y como se establecen en el informe de evaluación técnica, son coherentes con la evidencia aportada.

Esta certificación no constituye en sí misma una recomendación del producto por parte de la Agencia Nacional de Seguridad de los Sistemas de Información y no garantiza que el producto certificado esté completamente libre de vulnerabilidades explotables.

Traducido a petición de la parte interesada el día y registrada en mi protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Dieciocho (18) días del mes de febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de maintenance
ANSSI-CC-2021/20v2-M01

ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration

(Version 3.2.0.52)

Certificat de référence : ANSSI-CC-2021/20v2

Paris, le 28 septembre 2022

Le directeur général de l'Agence nationale
de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

COPY SOLUTIONS INTERNATIONAL SA
RNC 101038052

AVERTISSEMENT

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Página/Folio No.508 de 843

1 Références

[CER]	Rapport de certification ANSSI-CC-2021/20v2, ChipDoc v3.1 on JCOP 4 P71 in SSCD configuration (version 3.1.6.52).
[MAI]	Procédure : Continuité de l'assurance, référence ANSSI-CC-MAI-P-01.
[IAR]	*ChipDoc v3.2 on JCOP 4 P71 v3.2.0.52 Impact Analysis Report, rev 1.0*, 3 juin 2021.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.*
[CCRA]	*Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.*

2 Identification du produit maintenu

Le produit objet de la présente maintenance est « ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration, (Version 3.2.0.52) » développé par la société NXP SEMICONDUCTORS.

Le produit a été certifié avec réduction de portée sous la référence ANSSI-CC-2021/20v2 (référence [CER]).

La version maintenue du produit est identifiable par les éléments suivants :

- l'*applet* est identifiée en réponse à la commande GET_DATA par les valeurs suivantes :
  - Nom : 0x43686970446F63 ;
  - Version : 0x03020052 ;
  - *Card capabilities* : 0x00036FEF ;
- la plateforme est identifiée en réponse à la commande GET_DATA(IDENTIFY) par les valeurs suivantes :
  - *Patch ID* : 0x0000000000000001 ;
  - ROM ID : 2E5AD88409C9BADB ;
  - *Platform ID* : 4A335233353130314641394530343030DD0984593B0048EF ou 4A335233353130323336333130343030DCE5C19CFE6D0DCF ;
- la configuration SSCD de l'application est identifiée par la présence dans le fichier EF.DIR d'un AID au préfixe E828D080F.

3 Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- la correction de *bugs* ;
- l'ajout d'une option de configuration ;
- le retrait d'une commande inutile en phase opérationnelle.

Página/Folio No.509 de 843

4 Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M01] référence la présente maintenance.

[GUIDES]	*ChipDoc 3.2, User Guide Manual, ref 678510*, 22 avril 2021	[R-M01]
	ChipDoc 3.2, SSCD Personalization Guide, ref 678710, 26 avril 2021	[R-M01]
	ChipDoc 3.2, Crypto Guide, révision 1.0, 29 avril 2021	[R-M01]
	ChipDoc V3 Application Note, révision 1.4, 20 juin 2022	[CER]
[ST]	Cibles de sécurité de référence: ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration – Security Target, révision 1.2, 13 juillet 2022, NXP. Version publique : ChipDoc v3.2 on JCOP 4 P71 in SSCD configuration – Security Target Lite, révision 1.2, 13 juillet 2022, NXP.	[R-M01]
[CONF]	*Configuration Item List, CDv3.2_1_04920_ALC_CIL_v2.0*, 19 juillet 2022	[R-M01]

5 Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur.

Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.

6 Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

Página/Folio No.510 de 843

COPY SOGIS INTERNATIONAL SA
RNC. 101068652
Santo Domingo, R.D.

Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs.

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Página/Folio No.511 de 843

Yo, **LIC. SANTO C. SIERRA,** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en Francés, y cuya versión al Español, según mi mejor conocimiento, es el siguiente:

PRIMER MINISTRO

Secretaría General de Defensa y Seguridad Nacional

Libertad

Igualdad

Fraternidad

Agencia de Seguridad Nacional

Sistemas de información

Informe de mantenimiento

ANSSI-CC-2021/20v2-M01

ChipDoc v3.2 en JCOP 4 P71 en configuración SSCD
(Versión 3.2.0.52)

Certificado de referencia: ANSSI-CC-2021/20v2

París, 28 de septiembre de 2022

El Director General de la Agencia Nacional
de seguridad de los sistemas de información

Guillermo POUPARD

[FIRMA ORIGINAL]

ADVERTENCIA

El nivel de resistencia de un producto certificado se degrada con el tiempo. Como parte de este mantenimiento no se realizó un análisis de vulnerabilidad de esta versión del producto con respecto a nuevos ataques que han aparecido desde que se emitió el certificado. Sólo una reevaluación o seguimiento de esta nueva versión del producto permitiría mantener el nivel de confianza en el tiempo.

LIC. SANTO C. SIERRA
Procurador Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.
COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC. 101856852
Santo Domingo, R.D.

Toda correspondencia relacionada con este informe deberá dirigirse a:

Secretaría General de Defensa y Seguridad Nacional Agencia Nacional de Seguridad de los Sistemas de Información
Centro de certificación 51, boulevard de la Tour Maubourg 75700 París cedex 07 SP

certificación@ssi.gouv.fr

Se autoriza la reproducción de este documento sin alteración ni corte.

1 Referencias

[CER]	Informe de certificación ANSSI-CC-2021/20v2, ChipDoc v3.1 en JCOP 4 P71 en configuración SSCD (versión 3.1.6.52).
[PODER]	Procedimiento: Continuidad del seguro, referencia ANSSI-CC-MAI-P-01.
[Y]	Informe de análisis de impacto de ChipDoc v3.2 sobre JCOP 4 P71, v3.2.0.52, revisión 1.0, 3 de junio de 2021.
[SOG-ES]	Acuerdo de Reconocimiento Mutuo de Certificados de Evaluación de Seguridad de Tecnologías de la Información, versión 3.0, 8 de enero de 2010, Comité Directivo.
[ADRC]	Acuerdo sobre el reconocimiento de certificados de Criterios Comunes en el ámbito de la seguridad de las tecnologías de la información, 2 de julio de 2014.

2 Identificación del producto mantenido

El producto sujeto a este mantenimiento es " ChipDoc v3.2 en JCOP 4 P71 en configuración SSCD, (Versión 3.2.0.52)" desarrollado por NXP SEMICONDUCTORS.
El producto ha sido certificado con reducción de rango bajo la referencia ANSSI-CC-2021/20v2 (referencia [CER]).
La versión mantenida del producto se identifica mediante los siguientes elementos:
El subprograma se identifica en respuesta al comando GET_DATA mediante los siguientes valores:

Nombre: 0x43686970446F63;
Versión: 0x03020052;
Capacidades de la tarjeta: 0x00036FEF;

La plataforma se identifica en respuesta al comando GET_DATA(IDENTIFY) mediante los siguientes valores:

ID del parche: 0x000000000000000001;
Identificación de ROM: 2E5AD88409C9BADB;
Identificación de la plataforma: 4A335233353130314641394530343030DD0984593B0048EF o 4A335233353130323336333130343030DCE5C19CFE6D0DCF;

La configuración SSCD de la aplicación se identifica por la presencia en el archivo EF.DIR de un AID con el prefijo E828D080F.

3 Descripción de los desarrollos

El Informe de Análisis de Impacto de Seguridad (IAR) menciona que las modificaciones Se realizaron las siguientes operaciones:

Corrección de errores;
Añadiendo una opción de configuración;
La retirada de un pedido innecesario en la fase operativa.

4 Suministros aplicables

En la siguiente tabla se enumeran los suministros, incluidas las guías aplicables al producto al que se le realiza el mantenimiento. La última columna identifica el origen de la consideración por parte de ANSSI del documento correspondiente. En particular , [R-M01] hace referencia al presente mantenimiento .

[GUIAS]	de ChipDoc 3.2, n.º de pieza 678510, 22 de abril de 2021	[R-M01]
	ChipDoc 3.2, Guía de personalización de SSCD, ref. 678710, 26 de abril de 2021	[R-M01]
	ChipDoc 3.2, Guía de criptografía, revisión 1.0, 29 de abril de 2021	[R-M01]
	de ChipDoc V3, revisión 1.4, 20 de junio de 2022	[CER]
[CALLE]	Objetivos de seguridad de referencia: ChipDoc v3.2 en JCOP 4 P71 en configuración SSCD - Objetivo de seguridad, revisión 1.2, 13 de julio de 2022, NXP. Versión pública: ChipDoc v3.2 en JCOP 4 P71 en configuración SSCD - Objetivo de seguridad Lite, revisión 1.2, 13 de julio de 2022, NO.	[R-M01]
[CONF.]	Lista de elementos de configuración, CDv3.2_1_04920_ALC_CIL_v2.0, 19 de julio de 2022	[R-M01]

5 Conclusiones

Se considera que los desarrollos enumerados anteriormente tienen un impacto menor. Por tanto, el nivel de confianza en esta nueva versión del producto es idéntico al de la versión certificada.

6 Reconocimiento del certificado

Reconocimiento europeo (SOG-IS)

Este certificado se emite bajo los términos del Acuerdo SOG-IS [SOG-IS].

El Acuerdo de Reconocimiento Europeo SOG-IS 2010 permite el reconocimiento, por parte de los países firmantes del acuerdo, de los certificados ITSEC y Common Criteria. El reconocimiento europeo se aplica, para tarjetas inteligentes y dispositivos similares, hasta el nivel ITSEC E6 High y CC EAL7 cuando se cumplen las dependencias CC. Los certificados reconocidos bajo este acuerdo se emiten con la siguiente marca:

Reconocimiento internacional de criterios comunes (CCRA)

Este certificado se emite bajo los términos del Acuerdo CCRA [CCRA].

El acuerdo « Acuerdo de reconocimiento de criterios comunes » permite el reconocimiento, por parte de los países firmantes, de los certificados Criterios comunes.

Traducido a petición de la parte interesada y registrada en mi protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los dieciocho (18) del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

ISO 14443-1

ICUBE
TESTING CENTER

ilac-MRA

cofrac
ESSAIS
Accreditation
n°1-6797
Scope available
on www.cofrac.fr

TEST REPORT

Test of ISO/IEC 14443-1 parameters for eMRTD

REFERENCE:	IC.E.RE.1907.001
VERSION:	v1.0
DATE:	08/08/2019
APPLICANT:	NXP Semiconductors
PRODUCT:	ChipDoc v3 – 3.0

REPORT VALIDATED AND APPROVED BY:

S.JOBARD - Technical manager

IC.E.RE.1907.001_v1.0_SJ.sig

The reproduction of this report is authorized only in its integral format. It comprises 35 pages.

TEST REPORT
Ref.: IC.E.RE.1907.001
Version: v1.0
Date: 08/08/2019

SUMMARY

1 General Information 3
1.1 Test Laboratory Identification 3
1.2 Test Identification 3
1.3 Test Result Terminology 4
2 Object Under Test 5
2.1 Applicant information 5
2.2 Product Identification 5
2.3 Implementation Conformance Statement 6
2.4 Functionality check test 6
3 Test Results 7
3.1 Class-1 Verification Test (conditional) 7
3.2 Static Electricity (ESD) Test 9
3.3 Alternating Magnetic Field 12
4 Conclusion 13

The reproduction of this report is authorized only in its integral format. It comprises 13 pages.

Página/Folio No.519 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo, R.D.

1 GENERAL INFORMATION

1.1 TEST LABORATORY IDENTIFICATION

ICUBE TESTING CENTER
707 chemin du Quintin
13300 Salon de Provence
FRANCE

Contact: contact@icube-tc.com

1.2 TEST IDENTIFICATION

Test of ISO/IEC 14443-1 parameters for eMRTD

This document reports the results of the following tests:
ISO/IEC 18745-2 – Class-1 verification test (conditional)
ISO/IEC 18745-2 – Static Electricity (ESD) test
ISO/IEC 18745-2 – Alternating Magnetic Field test

The tests are performed according to the following reference documents:

[R1] ISO/IEC 18745-2:2016
Information Technology - Test methods for machine readable travel documents (MRTD) and associated devices
Part 2: Test methods for the contactless interface
First edition - Date: 2016-08-15

[R2] ISO/IEC JTC1/SC17/WG8 N2638
Application Profile Contactless Interface Doc 9303
Version v1.3 - Date: 2016-02-03

The tests are performed under ISO/IEC 17025 Cofrac accreditation.

Concerning the results expressed in the quantitative way, the conformity to the specification is declared without taking explicitly into account the uncertainties associated to the results. The samples are considered as "conform" if the result is in the range specified by the document **[R1]**.

Date of the test: 11th of July to 07th of August 2019.
Test performed by: M.GIROD.

The reproduction of this report is authorized only in its integral format. It comprises 13 pages.

Página/Folio No.520 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 1[illegible] Santo Domingo, R.D.

1.3 Test Result Terminology

Result	Description
PASS	Result conforms to the expected result specified in the reference test plan.
FAIL	Result does not conform to the expected result specified in the reference test plan.
NA	Test not applicable. For example for an optional function that is not supported by the product under test.
NE	Test not executed.
NI	Test not implemented.
INC	Inconclusive test.
INF	Informative test.

The reproduction of this report is authorized only in its integral format. It comprises 13 pages.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 01698852 Santo Domingo, R.D.

2 OBJECT UNDER TEST

2.1 APPLICANT INFORMATION

NXP Semiconductors
Mikronweg 1,
8101 Gratkorn,
Austria.

Represented by: Olga Lakusheva.

2.2 PRODUCT IDENTIFICATION

Product name:	ChipDoc v3
Product version:	3.0
Hardware identification and revision:	N7121 B1
Software revision:	JCOP 4 P71
Sample reception date (dd/mm/yyyy):	10/07/2019
Form factor:	Card ID-1 size
Quantity:	9

Reference of the objects under test:

Class -1 verification test
- 7K3704 (Serial number: Not provided)
- 8K3704 (Serial number: Not provided)
- 9K3704 (Serial number: Not provided)

Static electricity (ESD) test
- 4K3704 (Serial number: Not provided)
- 5K3704 (Serial number: Not provided)
- 6K3704 (Serial number: Not provided)

Alternating magnetic Field test
- 1K3704 (Serial number: Not provided)
- 2K3704 (Serial number: Not provided)
- 3K3704 (Serial number: Not provided)

Figure 1 - Sample overview

The reproduction of this report is authorized only in its integral format. It comprises 13 pages.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo R.D.

2.3 IMPLEMENTATION CONFORMANCE STATEMENT

The applicant has provided the information specified in the table below.

Implementation conformance statement	Applicant declaration
Physical size of product	ID-1: YES
Location of antenna within sample	Not provided
PICC class	PICC Class 1
Sample shielded or not and how (*blindage*)	NO
Signal interface • Type A or B	 Type A
Access control applied[1] • BAC • PACE	 YES YES

2.4 FUNCTIONALITY CHECK TEST

The verification is performed according to chapter 5.6.2 of document **[R1]**.

The purpose of this test is to check the eMRTD's mandatory LDS application data. It shall be verified that this information has not been altered by the destructive tests.

The following tools are used to verify the eMRTD's:
- Software tool: Universal Reader Tool – V3.1
- PC/SC contactless reader : SCM Microsystems SDI010

[1] Both supported Access control are applied during the functionality check test defined in § 2.4.

The reproduction of this report is authorized only in its integral format. It comprises 13 pages.

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

3 TEST RESULTS

3.1 CLASS-1 VERIFICATION TEST (CONDITIONAL)

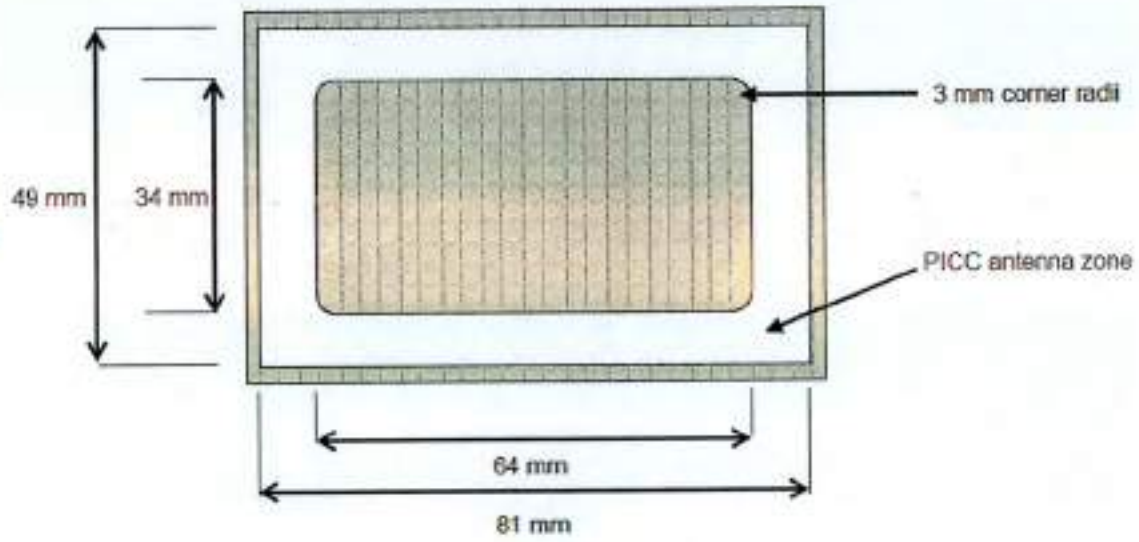
Test:

The test is performed on 3 samples according to chapter 5.2.1 of document **[R1]**.

The purpose of this test is to check if the physical coil dimensions meet the requirements of ISO/IEC 14443-1. The sample antenna shall be entirely located within a zone defined by two rectangles:

- external rectangle: 81mm x 49mm
- internal rectangle: 64mm x 34mm, 3mm radius

except for the connections to the ends of the antenna coil, with a maximum area of 300 mm².



Method:

The measurements are performed with a digital caliper CD-15CPX (Manufacturer: Mitutoyo) on a silver halide photography of the sample.

Test conditions:

Test environment:

- Temperature: 23°C ± 3°C
- Relative humidity: 50% ± 25%

The reproduction of this report is authorized only in its integral format. It comprises 53 pages.

Página/Folio No.524 de 843

COPY SOLUTIONS INTERNATIONAL S.A. de C.V. RNC

TEST REPORT
Ref.: IC.E.RE.1907.001
Version: v1.0
Date: 06/08/2019

Results:

➔ **Object under test:** 7K3704

Dimensions	Expected results according to document [R1]	Observed results	Result
External rectangle	≤ 81 x 49 mm	79.0 x 47.3 mm	PASS
Internal rectangle	≥ 64 x 34 mm 3mm radius	76.0 x 44.2 mm	PASS
Area for the connections to the ends of the antenna coil	≤ 300 mm²	33.0 mm²	PASS

➔ **Object under test:** 8K3704

Dimensions	Expected results according to document [R1]	Observed results	Result
External rectangle	≤ 81 x 49 mm	79.0 x 47.3 mm	PASS
Internal rectangle	≥ 64 x 34 mm 3mm radius	76.0 x 44.4 mm	PASS
Area for the connections to the ends of the antenna coil	≤ 300 mm²	30.6 mm²	PASS

➔ **Object under test:** 9K3704

Dimensions	Expected results according to document [R1]	Observed results	Result
External rectangle	≤ 81 x 49 mm	79.3 x 47.6 mm	PASS
Internal rectangle	≥ 64 x 34 mm 3mm radius	76.3 x 44.5 mm	PASS
Area for the connections to the ends of the antenna coil	≤ 300 mm²	36.5 mm ²	PASS

The reproduction of this report is authorized only in its integral format. It comprises 13 pages.

Página/Folio No.525 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101898852 Santo Domingo, R.D.

3.2 STATIC ELECTRICITY (ESD) TEST

Test:

The purpose of this test is to check the behavior of the sample after an electrostatic discharge (ESD) on the test sample. The device under test is exposed to a simulated electrostatic discharge (ESD, human body model). Its basic operation is checked after the exposure.

The test is performed on 3 samples, according to the test described in the chapter 5.2.2 of document **[R1]**.

Test equipment description:

- DITO ESD gun with air discharge tip, compliant to NF EN 61000-4-2 (Manufacturer: EMTEST)

Method:

The test is performed according to **[R1]** document and ISO/IEC 10373-6:2016, §6.2.2. A discharge is applied to each of the 20 test zones:

- in normal polarity +6kV, and then a discharge is applied in reverse polarity -6kV (ISO/IEC 7810:2003/Amd 1).

Sample is located with contact under the electrostatic discharges, provided by the ESD generator.

Figure 2 – Samples under the electrostatic discharges

The test is applied on 20 zones of the sample:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

The reproduction of this report is authorized only in its integral format. It comprises Página/Folio No.526 de 843

COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC: 101838852
Santo Domingo

The functionality check test defined in chapter 2.4 is done after this test to check whether the sample operates as intended after exposure to the electrostatic discharge.

Test conditions:

Test environment:

- Temperature: 23°C ± 3°C
- Relative humidity: 30% to 60%
- Atmospheric pressure: 96 kPA ± 10 kPA

Legend:

Y	Area tested
N	Area not tested (presence of direct contacts)
DL	Control OK for dual interface (contact and contactless)
CL	Control OK for contactless mode only
CT	Control OK for contact mode only
KO	Control NOK for all interfaces (contact and/or contactless)

The reproduction of this report is authorized only in its integral format. It comprises Página/Folio No.527 de 843

TEST REPORT
Ref.: IC.E.RE.1907.001
Version: v1.0
Date: 08/08/2019

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101896852
Santo Domingo, R.D.

Results:

➔ **Object under test:** 4K3704

Test area																				Controls	Result
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	After +/-6kV discharges	
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	CL	PASS

➔ **Object under test:** 5K3704

Test area																				Controls	Result
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	After +/-6kV discharges	
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	CL	PASS

➔ **Object under test:** 6K3704

Test area																				Controls	Result
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	After +/-6kV discharges	
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	CL	PASS

The reproduction of this report is authorized only in its integral format. It comprises 13 pages.

3.3 ALTERNATING MAGNETIC FIELD

Test:

The purpose of this test is to check the behavior of the sample in relation to alternating magnetic field exposure.

The test is performed on 3 samples according to chapter 5.2.3 of document **[R1]**.
The functionality check test defined in chapter 2.4 is done after the exposure.

Test conditions:

Test environment:

- Temperature: 23°C ± 3°C
- Relative humidity: 50% ± 25%

Test bench:

Tools	Identification and version
Software test environment	SCRIPTIS V01.03.07
Software test suite	ISO/IEC 14443 Test Suite for PICC Analog V05.03 + PATCH 02.12
PICC Contactless Reader	KEOLABS RGPA V3.07.14.409 KEOLABS ProxiLAB V3.24.15.1117
Test PCD Assembly	KEOLABS PCD Assembly ISO/IEC 10373-6
Probe	2 LeCroy PP008
Amplifier	Bowen M02.30.70SBET
Attenuator 10dB	R412.710.124
Oscilloscope	LeCroy WaveRunner 44MXi

Results:

Reference object under test	Information	Result
1K3704	Alternating Magnetic Field for sample 1	PASS
2K3704	Alternating Magnetic Field for sample 2	PASS
3K3704	Alternating Magnetic Field for sample 3	PASS

Página/Folio No.529 de 843

TEST REPORT
Ref.: IC.E.RE.1907.001
Version: v1.0
Date: 08/08/2019

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101888852 Santo Domingo, R.D.

4 CONCLUSION

The following table summarizes the results of the tests performed according to the reference documents identified in §1.2:

Reference of object under test	Test	Result
7K3704	Class -1 verification test (conditional)	PASS
8K3704	Class -1 verification test (conditional)	PASS
9K3704	Class -1 verification test (conditional)	PASS
4K3704	Static Electricity (ESD) test	PASS
5K3704	Static Electricity (ESD) test	PASS
6K3704	Static Electricity (ESD) test	PASS
1K3704	Alternating Magnetic Field Test	PASS
2K3704	Alternating Magnetic Field Test	PASS
3K3704	Alternating Magnetic Field Test	PASS

The samples under test conform to the reference documents identified in section 1.2.

END OF DOCUMENT

The reproduction of this report is authorized only in its integral format. It comprises 13 pages.

Página/Folio No.530 de 843

TRADUCCIÓN OFICIAL: ISO 14443-1

Yo, **LIC. SANTO C. SIERRA**, Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones CERTIFICO: Que he procedido a traducir las partes centrales de un documento, escrito originalmente en Inglés, y cuya versión al Español, según mi mejor conocimiento, es el siguiente:

ICUBE
TESTING CENTER

cofrac
ESSAIS
Accréditation
n°1-6707
Alcance disponible
en www.cofrac.fr

PRUEBA INFORME

Prueba de Normas ISO/IEC 14443-1 parámetros para eMRTD

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, D.N.

REFERENCIA:	IC.E.RE.1907.001
VERSIÓN:	v1.0
FECHA:	08/08/2019
SOLICITANTE:	NXP Semiconductores
PRODUCTO:	ChipDoc versión 3 – 3.0

INFORME VALIDADO Y APROBADO POR:
S. JOBARD - Técnico gerente
IC.E.RE.1905.009_v1.0_SJ.sig

El reproducción de este informe es autorizado solo en es integral formato. Consta de 13 páginas.

RESUMEN

1 **Información General** 3

1.1 Identificación del laboratorio de pruebas 3

1.2 Identificación de la prueba 3

1.3 Terminología de los resultados de las pruebas 4

2 Objeto Bajo Prueba 5

2.1 Información del solicitante 5

2.2 Identificación del producto 5

2.3 Declaración de conformidad de la implementación 6

2.4 Prueba de verificación de funcionalidad 6

3 Resultados de la prueba 7

3.1 Prueba de verificación de clase 1 (condicional) 7

3.2 Prueba de electricidad estática (ESD) 9

3.3 Campo magnético alterno 12

4 Conclusión 13

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 1[illegible]98852 Santo Domingo, R.D.

LIC. SANTO C. SIL... Interprete Judicial Juzg 1ra Instancia ... SANTO DOMINGO, D...

El reproducción de este informe es autorizado solo en es integral formato. Consta de 13 páginas

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101898852 Santo Domingo, R.D.

LIC. SANTO C. SIERRA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

1 INFORMACIÓN GENERAL

1.1 IDENTIFICACIÓN DEL LABORATORIO DE PRUEBAS

CENTRO DE PRUEBAS ICUBE
707 Chemin du Quintin
13300 Salon de Provence
FRANCIA

Contacto:contacto@icube-tc.com

1.2 PRUEBA DE IDENTIFICACION

Prueba de los parámetros ISO/IEC 14443-1 para eMRTD

Este documento informa los resultados de las siguientes pruebas: ISO/IEC 18745-2 – Prueba de verificación de clase 1 (condicional) ISO/IEC 18745-2 – Prueba de electricidad estática (ESD) ISO/IEC 18745-2 – Prueba de campo magnético alterno

Las pruebas se realizan de acuerdo con los siguientes documentos de referencia:

[R1]ISO/IEC 18745-2:2016

Tecnología de la información - Métodos de prueba para documentos de viaje legibles por máquina (MRTD) y dispositivos asociados

Parte 2: Métodos de prueba para la interfaz sin contacto

Primera edición - Fecha: 2016-08-15

[R2]Norma ISO/IEC JTC1/SC17/WG8 N2638

Perfil de aplicación Interfaz sin contacto Doc 9303 Versión v1.3 - Fecha: 2016-02-03

Las pruebas se realizan bajo la acreditación ISO/IEC 17025 Cofrac.

En lo que respecta a los resultados expresados de forma cuantitativa, la conformidad con la especificación se declara sin tener en cuenta explícitamente las incertidumbres asociadas a los resultados. Las muestras se consideran "conformes" si el resultado se encuentra dentro del rango especificado por el documento. [R1].

Fecha de la prueba: 11 de Julio al 07 de Agosto,2019
Prueba realizada por: 2019. M.GIROD.

El reproducción de este informe es autorizado solo en es integral formato. Consta de 13 páginas.

1.3 TERMINOLOGÍA DE RESULTADOS DE PRUEBAS

RESULTADO	Descripción
APROBAR	El resultado se ajusta al resultado esperado especificado en el plan de prueba de referencia
FALLAR	El resultado no se ajusta al resultado esperado especificado en el plan de prueba de referencia.
N / A	Prueba no aplicable. Por ejemplo, para una función opcional que no es compatible con el producto en prueba.
NE	Prueba no ejecutada.
NI	Prueba no implementada.
INC	Prueba no concluyente.
INF	Prueba informativa.

2 OBJETO BAJO PRUEBA

2.1 INFORMACIÓN DEL SOLICITANTE

Semiconductores NXP
Microvia 1,
8101 Gratkorn,
Austria.

Representada por: Olga Lakusheva.

2.2 PRODUCTOIDENTIFICACIÓN

Nombre del producto:	Chipdoc versión 3
Versión del producto:	3.0
Identificación y revisión del hardware:	N7121 B1
Revisión del software:	

Fecha de recepción de muestra (dd/mm/aaaa): 10/07/2019

Factor de forma:	Tamaño de la tarjeta ID-1
Cantidad:	9

Referencia de los objetos en prueba:

Prueba de verificación de clase 1
- 7K3704 (Número de serie: no proporcionado)
- 8K3704 (Número de serie: no proporcionado)
- 9K3704 (Número de serie: no proporcionado)

Prueba de electricidad estática (ESD)
- 4K3704 (Número de serie: no proporcionado)
- 5K3704 (Número de serie: no proporcionado)
- 6K3704 (Número de serie: no proporcionado)

Prueba de campo magnético alterno
- 1K3704 (Número de serie: no proporcionado)
- 2K3704 (Número de serie: no proporcionado)
- 3K3704 (Número de serie: no proporcionado)

Figura 1 - Ejemplo de descripción general

El reproducción de este informe es autorizado solo en es integral formato. Consta de 13 páginas

2.3 IMPLEMENTACIÓN de CONFORMIDAD DECLARACIÓN

El solicitante ha proporcionado la información especificada en la siguiente tabla.

Declaración de conformidad de implementación	Declaración del solicitante
Tamaño físico del producto	ID-1: SI
Ubicación de la antena dentro de la muestra	No proporcionado
Clase PICC	PICC Clase 1
Muestra blindada o no y como (*blindaje*)	NO
Interfaz de señal • Tipo A o B	Tipo A
Control de acceso aplicado - Nivel de alcohol en sangre • PASO	Sí Sí

2.4 PRUEBA DE VERIFICACIÓN DE FUNCIONALIDAD

La verificación se realiza de acuerdo con el capítulo 5.6.2 del documento [R1].

El objetivo de esta prueba es verificar los datos obligatorios de la solicitud de LDS del eMRTD. Se verificará que esta información no haya sido alterada por las pruebas destructivas.

Para verificar los eMRTD se utilizan las siguientes herramientas:

- **Herramienta de software: Universal Reader Tool – V3.1**
- **Lector sin contacto PC/SC: SCM Microsystems SDI010**

Ambos controles de acceso admitidos se aplican durante la prueba de verificación de funcionalidad definida en § 2.4.

El reproducción de este informe es autorizado solo en es integral formato. Consta de 13 páginas

3 RESULTADOS DE LA PRUEBA

3.1 CLASE-1 PRUEBA DE VERIFICACION (CONDICIONAL)

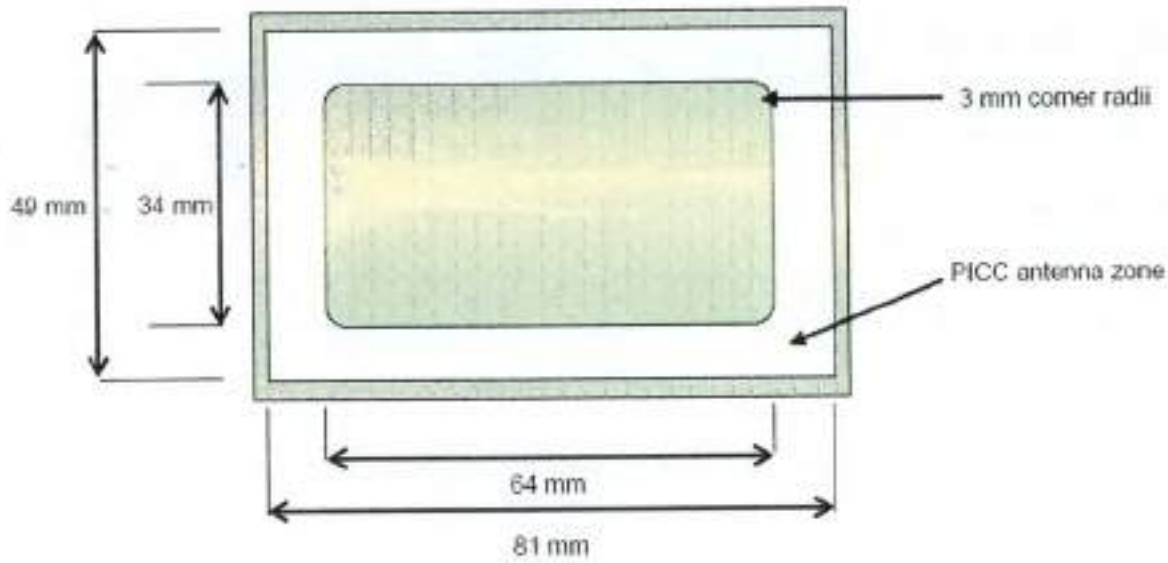
PRUEBA:

La prueba se realiza en 3 muestras de acuerdo con el capítulo 5.2.1 del documento [R1].

El objetivo de esta prueba es comprobar si las dimensiones físicas de la bobina cumplen los requisitos de la norma ISO/ IEC 14443-1. La antena de muestra deberá estar ubicada en su totalidad dentro de una zona definida por dos rectángulos:

- **Rectángulo Externo: 81 mm x 49 mm**
- **Rectángulo Interno:64 mm x 34 mm, radio de 3 mm**

Excepto las conexiones a los extremos de la bobina de la antena, con un área máxima de 300 mm2.



Método:

Las mediciones se realizan con un calibrador digital CD-15CPX (Fabricante: Mitutoyo) sobre una fotografía de haluro de plata de la muestra.

Condiciones de prueba:

Entorno de prueba:

- **Temperatura: 23°C ± 3°C**
- **Humedad relativa: 50% ± 25%**

Resultados:

-Objeto bajo prueba:7K3704

Dimensiones	Resultados esperados Según el documento [R1]	Resultados observados	Resultado
Rectángulo externo	≤ 81 x 49 mm	79,0 x 47,3 mm	APROBAR
Rectángulo interno	≥ 64 x 34 mm Radio de 3 mm	76,0 x 44,2 mm	APROBAR
Área para las conexiones a los extremos de la bobina de la antena.	≤ 300 mm2	33,0 mm²	APROBAR

-Objeto bajo prueba:8K3704

Dimensiones	Resultados esperados Según el documento [R1]	Resultados observados	Resultado
Rectángulo externo	≤ 81 x 49 mm	79,0 x 47,3 mm	APROBAR
Rectángulo interno	≥ 64 x 34 mm Radio de 3 mm	76,0 x 44,4 mm	APROBAR
Área para las conexiones a los extremos de la bobina de la antena.	≤ 300 mm2	30,6 mm²	APROBAR

-Objeto bajo prueba:9K3704

Dimensiones	Resultados esperados Según el documento [R1]	Resultados observados	Resultado
Rectángulo externo	≤ 81 x 49 mm	79,3 x 47,6 mm	APROBAR
Rectángulo interno	≥ 64 x 34 mm Radio de 3 mm	76,3 x 44,5 mm	APROBAR
Área para las conexiones a los extremos de la bobina de la antena.	≤ 300 mm2	36,5 mm²	APROBAR

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101[illegible]852 Santo Domingo, R.D.

LIC. SANTO C. SIERRA Intérprete Judicial Juzg 1ra Instancia SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101856852 Santo Domingo, R.D.

3.2 ESTADISTICA ELECTRICA (ESD) PRUEBA

PRUEBA:

El objetivo de esta prueba es comprobar el comportamiento de la muestra tras una descarga electrostática (ESD) sobre la muestra de prueba. El dispositivo sometido a prueba se expone a una descarga electrostática simulada (ESD, modelo de cuerpo humano). Su funcionamiento básico se comprueba después de la exposición.

La prueba se realiza en 3 muestras, según la prueba descrita en el capítulo 5.2.2 del documento[R1].

Descripción del equipo de prueba:

- **Pistola ESD DITO con boquilla de descarga de aire, conforme a NF EN 61000-4-2 (Fabricante: EMTEST)**

Método:

La prueba se realiza de acuerdo con [R1]documento y la norma ISO/IEC 10373-6:2016, §6.2.2. Se aplica una descarga a cada una de las 20 zonas de prueba:

- **en polaridad normal +6kV, y luego se aplica una descarga en polaridad inversa -6kV (ISO/IEC 7810:2003/Amd 1).**

La muestra se encuentra en contacto con las descargas electrostáticas proporcionadas por el generador ESD.

Figura 2 – Muestras bajo descargas electrostáticas

LIC. SANTO C. SIENA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

La prueba se aplica en 20 zonas de la muestra:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

COPY SOLUTIONS INTERNATIONAL SA
CSI
RNC. 101898652
Santo Domingo, R.D.

La prueba de verificación de funcionalidad definida en el capitulo 2.4 se realiza después de esta prueba para verificar si la muestra funciona según lo previsto después de la exposición a la descarga electrostática.

Condiciones de prueba:

Entorno de prueba:

- **Temperatura: 23°C ± 3°C**
- **Humedad relativa: 30% a 60%**
- **Presión atmosférica: 96 kPA ± 10 kPA**

Leyenda:

Y	Área probada
N	Área no probada (presencia de contactos directos) Control
DL	OK para interfaz dual (contacto y sin contacto) Control OK
CL	solo para modo sin contacto
CT	Control OK solo para modo de contacto
KO.	Control NOK para todas las interfaces (con contacto y/o sin contacto)

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101[illegible]
Santo Domingo R.D.

Resultados:

-Objeto bajo prueba:4K3704

Area de pruebas																			Controles	Resultado
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Después de +/-8kV descargas	
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	CL	APROBAR

-Objeto bajo prueba:5K3704

Area de pruebas																			Controles	Resultado
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Después de +/-8kV descargas	
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	CL	APROBAR

-Objeto bajo prueba:6K3704

Area de pruebas																			Controles	Resultado
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Después de +/-8kV descargas	
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	CL	APROBAR

LIC. SANTO C. SIERRA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101898852 Santo Domingo, R.D.

3.3 CAMPO MAGNÉTICO ALTERNO

PRUEBA:

El propósito de esta prueba es verificar el comportamiento de la muestra en relación con la exposición a un campo magnético alterno.

La prueba se realiza en 3 muestras de acuerdo con el capítulo 5.2.3 del documento[R1]La prueba de verificación de funcionalidad definida en el capítulo 2.4 se realiza después de la exposición.

LIC. SANTO C. SILVA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

CONDICIONES DE PRUEBA:

Entorno de prueba:

- **Temperatura: 23°C ± 3°C**
- **Humedad relativa: 50% ± 25%**

Banco de pruebas:

Herramientas	Identificación y versión
Entorno de prueba de software	SCRIPTIS V01.03.07
Conjunto de pruebas de software	Conjunto de pruebas ISO/IEC 14443 para PICC analógico V05.03 + PATCH_02.12
Lector PICC sin contacto	KEOLABS RGPA V3.07.14.409 KEOLABS ProxiLAB V3.24.15.1117
Prueba del conjunto PCD	Conjunto de PCD KEOLABS ISO/IEC 10373-6
Sonda	2 LeCroy PP008
Amplificador	Bowen M02.30.70SBET
Atenuador 10dB	R412.710.124
Osciloscopio	Moto acuática LeCroy WaveRunner 44MXI

Resultados:

Objeto de referencia bajo prueba	Información	Resultado
1K3704	Campo magnético alterno para la muestra 1	APROBAR
2K3704	Campo magnético alterno para la muestra 2	APROBAR
3K3704	Campo magnético alterno para la muestra 3	APROBAR

COPY SOLUTIONS INTERNATIONAL SA
CSI
RNC: 101098852
Santo Domingo, R.D.

4. CONCLUSIÓN

La siguiente tabla resume los resultados de las pruebas realizadas según los documentos de referencia identificados en el §1.2:

Referencia de objeto bajo prueba	Prueba	Resultado
7K3704	Prueba de verificación de clase -1 (condicional)	APROBAR
8K3704	Prueba de verificación de clase -1 (condicional)	APROBAR
9K3704	Prueba de verificación de clase -1 (condicional)	APROBAR
4K3704	Prueba de electricidad estática (ESD)	APROBAR
5K3704	Prueba de electricidad estática (ESD)	APROBAR
6K3704	Prueba de electricidad estática (ESD)	APROBAR
1K3704	Prueba de campo magnético alterno	APROBAR
2K3704	Prueba de campo magnético alterno	APROBAR
3K3704	Prueba de campo magnético alterno	APROBAR

Las muestras sometidas a ensayo se ajustan a los documentos de referencia identificados en el apartado 1.2.

FIN DEL DOCUMENTO

Traducido a petición de la parte interesada y registrada en mí protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Diecinueve (19) del mes de Febrero del año Dos Mil Veinticinco (2025).

MINISTERIO PUBLICO
CENTRO DE ATENCIÓN AL CIUDADANO DN
Procuraduría General de la República
Código QR: 001-5202-2880166-0
S.C.S / DPE
5184-12-8-96

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

ISO 14443-2

ICUBE
TESTING CENTER

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC 101898852
Santo Domingo, R.D.

ilac-MRA

cofrac
ESSAIS
Accreditation
n°1-6707
Scope available
on www.cofrac.fr

TEST REPORT

Test of ISO/IEC 14443-2 parameters for eMRTD

REFERENCE:	IC.E:RE.1905.009
VERSION:	v1.0
DATE:	17/06/2019
APPLICANT:	NXP Semiconductors
PRODUCT:	ChipDoc v3 – 3.0

REPORT VALIDATED AND APPROVED BY:
S.JOBARD - Technical manager
IC.E.RE.1905.009_v1.0_SJ.sig

The reproduction of this report is authorized only in its integral format. It comprises 84 pages.

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101898852
Santo Domingo

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

SUMMARY

1 General Information 3
1.1 Test Laboratory Identification 3
1.2 Test Identification 3
1.3 Test Environement 4
1.4 Test Tools 4
1.5 Test Result Terminology 5
2 Object Under Test 6
2.1 Applicant information 6
2.2 Product Identification 6
2.3 Implementation Conformance Statement 7
3 Test Results 8
3.1 eMRTD Transmission (Load Modulation Amplitude) 8
3.2 Operating Field Strength 26
3.3 eMRTD Reception 29
3.4 eMRTD Resonance Frequency 35
3.5 eMRTD Maximum Loading Effect 36
3.6 eMRTD Reading Performance Analysis 37
4 Conclusion 39

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

1 GENERAL INFORMATION

1.1 TEST LABORATORY IDENTIFICATION

ICUBE TESTING CENTER
707 chemin du Quintin
13300 Salon de Provence
FRANCE

Contact: contact@icube-tc.com

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101088852 Santo Domingo, R.D.

1.2 TEST IDENTIFICATION

Test of ISO/IEC 14443-2 parameters for eMRTD

This document reports the results of the following tests:
- eMRTD Transmission,
- Operating Field Strength,
- eMRTD Reception,
- eMRTD Resonance Frequency,
- eMRTD Maximum Loading Effect.

The test method used conforms to the following specification:

[R1] ISO/IEC 18745-2:2016
Information Technology Test methods for machine readable travel document (MRTD) and associated devices
Part 2: Test methods for the contactless interface
First edition Date: 2016-08-15

[R2] ISO/IEC JTC1/SC17/WG8 N2638
Application Profile Contactless Interface Doc 9303
Version v1.3 Date: 2016-02-03

[R3] ISO/IEC of ISO/IEC 10373-6:2016
Identification cards - Test methods - Part 6: Proximity cards
Third edition - Date: 2016-07-15

The resonance frequency test is not performed under ISO/IEC 17025 Cofrac accreditation.

Concerning the results expressed in the quantitative way, the conformity to the specification is declared without taking explicitly into account the uncertainties associated to the results. The samples are considered as "conform" if the result is in the range specified by the reference document.

Date of the test: 18th to 27th of June 2019.
Test performed by: M.GIROD.

The reproduction of this report is authorized only in its integral format. It comprises [illegible] pages.

Página/Folio No.548 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 1[illegible]852 Santo Domingo

1.3 TEST ENVIRONEMENT

The tests are performed under the following conditions:

Temperature	Relative humidity
+23°C ± 3°C	25% to 75%
+50°C ± 3°C	-
-10°C ± 3°C	-

The tests at +50°C and -10°C temperatures are performed in climate chamber.

1.4 TEST TOOLS

Hardware and software	Identification and version
Software test environment	SCRIPTIS™ v01.04.01 + Patch 4
Software test suite	ISO/IEC 14443 Test Suite for PICC Analog v06.00 + Patch 2 + Patch_Field_Offset + Patch Noise Measurement v2 ISO/IEC 18745-2 test Suite for PICC Analog v01.01 + Patch 1 + Patch Command2preconditions.py + ScriptisEPassportAnalog v01.16-IC.SW.1702.002
PICC Contactless Reader Software version	KEOLABS RGPA v3.12.17.0227 KEOLABS ProxiLAB v4.28.17.0628
PICC Contactless Reader Hardware version	KEOLABS ProxiLAB Quest v4.1
PCD Assembly	KEOLABS PCD Assembly ISO/IEC 10373-6 High Speed
	KEOLABS PCD Assembly ISO/IEC 10373-6 Low Speed
Reference PICC	KEOLABS Reference PICC ISO/IEC 10373-6 Class 1 at 13.56 MHz
Probes	2 LeCroy PP018 KEOLABS PICC Probe KEOLABS SC-PICC-Probe+ v1.9
Amplifier	Bowen M02.30.70S
Oscilloscope	LeCroy HDO 6034A
Climate chamber	BINDER MKF 240

The reproduction of this report is authorized only in its integral format. It comprises [illegible]

1.5 TEST RESULT TERMINOLOGY

Result	Description
PASS	Result conforms to the expected result specified in the reference test plan.
FAIL	Result does not conform to the expected result specified in the reference test plan.
NA	Test not applicable. For example, for an optional function that is not supported by the product under test.
NE	Test not executed.
NI	Test not implemented.
INC	Inconclusive test.
INF	Informative test.

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

Página/Folio No.550 de 843

2 OBJECT UNDER TEST

2.1 APPLICANT INFORMATION

NXP Semiconductors
Mikronweg 1,
8101 Gratkorn,
Austria

Represented by: Olga Iakusheva.

2.2 PRODUCT IDENTIFICATION

Product name:	ChipDoc v3
Product version:	3.0
Hardware identification and revision:	N7121 B1
Software revision:	JCOP 4 P71
Sample reception date (dd/mm/yyyy):	12/06/2019
Form factor:	Card ID-1 Size
Quantity:	3

Reference of the objects under test:
- 1K3606 (Serial number: Not provided)
- 2K3606 (Serial number: Not provided)
- 3K3606 (Serial number: Not provided)

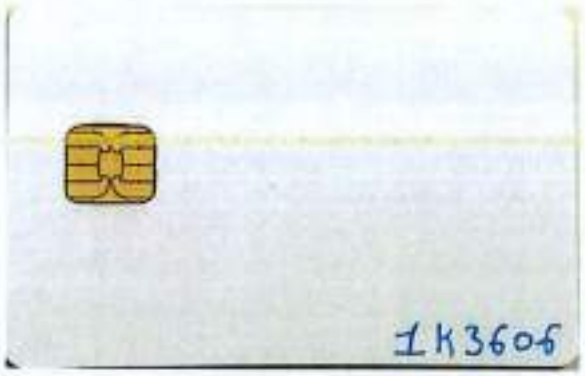


Figure 1 Sample overview

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.
Página/Folio No.551 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101898852 Santo Domingo, R.D.

2.3 IMPLEMENTATION CONFORMANCE STATEMENT

The applicant has provided the information specified in the table below.

Information for test setup	
Physical size of product	ID-1: YES
Location of antenna within e-MRTD	Not provided
PICC class	PICC Class 1
e-MRTD shielded or not and how (*blindage*)	NO
Resonance frequency range (if optional test is performed) Power	Not provided ☒ 0 dBm ☐ 10 dBm
Signal Interface • Type A or B	 Type A
Bit rates supported • From eMRTD to eMRTD reader o 106 kbit/s o 212 kbit/s o 424 kbit/s o 848 kbit/s o 1.7 Mbit/s o 3.4 Mbit/s o 6.8 Mbit/s • From eMRTD reader to eMRTD o 106 kbit/s o 212 kbit/s o 424 kbit/s o 848 kbit/s o 1.7 Mbit/s o 3.4 Mbit/s o 6.8 Mbit/s	 YES YES YES YES YES YES NO YES YES YES YES NO NO NO
Access control applied[1] • BAC • EAC • PACE	 NO YES YES
Active Authentication	YES
Extended APDU required for AA	YES
Cryptographic options: • Dynamic binding • Static binding	 YES NO

[1] TEST_COMMAND_SEQUENCE_1 used for Operating Field Strength test.

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC. 1 Santo Domingo

3 TEST RESULTS

3.1 eMRTD Transmission (Load Modulation Amplitude)

Method:

The test method used conforms to document **[R1]** chapter 5.3.1.

The results for bit rates higher than 848 kbit/s are performed according to document **[R3]** chapter 7.2.1.1.

This test is covered by ISO/IEC 17025 Cofrac accreditation.

Test conditions:

The test is performed under the conditions defined in §1.3.

At +50°C temperature, *Transmissions* at H= 6.5 A/m and 7.5A/m are not applicable. They are replaced by one test performed at 6 A/m.

3.1.1 Temperature -10°C

Results:

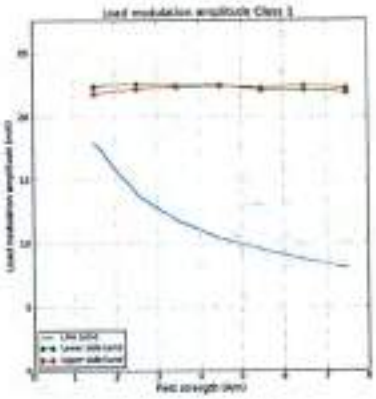
Load Modulation Amplitude at 106 kbit/s:

Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @106 kbit/s	1.5	18.0	21.8	22.4	PASS
		2.5	13.9	22.2	22.6	PASS
		3.5	11.8	22.3	22.4	PASS
		4.5	10.4	22.4	22.4	PASS
		5.5	9.4	22.2	22.1	PASS
		6.5	8.6	22.4	22.1	PASS
		7.5	8.0	22.2	21.9	PASS
2K3606	eMRTD Transmission for Sample 2 @106 kbit/s	1.5	18.0	22.2	22.7	PASS
		2.5	13.9	22.6	22.8	PASS
		3.5	11.8	22.8	22.6	PASS
		4.5	10.4	22.8	22.7	PASS
		5.5	9.4	22.8	22.6	PASS
		6.5	8.6	22.8	22.3	PASS
		7.5	8.0	22.8	22.3	PASS
3K3606	eMRTD Transmission for Sample 3 @106 kbit/s	1.5	18.0	21.9	22.7	PASS
		2.5	13.9	22.3	22.8	PASS
		3.5	11.8	22.4	22.8	PASS
		4.5	10.4	22.6	22.8	PASS
		5.5	9.4	22.6	22.5	PASS
		6.5	8.6	22.5	22.4	PASS
		7.5	8.0	21.7	21.4	PASS

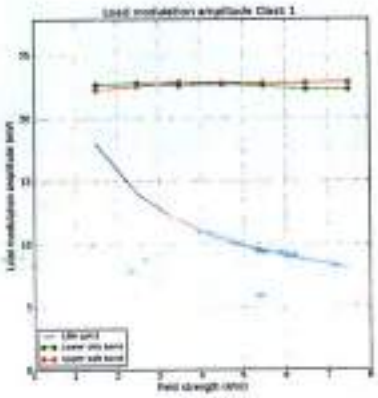
The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

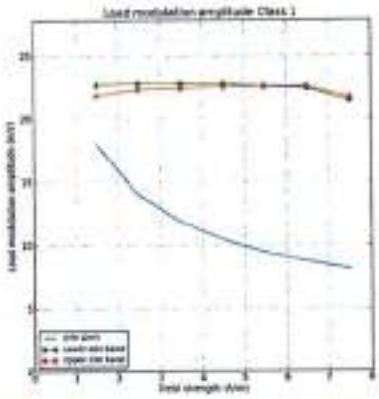
COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101895852
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @106 kbit/s



Curve Load Modulation Amplitude of the sample 2 @106 kbit/s



Curve Load Modulation Amplitude of the sample 3 @106 kbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.
Página/Folio No.554 de 843

COPY SOLUTIONS INTERNATIONAL S.R.L.
CSI
RNC 1-30-89-...
Santo Domingo

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

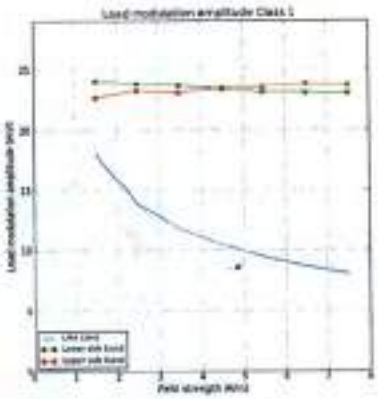
Load Modulation Amplitude at 1.7 Mbit/s:

Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @1.7 Mbit/s	1.5	18.0	22.7	24.1	PASS
		2.5	13.9	23.3	23.9	PASS
		3.5	11.8	23.1	23.7	PASS
		4.5	10.4	23.5	23.3	PASS
		5.5	9.4	23.5	23.1	PASS
		6.5	8.6	23.8	23.1	PASS
		7.5	8.0	23.7	23.0	PASS
2K3606	eMRTD Transmission for Sample 2 @1.7 Mbit/s	1.5	18.0	22.4	23.4	PASS
		2.5	13.9	22.7	23.1	PASS
		3.5	11.8	22.9	22.9	PASS
		4.5	10.4	23.0	22.8	PASS
		5.5	9.4	23.2	22.6	PASS
		6.5	8.6	23.4	22.4	PASS
		7.5	8.0	23.4	22.3	PASS
3K3606	eMRTD Transmission for Sample 3 @1.7 Mbit/s	1.5	18.0	22.0	23.5	PASS
		2.5	13.9	22.4	23.2	PASS
		3.5	11.8	22.5	23.1	PASS
		4.5	10.4	22.7	22.9	PASS
		5.5	9.4	23.1	22.7	PASS
		6.5	8.6	23.0	22.4	PASS
		7.5	8.0	23.1	22.4	PASS

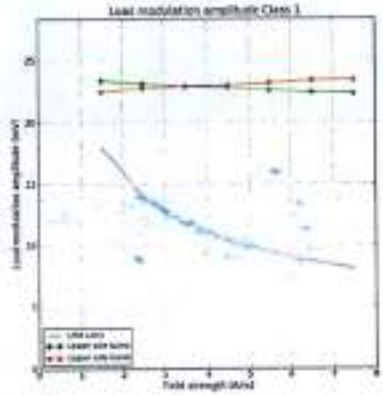
The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

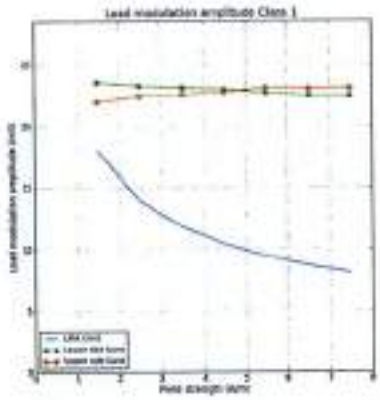
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898652
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @1.7 Mbit/s



Curve Load Modulation Amplitude of the sample 2 @1.7 Mbit/s



Curve Load Modulation Amplitude of the sample 3 @1.7 Mbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101698852 Santo Domingo, R.D.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

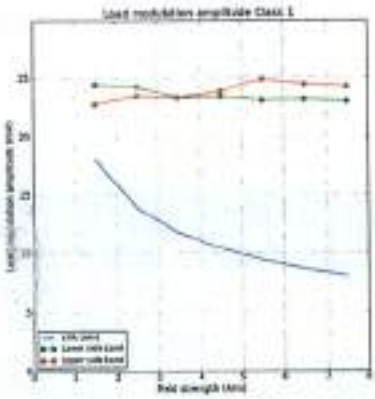
Load Modulation Amplitude at 3.4 Mbit/s:

Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @3.4 Mbit/s	1.5	18.0	22.7	24.4	PASS
		2.5	13.9	23.4	24.2	PASS
		3.5	11.8	23.3	23.3	PASS
		4.5	10.4	23.8	23.4	PASS
		5.5	9.4	24.8	23.0	PASS
		6.5	8.6	24.4	23.1	PASS
		7.5	8.0	24.2	23.0	PASS
2K3606	eMRTD Transmission for Sample 2 @3.4 Mbit/s	1.5	18.0	22.6	23.7	PASS
		2.5	13.9	23.1	23.4	PASS
		3.5	11.8	23.1	22.7	PASS
		4.5	10.4	23.2	22.4	PASS
		5.5	9.4	24.3	22.4	PASS
		6.5	8.6	24.1	22.1	PASS
		7.5	8.0	23.8	22.2	PASS
3K3606	eMRTD Transmission for Sample 3 @3.4 Mbit/s	1.5	18.0	22.0	24.2	PASS
		2.5	13.9	22.5	23.9	PASS
		3.5	11.8	22.5	23.1	PASS
		4.5	10.4	23.2	22.9	PASS
		5.5	9.4	23.5	22.8	PASS
		6.5	8.6	23.3	22.7	PASS
		7.5	8.0	23.3	22.4	PASS

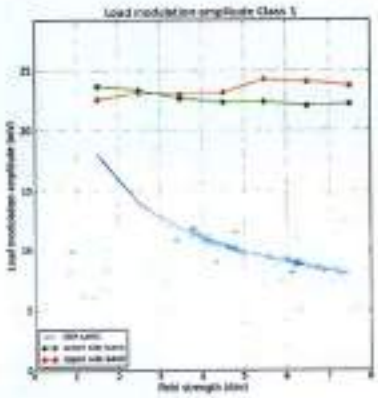
The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

Página/Folio No.557 de 843

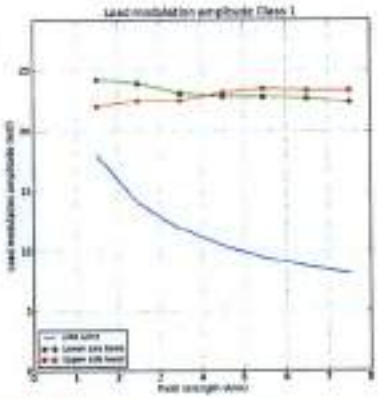
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @3.4 Mbit/s



Curve Load Modulation Amplitude of the sample 2 @3.4 Mbit/s



Curve Load Modulation Amplitude of the sample 3 @3.4 Mbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

Página/Folio No.558 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101698852 Santo Domingo, R.D.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

3.1.2 Temperature +23°C

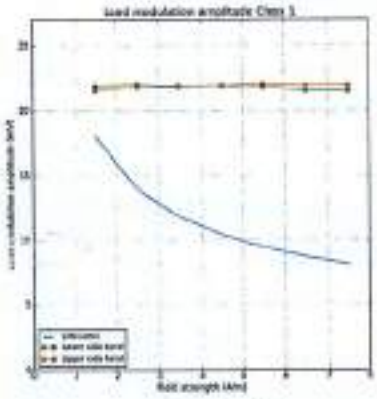
Results:

Load Modulation Amplitude at 106 kbit/s:

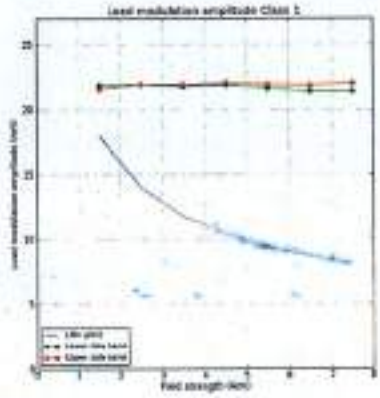
Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @106 kbit/s	1.5	18.0	21.5	21.9	PASS
		2.5	13.9	21.8	22.0	PASS
		3.5	11.8	21.8	21.8	PASS
		4.5	10.4	21.9	21.9	PASS
		5.5	9.4	22.0	21.8	PASS
		6.5	8.6	21.9	21.5	PASS
		7.5	8.0	21.9	21.4	PASS
2K3606	eMRTD Transmission for Sample 2 @106 kbit/s	1.5	18.0	21.6	21.9	PASS
		2.5	13.9	21.9	21.9	PASS
		3.5	11.8	21.9	21.8	PASS
		4.5	10.4	22.0	21.9	PASS
		5.5	9.4	21.9	21.7	PASS
		6.5	8.6	21.9	21.4	PASS
		7.5	8.0	22.0	21.4	PASS
3K3606	eMRTD Transmission for Sample 3 @106 kbit/s	1.5	18.0	21.3	21.9	PASS
		2.5	13.9	21.7	22.0	PASS
		3.5	11.8	21.8	21.8	PASS
		4.5	10.4	21.8	21.9	PASS
		5.5	9.4	21.8	21.7	PASS
		6.5	8.6	21.7	21.5	PASS
		7.5	8.0	21.9	21.5	PASS

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

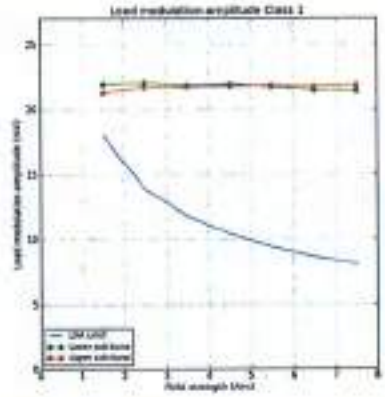
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @106 kbit/s



Curve Load Modulation Amplitude of the sample 2 @106 kbit/s



Curve Load Modulation Amplitude of the sample 3 @106 kbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC: 101882852 Santo Domingo

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

Load Modulation Amplitude at 1.7 Mbit/s:

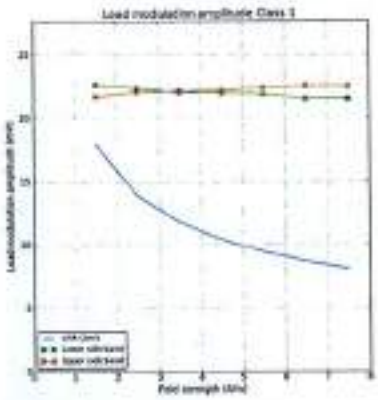
Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @1.7 Mbit/s	1.5	18.0	21.7	22.7	PASS
		2.5	13.9	22.1	22.4	PASS
		3.5	11.8	22.2	22.0	PASS
		4.5	10.4	22.2	22.0	PASS
		5.5	9.4	22.4	21.9	PASS
		6.5	8.6	22.5	21.5	PASS
		7.5	8.0	22.5	21.5	PASS
2K3606	eMRTD Transmission for Sample 2 @1.7 Mbit/s	1.5	18.0	21.9	22.6	PASS
		2.5	13.9	22.2	22.4	PASS
		3.5	11.8	22.3	22.0	PASS
		4.5	10.4	22.3	21.9	PASS
		5.5	9.4	22.5	21.7	PASS
		6.5	8.6	22.5	21.5	PASS
		7.5	8.0	22.6	21.4	PASS
3K3606	eMRTD Transmission for Sample 3 @1.7 Mbit/s	1.5	18.0	21.6	22.9	PASS
		2.5	13.9	22.1	22.5	PASS
		3.5	11.8	22.0	22.3	PASS
		4.5	10.4	22.2	22.1	PASS
		5.5	9.4	22.5	21.9	PASS
		6.5	8.6	22.5	21.7	PASS
		7.5	8.0	22.4	21.6	PASS

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

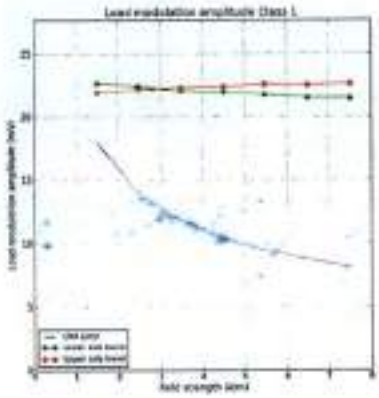
Página/Folio No.561 de 843

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

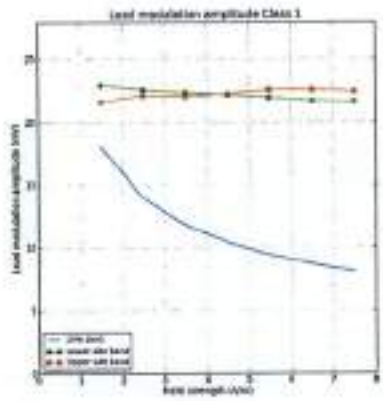
COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC: 101696852
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @1.7 Mbit/s



Curve Load Modulation Amplitude of the sample 2 @1.7 Mbit/s



Curve Load Modulation Amplitude of the sample 3 @1.7 Mbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101008852 Santo Domingo

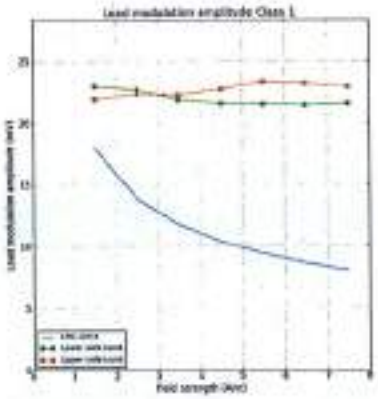
TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

Load Modulation Amplitude at 3.4 Mbit/s:

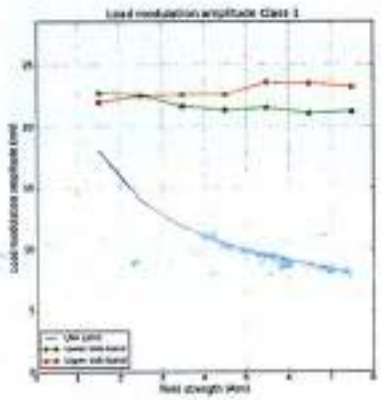
Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @3.4 Mbit/s	1.5	18.0	21.9	23.0	PASS
		2.5	13.9	22.4	22.7	PASS
		3.5	11.8	22.3	21.9	PASS
		4.5	10.4	22.7	21.6	PASS
		5.5	9.4	23.4	21.6	PASS
		6.5	8.6	23.2	21.4	PASS
		7.5	8.0	23.0	21.6	PASS
2K3606	eMRTD Transmission for Sample 2 @3.4 Mbit/s	1.5	18.0	21.9	22.7	PASS
		2.5	13.9	22.5	22.5	PASS
		3.5	11.8	22.6	21.6	PASS
		4.5	10.4	22.6	21.3	PASS
		5.5	9.4	23.6	21.5	PASS
		6.5	8.6	23.5	21.1	PASS
		7.5	8.0	23.2	21.2	PASS
3K3606	eMRTD Transmission for Sample 3 @3.4 Mbit/s	1.5	18.0	21.6	23.3	PASS
		2.5	13.9	22.3	22.9	PASS
		3.5	11.8	22.3	22.2	PASS
		4.5	10.4	22.7	21.9	PASS
		5.5	9.4	23.3	21.9	PASS
		6.5	8.6	23.0	21.6	PASS
		7.5	8.0	23.0	21.6	PASS

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

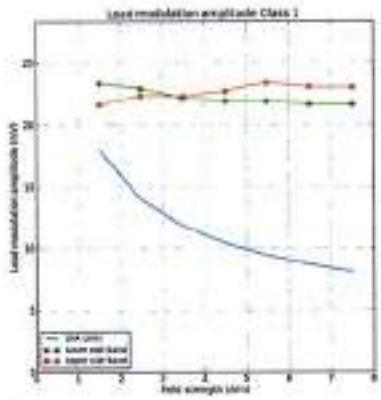
COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @3.4 Mbit/s



Curve Load Modulation Amplitude of the sample 2 @3.4 Mbit/s



Curve Load Modulation Amplitude of the sample 3 @3.4 Mbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL CSI RNC: 101 Santo Domingo

3.1.3 Temperature +50°C

Results:

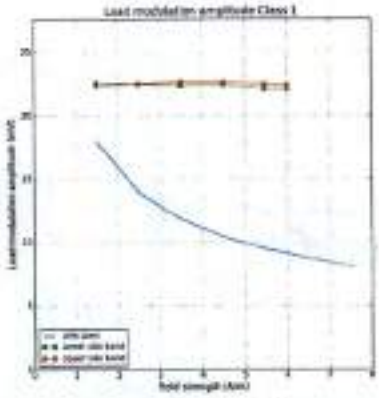
Load Modulation Amplitude at 106 kbit/s:

Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @106 kbit/s	1.5	18.0	22.3	22.5	PASS
		2.5	13.9	22.5	22.4	PASS
		3.5	11.8	22.6	22.3	PASS
		4.5	10.4	22.6	22.4	PASS
		5.5	9.4	22.4	22.0	PASS
		6.0	9.0	22.4	22.0	PASS
2K3606	eMRTD Transmission for Sample 2 @106 kbit/s	1.5	18.0	22.3	22.4	PASS
		2.5	13.9	22.7	22.4	PASS
		3.5	11.8	22.6	22.4	PASS
		4.5	10.4	22.7	22.4	PASS
		5.5	9.4	22.6	22.2	PASS
		6.0	9.0	22.5	22.0	PASS
3K3606	eMRTD Transmission for Sample 3 @106 kbit/s	1.5	18.0	21.3	21.7	PASS
		2.5	13.9	21.6	21.8	PASS
		3.5	11.8	21.7	21.7	PASS
		4.5	10.4	21.7	21.7	PASS
		5.5	9.4	21.7	21.5	PASS
		6.0	9.0	21.6	21.3	PASS

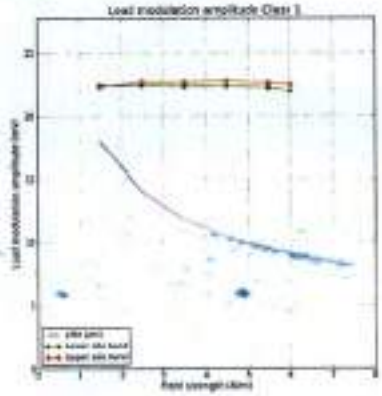
The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

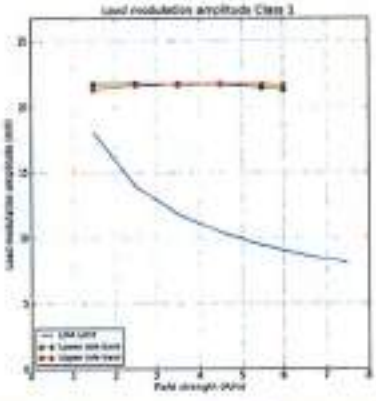
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @106 kbit/s



Curve Load Modulation Amplitude of the sample 2 @106 kbit/s



Curve Load Modulation Amplitude of the sample 3 @106 kbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101008852 Santo Domingo

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

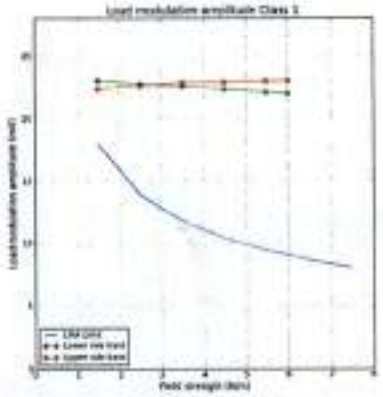
Load Modulation Amplitude at 1.7 Mbit/s:

Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @1.7 Mbit/s	1.5	18.0	22.4	23.1	PASS
		2.5	13.9	22.7	22.8	PASS
		3.5	11.8	22.9	22.6	PASS
		4.5	10.4	22.9	22.4	PASS
		5.5	9.4	23.0	22.1	PASS
		6.0	9.0	23.1	22.0	PASS
2K3606	eMRTD Transmission for Sample 2 @1.7 Mbit/s	1.5	18.0	22.4	22.8	PASS
		2.5	13.9	22.7	22.6	PASS
		3.5	11.8	23.0	22.3	PASS
		4.5	10.4	22.9	22.3	PASS
		5.5	9.4	23.0	21.9	PASS
		6.0	9.0	22.9	21.7	PASS
3K3606	eMRTD Transmission for Sample 3 @1.7 Mbit/s	1.5	18.0	21.5	22.4	PASS
		2.5	13.9	21.9	22.2	PASS
		3.5	11.8	21.9	21.8	PASS
		4.5	10.4	22.2	21.8	PASS
		5.5	9.4	22.2	21.6	PASS
		6.0	9.0	22.1	21.4	PASS

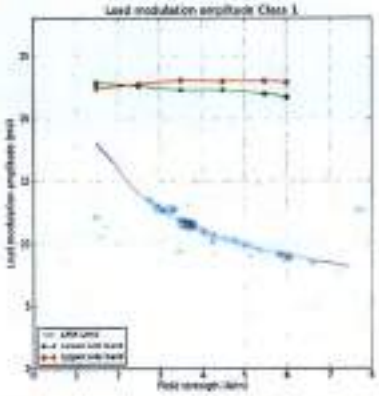
The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

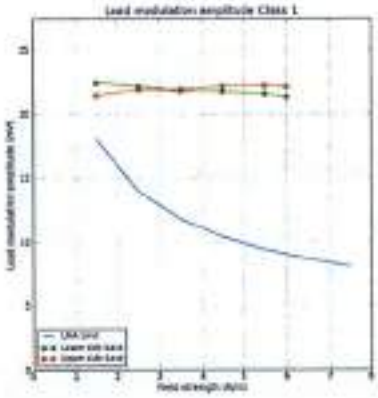
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC. 101898852
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @1.7 Mbit/s



Curve Load Modulation Amplitude of the sample 2 @1.7 Mbit/s



Curve Load Modulation Amplitude of the sample 3 @1.7 Mbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.
Página/Folio No.568 de 843

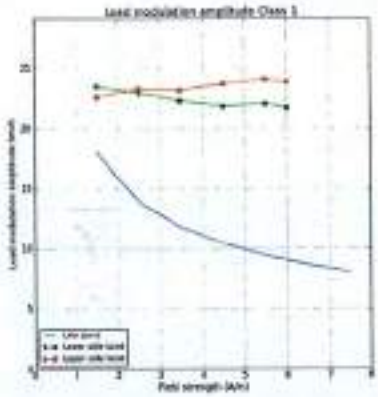
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101
Santo Domingo

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

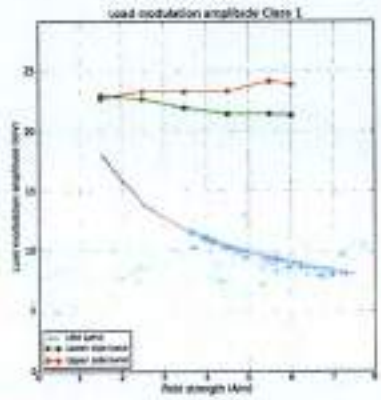
Load Modulation Amplitude at 3.4 Mbit/s:

Reference objects under test	Information	H (A/m)	V_{LMA} Limit (mV)	Upper sideband (mV)	Lower sideband (mV)	Result
1K3606	eMRTD Transmission for Sample 1 @3.4 Mbit/s	1.5	18.0	22.6	23.4	PASS
		2.5	13.9	23.2	23.0	PASS
		3.5	11.8	23.1	22.3	PASS
		4.5	10.4	23.6	21.8	PASS
		5.5	9.4	24.1	22.0	PASS
		6.0	9.0	23.8	21.7	PASS
2K3606	eMRTD Transmission for Sample 2 @3.4 Mbit/s	1.5	18.0	22.7	22.9	PASS
		2.5	13.9	23.3	22.6	PASS
		3.5	11.8	23.3	22.0	PASS
		4.5	10.4	23.3	21.5	PASS
		5.5	9.4	24.2	21.5	PASS
		6.0	9.0	23.9	21.4	PASS
3K3606	eMRTD Transmission for Sample 3 @3.4 Mbit/s	1.5	18.0	21.7	22.7	PASS
		2.5	13.9	22.1	22.4	PASS
		3.5	11.8	22.2	21.6	PASS
		4.5	10.4	22.4	21.3	PASS
		5.5	9.4	23.2	21.3	PASS
		6.0	9.0	23.4	20.7	PASS

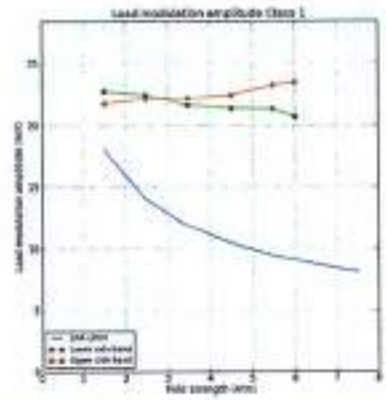
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.



Curve Load Modulation Amplitude of the sample 1 @3.4 Mbit/s



Curve Load Modulation Amplitude of the sample 2 @3.4 Mbit/s



Curve Load Modulation Amplitude of the sample 3 @3.4 Mbit/s

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC: 101898339 Santo Domingo

3.2 OPERATING FIELD STRENGTH

Method:

The test method used conforms to document **[R1]** chapter 5.3.2 and 7.2.1.
The following sequence of commands (following TEST_COMMAND_SEQUENCE1) is performed:

Step	Command
1	READ BINARY for EF.CardAccess
2	MSE: Set AT
3	GENERAL AUTHENTICATE for encrypted nonce
4	GENERAL AUTHENTICATE to map the nonce
5	GENERAL AUTHENTICATE to perform Key agreement
6	GENERAL AUTHENTICATE to perform Mutual Authenticate
7	SELECT
8	READ BINARY for EF.DG14
9	MSE: SET AT
10	GENERAL AUTHENTICATE
11	INTERNAL AUTHENTICATE*
12	READ BINARY for EF.CVCA
13	MSE: SET DST CVCA
14	PSO: VERIFY CERTIFICATE DV
15	MSE: SET DST DV
16	PSO: VERIFY CERTIFICATE IS
17	MSE: SET AT
18	GET CHALLENGE
19	EXTERNAL AUTHENTICATE
20	READ BINARY for EF.DG3
* AA is supported by eMRTD. INTERNAL AUTHENTICATE command is sent.	

Every supported symmetric bitrate and maximum bitrate in both directions (eMRTD to eMRTD Reader and eMRTD Reader to eMRTD) are tested.

Test conditions:

The tests is performed under the conditions defined in §1.3.

At T=50°C, *Operating Field Strength* at H= 6.5 A/m and 7.5A/m are not applicable. They are replaced by one test performed at 6 A/m.

Página/Folio No.571 de 843

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC. 01698852 Santo Domingo, R.D.

Results:

➔ Object under test: 1K3606

Information	H (A/m)	T (°C)	Results							
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s	Max[2]
Operation Field Strength for sample 1	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS

[2] Maximum bit rates in both directions are set as declared in chapter 2.3: at 3.4 Mbit/s for eMRTD to eMRTD Reader and at 848 Kbit/s for eMRTD Reader to eMRTD.

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL, SA
CSI
RNC: 101[illegible]
Santo Domingo

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

➔ Object under test: 2K3606

Information	H (A/m)	T (°C)	Results							
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s	Max²
Operation Field Strength for sample 2	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS

➔ Object under test: 3K3606

Information	H (A/m)	T (°C)	Results							
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s	Max²
Operation Field Strength for sample 3	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA	PASS
		+23	PASS	PASS	PASS	PASS	NA	NA	NA	PASS

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

3.3 eMRTD Reception

Method:

The test method used conforms to document **[R1]** chapter 5.3.3 and 7.2.2.

Tests conditions:

The test is performed under the conditions defined in §1.3

Results:

➔ Object under test: 1K3606

Condition 1:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 1 Condition 1	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

COPY SOLUTIONS INTERNATIONAL S.A. CSIQ RNC: 101 Santo Domingo

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

Condition 2:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 1 Condition 2	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

Condition 3:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 1 Condition 3	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

➔ Object under test: 2K3606

Condition 1:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 2 Condition 1	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

COPY SOLUTIONS INTERNATIONAL S.A. RNC 1-30-09852 Santo Domingo, R.D.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

Condition 2:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 2 Condition 2	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

Condition 3:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 2 Condition 3	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

➔ Object under test: 3K3606

Condition 1:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 3 Condition 1	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

COPY SOLUTIONS INTERNATIONAL S.R.L. CSI RNC: 101693852 Santo Domingo, R.D.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101898853 Santo Domingo, R.D.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

Condition 2:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 3 Condition 2	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		v	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

Condition 3:

Information	H (A/m)	T (°C)	Results						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Reception for Sample 3 Condition 3	1.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	2.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	3.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	4.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	5.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
		+50	PASS	PASS	PASS	PASS	NA	NA	NA
	6.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA
	6.0	+50	PASS	PASS	PASS	PASS	NA	NA	NA
	7.5	-10	PASS	PASS	PASS	PASS	NA	NA	NA
		+23	PASS	PASS	PASS	PASS	NA	NA	NA

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

Página/Folio No.579 de 843

3.4 eMRTD Resonance Frequency

Method:

This optional test is performed according to document **[R1]** chapter 5.3.4. A Vector Network Analyzer Agilent E5061A is used.

The measured values are given for information purpose only and no PASS/FAIL result is provided.

This test is not covered by ISO/IEC 17025 Cofrac accreditation.

Test conditions:

The test is performed under the following conditions:

- Temperature: +23°C ±3°C
- Relative humitity: 25% to 75%

Results:

Reference objects under test	Information	Power (dBm)	Resonance frequency	Result
1K3606	Resonance frequency	0	15.5	INF
2K3606	Resonance frequency	0	15.3	INF
3K3606	Resonance frequency	0	15.3	INF

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC. 101898852 Santo Domingo, R.D.

Página/Folio No.580 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo R.D.

3.5 eMRTD Maximum Loading Effect

Method:

This test is performed according to document **[R1]** chapter 5.3.5.

The eMRTD loading effect at H_{min} shall not exceed the loading effect of the selected Reference PICC tuned to 13.56 MHz and calibrated to obtain V_{load} at CON3 at H_{min}.
V_{load} and H_{min} depend to the PICC classes.

Test conditions:

The test is performed under the conditions defined in §1.3

Results:

Reference objects under test	Information	T (°C)	H_{min} (A/m)	Measured H (A/m)	Result
1K3606	Maximum loading effect for sample 1	-10	1.5	1.67	PASS
		+23		1.66	PASS
		+50		1.66	PASS
2K3606	Maximum loading effect for sample 2	-10	1.5	1.67	PASS
		+23		1.67	PASS
		+50		1.66	PASS
3K3606	Maximum loading effect for sample 3	-10	1.5	1.67	PASS
		+23		1.66	PASS
		+50		1.66	PASS

Página/Folio No.581 de 843

3.6 eMRTD Reading Performance Analysis

Method:

The applied method is not defined in [R1] and is not covered by ISO/IEC 17025 Cofrac accreditation. The measured values are given for information purpose only and no PASS/FAIL result is provided.

The eMRTD reading performance analysis is performed from the Operating Field Strength tests. The evaluation takes into account 3 samples, at -10°C, +23°C and +50°C temperatures and from H_{min} to H_{max}.
As requested, following bit rate conditions are considered:

- Bitrate condition 1: eMRTD Reader @848kbit/s / eMRTD @848kbit/s
- Bitrate condition 2: eMRTD Reader @848kbit/s / eMRTD @3.4Mbit/s

The timing **eMRTD processing time** reported in the result's tables is the sum of the delay between the end of each reader commands and the end of the associated eMRTD answer as shown in Figure 2.

Figure 2 Example of eMRTD Processing time measured on REQA

At T=50°C, *Operating Field Strength* at H= 6.5 A/m and 7.5A/m are not applicable. They are replaced by one test performed at 6 A/m.

Information:

- Bitrate condition 2 contains an additional processing time due to the S(PARAMETERS) exchange. This additional processing time is measured at 2.3 ms and is included to the eMRTD processing time.
- eMRTD transmission time is the sum of the duration of the eMRTD answers. This timing, included to the eMRTD processing time, has been measured at 28.8 ms for Bitrate condition 1 and at 9.9 ms for Bitrate condition 2.

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC. A-71898852

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101003852 Santo Domingo R.D.

TEST REPORT
Ref.: IC.E.RE.1905.009
Version: v1.0
Date: 17/06/2019

Results;

➔ Object under test: 1K3606

Information	H (A/m)	T (°C)	eMRTD Processing time (ms)				
			Bitrate condition 1 (1)		Bitrate condition 2 (2)		Delta (1) - (2)
			Reader 848 kbit/s	eMRTD 848 kbit/s	Reader 848 kbit/s	eMRTD 3.4 Mbit/s	
eMRTD reading time performance for sample 1	1.5	-10	3819.1		4338.4		-519.3
		+23	3355.2		3429.6		-74.4
		+50	4721.8		4547.8		174.0
	4.5	-10	1646.8		1628.3		18.5
		+23	1653.5		1635.6		17.9
		+50	1655.9		1637.1		18.8
	6.0	+50	1625.5		1594.5		31.0
	7.5	-10	1187.2		1169.5		17.7
		+23	1192.7		1175.4		17.3

➔ Object under test: 2K3606

Information	H (A/m)	T (°C)	eMRTD Processing time (ms)				
			Bitrate condition 1 (1)		Bitrate condition 2 (2)		Delta (1) - (2)
			Reader 848 kbit/s	eMRTD 848 kbit/s	Reader 848 kbit/s	eMRTD 3.4 Mbit/s	
eMRTD reading time performance for sample 2	1.5	-10	4657.6		4637.8		19.8
		+23	4647		4628.5		18.5
		+50	4715.1		4694.2		20.9
	4.5	-10	1639.4		1621.9		17.5
		+23	1647.7		1628.6		19.1
		+50	1649.8		1633.0		16.8
	6.0	+50	1651.8		1633.2		18.6
	7.5	-10	1198.5		1179.9		18.6
		+23	1204.7		1187.5		17.2

➔ Object under test: 3K3606

Information	H (A/m)	T (°C)	eMRTD Processing time (ms)				
			Bitrate condition 1 (1)		Bitrate condition 2 (2)		Delta (1) - (2)
			Reader 848 kbit/s	eMRTD 848 kbit/s	Reader 848 kbit/s	eMRTD 3.4 Mbit/s	
eMRTD reading time performance for sample 3	1.5	-10	4704.6		4685.3		19.3
		+23	4701.0		4672.0		29.0
		+50	4761.1		4744.8		16.3
	4.5	-10	1645.6		1626.9		18.7
		+23	1653.7		1635.5		18.2
		+50	1655.3		1638.2		17.1
	6.0	+50	1656.1		1639.1		17.0
	7.5	-10	1187.7		1168.6		19.1
		+23	1194.3		1176.1		18.2

The reproduction of this report is authorized only in its integral format. It comprises 39 pages.

4 CONCLUSION

The following table summarizes the results of the tests performed according to reference documents listed in §1.2.

Reference of object under test	Test	Temperature (°C)	Result
1K3606	eMRTD Transmission	-10	PASS
		+23	PASS
		+50	PASS
	Operating Field Strength	-10	PASS
		+23	PASS
		+50	PASS
	eMRTD Reception	-10	PASS
		+23	PASS
		+50	PASS
	eMRTD Resonance frequency (*)	+23	INF
	eMRTD Maximum Loading Effect	-10	PASS
		+23	PASS
		+50	PASS
2K3606	eMRTD Transmission	-10	PASS
		+23	PASS
		+50	PASS
	Operating Field Strength	-10	PASS
		+23	PASS
		+50	PASS
	eMRTD Reception	-10	PASS
		+23	PASS
		+50	PASS
	eMRTD Resonance frequency (*)	+23	INF
	eMRTD Maximum Loading Effect	-10	PASS
		+23	PASS
		+50	PASS
3K3606	eMRTD Transmission	-10	PASS
		+23	PASS
		+50	PASS
	Operating Field Strength	-10	PASS
		+23	PASS
		+50	PASS
	eMRTD Reception	-10	PASS
		+23	PASS
		+50	PASS
	eMRTD Resonance frequency (*)	+23	INF
	eMRTD Maximum Loading Effect	-10	PASS
		+23	PASS
		+50	PASS

(*) This test is not covered by ISO/IEC 17025 Cofrac accreditation.

END OF DOCUMENT

The reproduction of this report is authorized only in its integral format. It comprises Página/Folio No.584 de 843

TRADUCCIÓN OFICIAL: ISO 14443-2

Yo, **LIC. SANTO C. SIERRA**, Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones CERTIFICO: Que he procedido a traducir las partes centrales de un documento, escrito originalmente en Ingles, y cuya versión al Español, según mi mejor conocimiento, es el siguiente:

ICUBE
TESTING CENTER

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC: 1-27898852 Santo Domingo, R.D.

cofrac
ESSAIS
Accréditation
n°1-6707
Alcance disponible en www.cofrac.fr

PRUEBA INFORME

Prueba de Normas ISO/IEC 14443-
2 parámetros para eMRTD

LIC. SANTO C. SIERRA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

REFERENCIA:	IC.E.RE.1905.009
VERSIÓN:	v1.0
FECHA:	17/06/2019
SOLICITANTE:	NXP Semiconductores
PRODUCTO:	ChipDoc versión 3 – 3.0

INFORME VALIDADO Y APROBADO POR:
S. JOBARD - Técnico gerente
IC.E.RE.1905.009_v1.0_SJ.sig

El reproducción de este informe es autorizado solo en es integral formato. Él comprende 39 páginas.

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

RESUMEN

1 **General Información** 3
1.1 Prueba Laboratorio Identificación 3
1.2 Prueba Identificación 3
1.3 Prueba Medio ambiente 4
1.4 Prueba Herramientas 4
1.5 Prueba Resultado Terminología 5
2 **Objeto Bajo Prueba** 6
2.1 Solicitante información 6
2.2 Producto Identificación 6
2.3 Implementación Conformidad Declaración 7
3 **Prueba Resultados** 8
3.1 eMRTD Transmisión (Carga Modulación Amplitud) 8
3.2 Operante Campo Fuerza 26
3.3 eMRTD Recepción 29
3.4 eMRTD Resonancia Frecuencia 35
3.5 eMRTD Máximo Cargando Efecto 36
3.6 eMRTD Lectura Actuación Análisis 37
4 **Conclusión** 39

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101698852 Santo Domingo, R.D.

LIC. SANTO C. SILFA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

PRUEBA INFORME

Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

1 GENERAL INFORMACIÓN

1.1 PRUEBA LABORATORIO | IDENTIFICACIÓN

Cubo ICUBE PRUEBAS CENTRO
707 camino tú Quintín
13300 Salón Delaware Provenza
FRANCIA

Contacto: contacto@icube-tc.com

1.2 PRUEBA | IDENTIFICACIÓN

Prueba de Normas ISO/IEC 14443-2 parámetros para eMRTD

Este documento informes el resultados de el siguiente pruebas:
- eMRTD Transmisión,
- Operación Campo Fortaleza,
- eMRTD Recepción,
- eMRTD Resonancia Frecuencia,
- eMRTD Máximo Cargando Efecto.

El prueba método usado se ajusta a el siguiente especificación:

[R1] Normas ISO/IEC 18745-2:2016
Información Tecnología Prueba métodos para máquina legible viajar documento (Vehículo de marca registrada)
y asociado dispositivos
Parte 2: Prueba métodos para el Sin contacto interfaz
Primero edición Fecha: 15 de agosto de 2016

[R2] ISO/IEC JTC1/SC17/GT8 N2638
Solicitud Perfil Sin contacto Interfaz Doc 9303
Versión versión 1.3 Fecha: 03-02-2016

[R3] ISO/IEC de Normas ISO/IEC 10373-6:2016
Identificación tarjetas - Prueba métodos - Parte 6: Proximidad tarjetas
Tercero edición - Fecha: 15 de julio de 2016

El resonancia frecuencia prueba es no realizado bajo Normas ISO/IEC 17025 Cofrac acreditación.

Sobre el resultados expresado en el cuantitativo forma, el conformidad a el especificación es declarado sin tomando explícitamente en cuenta el Incertidumbres asociado a el resultados. El muestras son consideró como "ajustarse" si el resultado es en el rango especificado por el refer encia
documento.

Fecha de el prueba: 18 a 27º de Junio 2019.
Prueba realizado por: M.GIROD.

El reproducción de este informe es autorizado solo en es integral formato. Él comprende 39 páginas.

1.3 PRUEBA MEDIO AMBIENTE

El pruebas son realizado bajo el siguiente condiciones:

Temperatura	Relativo humedad
+23°C ± 3°C	25% a 75%
+50°C ± 3°C	-
-10°C ± 3°C	-

El pruebas en +50°C y -10°C temperaturas son realizado en clima cámara.

1.4 TEST TOOLS

Hardware y software	Identificación y versión
Software prueba ambiente	SCRIPTI S™ v01.04.01 + Parche 4
Software prueba suite	Normas ISO/IEC 14443 Prueba Suite para CCP Cosa análoga versión 06.00 + Parche 2 + Desplazamiento del campo de parche + Parche Ruido Medición versión 2 Normas ISO/IEC 18745-2 prueba Suite para CCP Cosa análoga versión 01.01 + Parche 1 + Parche Comando2precondiciones.py + ScriptisEPassportAnalog v01.16-IC.SW.1702.002
CCP Sin contacto Lector Software versión	KEOLABS Ley de Protección Ambiental (RGPA) versión 3.12.17.0227 KEOLABS Laboratorio Proxi versión 4.28.17.0628
PICC Sin contacto Lector Hardware versión	KEOLABS Laboratorio Proxi Búsqueda versión 4.1
PCD Asamblea	KEOLABS PCD Asamblea Normas ISO/IEC 10373-6 Alto Velocidad
	KEOLABS PCD Asamblea Normas ISO/IEC 10373-6 Bajo Velocidad
Referencia PICC	KEOLABS Referencia CCP Normas ISO/IEC 10373-
Sondas	2 LeCroy PP018 KEOLABS CCP Sonda KEOLABS Sonda SC-PICC+ versión 1.9
Amplificador	Bowen M02.30.70S
Osciloscopio	LeCroy ODH 6034A
Cambio climatico	AGLUTINANTE MKF 240

El reproducción de este informe es autorizado solo en es integral formato. El comprensión es [illegible]

1.5 TERMINOLOGIA DE RESULTADOS DE PRUEBAS

Resultado	Descripción
APROBADO	Resultado se ajusta a el esperado resultado especificado en referencia prueba plan.
FALLIDO	Resultado hace no ajustarse a el esperado resultado especificado en referencia prueba plan.
N/A	Prueba no aplicable. Para ejemplo, para un opcional función eso es no apoyado por el producto bajo prueba.
NE	Prueba no ejecutado.
NI	Prueba no implementado.
INC	Poco concluyente prueba.
INF	Informativo prueba.

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC: 101898952 Santo Domingo, R.D.

LIC. SANTO C. SILFA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

2 OBJETO BAJO PRUEBA

2.1 INFORMACIÓN DEL SOLICITANTE

NXP Semiconductores
Microvia 1,
8101 Gratkorn,
Austria

Representado por: Olga Iakusheva.

2.2 IDENTIFICACIÓN DEL PRODUCTO

Producto nombre:	ChipDoc versión 3
Producto Versión:	3.0
Hardware identificación y revisión:	N7121 B1
Software Revisión:	JCOP 4 P71

Muestra recepción fecha (dd/mm/aaaa): 06/12/2019

Forma factor:	Tarjeta Identificación-1 Tamaño
Cantidad:	3

Referencia de el objetos bajo prueba:
- 1K3606 (De serie número: No proporcionó)
- 2K3606 (De serie número: No proporcionó)
- 3K3606 (De serie número: No proporcionó)

Cifra 1 Muestra descripción general

2.3 DECLARACIÓN DE CONFORMIDAD DE IMPLEMENTACIÓN

El solicitante tiene proporcionó el información especificado en el mesa abajo.

Información para prueba configuración	
Físico tamaño de producto	Identificación-1: SÍ
Ubicación de antena dentro MRTD electrónico	No proporcionó
CCP clase	CCP Clase 1
MRTD electrónico blindado o no y cómo (*ceguer*	NO
Resonancia frecuencia rango (si opcional prueba es realizado) Fuerza	No proporcionó ☒ 0 dBm ☐ 10 dBm
Señal Interfaz • Tipo A o B	 Tipo A
Poco tarifas apoyado • De eMRTD a eMRTD lector o 106 kbit/s o 212 kbit/s o 424 kbit/s o 848 kbit/s o 1.7 Mbit/s o 3.4 Mbit/s o 6.8 Mbit/s • De eMRTD lector a eMRTD o 106 kbit/s o 212 kbit/s o 424 kbit/s o 848 kbit/s o 1.7 Mbit/s o 3.4 Mbit/s o 6.8 Mbit/s	 SÍ SÍ SÍ SÍ SÍ SÍ NO SÍ SÍ SÍ SÍ NO NO NO
Control de Acceso Aplicado • BAC • CAE • PASO	 NO SÍ SÍ
Activo Autenticación	SÍ
Extendido Unidad de Atención Primaria	SÍ
Criptográfico Opciones: • Dinámica vinculante • Estático vinculante	 SÍ NO

SECUENCIA DE COMANDO DE PRUEBA 1 usado para Operante Campo Fortaleza prueba.

El reproducción de este informe es autorizado solo en es integral formato. Él comprende 39 páginas.

PRUEBA INFORME

Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 131698852 Santo Domingo, R.D.

LIC. SANTO C. Intérprete Judicial Jurisdicción D.N. SANTO DOMINGO, R.D.

3 PRUEBA RESULTADOS

3.1 EMRTD TRANSMISION (AMPLITUD DE MODULACIÓN DE CARGA)

Método:
El prueba método usado se ajusta a documento **[R1]** capitulo 5.3.1.

El resultados para poco tarifas más alto que 848 kbit/s son realizado de acuerdo a a documento **[R3]**
capitulo 7.2.1.1.

Este prueba es cubierto por Normas ISO/IEC 17025 Cofrac acreditación.

Prueba condiciones:
El prueba es realizado bajo el condiciones definido en §1.3 .

En +50°C temperatura, *Transmisiones* en AI= 6.5 Soy y 7,5 A/m son no aplicable. Ellos son reemplazado por uno prueba realizado en 6 Soy.

3.1.1 Temperatura -10°C

Resultados:

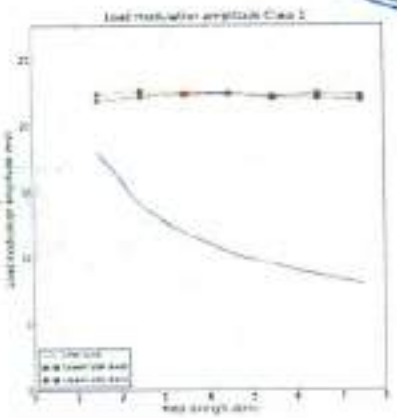
Referencia objetos bajo prueba	Información	H (A/m)	V -LIMA Límite (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @106 kbit/s	1.5	18.0	21.8	22.4	APROBAR
		2.5	13.9	22.2	22.6	APROBAR
		3.5	11.8	22.3	22.4	APROBAR
		4.5	10.4	22.4	22.4	APROBAR
		5.5	9.4	22.2	22.1	APROBAR
		6.5	8.6	22.4	22.1	APROBAR
		7.5	8.0	22.2	21.9	APROBAR
2K3606	eMRTD Transmisión para Muestra 2 @106 kbit/s	1.5	18.0	22.2	22.7	APROBAR
		2.5	13.9	22.6	22.8	APROBAR
		3.5	11.8	22.8	22.6	APROBAR
		4.5	10.4	22.8	22.7	APROBAR
		5.5	9.4	22.8	22.6	APROBAR
		6.5	8.6	22.8	22.3	APROBAR
		7.5	8.0	22.8	22.3	APROBAR
3K3606	eMRTD Transmisión para Muestra 3 @106 kbit/s	1.5	18.0	21.9	22.7	APROBAR
		2.5	13.9	22.3	22.8	APROBAR
		3.5	11.8	22.4	22.8	APROBAR
		4.5	10.4	22.6	22.8	APROBAR
		5.5	9.4	22.6	22.5	APROBAR
		6.5	8.6	22.5	22.4	APROBAR
		7.5	8.0	21.7	21.4	APROBAR

Amplitud de modulación de carga a 106 kbit/s:

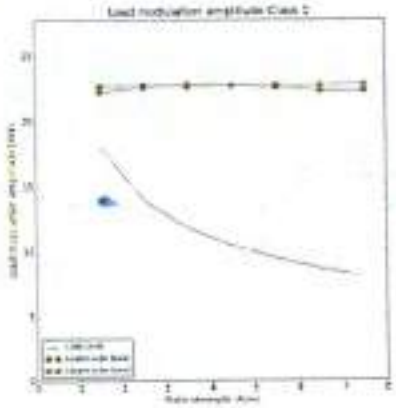
PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

COPY SOLUTIONS INTERNATIONAL SA
CSI
RNC 101898852
Santo Domingo R.D.

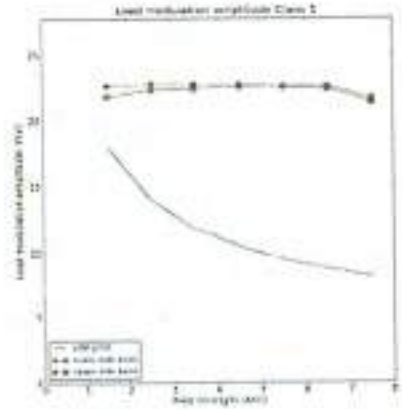
LIC. SANTO C.
Interprete Judicial Juzg 1ra Instancia C.N.
SANTO DOMINGO, R.D.



Curva Carga Modulación Amplitud de el muestra 1 @106 kbit/s



Curva Carga Modulación Amplitud de el muestra 2 @106 kbit/s



Curva Carga Modulación Amplitud de el muestra 3 @106 kbit/s

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

Amplitud de modulación de carga a 1,7 Mbit/s:

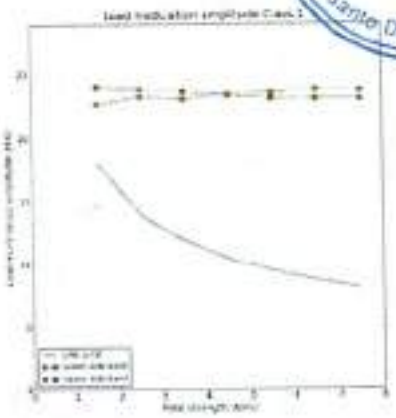
Referencia objetos bajo prueba	Información	H (A/M)	V LIMA Límite (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @1.7 Mbit/s	1.5	18.0	22.7	24.1	APROBADO
		2.5	13.9	23.3	23.9	APROBADO
		3.5	11.8	23.1	23.7	APROBADO
		4.5	10.4	23.5	23.3	APROBADO
		5.5	9.4	23.5	23.1	APROBADO
		6.5	8.6	23.8	23.1	APROBADO
		7.5	8.0	23.7	23.0	APROBADO
2K3606	eMRTD Transmisión para Muestra 2 @1.7 Mbit/s	1.5	18.0	22.4	23.4	APROBADO
		2.5	13.9	22.7	23.1	APROBADO
		3.5	11.8	22.9	22.9	APROBADO
		4.5	10.4	23.0	22.8	APROBADO
		5.5	9.4	23.2	22.6	APROBADO
		6.5	8.6	23.4	22.4	APROBADO
		7.5	8.0	23.4	22.3	APROBADO
3K3606	eMRTD Transmisión para Muestra 3 @1.7 Mbit/s	1.5	18.0	22.0	23.5	APROBADO
		2.5	13.9	22.4	23.2	APROBADO
		3.5	11.8	22.5	23.1	APROBADO
		4.5	10.4	22.7	22.9	APROBADO
		5.5	9.4	23.1	22.7	APROBADO
		6.5	8.6	23.0	22.4	APROBADO
		7.5	8.0	23.1	22.4	APROBADO

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101898852 Santo Domingo, R.D.
LIC. SANTO C. S. Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

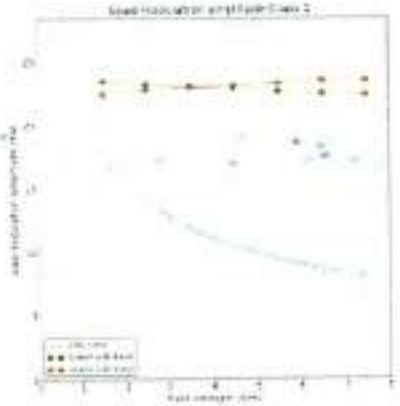
PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101038852
Santo Domingo, R.D.

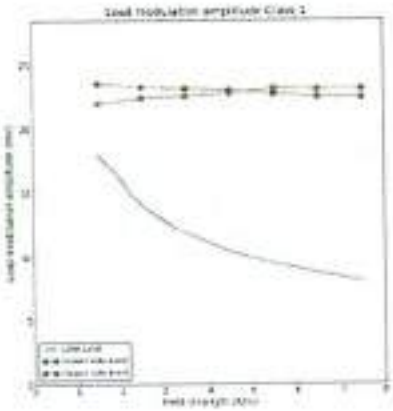
LIC. SANTO C. SILVA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.



Curva Carga Modulación Amplitud de el muestra 1 @1.7 Mbit/s



Curva Carga Modulación Amplitud de el muestra 2 @1.7 Mbit/s



Curva Carga Modulación Amplitud de el muestra 3 @1.7 Mbit/s

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC. 101168852 Santo Domingo, R.D.

PRUEBA INFORME

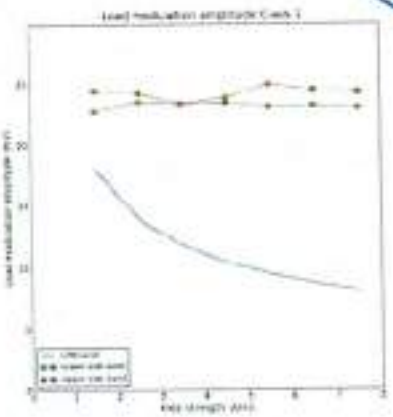
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

Referencia objetos bajo prueba	Información	H (A/M)	V LMA Limite (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @3.4 Mbit/s	1.5	18.0	22.7	24.4	APROBADO
		2.5	13.9	23.4	24.2	APROBADO
		3.5	11.8	23.3	23.3	APROBADO
		4.5	10.4	23.8	23.4	APROBADO
		5.5	9.4	24.8	23.0	APROBADO
		6.5	8.6	24.4	23.1	APROBADO
		7.5	8.0	24.2	23.0	APROBADO
2K3606	eMRTD Transmisión para Muestra 2 @3.4 Mbit/s	1.5	18.0	22.6	23.7	APROBADO
		2.5	13.9	23.1	23.4	APROBADO
		3.5	11.8	23.1	22.7	APROBADO
		4.5	10.4	23.2	22.4	APROBADO
		5.5	9.4	24.3	22.4	APROBADO
		6.5	8.6	24.1	22.1	APROBADO
		7.5	8.0	23.8	22.2	APROBADO
3K3606	eMRTD Transmisión para Muestra 3 @3.4 Mbit/s	1.5	18.0	22.0	24.2	APROBADO
		2.5	13.9	22.5	23.9	APROBADO
		3.5	11.8	22.5	23.1	APROBADO
		4.5	10.4	23.2	22.9	APROBADO
		5.5	9.4	23.5	22.8	APROBADO
		6.5	8.6	23.3	22.7	APROBADO
		7.5	8.0	23.3	22.4	APROBADO

Amplitud de modulación de carga a 3.4 Mbit/s:

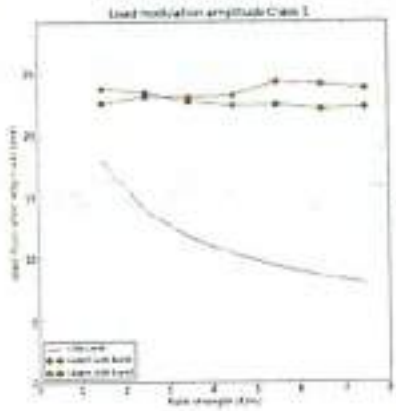
LIC. SANTO C. SILVA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 10[illegible]832
Santo Domingo, R.D.

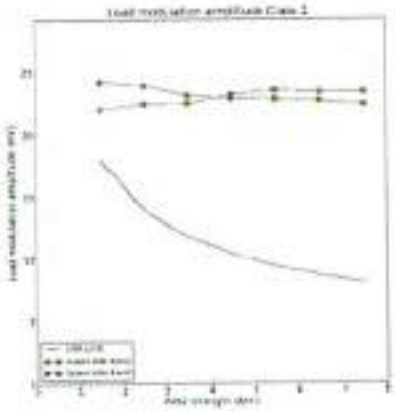


LIC. SANTO C. SILVA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

Curva Carga Modulación Amplitud de el muestra 1 @3.4 Mbit/s



Curva Carga Modulación Amplitud de el muestra 2 @3.4 Mbit/s



Curva Carga Modulación Amplitud de el muestra 3 @3.4 Mbit/s

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

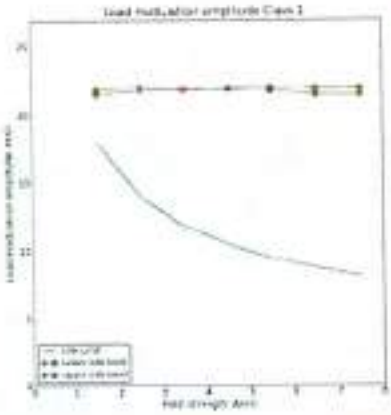
3.1.2 Temperatura +23°C

Resultados:

Amplitud de modulación de carga a 106 kbit/s:

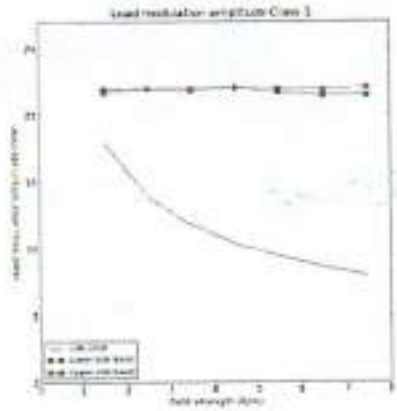
Referencia objetos bajo prueba	Información	H (A/M)	V LIMA Limit (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @106 kbit/s	1.5	18.0	21.5	21.9	APROBAR
		2.5	13.9	21.8	22.0	APROBAR
		3.5	11.8	21.8	21.8	APROBAR
		4.5	10.4	21.9	21.9	APROBAR
		5.5	9.4	22.0	21.8	APROBAR
		6.5	8.6	21.9	21.5	APROBAR
		7.5	8.0	21.9	21.4	APROBAR
2K3606	eMRTD Transmisión para Muestra 2 @106 kbit/s	1.5	18.0	21.6	21.9	APROBAR
		2.5	13.9	21.9	21.9	APROBAR
		3.5	11.8	21.9	21.8	APROBAR
		4.5	10.4	22.0	21.9	APROBAR
		5.5	9.4	21.9	21.7	APROBAR
		6.5	8.6	21.9	21.4	APROBAR
		7.5	8.0	22.0	21.4	APROBAR
3K3606	eMRTD Transmisión para Muestra 3 @106 kbit/s	1.5	18.0	21.3	21.9	APROBAR
		2.5	13.9	21.7	22.0	APROBAR
		3.5	11.8	21.8	21.8	APROBAR
		4.5	10.4	21.8	21.9	APROBAR
		5.5	9.4	21.8	21.7	APROBAR
		6.5	8.6	21.7	21.5	APROBAR
		7.5	8.0	21.9	21.5	APROBAR

COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC 101898852
Santo Domingo, R.D.

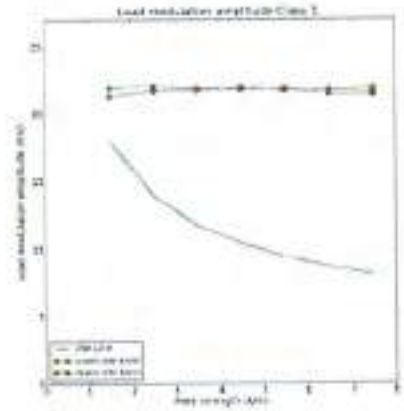


LIC. SANTO C. SILFA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

Curva Carga Modulación Amplitud de el muestra 1 @106 kbit/s



Curva Carga Modulación Amplitud de el muestra 2 @106 kbit/s



Curva Carga Modulación Amplitud de el muestra 3 @106 kbit/s

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

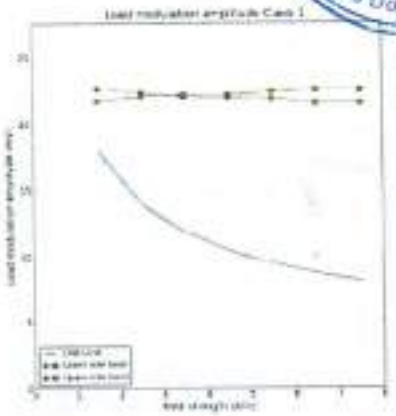
Amplitud de modulación de carga a 1,7 Mbit/s:

Referencia objetos bajo prueba	Información	H (A/M)	V -LIMA Límite (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @1.7 Mbit/s	1.5	18.0	21.7	22.7	APROBAR
		2.5	13.9	22.1	22.4	APROBAR
		3.5	11.8	22.2	22.0	APROBAR
		4.5	10.4	22.2	22.0	APROBAR
		5.5	9.4	22.4	21.9	APROBAR
		6.5	8.6	22.5	21.5	APROBAR
		7.5	8.0	22.5	21.5	APROBAR
2K3606	eMRTD Transmisión para Muestra 2 @1.7 Mbit/s	1.5	18.0	21.9	22.6	APROBAR
		2.5	13.9	22.2	22.4	APROBAR
		3.5	11.8	22.3	22.0	APROBAR
		4.5	10.4	22.3	21.9	APROBAR
		5.5	9.4	22.5	21.7	APROBAR
		6.5	8.6	22.5	21.5	APROBAR
		7.5	8.0	22.6	21.4	APROBAR
3K3606	eMRTD Transmisión para Muestra 3 @1.7 Mbit/s	1.5	18.0	21.6	22.9	APROBAR
		2.5	13.9	22.1	22.5	APROBAR
		3.5	11.8	22.0	22.3	APROBAR
		4.5	10.4	22.2	22.1	APROBAR
		5.5	9.4	22.5	21.9	APROBAR
		6.5	8.6	22.5	21.7	APROBAR
		7.5	8.0	22.4	21.6	APROBAR

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo, R.D.

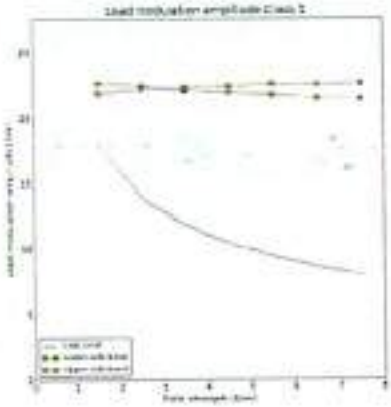
LIC. SANTO C. SIERRA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

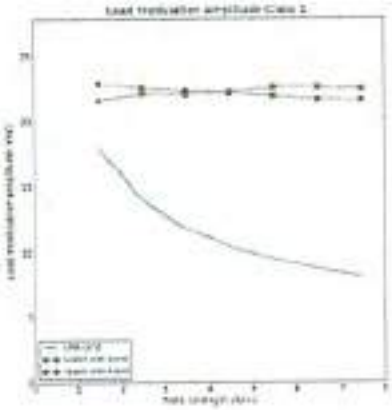


LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

Curva Carga Modulación Amplitud de el muestra 1 @1.7 Mbit/s



Curva Carga Modulación Amplitud de el muestra 2 @1.7 Mbit/s



Curva Carga Modulación Amplitud de el muestra 3 @1.7 Mbit/s

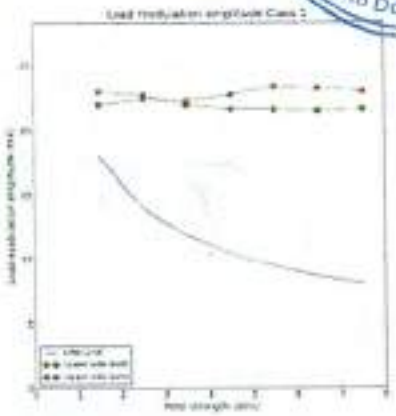
PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

Amplitud de modulación de carga a 3.4 Mbit/s:

Referencia objetos bajo prueba	Información	H (A/M)	V LIMA Límite (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @3.4 Mbit/s	1.5	18.0	21.9	23.0	APROBAR
		2.5	13.9	22.4	22.7	APROBAR
		3.5	11.8	22.3	21.9	APROBAR
		4.5	10.4	22.7	21.6	APROBAR
		5.5	9.4	23.4	21.6	APROBAR
		6.5	8.6	23.2	21.4	APROBAR
		7.5	8.0	23.0	21.6	APROBAR
2K3606	eMRTD Transmisión para Muestra 2 @3.4 Mbit/s	1.5	18.0	21.9	22.7	APROBAR
		2.5	13.9	22.5	22.5	APROBAR
		3.5	11.8	22.6	21.6	APROBAR
		4.5	10.4	22.6	21.3	APROBAR
		5.5	9.4	23.6	21.5	APROBAR
		6.5	8.6	23.5	21.1	APROBAR
		7.5	8.0	23.2	21.2	APROBAR
3K3606	eMRTD Transmisión para Muestra 3 @3.4 Mbit/s	1.5	18.0	21.6	23.3	APROBAR
		2.5	13.9	22.3	22.9	APROBAR
		3.5	11.8	22.3	22.2	APROBAR
		4.5	10.4	22.7	21.9	APROBAR
		5.5	9.4	23.3	21.9	APROBAR
		6.5	8.6	23.0	21.6	APROBAR
		7.5	8.0	23.0	21.6	APROBAR

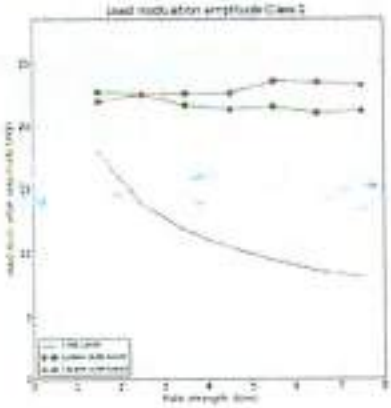
COPY SOLUTIONS INTERNATIONAL SA CSI RNC 101898852 Santo Domingo, R.D.
LIC. SANTO C. SIERRA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC. 101898852
Santo Domingo, R.D.

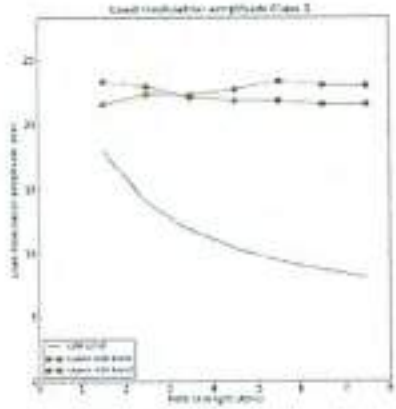


LIC. SANTO C. Sierra
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DO... R.D.

Curva Carga Modulación Amplitud de el muestra 1 @3.4 Mbit/s



Curva Carga Modulación Amplitud de el muestra 2 @3.4 Mbit/s



Curva Carga Modulación Amplitud de el muestra 3 @3.4 Mbit/s

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

3.1.3 Temperatura +50°C

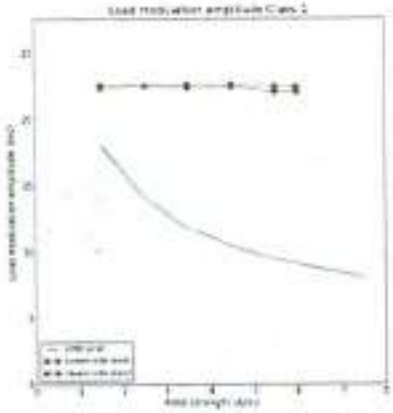
Resultados:

Amplitud de modulación de carga a 106 kbit/s:

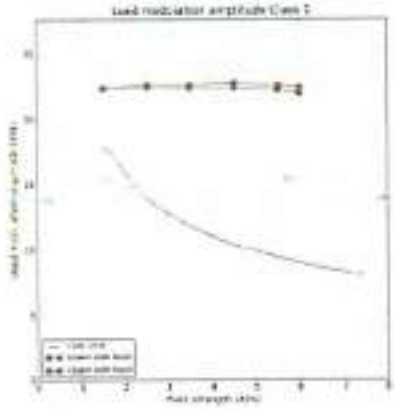
Referencia objetos bajo prueba	Información	H (A/M)	V-LIMA Limit (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @106 kbit/s	1.5	18.0	22.3	22.5	APROBAR
		2.5	13.9	22.5	22.4	APROBAR
		3.5	11.8	22.6	22.3	APROBAR
		4.5	10.4	22.6	22.4	APROBAR
		5.5	9.4	22.4	22.0	APROBAR
		6.0	9.0	22.4	22.0	APROBAR
2K3606	eMRTD Transmisión para Muestra 2 @106 kbit/s	1.5	18.0	22.3	22.4	APROBAR
		2.5	13.9	22.7	22.4	APROBAR
		3.5	11.8	22.6	22.4	APROBAR
		4.5	10.4	22.7	22.4	APROBAR
		5.5	9.4	22.6	22.2	APROBAR
		6.0	9.0	22.5	22.0	APROBAR
3K3606	eMRTD Transmisión para Muestra 3 @106 kbit/s	1.5	18.0	21.3	21.7	APROBAR
		2.5	13.9	21.6	21.8	APROBAR
		3.5	11.8	21.7	21.7	APROBAR
		4.5	10.4	21.7	21.7	APROBAR
		5.5	9.4	21.7	21.5	APROBAR
		6.0	9.0	21.6	21.3	APROBAR

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo, R.D.
LIC. SANTO C. SICARD Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

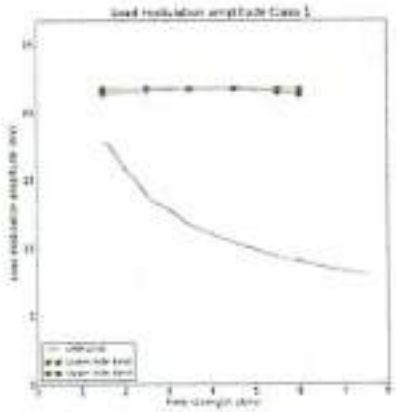
PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019



Curva Carga Modulación Amplitud de el muestra 1 @106 kbit/s



Curva Carga Modulación Amplitud de el muestra 2 @106 kbit/s



Curva Carga Modulación Amplitud de el muestra 3 @106 kbit/s

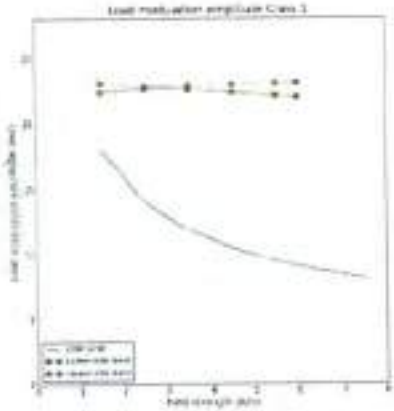
PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

Amplitud de modulación de carga a 1,7 Mbit/s:

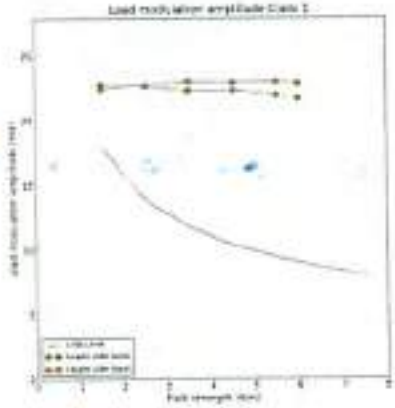
Referencia objetos bajo prueba	Información	H (A/M)	V -LIMA Límite (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @1.7 Mbit/s	1.5	18.0	22.4	23.1	APROBAR
		2.5	13.9	22.7	22.8	APROBAR
		3.5	11.8	22.9	22.6	APROBAR
		4.5	10.4	22.9	22.4	APROBAR
		5.5	9.4	23.0	22.1	APROBAR
		6.0	9.0	23.1	22.0	APROBAR
2K3606	eMRTD Transmisión para Muestra 2 @1.7 Mbit/s	1.5	18.0	22.4	22.8	APROBAR
		2.5	13.9	22.7	22.6	APROBAR
		3.5	11.8	23.0	22.3	APROBAR
		4.5	10.4	22.9	22.3	APROBAR
		5.5	9.4	23.0	21.9	APROBAR
		6.0	9.0	22.9	21.7	APROBAR
3K3606	eMRTD Transmisión para Muestra 3 @1.7 Mbit/s	1.5	18.0	21.5	22.4	APROBAR
		2.5	13.9	21.9	22.2	APROBAR
		3.5	11.8	21.9	21.8	APROBAR
		4.5	10.4	22.2	21.8	APROBAR
		5.5	9.4	22.2	21.6	APROBAR
		6.0	9.0	22.1	21.4	APROBAR

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC: 101898852 Santo Domingo, R.D.
LIC. SANTO C. SILVA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOM

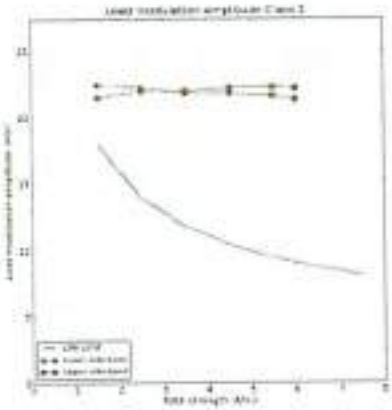
PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019



Curva Carga Modulación Amplitud de el muestra 1 @1.7 Mbit/s



Curva Carga Modulación Amplitud de el muestra 2 @1.7 Mbit/s



Curva Carga Modulación Amplitud de el muestra 3 @1.7 Mbit/s

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

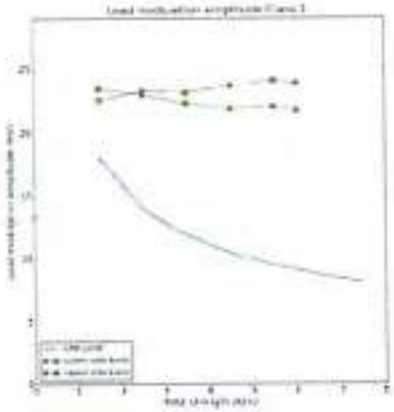
Amplitud de modulación de carga a 3,4 Mbit/s:

Referencia objetos bajo prueba	Información	H (A/M)	V_{LMA} Límite (mv)	Superior banda lateral (mv)	Más bajo banda lateral (mv)	Resultado
1K3606	eMRTD Transmisión para Muestra 1 @3.4 Mbit/s	1.5	18.0	22.6	23.4	APROBAR
		2.5	13.9	23.2	23.0	APROBAR
		3.5	11.8	23.1	22.3	APROBAR
		4.5	10.4	23.6	21.8	APROBAR
		5.5	9.4	24.1	22.0	APROBAR
		6.0	9.0	23.8	21.7	APROBAR
2K3606	eMRTD Transmisión para Muestra 2 @3.4 Mbit/s	1.5	18.0	22.7	22.9	APROBAR
		2.5	13.9	23.3	22.6	APROBAR
		3.5	11.8	23.3	22.0	APROBAR
		4.5	10.4	23.3	21.5	APROBAR
		5.5	9.4	24.2	21.5	APROBAR
		6.0	9.0	23.9	21.4	APROBAR
3K3606	eMRTD Transmisión para Muestra 3 @3.4 Mbit/s	1.5	18.0	21.7	22.7	APROBAR
		2.5	13.9	22.1	22.4	APROBAR
		3.5	11.8	22.2	21.6	APROBAR
		4.5	10.4	22.4	21.3	APROBAR
		5.5	9.4	23.2	21.3	APROBAR
		6.0	9.0	23.4	20.7	APROBAR

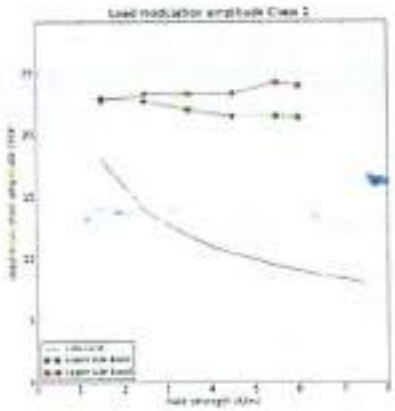
CSI SOLUTIONS INTERNATIONAL S.A. RNC. 101858852 Santo Domingo, R.D.

LIC. SANTO C. SIERRA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

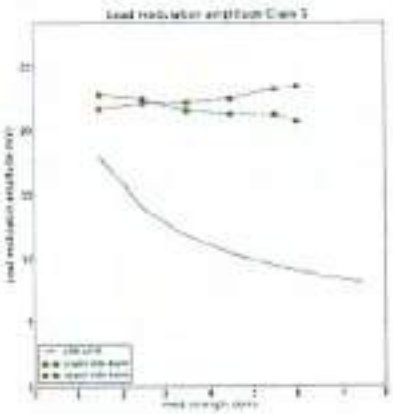
PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019



Curva Carga Modulación Amplitud de el muestra 1 @3.4 Mbit/s



Curva Carga Modulación Amplitud de el muestra 2 @3.4 Mbit/s



Curva Carga Modulación Amplitud de el muestra 3 @3.4 Mbit/s

3.2 FUNCIONAMIENTO CAMPO FORTALEZA

Método:

El prueba método usado se ajusta a documento **[R1]** capítulo 5.3.2 y 7.2.1.
El siguiente secuencia de Comandos (siguiente SECUENCIA_DE_COMANDO_DE_PRUEB A1) es realizado:

Paso	Dominio
1	LEER BINARIO para Acceso a tarjeta EF
2	MSE: Colocar EN
3	GENERAL AUTENTICAR para encriptado mientras tanto
4	GENERAL AUTENTICAR a mapa el mientras tanto
5	GENERAL AUTENTICAR a llevar a cabo Llave acuerdo
6	GENERAL AUTENTICAR a llevar a cabo Mutual Autenticar
7	SELECCIONAR
8	LEER BINARIO para EF.DG14
9	MSE: COLOCAR EN
10	GENERAL AUTENTICAR
11	INTERNO AUTENTICAR [a]
12	LEER BINARIO para EF.CVCA
13	MSE: COLOCAR Horario de verano CVCA
14	PSO: VERIFICAR CERTIFICADO DV
15	MSE: COLOCAR Horario de verano DV
16	PSO: VERIFICAR CERTIFICADO ES
17	MSE: COLOCAR EN
18	CONSEGUIR DESAFÍO
19	EXTERNO AUTENTICAR
20	LEER BINARIO para EF.DG3

[a] Automóvil club británico es apoyado por Documento de identidad electrónico

Cada apoyado simétrico tasa de bits y máximo tasa de bits en ambos instrucciones (eMRTD a eMRTD Lector y eMRTD Lector a documento de identidad electrónico (MRTD) son Probado.

Prueba condiciones:

El pruebas es realizado bajo el condiciones definido en §1.3 .

En T=50°C, *Operante Campo Fortaleza* en AI= 6.5 Soy y 7,5 A/m son no aplicable. Ellos son reemplazado por uno prueba realizado en 6 Soy.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo, R.D.

LIC. SANTO C. SIERRA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

Resultados:

➔ Objeto bajo prueba: 1K3606

Información	H (A/m)	T (°C)	Resultados 106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s	Máximo
Operación Campo Fortaleza para muestra 1	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	NO	NO	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR

[3] Máximo poco tarifas en ambos instrucciones son colocar como declarado en capítulo 2.3: en 3.4 Mbit/s para eMRTD a eMRTD Lector y en 848 Kbit/s para eMRTD Lector a Documento de identidad electrónico (MRTD).

Resultados:

➔ Objeto bajo prueba: 2K3606

Información	H (A/m)	T (°C)	Resultados 106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s	Máximo
Operación Campo Fortaleza para muestra 2	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	NO	NO	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR

➔ Objeto bajo prueba: 2K3606

Información	H (A/m)	T (°C)	Resultados 106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s	Máximo
Operación Campo Fortaleza para muestra 2	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	NO	NO	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	NO	NO	NO	APROBAR
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A	APROBAR

LIC. SANTO C. Sicilia
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, D.N.

3.3 E MRTD RECEPCIÓN

Método:
El prueba método usado se ajusta a documento **[R1]** capítulo 5.3.3 y 7.2.2.

Pruebas condiciones:
El prueba.es realizado bajo el condiciones definido en §1.3

Resultados:

➔ Objeto bajo prueba: 1K3606

Condición 1:

Información	H (A/m)	T (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 1 Condición 1	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	8.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

LIC. SANTO C. SIERRA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC 10 [illegible]852
Santo Domingo, R.D.

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

Condición 2:

Información	H (A/m)	T (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 1 Condición 2	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

Condición 3:

Información	H (A/m)	T (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 1 Condición 3	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

➔ Objeto bajo prueba: 2K3606

Condición 1:

Información	H (A/m)	T (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 2 Condición 1	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC: 101698852 Santo Domingo, R.D.

LIC. SANTO C. SILVA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

LIC. SANTO C. SILVA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO
CSI COMMUNICATIONS INTERNATIONAL, S.A.
RNC 101698852
Santo Domingo, R.D.

Condición 2:

Información	H (A/m)	T (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 2 Condición 2	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

Condición 3:

Información	H (A/m)	T (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 2 Condición 3	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

➔ Objeto bajo prueba: 3K3606

Condición 1:

Información	H (A/m)	T (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 3 Condición 1	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	8.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

LIC. SANTO C. SILVA
Interprete Judicial Juzg 1ra Instancia D.N
SANTO DOMINGO R.D.

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

Condición 2:

Información	H (A/m)	T (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 3 Condición 2	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		en	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

Condición 3:

Información	yo (Soy)	yo (°C)	Resultados						
			106 kbit/s	212 kbit/s	424 kbit/s	848 kbit/s	1.7 Mbit/s	3.4 Mbit/s	6.8 Mbit/s
eMRTD Recepción para Muestra 3 Condición 3	1.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	2.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	3.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	4.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	5.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	6.0	+50	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
	7.5	-10	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A
		+23	APROBAR	APROBAR	APROBAR	APROBAR	N/A	N/A	N/A

3.4 E MRTD R ESONANCIA FRECUENCIA

Método:

Este opcional prueba es realizado de acuerdo a a documento **[R1]** capítulo 5.3.4. A Vector Red Analizador Agilent E5061A es usado.

El mesurado valores son dado para información objetivo solo y No APROBADO/REPROBAD O resultado es proporcionó.

Este prueba es no cubierto por Normas ISO/IEC 17025 Cofrac acreditación.

Prueba condiciones:

El prueba es realizado bajo el siguiente condiciones:

- Temperatura: +23°C ±3 °C
- Relativo Humedad: 25% a 75%

Referencia objetos bajo prueba	Información	Fuerza (dBm)	Resonancia frecuencia	Resultado
1K3606	Resonancia frecuencia	0	15.5	INF
2K3606	Resonancia frecuencia	0	15.3	INF
3K3606	Resonancia frecuencia	0	15.3	INF

Resultados:

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC 101898852 Santo Domingo, R.D.

LIC. SANTO C. Silfa... Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO D.N.

3.5 E MRTD MÁXIMO CARGANDO EFECTO

Método:

Este prueba es realizado de acuerdo a a documento **[R1]** capitulo 5.3.5.

El eMRTD cargando efecto en $H_{min.}$ deber no superar el cargando efecto de el seleccionado Referencia CCP sintonizado a 13.56 megahercio y calibrado a obtener $_{Carga}V$ en CON3 en $H_{min.}$. $_{Carga}V$ y $H_{min.}$ depender a el CCP clases.

Prueba condiciones:

El prueba es realizado bajo el condiciones definido en §1.3

Resultados:

Referencia objetos bajo prueba	Información	T (°C)	$H_{min.}$ (A/m)	Mesurado H (A/m)	Resultado
1K3606	Máximo cargando efecto para muestra 1	-10	1.5	1.67	APROBAR
		+23		1.66	APROBAR
		+50		1.66	APROBAR
2K3606	Máximo cargando efecto para muestra 2	-10	1.5	1.67	APROBAR
		+23		1.67	APROBAR
		+50		1.66	APROBAR
3K3606	Máximo cargando efecto para muestra 3	-10	1.5	1.67	APROBAR
		+23		1.66	APROBAR
		+50		1.66	APROBAR

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC 101856852 Santo Domingo, R.D.

LIC. SANTO C. S... Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, D.N.

3.6 E MRTD LECTURA ACTUACIÓN ANÁLISIS

Método:

El aplicado método es no definido en [R1] y es no cubierto por Normas ISO/IEC 17025 Cofrac acreditación. El mesurado valores son dado para información objetivo solo y No APROBADO/REPROBADO resultado es proporcionó.

El eMRTD lectura actuación análisis es realizado de el Operante Campo Fortaleza pruebas. El evaluación acepta en cuenta 3 muestras, en -10°C, +23°C y +50°C temperaturas y de H_{min} a *Hmáx* .
Como solicitado, siguiente poco tasa condiciones son consideró:

- Tasa de bits condición 1: eMRTD Lector @848 kbit/s / eMRTD @848 kbit/s
- Tasa de bits condición 2: eMRTD Lector @848 kbit/s / eMRTD @3,4 Mbit/s

El momento **eMRTD tratamiento tiempo** reportado en el resultados mesas es el suma de el demora entre el fin de cada lector Comandos y el fin de el asociado eMRTD respuesta como mostrado en Cifra 2.

Cifra 2 Ejemplo de eMRTD Tratamiento tiempo mesurado en REQA

En T=50°C, *Operante Campo Fortaleza* en AI= 6.5 Soy y 7,5 A/m son no aplicable. Ellos son reemplazado por uno prueba realizado en 6 Soy.

Información:

- Tasa de bits condición 2 contiene un adicional tratamiento tiempo pendiente a el S(PARÁMETROS) intercambio. Este adicional tratamiento tiempo es mesurado en 2.3 EM y es incluido a el eMRTD tratamiento tiempo.
- eMRTD transmisión tiempo es el suma de el duración de el eMRTD respuestas. Este momento, incluido a el eMRTD tratamiento tiempo, tiene estado mesurado en 28.8 EM para Tasa de bits condición 1 y en 9.9 EM para Tasa de bits condición 2.

COPY SOLUTIONS INTERNATIONAL, S.A. CSI RNC. 101698852 Santo Domingo, R.D.

LIC. SANTO C. SILVA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO R.D.

PRUEBA INFORME
Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

Resultados:

➔ Objeto bajo prueba: 1K3606

Información	H (A/m)	T (°C)	eMRTD Tratamiento tiempo (EM)				Delta (1) - (2)
			Tasa de bits condición 1 (1)		Tasa de bits condición 2 (2)		
			Lector 848 kbit/s	eMRTD 848 kbit/s	Lector 848 kbit/s	eMRTD 3.4 Mbit/s	
eMRTD lectura tiempo actuación para muestra 1	1.5	-10	3819.1		4338.4		-519.3
		+23	3355.2		3429.6		-74.4
		+50	4721.8		4547.8		174.0
	4.5	-10	1646.8		1628.3		18.5
		+23	1653.5		1635.6		17.9
		+50	1655.9		1637.1		18.8
	6.0	+50	1625.5		1594.5		31.0
	7.5	-10	1187.2		1169.5		17.7
		+23	1192.7		1175.4		17.3

➔ Objeto bajo prueba:: 2K3606

Información	H (A/m)	T (°C)	eMRTD Tratamiento tiempo (EM)				Delta (1) - (2)
			Tasa de bits condición 1 (1)		Tasa de bits condición 2 (2)		
			Lector 848 kbit/s	eMRTD 848 kbit/s	Lector 848 kbit/s	eMRTD 3.4 Mbit/s	
eMRTD lectura tiempo actuación para muestra 2	1.5	-10	4657.6		4637.8		19.8
		+23	4647		4628.5		18.5
		+50	4715.1		4694.2		20.9
	4.5	-10	1639.4		1621.9		17.5
		+23	1647.7		1628.6		19.1
		+50	1649.8		1633.0		16.8
	6.0	+50	1651.8		1633.2		18.6
	7.5	-10	1198.5		1179.9		18.6
		+23	1204.7		1187.5		17.2

➔ Objeto bajo prueba: 3K3606

Información	H (A/m)	T (°C)	eMRTD Tratamiento tiempo (EM)				Delta (1) - (2)
			Tasa de bits condición 1 (1)		Tasa de bits condición 2 (2)		
			Lector 848 kbit/s	eMRTD 848 kbit/s	Lector 848 kbit/s	eMRTD 3.4 Mbit/s	
eMRTD lectura tiempo actuación para muestra 3	1.5	-10	4704.6		4685.3		19.3
		+23	4701.0		4672.0		29.0
		+50	4761.1		4744.8		16.3
	4.5	-10	1645.6		1626.9		18.7
		+23	1653.7		1635.5		18.2
		+50	1655.3		1638.2		17.1
	6.0	+50	1656.1		1639.1		17.0
	7.5	-10	1187.7		1168.6		19.1
		+23	1194.3		1176.1		18.2

LIC. SANTO C. SILVA ... Intérprete Judicial Juzg 1ra Instancia D.N
CRUZ SOLUTIONS INTERNATIONAL S.A. RNC 1-30-898852 Santo Domingo, R.D.

PRUEBA INFORME

Ref.: IC.E.RE.1905.009
Versión: v1.0
Fecha: 17/06/2019

4 CONCLUSIÓN

El siguiente mesa resume el resultados de el pruebas realizado de acuerdo a a referencia documentos listado en §1.2 .

Referencia de objeto bajo prueba	Prueba	Temperatura (°C)	Resultado
1K3606	eMRTD Transmisión	-10	APROBAR
		+23	APROBAR
	Operante Campo Fortaleza	-10	APROBAR
		+23	APROBAR
	eMRTD Recepción	-10	APROBAR
		+23	APROBAR
	eMRTD Resonancia frecuencia (*)	+23	INF
	eMRTD Máximo Cargando Efecto	-10	APROBAR
		+23	APROBAR
2K3606	eMRTD Transmisión	-10	APROBAR
		+23	APROBAR
	Operante Campo Fortaleza	-10	APROBAR
		+23	APROBAR
	eMRTD Recepción	-10	APROBAR
		+23	APROBAR
	eMRTD Resonancia frecuencia (*)	+23	INF
	eMRTD Máximo Cargando Efecto	-10	APROBAR
		+23	APROBAR
		+50	APROBAR
3K3606	eMRTD Transmisión	-10	APROBAR
		+23	APROBAR
	Operante Campo Fortaleza	-10	APROBAR
		+23	APROBAR
	eMRTD Recepción	-10	APROBAR
		+23	APROBAR
		+50	APROBAR
	eMRTD Resonancia frecuencia (*)	+23	INF
	eMRTD Máximo Cargando Efecto	-10	APROBAR
		+23	APROBAR
		+50	APROBAR

(*) Este prueba es no cubierto por Normas ISO/IEC 17025 Cofrac acreditación.

FIN DE DOCUMENTO

El reproducción de este informe es autorizado solo en es integral formato. El comprende 39 páginas.

Traducido a petición de la parte interesada y registrada en mi protocolo. En Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Diecinueve (19) del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

S.C.S / DPE
5184-12-8-96

Página/Folio No.624 de 843

Prueba ISO de Durabilidad de la Tarjeta

fime

Test report

Report object

ISO card durability test session (partial coverage)

Report reference

C22REP01-612_ISO

Vendor name SELP ANGOULEME	**Product name and version** PAK National ID Card Engraved Module
Report version V1.0	**Report issue date** 2022/11/25
Testing dates From 2022/11/04 to 2022/11/22	Authorized by Luc Morcel Expert 2022-11-25 16:29+01:00
Number of pages 37 pages	

cofrac
ESSAIS
Accréditation
N° 1-1709
Portée disponible
sur www.cofrac.fr

The tests listed in Chapter 4.2 are covered by accreditation.
The current version supersedes and replaces all previous versions.
This report shall not be reproduced or communicated except in its full unmodified latest version.

COPY SOLO PARA CSI INTERNATIONAL S.A. RNC: 101[illegible]852 Santo Domingo, R.D.

Table of contents

1. Revision history 4
2. Test results summary 4
2.1 Codification 4
2.2 Summary 4
2.3 Conclusion 5
3. References documents 6
4. Laboratory information 7
4.1 Testing laboratory identification 7
4.2 Accreditation status 7
4.3 Personnel 7
4.4 Operating procedures 7
4.5 Subcontracting 8
4.6 Operating conditions 8
5. Customer & samples information 9
5.1 Customer identification 9
5.2 Sample information 9
5.3 Sample picture 9
6. Test equipment information 10
7. Measurement's uncertainties 12
7.1 Statement of compliance 12
8. Evaluation methods 13
9. Requirements of ISO 7810:2019 chapter 8 14
9.1 Dimensions of cards: thickness 14
9.2 Dimensions of cards: height & width 16
9.3 Dimensions of cards: corners 17
9.4 Bending stiffness 18
9.5 Resistance to chemicals 19
9.6 Card dimensional stability and warpage with temperature and humidity 21
9.7 Peel strength 23
9.8 Adhesion or blocking 24
9.9 Opacity 25
9.10 Card warpage 26
9.11 Resistance to heat 27

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version Página/Folio No.627 de 843

© 2021 Fime – all rights reserved- CONFIDENTIAL

9.12 Dynamic bending stress 28

10. Requirements of ISO 7810:2019 chapter 9 29
10.1 Electrical surface resistance of contacts 29
10.2 Resistance to chemicals: salt mist 30
10.3 Dynamic torsional stress 32

11. Requirements of ISO 7816-1 33
11.1 Surface profile of contacts 33

12. Requirements of ISO 7816-2 34
12.1 Dimension and location of contacts 34

13. Requirements of previous versions of standards 36
13.1 Ultraviolet light 36

14. Terms and conditions 37
14.1 Disclaimers 37
14.2 Commitment 37
14.3 Intellectual property 37
14.4 Storage 37
14.5 Complaint procedure 37

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

1. Revision history

Date	Version	Author	Comment
2022/11/25	1.0	YBR	Initial version

2. Test results summary

2.1 Codification

PASS: passed test
FAIL: failed test
N/A: not applicable test

2.2 Summary

Test	Verdict
ISO 7810 chapter 8 requirements	
Dimensions of cards: thickness*	PASS
Dimensions of cards: height & width*	PASS
Dimensions of cards: corners	PASS
Bending stiffness	PASS
Resistance to chemicals	PASS
Card dimensional stability and warpage with temperature and humidity*	PASS
Peel strength	PASS
Adhesion or blocking	PASS
Opacity	PASS
Card warpage*	PASS
Resistance to heat	PASS
Dynamic bending stress	PASS
ISO 7810 chapter 9 requirements	
Electrical surface resistance of contacts of ICCs with contacts	PASS
Resistance to chemicals: salt mist	PASS
Dynamic torsional stress	PASS
ISO 7816-1 requirements	
Surface profile of contacts of ICCs with contacts*	PASS
ISO 7816-2 requirements	
Dimension and location of contacts for ICCs with contacts	PASS
Requirements from previous versions of standards	
Ultraviolet light	PASS

*: FIME is accredited by COFRAC for this test.

Página/Folio No.629 de 843

© 2021 Fime – all rights reserved- CONFIDENTIAL

2.3 Conclusion

Test session results show that the tested samples meet the requirements necessary to pass the customer's test plan based on ISO, as detailed in this report.
The decision rule applied for the test results is detailed on Measurement's uncertainties section.

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

3. References documents

References		
[R1]	ISO/IEC 10373-1:2020	Identification cards – Test methods – General characteristics
[R2]	ISO/IEC 10373-2:2015	Identification cards – Test methods – Part 2: Cards with magnetic stripes
[R4]	ISO/IEC 10373-6:2016	Test Methods for Proximity Cards
[R20]	ISO/CEI 7810:2019	Identification cards – Physical characteristics
[R21]	ISO/CEI 7811-1:2018	Identification cards – Recording technique – Embossing
[R23]	ISO/CEI 7811-6:2014	Identification cards – Recording technique – Part 6: Magnetic stripe – High coercivity
[R30]	ISO/CEI 7816-1:2011	Identification cards – Integrated circuit cards – Part 1: Physical characteristics
[R31]	ISO/CEI 7816-2:2007	Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of contact
[R41]	ISO/IEC 24789-2:2011	Identification cards – Card Service Life – Part 2: Method of Evaluation

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC 101858852
Santo Domingo, R.D.

4. Laboratory information

4.1 Testing laboratory identification

Name and address of the laboratory that performed the tests and issued this test report:

Fime EMEA
Z.I. de la Folie Couvrechef
8, rue Commodore J.H. Hallet
14000 Caen – France
Telephone: +332 31 44 08 07

4.2 Accreditation status

The laboratory is accredited by COFRAC Essais for ISO 17025, reference 1.1709, scope available on www.cofrac.fr, covering the tests identified with an asterisk in the Tests Results Summary section.

4.3 Personnel

The following persons have collaborated on the preparation, execution or reporting of the tests contained in this report:

Tests	
G. Béhue	Experienced Test Technician
Y. Briard	Experienced Test Technician
L. Morcel	Expert

Report		
Owned by	Y. Briard	Experienced Test Technician
Reviewed by	L. Morcel	Expert
Authorized by	L. Morcel	Expert

4.4 Operating procedures

The internal procedures that relate to the execution of the tests are available in the **Quality Assurance Plan CARD_DURABILITY.**
The template used to create this report is **rep_Generic_Physical_v7.0.**

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.632 de 843

COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC 101899852
Santo Domingo, R.D.

4.5 Subcontracting

In accordance with the estimate accepted by the Customer, the following tests have been subcontracted to: salt mist exposure.

4.6 Operating conditions

The tests have been run with the following external conditions throughout the session:

Parameter	Required range
Temperature	23°C ± 3°C
Relative humidity	40% to 60%

Environmental conditions are recorded with thermo-hygrometer (continuously for test room, during operations for test chambers).

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.633 de 843

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101698852
Santo Domingo, R.D.

5. Customer & samples information

5.1 Customer identification

Company name	SELP ANGOULEME
Address	Rue Louis Pergaud, 16000 Angouleme, France
Contact	CHAMBRE Sebastien
Tel	+33545255114
E-mail	s.chambre@gmail.com

5.2 Sample information

Product name:	PAK National ID Card Engraved Module
Type:	ICC 6 pins
Features:	logos

Samples tested by the Testing Laboratory are identified in the following tables:

Products	Tracking number	Internal ID	Reception date
PAK National ID Card Engraved Module	C22STN01-612	1X217 to 70X217	2022/11/02

5.3 Sample picture

© 2021 Fime – all rights reserved- CONFIDENTIAL

6. Test equipment information

TYPE	DESCRIPTION	ADDITIONAL INFORMATION
3D measuring station	Internal reference: 13/04 Brand: MicroVu	Verified on: 2022/04/04 Width uncertainty: ± 12 µm Height uncertainty: ± 8 µm Corner radius: ± 40 µm Z axis MPE: compliant with ± 2.2 µm +(5L/1000)
4 wires resistance measurement bench	Internal reference: 49/01 Brand: FIME	Verified on: 2022/07/04 Tolerance for applied force: compliant with a ± 0.1 N MPE Tolerance for contacts locations: compliant with 14/03 pattern
Bending stiffness bench	Internal reference: 52/04	Verified on: 2022/01/28
Bending stress machine	Internal reference: 40/07 & 07B Brand: BGI Model or Type: BGI110A:FT2	Verified on: 2022/03/04 Tolerance for deflection: compliant with a ± 1mm MPE Tolerance for frequency: compliant with a ± 0.025Hz MPE
Caliper	Internal reference: 20/01 Brand: Mitutoyo	Verified on: 2022/02/23 Uncertainty: ± 0.03 mm
Chronometer	Internal reference: 60/01 Brand: TIM	Verified on: 2022/07/01 Uncertainty: ± 1 s (on 60 s)
Climatic chamber	Internal reference: C02/05 Brand: Vöstch Model or Type: VC3 4018	Verified on: 2022/05/11 Tolerance for temperature: compliant to a MPE of 3°C Tolerance for humidity: compliant to a MPE of 5%
Comparator	Internal reference: 18/01 Brand: Mitutoyo	Verified on: 2021/12/03 Uncertainty: ± 16 µm (ISO/CQM) ± 7 µm (CB)
Contacts reference block	Internal reference: 14/03 Brand: FIME	Verified on: 2021/09/13 Tolerance: compliant to a ± 10 µm MPE
Cutting tool	Internal reference: 41/12 Brand: Elcometer	Verified on: 2021/11/10
Double disc shearing tool	Internal reference: 22/39 Brand: Noviprofibre Model or Type: N1310	Verified on: 2021/11/10 Tolerance for specimen width: compliant with a ± 0.1 mm MPE
Force sensor	Internal reference: 55/04 Brand: Mecmesin Model or Type: ELS-S 250 N	Verified on: 2022/01/19 Uncertainty: ± 0.22 N @ 3.5 N
Granite surface plate	Internal reference: 21/03	Verified on: 2022/06/30 Tolerance for roughness: compliant with a < 3.2 µm MPE

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version Página/Folio No.635 de 843

© 2021 Fime – all rights reserved- CONFIDENTIAL

TYPE	DESCRIPTION	ADDITIONAL INFORMATION
Height gage	Internal reference: 22/38 Brand: Linear tool	Verified on: 2022/03/18 Uncertainty: ± 0.33 mm (stiffness) Uncertainty: ± 0.68 mm (resistance to heat)
ICC holder	Internal reference: 52/05 Brand: BGI	-
Load	Internal reference: 22/11 to 22/15 Model or Type: 2.2 N	Verified on: 2021/01/22 Tolerance: compliant to a MPE of 0.11 N
Load	Internal reference: 22/29 Model or Type: 23.1 N	Verified on: 2022/02/23 Tolerance: compliant to a MPE of 1.2 N
Micrometer	Internal reference: 19/10 Brand: Mitutoyo Model or Type: Digital 0-25 mm	Verified on: 2021/12/03 Uncertainty: ± 5 µm (thickness)
Micro-ohmmeter	Internal reference: C28/30 Brand: Keysight Model or Type: 34420A	Verified on: 2022/06/30 Uncertainty: ± 6 mOhm
Multimeter	Internal reference: 07/02 Brand: Agilent Model or Type: 34401A	Verified on: 2022/03/29 Uncertainty: ± 10 mOhm
Opacity tester	Internal reference: 41/04 Brand: Q-Card Model or Type: 905703-2	Verified before use Uncertainty: ± 0.9% at 860 nm ± 0.8% at 950 nm
Pattern for location of contacts	Brand: FIME	Used with contacts reference block
PC/SC reader	Internal reference: C36/106 Brand: FIME / Identive Model or Type: SDI 011 with landing connector	Contact and contactless
Profile projector	Internal reference: 13/02 Brand: Nikkon Model or Type: V-12	Verified on: 2022/07/01 Magnification: compliant to a MPE of 1 (ratio) Uncertainty: ± 80 µm (warpage) ± 3 µm (edge)
Software: Thickness acquisition and treatment	Software name: Thickness Brand: FIME	Software version: v1.06
Software: PC/SC reader interface	Software name: ATR reader Brand: FIME	Software version: v1.5
Software: Treatment of raw data of force sensor	Software name: LBC Brand: FIME	Software version: v2.37
Software: Resistance acquisition	Software name: Ohmmeter Brand: FIME	Software version: v2.1
Software: Warpage acquisition and treatment	Software name: Profile Brand: FIME	Software version: v1.9
Thermo-hygrometer (test room)	Internal reference: C09/33 Brand: ELPRO Model or Type: Ecolog LH2	Verified on: 2022/06/16 Uncertainty: ± 0.3 °C; ± 2 %
Thermo-hygrometer (test chamber)	Internal reference: C09/09 Brand: ELPRO Model or Type: Ecolog TH2	Verified on: 2022/07/11 Uncertainty: ± 1 °C

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

TYPE	DESCRIPTION	ADDITIONAL INFORMATION
Thermo-hygrometer (test chamber)	Internal reference: C09/11 Brand: ELPRO Model or Type: Ecolog TH2	Verified on: 2022/05/30 Uncertainty: ± 1 °C; ± 12 %
Thermo-hygrometer (test chamber)	Internal reference: C09/18 Brand: ELPRO Model or Type: Ecolog TH2	Verified on: 2022/02/09 Uncertainty: ± 1 °C; ± 3 %
Torsional stress machine	Internal reference: 40/07&40/07A Brand: BGI Model or Type: BGI110A:FT2	Verified on: 2022/02/25 Tolerance for angle: compliant with a ± 1.5° MPE Tolerance for frequency: compliant with a ± 0.025Hz MPE
Traction test bench	Internal reference: C25/05 Brand: Mecmesin Model or Type: Multitest 2.5 dV	Verified on: 2022/09/14 Tolerance for speed: compliant with a ± 10 mm/min MPE
UV generator	Internal reference: 36/02 Brand: LEAP ELECTRONIC Model or Type: EPROM ERASER LER-123A	-

7. Measurement's uncertainties

7.1 Statement of compliance

In this report, uncertainties are given at a confidence level of k = 2.
To state on compliance, uncertainties of measurement have not been considered. Statements established on measurements included in the uncertainty area are identified with asterisk.

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SOLO CSI INTERNATIONAL S.A. RNC: 101898652 Santo Domingo R.D.

8. Evaluation methods

Whenever test method requires that a sample remains 'testably functional', the following evaluations are performed when applicable (depending on functionalities present):

- For contact and dual products: detection of an ATR using a PC/SC reader; conformity to electrical surface resistance of contacts ([R1] §6.7 (criteria in [R20] §9.6).
- For contactless and dual products: detection of a request to WAKEUP command using a PC/SC reader ([R4]); resonance frequencies (in MHz) before and after tests are indicated for information only.
- For magnetic stripe products: dynamic characteristics shall remain compliant to [R23] §7.3. For Resistance to Chemicals and Wear Test, magnetic stripe is first encoded and signal amplitude measured. After exposure signal amplitude is measured again and compared to initial value according to [R23] §6.4 & §6.5 criteria.

Aspect criterion is met when the following defects are absent after test:

- Cracks (cracks going through the material, visible on both side of the card. Surface cracks are not considered).
- Layers delamination (overlay or inner layers).
- Module detachment from card body.
- Discoloration and dye transfer that prevents expected use (faded printings or picture).
- Deterioration of security features (unless otherwise specified).
- Any other damage that deteriorates card functionality or information.

These evaluations are also performed prior to the tests, to ensure that samples were intact before stresses.

Página/Folio No.638 de 843

© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC: 1[illegible]38852
Santo Domingo, R.D.

9. Requirements of ISO 7810:2019 chapter 8

9.1 Dimensions of cards: thickness

Reference

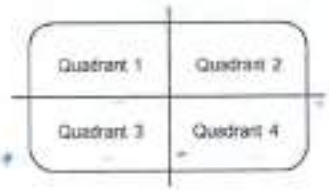
Based on [R1] §5.2.2 (criteria in [R20] §5.2). The purpose of this test is to measure the thickness of a card.

Test bench

Micrometer (see chapter 6)
Acquisition software

Procedure

Use micrometer to measure the thickness of card under test. Thickness is measured at four locations. Measurement can be performed anywhere in a quadrant, except on chip's contacts, signature panel, magnetic stripe or any other raised areas.



Criteria

Thickness: *[680 µm – 840 µm]*

Results

Values in the table below are in µm.

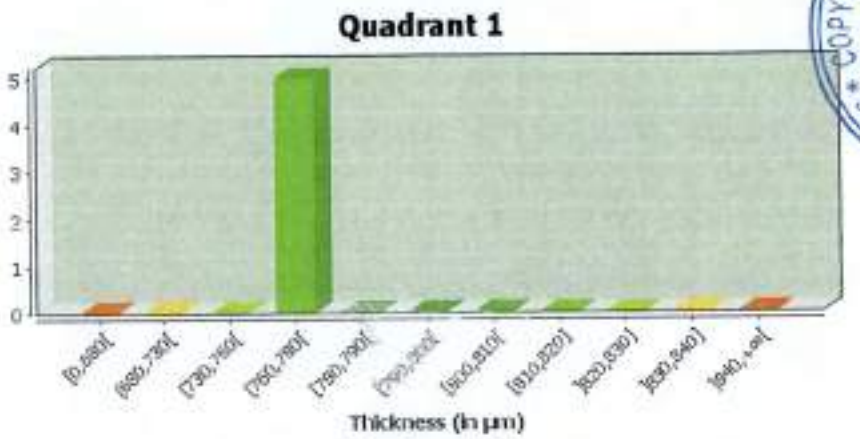
Sample	Q1 thickness	Q2 thickness	Q3 thickness	Q4 thickness	Verdict
1X217	773	772(m)	776	785(M)	PASS
2X217	775	778	773(m)	791(M)	PASS
3X217	776	775	774(m)	786(M)	PASS
4X217	772(m)	773	773	776(M)	PASS
5X217	775	775	776(M)	773(m)	PASS

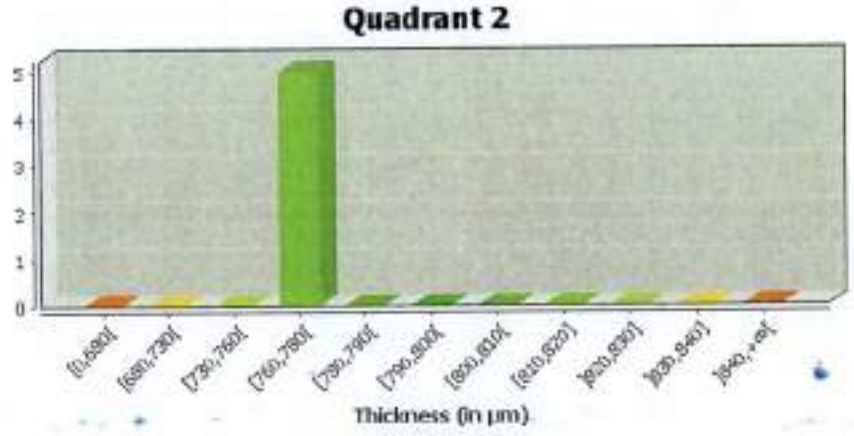
(m) stands for minimum value and (M) for maximum value

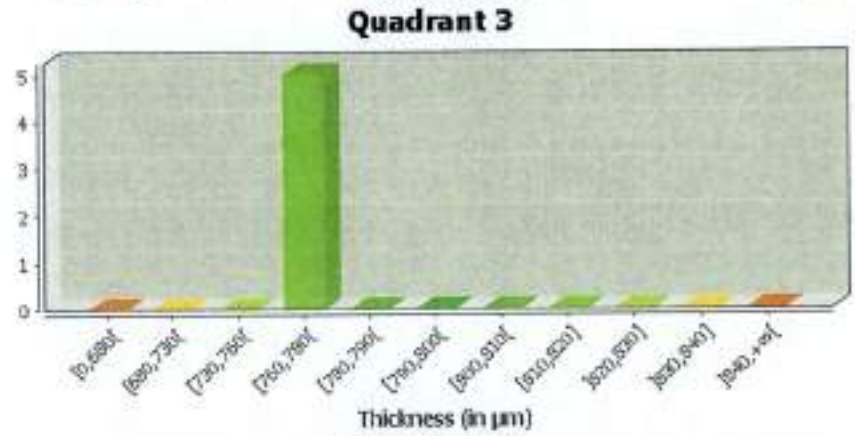
The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

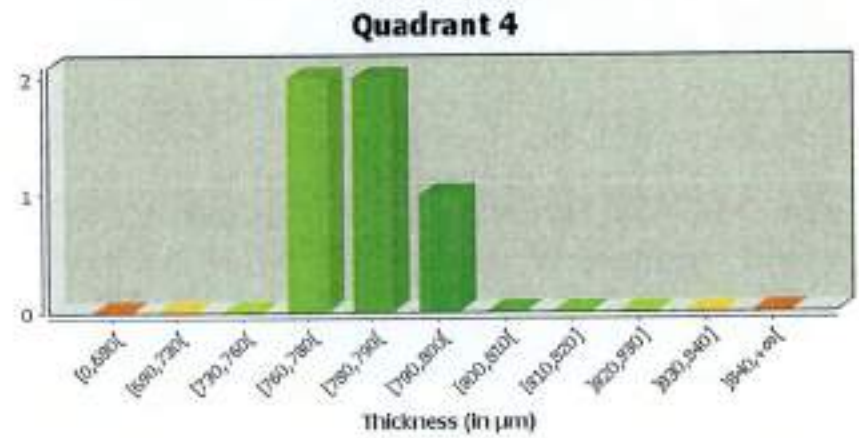
© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 131698852
Santo Domingo, R.D.









The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

Página/Folio No.640 de 843

© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SOLUTIONS INTERNATIONAL
CSI
RNC: 01898852

9.2 Dimensions of cards: height & width

Reference

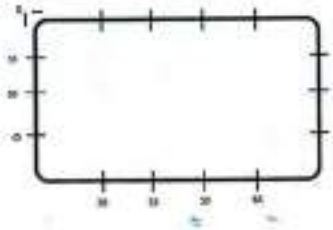
Based on [R1] §5.2.3 (criteria in [R20] §5.2). The purpose of this test is to verify card's size and its parallelism.

Test bench

3D measuring station and software (see chapter 6)
Load
Data processing (LBC)

Procedure

Place tested cards on station's holder.
Then use 3D measuring station software (ISO program) to determine the size of inner and outer rectangles.
Then state on card conformity.



Criteria

Inner rectangle (height x width): *53.920 mm x 85.470 mm*
Outer rectangle (height x width): *54.030 mm x 85.720 mm*

Results

Sample	Inner rectangle height (mm) X width (mm)	Outer rectangle height (mm) X width (mm)	Verdict
1X217	53.973 mm x 85.594 mm	53.990 mm x 85.610 mm	PASS
2X217	53.967 mm x 85.594 mm	54.012 mm x 85.607 mm	PASS
3X217	53.971 mm x 85.601 mm	54.002 mm x 85.611 mm	PASS
4X217	53.960 mm x 85.600 mm	54.007 mm x 85.613 mm	PASS
5X217	53.968 mm x 85.597 mm	54.000 mm x 85.610 mm	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version
Página/Folio No.641 de 843

© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC: 101896852
Santo Domingo, R.D.

9.3 Dimensions of cards: corners

Reference

Based on [R1] §5.2.3 (criteria in [R20] §5.1.1). The purpose of this test is to verify the radius of card's corners.

Test bench

3D measuring station and software (see chapter 6)
Load

Procedure

Place tested cards on station's holder. Then launch the 3D measuring station program for corner measurement.

Criteria

Radius: *[2.88 mm – 3.48 mm]*

Results

Sample	Top left corner value	Top right corner value	Bottom left corner value	Bottom right corner value	Verdict
1X217	3.194	3.260	3.192	3.049	PASS
2X217	3.121	3.320	3.170	3.229	PASS
3X217	3.278	3.273	3.170	3.217	PASS
4X217	3.151	3.158	3.191	3.183	PASS
5X217	3.179	3.177	3.201	3.259	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.642 de 843

COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC: 101898852
Santo Domingo, R.D.

9.4 Bending stiffness

Reference

Based on [R1] §5.8 (criteria in [R20] §8.1). The purpose of this test is to determine if the bending stiffness of card meet the requirement of the standard.

Test bench

Bending stiffness bench
Height gage (see chapter 6)

Procedure

Clamp a card along its left side, front side upward.
Move the height gage probe to card's right side level and reset it.
Apply the load at right side of card and wait for 1 minute.
Using height gage, measure the deflection of right side.
Remove the load and wait for 1 minute.
Using height gage measure the residual deformation.

Criteria

Deflection: *[13 mm – 35 mm]*
Deformation: *[-1.5 mm – 1.5 mm]*

Results

Sample	Deflection (mm)	Deformation (mm)	Verdict
41X217	19.16	-0.09	PASS
42X217	19.27	-0.20	PASS
43X217	19.26	-0.11	PASS
44X217	19.14	-0.27	PASS
45X217	20.99	-0.05	PASS

Note: h_1 value from test method is arbitrarily set at 0 mm, before load application. So h_2 is deflection and h_3 is deformation (see [R1] §5.7).

© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 401898852 Santo Domingo R.D.

9.5 Resistance to chemicals

Reference

Based on [R1] §5.5 (criteria in [R20] §8.3). The purpose of this test is to determine if common chemicals can damage card or affect its functionality.

Test bench

Tools for dimensions measurements (warpage, thickness and height & width)
Chronometer
PC/SC reader
Micro-ohmmeter and 4 wires resistance measurement test bench
(see chapter 6)

Procedure

Perform all required measurements and tests before exposure according to card's features.
Select one sample for each solution. Expose sample to its associated solution for the required duration (1 min for short term exposure and 24 hours for long term exposure). After removal from solution, rinse the card and dry it with absorbent tissue. Then they are return to default environment for 24 hours.
Perform all 'after exposure' required measurements and tests according to card's features.

Solution	Code	Type
Sodium chloride	a	Short term
Acetic acid	b	Short term
Sodium carbonate	c	Short term
Ethyl alcohol	d	Short term
Sucrose	e	Short term
Fuel B (ISO 1817)	f	Short term
Ethylene glycol	g	Short term
Alkaline artificial perspiration	h	Long term
Acid artificial perspiration	i	Long term

Criteria

Dimensions:	*conformity to warpage, thickness and height & width criteria.*
Functionality:	*samples shall remain testably functional (see chapter 8).*
Aspect:	*visual examination shall not reveal any defects.*

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.644 de 843

Results

Dimensions:

Sample	Code	Thickness	Height & Width	Warpage
6X217	a	PASS	PASS	PASS
7X217	b	PASS	PASS	PASS
8X217	c	PASS	PASS	PASS
9X217	d	PASS	PASS	PASS
10X217	e	PASS	PASS	PASS
11X217	f	PASS	PASS	PASS
12X217	g	PASS	PASS	PASS
13X217	h	PASS	PASS	PASS
14X217	i	PASS	PASS	PASS

Functionality & aspect:

Sample	Code	Aspect	Contact funct.	Electrical resistance of contacts
6X217	a	PASS	PASS	PASS
7X217	b	PASS	PASS	PASS
8X217	c	PASS	PASS	PASS
9X217	d	PASS	PASS	PASS
10X217	e	PASS	PASS	PASS
11X217	f	PASS	PASS	PASS
12X217	g	PASS	PASS	PASS
13X217	h	PASS	PASS	PASS
14X217	i	PASS	PASS	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version
Página/Folio No.645 de 843

© 2021 Fime – all rights reserved- CONFIDENTIAL

CSI SOLUTIONS INTERNATIONAL S.A.
RNC. 101898852
Santo Domingo, R.D.

9.6 Card dimensional stability and warpage with temperature and humidity

Reference

Based on [R1] §5.6 (criteria in [R20] §8.4). The purpose of this test is to verify that dimensions and warpage of cards remain within standard requirements after exposures to conditions detailed below.

Test bench

Tools for dimensions measurements (warpage, thickness and height & width)
Climatic chamber
(see chapter 6)

Procedure

Measure the thickness, height, width and warpage of the cards before exposures (t_0).
Place samples on a horizontal flat surface and expose them to the climatic conditions below for 60 minutes:

- t_1: -35°C
- t_2: +50°C / 95% RH

After each sequence, return samples to default environment conditions for 24 hours before performing the dimensions and warpage measurements.
Evaluate dimensions at t_1 (after cold exposure) and t_2 (after damp heat exposure).

Criteria

Thickness:	*[680 µm – 840 µm]*
Inner rectangle (height x width):	*53.920 mm x 85.470 mm*
Outer rectangle (height x width):	*54.030 mm x 85.720 mm*
Warpage:	*lower than 1.5 mm*

© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SOLUTIONS INTERNATIONAL S.A. CSI 1698852 Rio Domingo, R.D.

Results

Sample	Inner rectangle @ t_0 height (mm) X width (mm)	Outer rectangle @ t_0 height (mm) X width (mm)	Verdict
1X217	53.973 mm x 85.594 mm	53.990 mm x 85.610 mm	PASS
2X217	53.967 mm x 85.594 mm	54.012 mm x 85.607 mm	PASS
3X217	53.971 mm x 85.601 mm	54.002 mm x 85.611 mm	PASS
4X217	53.960 mm x 85.600 mm	54.007 mm x 85.613 mm	PASS
5X217	53.968 mm x 85.597 mm	54.000 mm x 85.610 mm	PASS

Sample	Inner rectangle @ t_1 height (mm) X width (mm)	Outer rectangle @ t_1 height (mm) X width (mm)	Verdict
1X217	53.967 mm x 85.592 mm	53.995 mm x 85.609 mm	PASS
2X217	53.960 mm x 85.592 mm	54.002 mm x 85.607 mm	PASS
3X217	53.969 mm x 85.598 mm	54.014 mm x 85.614 mm	PASS
4X217	53.961 mm x 85.603 mm	53.999 mm x 85.611 mm	PASS
5X217	53.971 mm x 85.595 mm	54.002 mm x 85.610 mm	PASS

Sample	Inner rectangle @ t_2 height (mm) X width (mm)	Outer rectangle @ t_2 height (mm) X width (mm)	Verdict
1X217	53.958 mm x 85.580 mm	53.985 mm x 85.596 mm	PASS
2X217	53.954 mm x 85.581 mm	54.007 mm x 85.597 mm	PASS
3X217	53.964 mm x 85.590 mm	54.006 mm x 85.600 mm	PASS
4X217	53.953 mm x 85.591 mm	53.989 mm x 85.605 mm	PASS
5X217	53.962 mm x 85.588 mm	53.993 mm x 85.599 mm	PASS

Sample	Thickness @ t_0 (µm)	Verdict	Thickness @ t_1 (µm)	Verdict	Thickness @ t_2 (µm)	Verdict
1X217	785	PASS	791	PASS	796	PASS
2X217	791	PASS	790	PASS	793	PASS
3X217	786	PASS	794	PASS	796	PASS
4X217	776	PASS	796	PASS	797	PASS
5X217	776	PASS	793	PASS	794	PASS

Sample	Warpage @ t_0 (mm)	Verdict	Warpage @ t_1 (mm)	Verdict	Warpage @ t_2 (mm)	Verdict
1X217	0.845	PASS	0.845	PASS	0.877	PASS
2X217	0.856	PASS	0.856	PASS	0.846	PASS
3X217	0.871	PASS	0.860	PASS	0.837	PASS
4X217	0.855	PASS	0.859	PASS	0.838	PASS
5X217	0.818	PASS	0.813	PASS	0.789	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.647 de 843

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101898852
Santo Domingo R.D.

9.7 Peel strength

Reference

Based on [R1] §5.3 & §5.4 (criteria in [R20] §8.7). The purpose of this test is to measure the peel strength between the layers of the card body.

Test bench

Double disk shearing tool
Traction test bench
Dynamometer & force sensor
Data treatment software
(see chapter 6)

Procedure

Cut the card to make sections 10 mm wide (± 0.2 mm).
Using a sharp knife, cut the layer to test from the core on approximately 10 mm long, insert it between the rollers and attach it to the force sensor.
Stick them on a stabilizing plate if sections are too flexible and/or to measure the peel strength at the edge of the card. For measurement at the edge, add a spacer of same thickness as test specimen.
Launch the peel test at 300 mm/min, watching for tearing or rupture.
Analyse the trace, excluding first and last 5 mm of record, to find the lowest point (negative peaks that have a length lower than 1 mm at criteria level are ignored).

Criteria

Peeling force (card's layer): ≥ 3.5 N

Results

Sample	Stripe	Interface	Min force (N)	Comment	Verdict
54X217	A	Front overlay	-	Specimen preparation not possible*	PASS
54X217	B	Back overlay	-	Specimen preparation not possible*	PASS
55X217	A	Front overlay	-	Specimen preparation not possible*	PASS
55X217	B	Back overlay	-	Specimen preparation not possible*	PASS
56X217	A	Front overlay	-	Specimen preparation not possible*	PASS
56X217	B	Back overlay	-	Specimen preparation not possible*	PASS

*: in such case [R20] §8.7 states that this behaviour is automatically deemed acceptable.

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.648 de 843

COPY SOLELY FOR INTERNATIONAL S.A.
CSI
RNC: 101098852
Santo Domingo R.D.

9.8 Adhesion or blocking

Reference

Based on [R1] §5.7 (criteria in [R20] §8.8). The purpose of this test is to determine any negative effects of stacking unembossed cards.

Test bench

Climatic chamber
Caliper
Load
(see chapter 6)

Procedure

Make a stack of five tested cards (all cards shall have backsides downward). Prepare another stack with five dummy cards. Use the load to generate the specified pressure.
Expose the assembly to test environment (40°C / 50% RH) for 48 hours.
Then return cards to default environment.

Criteria

Adhesion:	*cards shall be easily separated manually.*
Aspect:	*visual examination shall not reveal any defects.*

Results

Sample	Manual separation	Aspect
49X217	PASS	PASS
50X217	PASS	PASS
51X217	PASS	PASS
52X217	PASS	PASS
53X217	PASS	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.649 de 843

COPY SOLO CSI INTERNATIONAL S.A
CSI
RNC: 101898852
Santo Domingo R.D.

9.9 Opacity

Reference

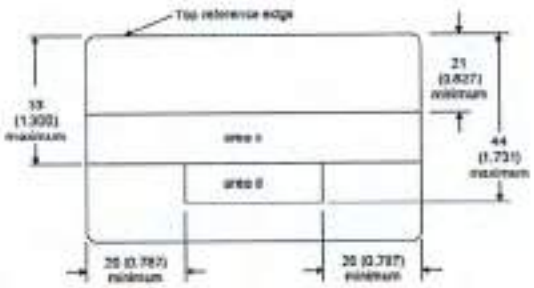
Based on [R1] §5.11 (criteria in [R20] §8.9). The purpose of this test is to determine the opacity of card body at 860 nm and 950 nm wavelengths.

Test bench

Opacity tester (see chapter 6)
Black and ORM 7810 reference screens

Procedure

Select 860 nm wavelength and allow the tester to warm-up.
Check black reference screen value is 0.
Record value measured for ORM 7810 reference screen.
Card is scanned to find the location showing the lowest opacity value (which matches with the maximum percentage value returned by the opacity tester).
Lowest opacity location may be anywhere on the card except in area 'c' and 'd', as shown on the diagram.
Repeat with 950 wavelength.



Criteria

Maximum percentage value measured on tested card shall be lower than the value measured on ORM 7810 reference screen (for both wavelengths).

Results

Sample	860 nm	950 nm	Verdict
Black reference screen	0	0	-
ORM 7810 reference screen	3.7	3.6	-
46X217	0.1@ (15, 15)	0.1@ (15, 40)	PASS
46X217	0.1@ (45, 15)	0.1@ (45, 40)	PASS
47X217	0.1@ (70, 15)	0.1@ (70, 40)	PASS
47X217	0.1@ (15, 15)	0.1@ (15, 40)	PASS
48X217	0.1@ (45, 15)	0.1@ (45, 40)	PASS
48X217	0.1@ (70, 15)	0.1@ (70, 40)	PASS

© 2021 Fime – all rights reserved- CONFIDENTIAL

COPY SUBJECT TO INTERNAL
CSI
RNC: 101698852
Santo Domingo, R.D.

9.10 Card warpage

Reference

Based on [R1] §5.1 (criteria in [R20] §8.10). The purpose of this test is to measure the warpage of a card.

Test bench

Profile projector (see chapter 6)
Sample holder
Acquisition software

Procedure

Place the sample holder on profile projector.
Place the card under test in the sample holder.
Move to the lower point of the card and reset the micrometer.
Found the farthest point on the opposite card's side and measure the height distance from lower point.

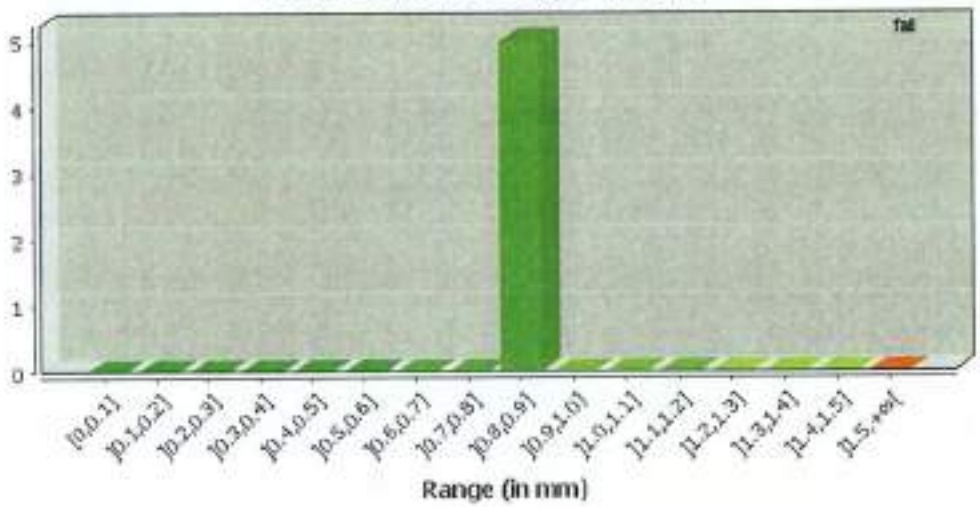
Criteria

Warpage: *lower than 1.5 mm.*

Results

Sample	Warpage (mm)	Verdict
1X217	0.845	PASS
2X217	0.856	PASS
3X217	0.871	PASS
4X217	0.855	PASS
5X217	0.818	PASS

Card dimension (warpage)



© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.651 de 843

COPY SOLO PARA CSI INTERNATIONAL S.A. RNC: 101896852 Santo Domingo, R.D.

9.11 Resistance to heat

Reference

Based on [R1] §5.14 (criteria in [R20] §8.12). The purpose of this test is to determine if an exposure to high temperature affects cards stiffness.

Test bench

Bending stiffness bench
Height gage
Climatic chamber
Granite surface plate
(see chapter 6)

Procedure

Clamp cards along theirs rights sides, front side upward (contacts location shall if opposite the clamping device).
Lower the height gage probe down to the granite surface plate, and reset it.
Move the height gage probe to each card's left side level, and record the measured height.
Expose cards to a temperature of 50°C for 4 hours.
Return cards to default environment and wait for at least half an hour.
Using height gage, measure the residual deformation of each card.

Criteria

Deformation: *< 10 mm*

Results

Sample	Orientation	Deformation (mm)	Verdict
59X217	Front side up	0.32	PASS
60X217	Front side up	0.20	PASS
61X217	Front side up	0.31	PASS
62X217	Backside up	0.09	PASS
63X217	Backside up	0.09	PASS

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.652 de 843

COPY SOLO PARA USO INTERNACIONAL S.A
CSI
RNC: 1-31898852
Santo Domingo R.D.

9.12 Dynamic bending stress

Reference

Based on [R1] §5.9 (criteria in [R20] §8.14). The purpose of this test is to determine if bending stress can damage card or affect its functionality.

Test bench

Bending stress machine
PC/SC reader
Micro-ohmmeter and 4 wires resistance measurement test bench
(see chapter 6)

Procedure

Cards are bent 1000 times, following these steps:

- Machine is set to bend card by curvature of the long sides.
- Place cards front side upward. Run 250 cycles at 0.5 Hz.
- Reposition cards backside upward and run 250 cycles at 0.5 Hz.
- Set machine to bend card by curvature of the short sides.
- Place cards front side upward. Run 250 cycles at 0.5 Hz.
- Reposition cards backside upward and run 250 cycles at 0.5 Hz.

Criteria

Functionality:	*samples shall remain testably functional (see chapter 8).*
Aspect:	*visual examination shall not reveal any cracked part.*

Results

Sample	Aspect	Contact funct. (ATR)	Electrical resistance of contacts
18X217	PASS	PASS	PASS
19X217	PASS	PASS	PASS
20X217	PASS	PASS	PASS
21X217	PASS	PASS	PASS
22X217	PASS	PASS	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.653 de 843

COPY CSI RNC: 101893852 Santo Domingo R.D.

10. Requirements of ISO 7810:2019 chapter 9

10.1 Electrical surface resistance of contacts

Reference

Based on [R1] §6.7 (criteria in [R20] §9.6). The purpose of this test is to determine if electrical surface resistances of the contacts meet standard requirements.

Test bench

Micro-ohmmeter
4 wires resistance measurement test bench
Resistance acquisition software
(see chapter 6)

Procedure

Using the 4 wires resistance measurement test bench, place the two probes on the first contact.
Micro-ohmmeter performs the measurement and sends it to acquisition software.
Continue this other contacts and other samples.

Criteria

Electrical surface resistance: *≤ 500 mΩ*

Results

Sample	C1	C2	C3	C4	C5	C6	C7	C8	Verdict
6X217	39mΩ	39mΩ	40mΩ	N/A	39mΩ	39mΩ	40mΩ	N/A	PASS
7X217	40mΩ	39mΩ	39mΩ	N/A	39mΩ	39mΩ	39mΩ	N/A	PASS
8X217	39mΩ	39mΩ	39mΩ	N/A	38mΩ	38mΩ	39mΩ	N/A	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.654 de 843

COPY SOLO CSI RNC: 1019[illegible]852 SELP INTERNATIONAL S.A.

10.2 Resistance to chemicals: salt mist

Reference

Based on [R1] §5.5 and ISO 9227 (criteria in [R20] §9.8). The purpose of this test is to determine if common chemicals can damage card or affect its functionality.

Test bench

Salt mist chamber (subcontractor's equipment)
PC/SC reader
Micro-ohmmeter and 4 wires resistance measurement test bench
(see chapter 6)

Procedure

Expose cards to salt mist environment. Parameters of test chamber shall be set to the following values:

- Concentration of sodium chlorate: 50 ± 5 g/L
- Solution density: $1029 < \rho\ (kg/m^3) < 1036$
- pH of salt solution: $6.5 < pH < 7.2$

Exposure lasts 24 hours. After exposure, test parameters are:

- pH of solution: 7.1
- Solution density: $\rho = 1034\ kg/m^3$
- Pressure: 1.0 bar
- Temperature: 35°C

After exposure cards are rinsed and dried with absorbent tissue. Then they are return to default environment for 24 hours.

Criteria

Dimensions:	*conformity to warpage, thickness and height & width criteria.*
Functionality:	*samples shall remain testably functional (see chapter 8).*
Aspect:	*visual examination shall not reveal any defects.*

Note

Salt mist exposure is subcontracted.

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.655 de 843

COPY SOLO CSIQ RNC: 101808852 Santo Domingo R.D.

Results

Dimensions:

Sample	Thickness	Height & Width	Warpage
15X217	PASS	PASS	PASS
16X217	PASS	PASS	PASS
17X217	PASS	PASS	PASS

Functionality & aspect:

Sample	Aspect	Contact functionality	Electrical resistance of contacts
15X217	PASS	PASS	PASS
16X217	PASS	PASS	PASS
17X217	PASS	PASS	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.656 de 843

COPY SOLO PARA USO INTERNO
CSI
RNC: 101038852
Santo Domingo, R.D.

10.3 Dynamic torsional stress

Reference

Based on [R1] §5.10 (criteria in [R20] §9.11). The purpose of this test is to determine if torsional stress can damage card or affect its functionality.

Test bench

Torsional stress machine
PC/SC reader
Micro-ohmmeter and 4 wires resistance measurement test bench
(see chapter 6)

Procedure

Cards are twisted 1000 times with an angle of 2x 15° and a frequency of 0.5 Hz.

Criteria

Functionality: *samples shall remain testably functional (see chapter 8).*
Aspect: *visual examination shall not reveal any cracked part.*

Results

Sample	Aspect	Contact functionality	Electrical resistance of contacts
23X217	PASS	PASS	PASS
24X217	PASS	PASS	PASS
25X217	PASS	PASS	PASS
26X217	PASS	PASS	PASS
27X217	PASS	PASS	PASS

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.657 de 843

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101893852
Santo Domingo R.D.

11. Requirements of ISO 7816-1

11.1 Surface profile of contacts

Reference

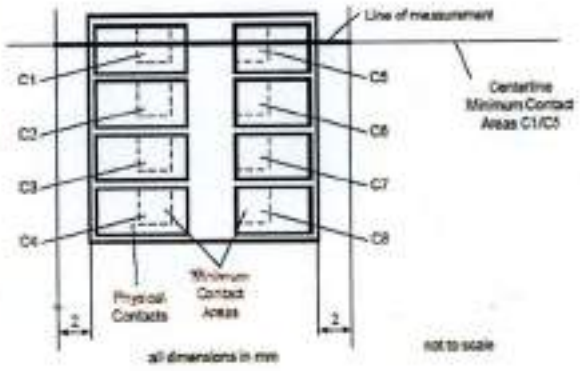
Based on [R1] §6.9 (criteria in [R30] §4.2). The purpose of this test is to measure the height of each contact, using card's front side surface as a reference.

Test bench

Comparator (see chapter 6)

Procedure

Visualize a line crossing the first pair of contacts (C1 and C5) in their center. Start and end of this line are 2 mm away from metallized surface.
Measure the height of start and end points. Base thickness is the average of these two values.
Along the measurement line, measure heights of C1 and C5. Calculate the difference between heights and base thickness.
Proceed the same way with the other pairs of contacts (C2 – C6, C3 – C7 and C4 – C8 if presents).



Criteria

Height of contacts from card body surface: *[-100 µm - +100 µm]*

Results

Values in the table below are in µm.

Sample	C1	C2	C3	C4	C5	C6	C7	C8	Verdict
46X217	-8	1,5	-6	N/A	-13	-8,5	-6	N/A	PASS
47X217	-9	17	-9	N/A	-6	-6	-5	N/A	PASS
48X217	-13	18	-18,5	N/A	-12	4	11,5	N/A	PASS

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.658 de 843

COPY SOLUTIONS INTERNATIONAL S.A
CSI
RNC: 101[illegible]852
Santo Domingo R.D.

12. Requirements of ISO 7816-2

12.1 Dimension and location of contacts

Reference

Based on [R1] §6.3 (criteria in [R31] §4). The purpose of this test is to determine if dimension and location of card's contacts meet standard requirements.

Test bench

Profile projector (see chapter 6)
Pattern for location of contacts
Contacts reference block
Load

Procedure

Place the contacts reference block on profile projector plate and align it with contacts pattern (on profile projector screen), moving profile projector's axis.
Place card under test on profile projector plate and maintain it with load.
Check if the materialized minimum contact areas of the pattern are fully covered by the metallization.
Check if metallization within materialized minimum contact areas are not connected to any other contacts.
In case of doubt, use 3D measuring station to measure the actual dimension and location.

Criteria

Values in the table below are in mm.

Contact	Left border	Right border	Bottom border	Top border
C1	≤10.25	≥12.25	≤19.23	≥20.93
C2	≤10.25	≥12.25	≤21.77	≥23.47
C3	≤10.25	≥12.25	≤24.31	≥26.01
C4	≤10.25	≥12.25	≤26.85	≥28.55
C5	≤17.87	≥19.87	≤19.23	≥20.93
C6	≤17.87	≥19.87	≤21.77	≥23.47
C7	≤17.87	≥19.87	≤24.31	≥26.01
C8	≤17.87	≥19.87	≤26.85	≥28.55

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.659 de 843

COPY CSVS INTERNATIONAL S.A.
CSVS
RNC: 101852852

Results

Sample	Item	C1	C2	C3	C4	C5	C6	C7	C8
46X217	Dimension	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
	No connection	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
47X217	Dimension	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
	No connection	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
48X217	Dimension	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
	No connection	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
49X217	Dimension	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
	No connection	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
50X217	Dimension	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A
	No connection	PASS	PASS	PASS	N/A	PASS	PASS	PASS	N/A

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.660 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101[illegible]852 Santo Domingo, R.D.

13. Requirements of previous versions of standards

13.1 Ultraviolet light

Reference

Based on ISO/IEC 10373-1:2006 §5.11 (criteria in ISO/IEC 7816-1:1998 §4.2.1). The purpose of this test is to determine if ultraviolet light can damage card or affect its functionality.

Test bench

Ultraviolet generator
PC/SC reader
Micro-ohmmeter and 4 wires resistance measurement test bench
(see chapter 6)

Procedure

Cards are exposed to a monochromatic light (wavelength: 254 nm). First front side is exposed to a total of 0.15 Ws/mm². Then repeat the exposure for backside of cards.

Criteria

Functionality: *samples shall remain testably functional (see chapter 8).*

Results

Sample	Contact functionality	Electrical resistance of contacts
36X217	PASS	PASS
37X217	PASS	PASS
38X217	PASS	PASS

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.661 de 843

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101008852 R.D.

14. Terms and conditions

These Specific Terms and Conditions complement Fime's General Terms and Conditions of Sale and Supply which were provided to, and accepted by the Customer prior to providing the services.

14.1 Disclaimers

This test report contains only information about the tested samples. It is not an endorsement of the entire production of the product.
This test report doesn't constitute an official approval by the test authority.

14.2 Commitment

We certify that the results included in this test report are the precise results of the tests performed on the tested samples.
Tests are performed on a qualified and accepted test bench at the time of test session.

14.3 Intellectual property

Please refer to Fime's General Terms & Conditions of Sale and Supply that were accepted by the Customer when Fime's Commercial Offer was accepted.

Please note that this report may contain references to third party trademarks.

In particular, please note that the COFRAC logo is reproduced on the first page of this report. In accordance with COFRAC's GEN REF 11 Rev8, the COFRAC logo is used only to indicate that this report has been prepared by Fime SAS doing business as Fime EMEA. The Customer acquires rights in any of the trademarks used in this document, and in particular is forbidden to reproduce the COFRAC logo in any document other than an exact copy of this Test Report. Fime is required to report any abusive uses of the COFRAC logo according to the terms of our accreditation. More information is available on the COFRAC website: www.cofrac.fr.

14.4 Storage

The test results are kept 10 years by the testing laboratory.
Samples are managed according to customer's request and/or according to Test Authority's requirement.

14.5 Complaint procedure

The laboratory has a policy and appropriate procedures for the resolution of complaints from customers or other parties. This procedure includes an investigation and corrective actions if the problem is confirmed. An e-mail may be addressed directly to quality service at quality@fime.com. This procedure is available on request.

----------END OF DOCUMENT----------

© 2021 Fime – all rights reserved- CONFIDENTIAL

Página/Folio No.662 de 843

TRADUCCIÓN OFICIAL: Prueba ISO de Durabilidad de la Tarjeta

Yo, **LIC SANTOS C. SIERRA,** Intérprete Judicial del Juzgado de Primera Instancia, debidamente juramentado para el ejercicio de mis funciones **CERTIFICO:** Que he procedido a traducir las partes centrales de un documento, escrito originalmente en Inglés, y cuya versión al Español, según mi mejor conocimiento, es el siguiente:

Informe de Prueba

Objeto del informe
Sesión de prueba de durabilidad de tarjeta ISO (cobertura parcial)

Referencia del informe
C22REP01-612_ISO

Nombre del proveedor SELP ANGOULEME	Nombre y versión del producto PAK National ID Card Engraved Module
Versión del informe V1.0	Fecha de emisión del informe 25/11/2022
Fechas de prueba Del 04/11/2022 al 22/11/2022	Autorizado por:
Número de páginas 37 páginas	Autorizado por Luc Morcel Expert 25/11/2022 16:29+01:00

Las pruebas enumeradas en el Capítulo 4.2 están cubiertas por la acreditación.
La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

Tabla de Contenido

1. Historial de revisiones 4
2. Resumen de resultados de la prueba 4
   2.1. Codificación 4
   2.2. Resumen 5
   2.3. Conclusiones 6
3. Documentos de referencia 6
4. Información del laboratorio 7
   4.1. Identificación del laboratorio de pruebas 7
   4.2 Estado de acreditación 7
   4.3 Personal 7
   4.4 Procedimientos operativos 8
   4.5 Subcontratación 8
   4.6 Condiciones de operación 8
5. Información del cliente y de las muestras 9
   5. Identificación del cliente 9
   5.2 Información de la muestra 9
   5.3 Imagen de la muestra 9
6. Información del equipo de prueba 10
7. Incertidumbres de medición 12
   7.1 Declaración de conformidad 12
8. Métodos de evaluación 13
9. Requisitos de la norma ISO 7810:2019 capítulo 8 14
   9.1 Dimensiones de las tarjetas: grosor 14
   9.2 Dimensiones de las tarjetas: alto y ancho 16
   9.3 Dimensiones de las tarjetas: esquinas 17
   9.4 Rigidez a la flexión 18
   9.5 Resistencia a los productos químicos 19
   9.6 Estabilidad dimensional y deformación de la tarjeta con temperatura y humedad 21
   9.7 Resistencia al pelado 23
   9.8 Adhesión o bloqueo 24
   9.9 Opacidad 25
   9.10 Deformación de la tarjeta 26
   9.11 Resistencia al calor 27

LIC. SANTO C. SIERRA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898852 Santo Domingo, R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.12 Estrés dinámico por flexión 28
10. Requisitos de la norma ISO 7810:2019 capítulo 9 28
10.1 Resistencia eléctrica superficial de los contactos 29
10.2 Resistencia a los productos químicos: niebla salina 30
10.3 Estrés torsional dinámico 32
11. Requisitos de la norma ISO 7816-1 33
11.1 Perfil de superficie de los contactos 33
12. Requisitos de la norma ISO 7816-2 34
12.1 Dimensión y ubicación de los contactos 34
13. Requisitos de versiones anteriores de las normas 36
13.1 Luz ultravioleta 36
14. Términos y condiciones 37
14.1 Descargos de responsabilidad 37
14.2 Compromiso 37
14.3 Propiedad intelectual 37
14.4 Almacenamiento 37
14.5 Procedimiento de queja 37

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg. 1ra Instancia D.N.
SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL, SA
CSI
RNC 101898852
Santo Domingo, R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

1. Historial de revisiones

Fecha	Versión	Autor	Comentario
25/11/2022	1.0	YBR	Versión inicial

2. Resumen de resultados de pruebas

2.1 Codificación

- **APROBADO:** prueba superada
- **FAIL:** prueba fallida
- **N/A:** prueba no aplicable

2.2 Resumen

Prueba	Veredicto
Requisitos del capítulo 8 de la norma ISO 7810	
Dimensiones de las tarjetas: grosor*	Aprobado
Dimensiones de las tarjetas: altura y ancho*	Aprobado
Dimensiones de las tarjetas: esquinas	Aprobado
Rigidez a la flexión	Aprobado
Resistencia a los productos químicos	Aprobado
Estabilidad dimensional de la tarjeta y alabeo con temperatura y humedad*	Aprobado
Resistencia a la peladura	Aprobado
Adhesión o bloqueo	Aprobado
Opacidad	Aprobado
Alabeo de la tarjeta*	Aprobado
Resistencia al calor	Aprobado
Resistencia a la flexión dinámica	Aprobado
Requisitos del capítulo 9 de la norma ISO 7810	
Resistencia superficial eléctrica de los contactos de ICCs con contactos	Aprobado
Resistencia a los productos químicos: niebla salina	Aprobado
Resistencia a la torsión dinámica	Aprobado
Requisitos de la norma ISO 7816-1	
Perfil de la superficie de los contactos de ICCs con contactos*	Aprobado
Requisitos de la norma ISO 7816-2	
Dimensión y ubicación de los contactos de ICCs con contactos	Aprobado
Requisitos de versiones anteriores de las normas	
Luz ultravioleta	Aprobado

* Nota: FIME está acreditado por COFRAC para esta prueba.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

2.3 Conclusión

Los resultados de la sesión de prueba muestran que las muestras probadas cumplen con los requisitos necesarios para
Aprobar el plan de prueba del cliente basado en ISO, como se detalla en este informe.
La regla de decisión aplicada para los resultados de las pruebas se detalla en Incertidumbres de medición. sección.

J.C. SANTO C. SIERRA
Juzgado de Primera Instancia Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

3. Documentos de Referencia

Referencias		Documentos de Referencia
[R1]	ISO/IEC 10373-1:2020	Tarjetas de identificación - Métodos de prueba - Características generales
[R2]	ISO/IEC 10373-2:2015	Tarjetas de identificación - Métodos de prueba - Parte 2: Tarjetas con bandas magnéticas
[R4]	ISO/IEC 10373-6:2016	Métodos de Prueba para Tarjetas de Proximidad
[R20]	ISO/CEI 7810:2019	Tarjetas de identificación - Características físicas
[R21]	ISO/CEI 7811-1:2018	Tarjetas de identificación - Técnica de grabación - Relieve
[R23]	ISO/CEI 7811-6:2014	Tarjetas de identificación - Técnica de grabación - Parte 6: Banda magnética - Alta coercitividad
[R30]	ISO/CEI 7816-1:2011	Tarjetas de identificación - Tarjetas de circuitos integrados - Parte 1: Características físicas
[R31]	ISO/CEI 7816-2:2007	Tarjetas de identificación - Tarjetas de circuitos integrados con contactos - Parte 2: Tarjetas con contactos - Dimensión y ubicación del contacto
[R41]	ISO/IEC 24789-2:2011	Tarjetas de identificación - Vida útil de la tarjeta - Parte 2: Método de Evaluación

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

CSI SOLUTIONS INTERNATIONAL S.A.
RNC. 101898852
Santo Domingo, R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

4. Información del laboratorio

4.1 Identificación del laboratorio de pruebas

Nombre y dirección del laboratorio que realizó las pruebas y emitió este informe:

Fime EMEA
Z.I. de la Folie Couvrechef
8, rue Commodore J.H. Hallet
14000 Caen – Francia
Teléfono: +332 31 44 08 07

4.2 Estado de acreditación

El laboratorio está acreditado por COFRAC Essais para ISO 17025, referencia 1.1709, el alcance está disponible en www.cofrac.fr, cubriendo las pruebas identificadas con un asterisco en la sección de Resumen de Resultados de Pruebas.

4.3 Personal

Las siguientes personas han colaborado en la preparación, ejecución o elaboración de los informes de las pruebas contenidas en este informe:

Examen	
G. Béhue	Técnico de pruebas experimentado
Y. Briard	Técnico de pruebas experimentado
L. Morcel	Experto

Reporte		
Elaborado por	Y. Briard	Técnico de pruebas experimentado
Revisado por	L. Morcel	Experto
Autorizado por	L. Morcel	Experto

4.4 Procedimientos operativos

Los procedimientos internos que se relacionan con la ejecución de las pruebas están disponibles en el Plan de Aseguramiento de la Calidad CARD_DURABILITY. La plantilla utilizada para crear este informe es rep_Generic_Physical_v7.0.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

4.5 Subcontratación

De acuerdo con el presupuesto aceptado por el Cliente, las siguientes pruebas han sido subcontratadas: exposición a la niebla salina.

4.6 Condiciones operativas

Las pruebas se han realizado con las siguientes condiciones externas durante toda la sesión:

Parámetro	Rango requerido
Temperatura	**23°C ± 3°C**
Humedad relativa	40% a 60%

Las condiciones ambientales se registran con termo-higrómetro (continuamente para la sala de pruebas, durante las operaciones para las cámaras de prueba).

La version actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

5. Información del cliente y muestras

5.1 Identificación del cliente

- Nombre de la empresa: SELP ANGOULEME
- Dirección: Rue Louis Pergaud, 16000 Angouleme, Francia
- Contacto: CHAMBRE Sebastien
- Tel: +33545255114
- Correo electrónico: s.chambre@gmail.com

5.2 Información de la muestra

- Nombre del producto: Módulo grabado de la tarjeta de identificación nacional PAK
- Tipo: ICC 6 pines
- Características: logotipos

Las muestras probadas por el Laboratorio de Pruebas se identifican en las siguientes tablas:

Producto	Número de seguimiento	ID interno	Fecha de recepción
Módulo grabado de la tarjeta de identificación nacional PAK	C22STN01-612	1X217 a 70X217	02/11/2022

5.3 Imagen de la muestra

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

6. Información del equipo de prueba

Tipo	Descripción	Información adicional
Estación de medición 3D	Referencia interna: 13/04	Marca: MicroVu
	Verificado el: 04/04/2022	Incertidumbre de ancho: ± 12 µm; Incertidumbre de altura: ± 8 µm; Radio de esquina: ± 40 µm; Eje Z MPE conforme con ± 2.2 µm +(5L/1000)
Banco de medición de resistencia a 4 hilos	Referencia interna: 49/01	Marca: FIME
	Verificado el: 04/07/2022	Tolerancia para la fuerza aplicada: conforme con una MPE de ± 0.1 N; Tolerancia para ubicaciones de contactos: conforme con el patrón 14/03
Banco de rigidez a la flexión	Referencia interna: 52/04	Verificado el: 28/01/2022
Máquina de estrés de flexión	Referencia interna: 40/07 & 07B	Marca: BGI; Modelo o tipo: BGI110A
	Verificado el: 04/03/2022	Tolerancia para la deflexión: conforme con una MPE de ± 1mm; Tolerancia para la frecuencia: conforme con una MPE de ± 0.025Hz
Calibrador	Referencia interna: 20/01	Marca: Mitutoyo
	Verificado el: 23/02/2022	Incertidumbre: ± 0.03 mm
Cronómetro	Referencia interna: 60/01	Marca: TIM
	Verificado el: 01/07/2022	Incertidumbre: ± 1 s (en 60 s)
Cámara climática	Referencia interna: C02/05	Marca: Vöstch; Modelo o tipo: VC3 4018
	Verificado el: 11/05/2022	Tolerancia para la temperatura: conforme con una MPE de 3°C; Tolerancia para la humedad: conforme con una MPE de 5%
Comparador	Referencia interna: 18/01	Marca: Mitutoyo
	Verificado el: 03/12/2021	Incertidumbre: ± 16 µm (ISO/CQM); ± 7 µm (CB)
Bloque de referencia de contactos	Referencia interna: 14/03	Marca: FIME
	Verificado el: 13/09/2021	Tolerancia: conforme con una MPE de ± 10 µm
Herramienta de corte	Referencia interna: 41/12	Marca: Elcometer
	Verificado el: 10/11/2021	
Herramienta de corte de doble disco	Referencia interna: 22/39	Marca: Noviprofibre; Modelo o tipo: N1310
	Verificado el: 10/11/2021	Tolerancia para el ancho de la muestra: conforme con una MPE de ± 0.1 mm
Sensor de fuerza	Referencia interna: 55/04	Marca: Mecmesin; Modelo o tipo: ELS-S 250 N
	Verificado el: 19/01/2022	Incertidumbre: ± 0.22 N @ 3.5 N
Placa de superficie de granito	Referencia interna: 21/03	Verificado el: 30/06/2022
	Tolerancia para la rugosidad: conforme con una MPE < 3.2 µm	
Medidor de altura	Referencia interna: 22/38	Marca: Linear tool
	Verificado el: 18/03/2022	Incertidumbre: ± 0.33 mm (rigidez); Incertidumbre: ± 0.68 mm (resistencia al calor)
Soporte para ICC	Referencia interna: 52/05	Marca: BGI
Carga	Referencia interna: 22/11 a 22/15	Modelo o tipo: 2.2 N
	Verificado el: 22/01/2021	Tolerancia: conforme con una MPE de 0.11 N
Carga	Referencia interna: 22/29	Modelo o tipo: 23.1 N
	Verificado el: 23/02/2022	Tolerancia: conforme con una MPE de 1.2 N
Micrómetro	Referencia interna: 19/10	Marca: Mitutoyo; Modelo o tipo: Digital 0-25 mm
	Verificado el: 03/12/2021	Incertidumbre: ± 5 µm (espesor)
Micro-ohmímetro	Referencia interna: C28/30	Marca: Keysight; Modelo o tipo: 34420A
	Verificado el: 30/06/2022	Incertidumbre: ± 6 mOhm
Multímetro	Referencia interna: 07/02	Marca: Agilent; Modelo o tipo: 34401A
	Verificado el: 29/03/2022	Incertidumbre: ± 10 mOhm
Probador de opacidad	Referencia interna: 41/04	Marca: Q-Card; Modelo o tipo: 905703-2
	Verificado antes de su uso	Incertidumbre: ± 0.9% a 860 nm; ± 0.8% a 950 nm

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.
CSI SOLUTIONS INTERNATIONAL S.A.
CSI
RNC 1-31-01898852
Santo Domingo, R.D.

Patrón para la ubicación de contactos	Marca: FIME	Usado con el bloque de referencia de contactos
Lector PC/SC	Referencia interna: C36/106	Marca: FIME / Identive; Modelo o tipo: SDI 011 con conector de aterrizaje
Proyector de perfil	Referencia interna: 13/02	Marca: Nikkon; Modelo o tipo: V-12
	Verificado el: 01/07/2022	Magnificación: conforme con una MPE de 1 (relación); Incertidumbre: ± 80 µm (deformación); ± 3 µm (borde)
Software: Adquisición y tratamiento de espesor	Nombre del software: Thickness; Marca: FIME	Versión del software: v1.06
Software: Interfaz del lector PC/SC	Nombre del software: ATR reader; Marca: FIME	Versión del software: v1.5
Software: Tratamiento de datos en bruto del sensor de fuerza	Nombre del software: LBC; Marca: FIME	Versión del software: v2.37
Software: Adquisición de resistencia	Nombre del software: Ohmmeter; Marca: FIME	Versión del software: v2.1
Software: Adquisición y tratamiento de la deformación	Nombre del software: Profile; Marca: FIME	Versión del software: v1.9
Termo-higrómetro (sala de pruebas)	Referencia interna: C09/33	Marca: ELPRO; Modelo o tipo: Ecolog TH2
	Verificado el: 16/06/2022	Incertidumbre: ± 0,3 °C; ± 2 %
Termo-higrómetro (cámara de pruebas)	Referencia interna: C09/09	Marca: ELPRO; Modelo o tipo: Ecolog TH2
	Verificado el: 11/07/2022	Incertidumbre: ± 1 °C
Termo-higrómetro (cámara de pruebas)	Referencia interna: C09/11	Marca: ELPRO; Modelo o tipo: Ecolog TH2
	Verificado el: 30/05/2022	Incertidumbre: ± 1 °C; ± 12 %
Termo-higrómetro (cámara de pruebas)	Referencia interna: C09/18	Marca: ELPRO; Modelo o tipo: Ecolog TH2
	Verificado el: 09/02/2022	Incertidumbre: ± 1 °C; ± 3 %
Máquina de estrés torsional	Referencia interna: 40/07 & 40/07A	Marca: BGI; Modelo o tipo: BGI110A
	Verificado el: 25/02/2022	Tolerancia para el ángulo: conforme con una MPE de ± 1.5°; Tolerancia para la frecuencia: conforme con una MPE de ± 0.025Hz
Banco de pruebas de tracción	Referencia interna: C25/05	Marca: Mecmesin; Modelo o tipo: Multitest 2.5 dV
	Verificado el: 14/09/2022	Tolerancia para la velocidad: conforme con una MPE de ± 10 mm/min
Generador de UV	Referencia interna: 36/02	Marca: LEAP ELECTRONIC; Modelo o tipo: EPROM ERASER LER-123A

7. Incertidumbres de las mediciones

7.1 Declaración de cumplimiento

En este informe, las incertidumbres se dan a un nivel de confianza de k = 2. Para declarar el cumplimiento, no se han considerado las incertidumbres de medición. Las declaraciones establecidas sobre mediciones incluidas en el área de incertidumbre se identifican con un asterisco.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

8. Métodos de evaluación

Siempre que el método de prueba requiera que una muestra permanezca 'funcionalmente probada', se realizan las siguientes evaluaciones cuando sea aplicable (dependiendo de las funcionalidades presentes):

- Para productos de contacto y duales: detección de un ATR utilizando un lector PC/SC; conformidad con la resistencia eléctrica de la superficie de los contactos ([R1] §6.7 (criterios en [R20] §9.6).
- Para productos sin contacto y duales: detección de una solicitud de comando WAKEUP utilizando un lector PC/SC ([R4]); las frecuencias de resonancia (en MHz) antes y después de las pruebas se indican solo para información.
- Para productos con banda magnética: las características dinámicas deben seguir siendo conformes con [R23] §7.3. Para la prueba de resistencia a productos químicos y al desgaste, la banda magnética se codifica primero y se mide la amplitud de la señal. Después de la exposición, se vuelve a medir la amplitud de la señal y se compara con el valor inicial según los criterios de [R23] §6.4 & §6.5.

El criterio de aspecto se cumple cuando los siguientes defectos están ausentes después de la prueba:

- Grietas (grietas que atraviesan el material, visibles en ambos lados de la tarjeta. Las grietas superficiales no se consideran).
- Delaminación de capas (sobrecapa o capas internas).
- Desprendimiento del módulo del cuerpo de la tarjeta.
- Decoloración y transferencia de tinte que impide el uso esperado (impresiones o imágenes descoloridas).
- Deterioro de las características de seguridad (a menos que se especifique lo contrario).
- Cualquier otro daño que deteriore la funcionalidad de la tarjeta o la información.

Estas evaluaciones también se realizan antes de las pruebas, para garantizar que las muestras estaban intactas antes de las tensiones.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9. Requisitos de ISO 7810:2019 capítulo 8

9.1 Dimensiones de las tarjetas: espesor

Referencia

Basado en [R1] §5.2.2 (criterios en [R20] §5.2). El propósito de esta prueba es medir el espesor de una tarjeta.

Banco de pruebas

Micrómetro (ver capítulo 6) Software de adquisición

Procedimiento

Utilice el micrómetro para medir el espesor de la tarjeta en prueba. El espesor se mide en cuatro ubicaciones. La medición puede realizarse en cualquier lugar de un cuadrante, excepto en los contactos del chip, panel de firma, banda magnética o cualquier otra área elevada.

Criterios

Espesor: [680 µm – 840 µm]

Resultados

Valores en la tabla a continuación en µm.

Muestra	Espesor Q1	Espesor Q2	Espesor Q3	Espesor Q4	Veredicto
1X217	773	772(m)	776	785(M)	Aprobado
2X217	775	778	773(m)	791(M)	Aprobado
3X217	776	775	774(m)	786(M)	Aprobado
4X217	772(m)	773	773	776(M)	Aprobado
5X217	775	775	776(M)	773(m)	Aprobado

(m) significa valor mínimo y (M) valor máximo

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.2 Dimensiones de las tarjetas: altura y ancho

Referencia

Basado en [R1] §5.2.3 (criterios en [R20] §5.2). El propósito de esta prueba es verificar el tamaño de la tarjeta y su paralelismo.

Banco de pruebas

Estación de medición 3D y software (ver capítulo 6) Carga Procesamiento de datos (LBC)

Procedimiento

Coloque las tarjetas probadas en el soporte de la estación. Luego use el software de la estación de medición 3D (programa ISO) para determinar el tamaño de los rectángulos interior y exterior. Luego determine la conformidad de la tarjeta.

Criterios

Rectángulo interior (altura x ancho): 53.920 mm x 85.470 mm Rectángulo exterior (altura x ancho): 54.030 mm x 85.720 mm

Resultados

Muestra	Altura x Ancho del rectángulo interior	Altura x Ancho del rectángulo exterior	Veredicto
1X217	53.973 mm x 85.594 mm	53.990 mm x 85.610 mm	Aprobado
2X217	53.967 mm x 85.594 mm	54.012 mm x 85.607 mm	Aprobado
3X217	53.971 mm x 85.601 mm	54.002 mm x 85.611 mm	Aprobado
4X217	53.960 mm x 85.600 mm	54.007 mm x 85.613 mm	Aprobado
5X217	53.968 mm x 85.597 mm	54.000 mm x 85.610 mm	Aprobado

LIC. SANTO C. SIERRA Interprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101698852 Santo Domingo, R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.3 Dimensiones de las tarjetas: esquinas

Referencia

Basado en [R1] §5.2.3 (criterios en [R20] §5.1.1). El propósito de esta prueba es verificar el radio de las esquinas de la tarjeta.

Banco de pruebas

Estación de medición 3D y software (ver capítulo 6) Carga

Procedimiento

Coloque las tarjetas probadas en el soporte de la estación. Luego inicie el programa de la estación de medición 3D para la medición de las esquinas.

Criterios

Radio: [2.88 mm – 3.48 mm]

Resultados

Muestra	Esquina superior izquierda	Esquina superior derecha	Esquina inferior izquierda	Esquina inferior derecha	Veredicto
1X217	3.194	3.260	3.192	3.049	Aprobado
2X217	3.121	3.320	3.170	3.229	Aprobado
3X217	3.278	3.273	3.170	3.217	Aprobado
4X217	3.151	3.158	3.191	3.183	Aprobado
5X217	3.179	3.177	3.201	3.259	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.4 Rigidez a la flexión

Referencia

Basado en [R1] §5.8 (criterios en [R20] §8.1). El propósito de esta prueba es determinar si la rigidez a la flexión de la tarjeta cumple con el requisito de la norma.

Banco de pruebas

Banco de rigidez a la flexión Medidor de altura (ver capítulo 6)

Procedimiento

Sujete una tarjeta a lo largo de su lado izquierdo, con el lado frontal hacia arriba. Mueva la sonda del medidor de altura al nivel del lado derecho de la tarjeta y restablezca. Aplique la carga en el lado derecho de la tarjeta y espere 1 minuto. Usando el medidor de altura, mida la deflexión del lado derecho. Retire la carga y espere 1 minuto. Usando el medidor de altura, mida la deformación residual.

Criterios

Deflexión: [13 mm – 35 mm] Deformación: [-1.5 mm – 1.5 mm]

Resultados

Muestra	Deflexión (mm)	Deformación (mm)	Veredicto
41X217	19.16	-0.09	Aprobado
42X217	19.27	-0.20	Aprobado
43X217	19.26	-0.11	Aprobado
44X217	19.14	-0.27	Aprobado
45X217	20.99	-0.05	Aprobado

Nota: El valor h1 del método de prueba se establece arbitrariamente en 0 mm, antes de la aplicación de la carga. Por lo tanto, h2 es la deflexión y h3 es la deformación (ver [R1] §5.7).

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.5 Resistencia a productos químicos

Referencia

Basado en [R1] §5.5 (criterios en [R20] §8.3). El propósito de esta prueba es determinar si los productos químicos comunes pueden dañar la tarjeta o afectar su funcionalidad.

Banco de pruebas

Herramientas para mediciones de dimensiones (deformación, espesor y altura & ancho)
Cronómetro
Lector PC/SC
Micro-ohmímetro y banco de medición de resistencia a 4 hilos (ver capítulo 6)

Procedimiento

Realice todas las mediciones y pruebas necesarias antes de la exposición según las características de la tarjeta. Seleccione una muestra para cada solución. Exponer la muestra a su solución asociada durante la duración requerida (1 min para exposición a corto plazo y 24 horas para exposición a largo plazo). Después de la eliminación de la solución, enjuague la tarjeta y séquela con un tejido absorbente. Luego, vuelva a las condiciones ambientales predeterminadas durante 24 horas. Realice todas las mediciones y pruebas necesarias 'después de la exposición' según las características de la tarjeta.

Solución	Codigo	Tipo
Cloruro de sodio	a	Corto Plazo
Ácido acético	b	Corto Plazo
Carbonato de sodio	c	Corto Plazo
Alcohol etílico	d	Corto Plazo
Sacarosa	e	Corto Plazo
Combustible B (ISO 1817)	f	Corto Plazo
Etilenglicol	g	Corto Plazo
Transpiración artificial alcalina	h	Largo Plazo
Transpiración artificial ácida	i	Largo Plazo

Criterios

Dimensiones: conformidad con los criterios de deformación, espesor y altura & ancho. Funcionalidad: las muestras deben permanecer funcionalmente probadas (ver capítulo 8). Aspecto: el examen visual no debe revelar ningún defecto.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.5 Resistencia a productos químicos

Referencia

Basado en [R1] §5.5 (criterios en [R20] §8.3). El propósito de esta prueba es determinar si los productos químicos comunes pueden dañar la tarjeta o afectar su funcionalidad.

Banco de pruebas

Herramientas para mediciones de dimensiones (deformación, espesor y altura & ancho)
Cronómetro
Lector PC/SC
Micro-ohmímetro y banco de medición de resistencia a 4 hilos (ver capítulo 6)

Procedimiento

Realice todas las mediciones y pruebas necesarias antes de la exposición según las características de la tarjeta. Seleccione una muestra para cada solución. Exponer la muestra a su solución asociada durante la duración requerida (1 min para exposición a corto plazo y 24 horas para exposición a largo plazo). Después de la eliminación de la solución, enjuague la tarjeta y séquela con un tejido absorbente. Luego, vuelva a las condiciones ambientales predeterminadas durante 24 horas. Realice todas las mediciones y pruebas necesarias 'después de la exposición' según las características de la tarjeta.

Solución	Código	Tipo
Cloruro de sodio	a	Corto Plazo
Ácido acético	b	Corto Plazo
Carbonato de sodio	c	Corto Plazo
Alcohol etílico	d	Corto Plazo
Sacarosa	e	Corto Plazo
Combustible B (ISO 1817)	f	Corto Plazo
Etilenglicol	g	Corto Plazo
Transpiración artificial alcalina	h	Largo Plazo
Transpiración artificial ácida	i	Largo Plazo

Criterios

Dimensiones: conformidad con los criterios de deformación, espesor y altura & ancho. Funcionalidad: las muestras deben permanecer funcionalmente probadas (ver capítulo 8). Aspecto: el examen visual no debe revelar ningún defecto.

La versión actual completa y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

Resultados

Dimensiones:

Muestra	Código	Espesor	Altura y Anchura	Combeo
6X217	a	Aprobado	Aprobado	Aprobado
7X217	b	Aprobado	Aprobado	Aprobado
8X217	c	Aprobado	Aprobado	Aprobado
9X217	d	Aprobado	Aprobado	Aprobado
10X217	e	Aprobado	Aprobado	Aprobado
11X217	f	Aprobado	Aprobado	Aprobado
12X217	g	Aprobado	Aprobado	Aprobado
13X217	h	Aprobado	Aprobado	Aprobado
14X217	i	Aprobado	Aprobado	Aprobado

Funcionalidad y aspecto:

Muestra	Código	Aspecto	Func. de contacto	Resistencia electrica de los contactos
6X217	a	Aprobado	Aprobado	Aprobado
7X217	b	Aprobado	Aprobado	Aprobado
8X217	c	Aprobado	Aprobado	Aprobado
9X217	d	Aprobado	Aprobado	Aprobado
10X217	e	Aprobado	Aprobado	Aprobado
11X217	f	Aprobado	Aprobado	Aprobado
12X217	g	Aprobado	Aprobado	Aprobado
13X217	h	Aprobado	Aprobado	Aprobado
14X217	i	Aprobado	Aprobado	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.6 Estabilidad dimensional de la tarjeta y deformación con temperatura y humedad

Referencia

Basado en [R1] §5.6 (criterios en [R20] §8.4). El propósito de esta prueba es verificar que las dimensiones y la deformación de las tarjetas permanezcan dentro de los requisitos estándar después de exposiciones a las condiciones detalladas a continuación.

Banco de pruebas

Herramientas para mediciones de dimensiones (deformación, espesor y altura & ancho) Cámara climática (ver capítulo 6)

Procedimiento

Mida el espesor, altura, ancho y deformación de las tarjetas antes de las exposiciones (t0). Coloque las muestras en una superficie plana horizontal y expóngalas a las condiciones climáticas a continuación durante 60 minutos:

- t1: -35°C
- t2: +50°C / 95% HR

Después de cada secuencia, devuelva las muestras a las condiciones ambientales predeterminadas durante 24 horas antes de realizar las mediciones de dimensiones y deformación. Evalúe las dimensiones en t1 (después de la exposición al frío) y t2 (después de la exposición al calor húmedo).

Criterios

Espesor:	[680 µm – 840 µm]
Rectángulo interior (altura x ancho):	53.920 mm x 85.470 mm
Rectángulo exterior (altura x ancho):	54.030 mm x 85.720 mm
Deformación:	inferior a 1.5 mm

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Esta información debe ser reproducida o comunicada excepto en su última versión completa sin modificar.

Resultados

Muestra	Rectángulo interior @ t0 altura (mm) X ancho (mm)	Rectángulo exterior @ t0 altura (mm) X ancho (mm)	Veredicto
1X217	53.973 mm x 85.594 mm	53.990 mm x 85.610 mm	Aprobado
2X217	53.967 mm x 85.594 mm	54.012 mm x 85.607 mm	Aprobado
3X217	53.971 mm x 85.601 mm	54.002 mm x 85.611 mm	Aprobado
4X217	53.960 mm x 85.600 mm	54.007 mm x 85.613 mm	Aprobado
5X217	53.968 mm x 85.597 mm	54.000 mm x 85.610 mm	Aprobado

Muestra	Rectángulo interior @ t1 altura (mm) X ancho (mm)	Rectángulo exterior @ t1 altura (mm) X ancho (mm)	Veredicto
1X217	53.967 mm x 85.592 mm	53.995 mm x 85.609 mm	Aprobado
2X217	53.960 mm x 85.592 mm	54.002 mm x 85.607 mm	Aprobado
3X217	53.969 mm x 85.598 mm	54.014 mm x 85.614 mm	Aprobado
4X217	53.961 mm x 85.603 mm	53.999 mm x 85.611 mm	Aprobado
5X217	53.971 mm x 85.595 mm	54.002 mm x 85.610 mm	Aprobado

Muestra	Rectángulo interior @ t2 altura (mm) X ancho (mm)	Rectángulo exterior @ t2 altura (mm) X ancho (mm)	Veredicto
1X217	53.958 mm x 85.580 mm	53.985 mm x 85.596 mm	Aprobado
2X217	53.954 mm x 85.581 mm	54.007 mm x 85.597 mm	Aprobado
3X217	53.964 mm x 85.590 mm	54.006 mm x 85.605 mm	Aprobado
4X217	53.953 mm x 85.591 mm	53.989 mm x 85.605 mm	Aprobado
5X217	53.962 mm x 85.588 mm	53.993 mm x 85.599 mm	Aprobado

Muestra	Espesor @ t0 (µm)	Veredicto	Espesor @ t1 (µm)	Veredicto	Espesor @ t2 (µm)	Veredicto
1X217	785	Aprobado	791	Aprobado	796	Aprobado
2X217	791	Aprobado	790	Aprobado	793	Aprobado
3X217	786	Aprobado	794	Aprobado	797	Aprobado
4X217	776	Aprobado	796	Aprobado	799	Aprobado
5X217	776	Aprobado	793	Aprobado	794	Aprobado

Muestra	Alabeo @ t0 (mm)	Veredicto	Alabeo @ t1 (mm)	Veredicto	Alabeo @ t2 (mm)	Veredicto
1X217	0.845	Aprobado	0.845	APROBADO	0.877	Aprobado
2X217	0.856	Aprobado	0.856	APROBADO	0.846	Aprobado
3X217	0.871	Aprobado	0.860	APROBADO	0.837	Aprobado
4X217	0.855	Aprobado	0.859	APROBADO	0.838	Aprobado
5X217	0.818	Aprobado	0.813	APROBADO	0.789	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.7 Resistencia a la delaminación

Referencia

Basado en [R1] §5.3 & §5.4 (criterios en [R20] §8.7). El propósito de esta prueba es medir la fuerza de despegue entre las capas del cuerpo de la tarjeta.

Banco de pruebas

Herramienta de corte de doble disco Banco de pruebas de tracción Dinamómetro y sensor de fuerza Software de tratamiento de datos (ver capítulo 6)

Procedimiento

Corte la tarjeta para hacer secciones de 10 mm de ancho (± 0.2 mm). Usando un cuchillo afilado, corte la capa a probar del núcleo en aproximadamente 10 mm de largo, insértela entre los rodillos y fíjela al sensor de fuerza. Péguelas en una placa estabilizadora si las secciones son demasiado flexibles y/o para medir la fuerza de despegue en el borde de la tarjeta. Para la medición en el borde, agregue un espaciador del mismo grosor que la muestra de prueba. Inicie la prueba de despegue a 300 mm/min, observando si hay desgarro o ruptura. Analice la traza, excluyendo los primeros y últimos 5 mm del registro, para encontrar el punto más bajo (los picos negativos que tienen una longitud inferior a 1 mm en el nivel de criterio se ignoran).

Criterios

Fuerza de despegue (capa de la tarjeta): ≥ 3.5 N

Resultados

Muestra	Interfaz de la banda	Fuerza mínima (N)	Comentario	Veredicto
54X217	A Frontal	-	Preparación de la muestra no posible*	Aprobado
54X217	B Posterior	-	Preparación de la muestra no posible*	Aprobado
55X217	A Frontal	-	Preparación de la muestra no posible*	Aprobado
55X217	B Posterior	-	Preparación de la muestra no posible*	Aprobado
56X217	A Frontal	-	Preparación de la muestra no posible*	Aprobado
56X217	B Posterior	-	Preparación de la muestra no posible*	Aprobado

*: en tal caso, [R20] §8.7 establece que este comportamiento se considera automáticamente aceptable.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.8 Adhesión o bloqueo

Referencia

Basado en [R1] §5.7 (criterios en [R20] §8.8). El propósito de esta prueba es determinar cualquier efecto negativo del apilamiento de tarjetas no grabadas.

Banco de pruebas

Cámara climática Calibrador Carga (ver capítulo 6)

Procedimiento

Haga una pila de cinco tarjetas probadas (todas las tarjetas deben tener los lados posteriores hacia abajo). Prepare otra pila con cinco tarjetas de prueba. Use la carga para generar la presión especificada. Exponer el conjunto al ambiente de prueba (40°C / 50% HR) durante 48 horas. Luego devuelva las tarjetas al ambiente predeterminado.

Criterios

Adhesión: las tarjetas deben separarse fácilmente de manera manual. Aspecto: el examen visual no debe revelar ningún defecto.

Resultados

Muestra	Exposición carga	Aspecto
49X217	Aprobado	Aprobado
50X217	Aprobado	Aprobado
51X217	Aprobado	Aprobado
52X217	Aprobado	Aprobado
53X217	Aprobado	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.9 Opacidad

Referencia

Basado en [R1] §5.11 (criterios en [R20] §8.9). El propósito de esta prueba es determinar la opacidad del cuerpo de la tarjeta en las longitudes de onda de 860 nm y 950 nm.

Banco de pruebas

Probador de opacidad (ver capítulo 6) Pantallas de referencia negras y ORM 7810

Procedimiento

Seleccione la longitud de onda de 860 nm y permita que el probador se caliente. Verifique que el valor de la pantalla de referencia negra sea 0. Registre el valor medido para la pantalla de referencia ORM 7810. La tarjeta se escanea para encontrar la ubicación que muestra el valor de opacidad más bajo (que coincide con el valor máximo del porcentaje devuelto por el probador de opacidad). La ubicación de la opacidad más baja puede estar en cualquier parte de la tarjeta, excepto en las áreas 'c' y 'd', como se muestra en el diagrama. Repita con la longitud de onda de 950 nm.

Criterios

El valor máximo del porcentaje medido en la tarjeta probada debe ser inferior al valor medido en la pantalla de referencia ORM 7810 (para ambas longitudes de onda).

Resultados

Muestra	860 nm	950 nm	Veredicto
Pantalla de referencia negra	0	0	-
Pantalla de referencia ORM 7810	3.7	3.6	-
46X217	0.1@ (15, 15)	0.1@ (15, 40)	Aprobado
46X217	0.1@ (45, 15)	0.1@ (45, 40)	Aprobado
47X217	0.1@ (70, 15)	0.1@ (70, 40)	Aprobado
47X217	0.1@ (15, 15)	0.1@ (15, 40)	Aprobado
48X217	0.1@ (45, 15)	0.1@ (45, 40)	Aprobado
48X217	0.1@ (70, 15)	0.1@ (70, 40)	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.10 Deformación de la tarjeta

Referencia

Basado en [R1] §5.1 (criterios en [R20] §8.10). El propósito de esta prueba es medir la deformación de una tarjeta.

Banco de pruebas

Proyector de perfil (ver capítulo 6) Soporte de muestras Software de adquisición

Procedimiento

Coloque el soporte de muestras en el proyector de perfil. Coloque la tarjeta en prueba en el soporte de muestras. Mueva al punto más bajo de la tarjeta y restablezca el micrómetro. Encuentre el punto más alejado en el lado opuesto de la tarjeta y mida la distancia de altura desde el punto más bajo.

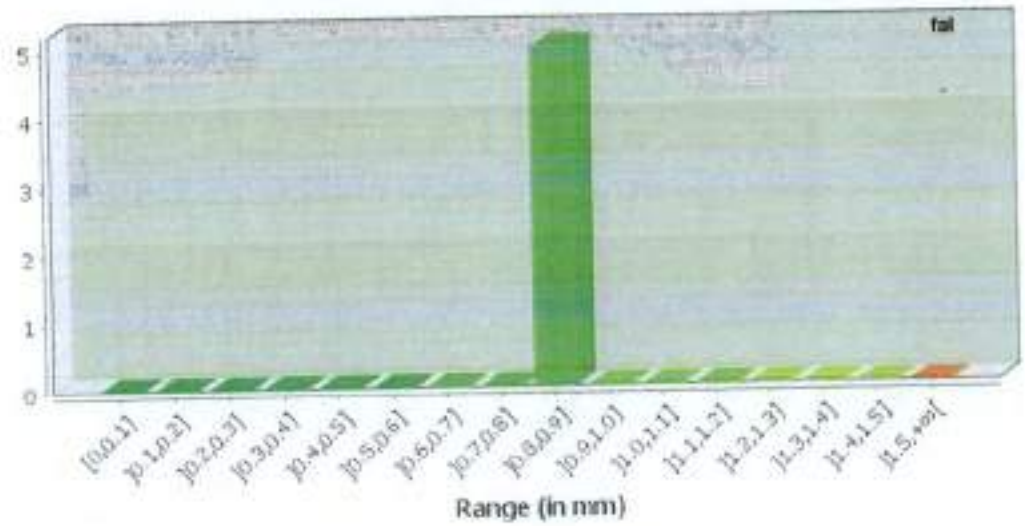
Criterios

Deformación: inferior a 1.5 mm.

Resultados

Muestra	Deformación (mm)	Veredicto
1X217	0.845	Aprobado
2X217	0.856	Aprobado
3X217	0.871	Aprobado
4X217	0.855	Aprobado
5X217	0.818	Aprobado

DIMENSIÓN DE LA TARJETA deformación



La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.11 Resistencia al calor

Referencia

Basado en [R1] §5.14 (criterios en [R20] §8.12). El propósito de esta prueba es determinar si una exposición a alta temperatura afecta la rigidez de las tarjetas.

Banco de pruebas

Banco de rigidez a la flexión Medidor de altura Cámara climática Placa de superficie de granito (ver capítulo 6)

Procedimiento

Sujete las tarjetas a lo largo de sus lados derechos, con el lado frontal hacia arriba (la ubicación de los contactos debe estar opuesta al dispositivo de sujeción). Baje la sonda del medidor de altura hasta la placa de superficie de granito y restablezca. Mueva la sonda del medidor de altura al nivel del lado izquierdo de cada tarjeta y registre la altura medida. Exponer las tarjetas a una temperatura de 50°C durante 4 horas. Devuelva las tarjetas al ambiente predeterminado y espere al menos media hora. Usando el medidor de altura, mida la deformación residual de cada tarjeta.

Criterios

Deformación: < 10 mm

Resultados

Muestra	Orientación	Deformación (mm)	Veredicto
59X217	Lado frontal arriba	0.32	Aprobado
60X217	Lado frontal arriba	0.20	Aprobado
61X217	Lado frontal arriba	0.31	Aprobado
62X217	Lado posterior arriba	0.09	Aprobado
63X217	Lado posterior arriba	0.09	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

9.12 Estrés de flexión dinámica

Referencia

Basado en [R1] §5.9 (criterios en [R20] §8.14). El propósito de esta prueba es determinar si el estrés de flexión puede dañar la tarjeta o afectar su funcionalidad.

Banco de pruebas

Máquina de estrés de flexión Lector PC/SC Micro-ohmímetro y banco de medición de resistencia a 4 hilos (ver capítulo 6)

Procedimiento

Las tarjetas se doblan 1000 veces, siguiendo estos pasos:

- La máquina se configura para doblar la tarjeta por la curvatura de los lados largos.
- Coloque las tarjetas con el lado frontal hacia arriba. Ejecute 250 ciclos a 0.5 Hz.
- Reposicione las tarjetas con el lado posterior hacia arriba y ejecute 250 ciclos a 0.5 Hz.
- Configure la máquina para doblar la tarjeta por la curvatura de los lados cortos.
- Coloque las tarjetas con el lado frontal hacia arriba. Ejecute 250 ciclos a 0.5 Hz.
- Reposicione las tarjetas con el lado posterior hacia arriba y ejecute 250 ciclos a 0.5 Hz.

Criterios

Funcionalidad: las muestras deben permanecer funcionalmente probadas (ver capítulo 8). Aspecto: el examen visual no debe revelar ninguna parte agrietada.

Resultados

Muestra	Aspecto	Funcionalidad del contacto (ATR)	Resistencia eléctrica de los contactos
18X217	Aprobado	Aprobado	Aprobado
19X217	Aprobado	Aprobado	Aprobado
20X217	Aprobado	Aprobado	Aprobado
21X217	Aprobado	Aprobado	Aprobado
22X217	Aprobado	Aprobado	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

10. Requisitos de ISO 7810:2019 capítulo 9

10.1 Resistencia eléctrica de la superficie de los contactos

Referencia

Basado en [R1] §6.7 (criterios en [R20] §9.6). El propósito de esta prueba es determinar si las resistencias eléctricas de la superficie de los contactos cumplen con los requisitos estándar.

Banco de pruebas

Micro-ohmímetro Banco de medición de resistencia a 4 hilos Software de adquisición de resistencia (ver capítulo 6)

Procedimiento

Usando el banco de medición de resistencia a 4 hilos, coloque las dos sondas en el primer contacto. El micro-ohmímetro realiza la medición y la envía al software de adquisición. Continúe con los otros contactos y otras muestras.

Criterios

Resistencia eléctrica de la superficie: ≤ 500 mΩ

Resultados

Muestra	C1	C2	C3	C4	C5	C6	C7	C8	Veredicto
6X217	39mΩ	39mΩ	40mΩ	N/A	39mΩ	39mΩ	40mΩ	N/A	Aprobado
7X217	40mΩ	39mΩ	39mΩ	N/A	39mΩ	39mΩ	39mΩ	N/A	Aprobado
8X217	39mΩ	39mΩ	39mΩ	N/A	38mΩ	38mΩ	39mΩ	N/A	Aprobado

LIC. SANTO C. SIERRA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.
COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 101898852 Santo Domingo, R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

10.2 Resistencia a productos químicos: niebla salina

Referencia

Basado en [R1] §5.5 y ISO 9227 (criterios en [R20] §9.8). El propósito de esta prueba es determinar si los productos químicos comunes pueden dañar la tarjeta o afectar su funcionalidad.

Banco de pruebas

Cámara de niebla salina (equipos del subcontratista) Lector PC/SC Micro-ohmímetro y banco de medición de resistencia a 4 hilos (ver capítulo 6)

Procedimiento

Exponer las tarjetas a un ambiente de niebla salina. Los parámetros de la cámara de prueba deben establecerse en los siguientes valores:

- Concentración de cloruro de sodio: 50 ± 5 g/L
- Densidad de la solución: $1029 < \rho\ (kg/m^3) < 1036$
- pH de la solución salina: $6.5 < pH < 7.2$

La exposición dura 24 horas. Después de la exposición, los parámetros de prueba son:

- pH de la solución: 7.1
- Densidad de la solución: $\rho = 1034\ kg/m^3$
- Presión: 1.0 bar
- Temperatura: 35°C

Después de la exposición, las tarjetas se enjuagan y se secan con un tejido absorbente. Luego, se devuelven al ambiente predeterminado durante 24 horas.

Criterios

Dimensiones: conformidad con los criterios de deformación, espesor y altura & ancho.
Funcionalidad: las muestras deben permanecer funcionalmente probadas (ver capítulo 8). Aspecto: el examen visual no debe revelar ningún defecto.

Nota: La exposición a la niebla salina es subcontratada.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

Resultados

Dimensiones:

Muestra	Espesor	Altura y Anchura	Alabeo
15X217	Aprobado	Aprobado	Aprobado
16X217	Aprobado	Aprobado	Aprobado
17X217	Aprobado	Aprobado	Aprobado

Funcionalidad y aspecto:

Muestra	Aspecto	Funcionalidad de contacto	Resistencia eléctrica de contacto
15X217	Aprobado	Aprobado	Aprobado
16X217	Aprobado	Aprobado	Aprobado
17X217	Aprobado	Aprobado	Aprobado

LIC. SANTO C. SIERRA
Interprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC. 101698652
Santo Domingo, R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

10.3 Estrés torsional dinámico

Referencia

Basado en [R1] §5.10 (criterios en [R20] §9.11). El propósito de esta prueba es determinar si el estrés torsional puede dañar la tarjeta o afectar su funcionalidad.

Banco de pruebas

Máquina de estrés torsional Lector PC/SC Micro-ohmímetro y banco de medición de resistencia a 4 hilos (ver capítulo 6)

Procedimiento

Las tarjetas se retuercen 1000 veces con un ángulo de 2x 15° y una frecuencia de 0.5 Hz.

Criterios

Funcionalidad: las muestras deben permanecer funcionalmente probadas (ver capítulo 8). Aspecto: el examen visual no debe revelar ninguna parte agrietada.

Resultados

Muestra	Aspecto	Funcionalidad del contacto	Resistencia eléctrica de los contactos
23X217	Aprobado	Aprobado	Aprobado
24X217	Aprobado	Aprobado	Aprobado
25X217	Aprobado	Aprobado	Aprobado
26X217	Aprobado	Aprobado	Aprobado
27X217	Aprobado	Aprobado	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

11. Requisitos de ISO 7816-1

11.1 Perfil de la superficie de los contactos

Referencia

Basado en [R1] §6.9 (criterios en [R30] §4.2). El propósito de esta prueba es medir la altura de cada contacto, utilizando la superficie frontal de la tarjeta como referencia.

Banco de pruebas

Comparador (ver capítulo 6)

Procedimiento

Visualice una línea que cruce el primer par de contactos (C1 y C5) en su centro. El inicio y el final de esta línea están a 2 mm de la superficie metalizada. Mida la altura de los puntos de inicio y final. El grosor base es el promedio de estos dos valores. A lo largo de la línea de medición, mida las alturas de C1 y C5. Calcule la diferencia entre las alturas y el grosor base. Proceda de la misma manera con los otros pares de contactos (C2 – C6, C3 – C7 y C4 – C8 si están presentes).

Criterios

Altura de los contactos desde la superficie del cuerpo de la tarjeta: [-100 µm - +100 µm]

Resultados

Valores en la tabla a continuación en µm.

Muestra	C1	C2	C3	C4	C5	C6	C7	C8	Veredicto
46X217	-8	1,5	-6	N/A	-13	-8,5	-6	N/A	Aprobado
47X217	-9	17	-9	N/A	-6	-6	-5	N/A	Aprobado
48X217	-13	18	-18,5	N/A	-12	4	11,5	N/A	Aprobado

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC 101898652
Santo Domingo, R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

12. Requisitos de ISO 7816-2

12.1 Dimensión y ubicación de los contactos

Referencia

Basado en [R1] §6.3 (criterios en [R31] §4). El propósito de esta prueba es determinar si la dimensión y ubicación de los contactos de la tarjeta cumplen con los requisitos estándar.

Banco de pruebas

Proyector de perfil (ver capítulo 6) Patrón para la ubicación de contactos Bloque de referencia de contactos Carga

Procedimiento

Coloque el bloque de referencia de contactos en la placa del proyector de perfil y alinéelo con el patrón de contactos (en la pantalla del proyector de perfil), moviendo el eje del proyector de perfil. Coloque la tarjeta en prueba en la placa del proyector de perfil y manténgala con la carga. Verifique si las áreas mínimas de contacto materializadas del patrón están completamente cubiertas por la metalización. Verifique si la metalización dentro de las áreas mínimas de contacto materializadas no está conectada a ningún otro contacto. En caso de duda, utilice la estación de medición 3D para medir la dimensión y ubicación reales.

Criterios

Valores en la tabla a continuación en mm.

Contacto	Borde izquierdo	Borde derecho	Borde inferior	Borde superior
C1	≤10.25	≥12.25	≤19.23	≥20.93
C2	≤10.25	≥12.25	≤21.77	≥23.47
C3	≤10.25	≥12.25	≤24.31	≥26.01
C4	≤10.25	≥12.25	≤26.85	≥28.55
C5	≤17.87	≥19.87	≤19.23	≥20.93
C6	≤17.87	≥19.87	≤21.77	≥23.47
C7	≤17.87	≥19.87	≤24.31	≥26.01
C8	≤17.87	≥19.87	≤26.85	≥28.55

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

Resultados

Muestra	Elemento	C1	C2	C3	C4	C5	C6	C7	
46X217	Dimensión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
46X217	Sin conexión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
47X217	Dimensión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
47X217	Sin conexión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
48X217	Dimensión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
48X217	Sin conexión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
49X217	Dimensión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
49X217	Sin conexión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
50X217	Dimensión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A
50X217	Sin conexión	Aprobado	Aprobado	Aprobado	N/A	Aprobado	Aprobado	Aprobado	N/A

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg 1ra Instancia D.N.
SANTO DOMINGO, R.D.

SOLUTIONS INTERNATIONAL SA
CSI
RNC 4018698852
Santo Domingo R.D.

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

13. Requisitos de versiones anteriores de normas

13.1 Luz ultravioleta

Referencia

Basado en ISO/IEC 10373-1:2006 §5.11 (criterios en ISO/IEC 7816-1:1998 §4.2.1). El propósito de esta prueba es determinar si la luz ultravioleta puede dañar la tarjeta o afectar su funcionalidad.

Banco de pruebas

Generador de luz ultravioleta Lector PC/SC Micro-ohmímetro y banco de medición de resistencia a 4 hilos (ver capítulo 6)

Procedimiento

Las tarjetas se exponen a una luz monocromática (longitud de onda: 254 nm). Primero se expone el lado frontal a un total de 0.15 Ws/mm². Luego, repita la exposición para el lado posterior de las tarjetas.

Criterios

Funcionalidad: las muestras deben permanecer funcionalmente probadas (ver capítulo 8).

Resultados

Muestra	Funcionalidad del contacto	Resistencia eléctrica de los contactos
36X217	Aprobado	Aprobado
37X217	Aprobado	Aprobado
38X217	Aprobado	Aprobado

La versión actual reemplaza y sustituye a todas las versiones anteriores.
Este informe no debe ser reproducido o comunicado excepto en su última versión completa sin modificar.

14. Términos y condiciones

Estos Términos y Condiciones Específicos complementan los Términos y Condiciones Generales de Venta y Suministro de Fime, que fueron proporcionados y aceptados por el Cliente antes de proporcionar los servicios.

14.1 Descargos de responsabilidad

Este informe de prueba contiene solo información sobre las muestras probadas. No es una aprobación de toda la producción del producto. Este informe de prueba no constituye una aprobación oficial por la autoridad de prueba.

14.2 Compromiso

Certificamos que los resultados incluidos en este informe de prueba son los resultados precisos de las pruebas realizadas en las muestras probadas. Las pruebas se realizan en un banco de pruebas calificado y aceptado en el momento de la sesión de pruebas.

14.3 Propiedad intelectual

Consulte los Términos y Condiciones Generales de Venta y Suministro de Fime, que fueron aceptados por el Cliente cuando se aceptó la Oferta Comercial de Fime. Tenga en cuenta que este informe puede contener referencias a marcas comerciales de terceros. En particular, tenga en cuenta que el logotipo de COFRAC se reproduce en la primera página de este informe. De acuerdo con GEN REF 11 Rev8 de COFRAC, el logotipo de COFRAC se utiliza solo para indicar que este informe ha sido preparado por Fime SAS haciendo negocios como Fime EMEA. El Cliente adquiere derechos en cualquiera de las marcas comerciales utilizadas en este documento, y en particular está prohibido reproducir el logotipo de COFRAC en cualquier documento que no sea una copia exacta de este Informe de Prueba. Fime está obligado a informar cualquier uso abusivo del logotipo de COFRAC de acuerdo con los términos de nuestra acreditación.

14.4 Almacenamiento

El almacenamiento de las muestras se realizará durante 3 meses después de la emisión del informe. El almacenamiento de los datos de prueba se realizará durante 10 años después de la emisión del informe.

14.5 Procedimiento de quejas

El laboratorio tiene una política y procedimientos adecuados para la resolución de quejas de clientes u otras partes. Este procedimiento incluye una investigación y acciones correctivas si se confirma el problema. Un correo electrónico puede ser enviado directamente al servicio de calidad a quality@fime.com. Este procedimiento está disponible a solicitud.

Instrumento redactado a solicitud del interesado e inscrito en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, hoy Diez (10) del mes de Julio del año Dos Mil Veinticuatro (2024).

LIC. SANTO C. SIERRA

Este informe no debe ser reproducido excepto en su totalidad sin la aprobación escrita del laboratorio.
HELP

Carta jurada de realización de Prueba ISO de Durabilidad de la tarjeta

SELP

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 1-30-18398852 Santo Domingo, R.D.

Paris, 13 de junio del 2024

Junta Electoral Central

Ref: JCE-CCC-LPI-2024-0001 "Pliego de Condiciones específicas destinado a la contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)"

A quien corresponda:

Por la presente certifico que la empresa SELP S.A.S. llevó a cabo, a través del laboratorio externo internacional Fime, pruebas ISO de durabilidad de tarjetas fabricadas por nosotros. Anexo encontrarán el documento que describe dichas pruebas, así como los resultados obtenidos.

Atentamente,

Bastien Blanc
Representante
SELP S.A.S.

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tél. : 05 53 60 84 44 - Fax : 05 53 60 84 45
SIRET : 351 667 928 00011

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC
apposée ci-dessus.

Página/Folio No.701 de 843

COPY SOLUTIONS INTERNATIONAL SA
CSI
RNC: 101
Santo Domingo

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

REPUBLIQUE DOMINICAINE

1. *République française*

Le présent acte public

2. a été signé par **Me** MILLIER

3. agissant en qualité de **Notaire**

4. est revêtu du sceau timbre de **Son étude**

Attesté

5. à Paris

6. le 13 JUIN 2024

7. *par le Procureur général près la Cour d'appel de Paris*

8. SYLVIE SCHLANGER signature

AVOCAT GENERAL

9. *Cette apostille confirme seulement l'authenticité de la signature, du sceau ou timbre sur le document. Elle ne signifie pas que le contenu du document est correct ou que la République française approuve son contenu.*

COUR D'APPEL DE PARIS

TRADUCCIÓN OFICIAL: Carta jurada de realización de Prueba ISO de Durabilidad de la tarjeta

Yo **LIC. SANTO C. SIERRA,** intérprete judicial, debidamente juramentada para el ejercicio de mis funciones **CERTIFICO** que he procedido a traducir las partes centrales de un documento escrito originalmente en Francés, cuya versión en idioma Español de acuerdo a mí mejor el conocimiento es el siguiente:

LIC. SANTO C. SIERRA Intérprete Judicial Juzg 1ra Instancia D.N. SANTO DOMINGO, R.D.

SELP

Paris, 13 de junio del 2024

Junta Electoral Central

Ref: JCE-CCC-LPI-2024-0001 "Pliego de Condiciones específicas destinado a la contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)"

SOLUTIONS INTERNATIONAL S.A. RNC 401898852 Santo Domingo, R.D.

A quien corresponda:

Por la presente certifico que la empresa SELP S.A.S. llevó a cabo, a través del laboratorio externo internacional Fime, pruebas ISO de durabilidad de tarjetas fabricadas por nosotros. Anexo encontrarán el documento que describe dichas pruebas, así como los resultados obtenidos.

Atentamente,

Atentamente,

Bastien Blanc
representante
SELP S.A.S.

SELP SAS
187 Avenida de las Plagnes
24340 MAREUIL-EN-PERIGORD
Tél.: 05 53 60 84 44 - Fax: 05 53 60 84 45
SIRET 351 667 928 00011

Sr. François MILLIER
Notario de París, abajo firmante
Certifica la firma de
M.BLANG
pegado arriba

APOSTILLA

(Convenio de La Haya del 5 de octubre de 1961)

1. República Francesa REPUBLICA DOMINICANA

El presente acto público

2. ha sido firmado por: Me MILLER

3. actuando en calidad de: Notario

4. está revestido del sello estampado de: Su despacho

Atestiguado

5. en París

6. el 19 JUN 2023

7. por el Procurador General ante la Corte de Apelación de París

Sello

8. Nosotros

9. Sello 10. Firma

SYLVIE SCHLANGER

ABOGADA GENERAL

Sello en el documento. No significa que el contenido del documento sea "La Apostilla sólo confirma la autenticidad de la firma, el significado o corrección o que la República Francesa aprueba su contenido".

Traducido a petición de la parte interesada y registrada en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Veintitrés (23) días del mes de Octubre del año Dos Mil Veinticuatro (2024).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

S.C.S / DPE
5184-12-8-96

Prueba ISO 18745-1 Resistencia

FIME

One Account. A billion transactions.

TEST REPORT

REPORT OBJECT	**ISO 18745-1 test session**
REPORT REFERENCE	**C19REP02-060**

REPORT VERSION V1.0	REPORT ISSUE DATE 2019/12/11
NUMBER OF PAGES 16 pages	TESTING DATES From 2019/11/15 to 2019/12/05
VENDOR NAME SELP	AUTHORIZED BY Luc Morcel Expert 2019-12-11 08:18+01:00
PRODUCT NAME AND VERSION ePassport	

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101[illegible]852
Santo Domingo

TABLE OF CONTENTS

1 REVISION HISTORY 4

2 TEST RESULTS SUMMARY 4

2.1 Codification 4
2.2 Summary of ISO 18745-1 stand alone tests 4
2.3 Summary of ISO 18745-1 test sequence 4
2.4 Conclusion 4

3 REFERENCE DOCUMENTS 5

4 LABORATORY INFORMATION 6

4.1 Testing Laboratory Identification 6
4.2 Personnel 6
4.3 Operating Procedures 6
4.4 Subcontracting 6
4.5 Operating Conditions 6

5 INFORMATION CLIENT ET PRODUIT 7

5.1 Customer identification 7
5.2 Sample information 7
5.3 Sample picture 7

6 TEST EQUIPMENT INFORMATION 8

7 MEASUREMENT'S UNCERTAINTIES 8

8 EVALUATION METHODS 8

8.1 Functional evaluation 8
8.2 Physical damage evaluation 9

9 DETAILED RESULTS: STAND ALONE TESTS 10

9.1 Thermal cycling sequence 10
9.2 Bending fatigue sequence 11

10 DETAILED RESULTS: TEST SEQUENCE 13

10.1 Thermal cycling sequence 13

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

10.2 Bending fatigue sequence 14

11 TERMS AND CONDITIONS 16

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo R.D.

The current version supersedes and replaces all previous reports.
This report shall not be reproduced or communicated except in its full unmodified latest version

1 REVISION HISTORY

DATE	VERSION	AUTHOR	COMMENT
2019/12/11	1.0	YBR	Initial version

2 TEST RESULTS SUMMARY

2.1 Codification

PASS: Passed test
FAIL: Failed test
N/A: Not applicable

2.2 Summary of ISO 18745-1 stand alone tests

TEST	VERDICT
Thermal Cycling Sequence	PASS
Bending Fatigue Sequence	PASS

2.3 Summary of ISO 18745-1 test sequence

TEST	VERDICT
Thermal Cycling Sequence	PASS
Bending Fatigue Sequence	PASS

2.4 Conclusion

Test session results show that the tested samples meet the requirements necessary to pass the test plan defined with customer, as detailed in this report.

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

3 REFERENCE DOCUMENTS

REFERENCES		
[R20]	ISO/CEI 7810:2003	Identification cards – Physical characteristics
[R60]	ICAO (6th edition, 2005)	Doc 9303 Part 1 Vol.2
[R90]	ISO/IEC 18745-1:2018	Information technology -- Test methods for machine readable travel documents (MRTD) and associated devices -- Part 1: Physical test methods for passport books (durability)
[R91]	ISO/IEC 18745-2:2016	Information technology -- Test methods for machine readable travel documents (MRTD) and associated readers -- Part 2: Test methods for the contactless interface

COPY SOLUTIONS INTERNATIONAL, S.A.
Santo Domingo, R.D.

4 LABORATORY INFORMATION

4.1 Testing Laboratory Identification

Name and address of the laboratory that performed the tests and issued this test report:

FIME EMEA
8 rue Commodore J.H. Hallet
14000 Caen, FRANCE
Tel.: +33 (0)231 440 807

4.2 Personnel

The following persons have collaborated on the preparation, execution or reporting of the tests contained in this report:

TESTS	
G. Béhue	Experienced Test Technician
Y. Briard	Experienced Test Technician
L. Morcel	Expert

REPORT		
Owned by	L. Morcel	Expert
Reviewed by	Y. Briard	Experienced Test Technician
Authorized by	Y. Linot	Activity Manager

4.3 Operating Procedures

The internal procedures that relate to the execution of the tests are available in the Quality Assurance Plan e-Passport.
The template used to create this report is rep_ISO18745-1 v3.0.

4.4 Subcontracting

The following tests have been subcontracted: thermal cycling sequence.

4.5 Operating Conditions

The tests have been run under following environmental conditions throughout the session:

Temperature	20°C to 26°C
Relative Humidity	40%RH to 60%RH

Environmental conditions are recorded with thermo-hygrometer (continuously for test room, during operations for test chambers).

COPY SOLD INTERNATIONAL S.A. CSI RNC 01896852 Santo Domingo, R.D.

5 INFORMATION CLIENT ET PRODUIT

5.1 Customer identification

Company name	SELP
Address	Rue Louis Pergaud, 16000-Angoulême, France
Contact	Brice Chaveroux
Tel	+33545251895
E-mail	b.chaveroux@selp.fr

5.2 Sample information

Product name:	ePassport
Version:	with eDatapage
Form factor:	booklet
Number of pages:	32 pages
Datapage format:	plastic
Chip /Application:	MOB10 / P60
Feature:	hot stamp on cover

Samples tested by the Testing Laboratory are identified in the following table:

PRODUCTS	BATCH	INTERNAL ID	RECEPTION DATE
ePassport	C19STN02-060	1P497 to 9P497	2019/11/08

5.3 Sample picture

6 TEST EQUIPMENT INFORMATION

TYPE	DESCRIPTION	ADDITIONAL INFORMATION
Bending stress machine	Internal reference: 40/04 Brand: BGI Model or Type: BGI087	Verified on: 2019/04/29 Tolerance for deflection: compliant with a ± 1mm MPE Tolerance for frequency: compliant with a ± 0.025Hz MPE
Caliper	Internal reference: 20/01 Brand: Mitutoyo	Verified on: 2019/02/11 Uncertainty: ± 0.03 mm
Software: PC/SC reader interface	Software name: ATR reader Brand: FIME	Software version: v1.5
Thermo-hygrometer (test room)	Internal reference: C09/33 Brand: ELPRO Model or Type: Ecolog LH2	Verified on: 2019/05/21 Uncertainty: ± 0.2 °C; ± 2 %
Vectorial Network Analyzer	Internal reference: C07/01 Brand: Rohde & Schwarz Model or Type: ZVL6 Calibration kit: ZV-Z135 (C07/01A)	Verified on: 2018/10/29 Uncertainty: ± 0.1 MHz

7 MEASUREMENT'S UNCERTAINTIES

In this report, uncertainties are given at a confidence level of k = 2.
To state on compliance, uncertainties of measurement have not been considered. Statements established on measurements included in the uncertainty area are identified with asterisk.

8 EVALUATION METHODS

8.1 Functional evaluation

Reference: [R90] §9.1, [R91] §5.6.2 & § 5.6.3

- Check if the e-passport's mandatory LDS application data can be retrieved from the sample. Alternatively, check that the sample is able to answer an "ATR" request, using a PC/SC reader. For some subcontracted tests, functional evaluation is not performed 30 minutes after test completion, contrary to requirement of [R90] §9.1.5.
- Resonance frequencies before and after test are given for information.

The current version supersedes and replaces all previous reports.
This report shall not be reproduced or communicated except in its full unmodified latest version

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 131898852
Santo Domingo, R.D.

8.2 Physical damage evaluation

Reference: [R90] §9.2

- The picture shall be recognizable.
- Written information shall be legible, with no missing letters or words.
- The MRZ shall be machine readable.
- The MRP shall be intact – no pages shall be separated.
- Opening the MRP to the datapage (180°) shall not incur any further damage.
- Opening the MRP to a visa page (180°) shall not incur any further damage.
- The PIC containing part (cover, data page, special visa page) does not allow direct access to the chip or the antenna.
- No part of the datapage shall be missing.
- For datapages, more than 90% of the binding shall be intact.
- For other pages, more than 90% of the binding shall be intact.
- At least 50% of the hot-stamp on the cover shall be intact.
- Any holes in any sheets shall be less than 2mm in diameter.
- Areas of delamination along the edges shall be less than 3mm deep, and 3mm in length. Delamination within the sheet shall be less than 3mm in length

The current version supersedes and replaces all previous reports
This report shall not be reproduced or communicated except in its full unmodified latest version

COPY SOLUTIONS INTERNATIONAL, S.A.
RNC 101858852
Santo Domingo, R.D.

9 DETAILED RESULTS: STAND ALONE TESTS

9.1 Thermal cycling sequence

Reference

[R90] §10.11. This stress method subjects the MRP to cycling between two temperature extremes. This stress simulates the thermal shock the MRP could experience due to thermal expansion and contraction of each MRP component. The test is conducted over a short period of time for each stress cycle.

Test bench

Thermal shocks chamber (subcontractor's equipment)
PC/SC reader
Vector network analyzer
(see chapter 6)

Procedure

Place in a climate controlled chamber at temperature of 77 °C ± 3 °C for 15mn (Control of relative humidity in the climate controlled chambers is not required for this test).
Transfer the sample to a second climate controlled chamber held at a temperature of –32 °C ± 3 °C in less than 15 seconds. Cold exposure duration is 15 min, and then the sample is moved to the first chamber. The position of the sample in the holder should not be modified during the transfer process.
Repeat the process for 20 cycles.

Criteria

Functional evaluation: samples shall comply with requirements of [R90] (see §8.1).
Physical Damage evaluation: samples shall comply with requirements of [R90] (see §8.2).

Results

Sample	Application functionality	Physical damage	Resonance frequency (before/after in MHz)
1P497	PASS	PASS	0% (16,70 / 16,70)
2P497	PASS	PASS	1% (16,75 / 16,65)
3P497	PASS	PASS	1% (16,75 / 16,85)

Note

This exposure is subcontracted.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101[illegible]852
Santo Domingo, R.D.

9.2 Bending fatigue sequence

Reference

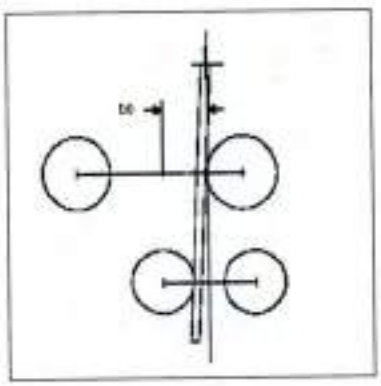
[R90] §10.10. The purpose of this test is to determine the bending fatigue resistance of the booklet construction to fully reversed loading. This method differs from the back pocket stress method by avoiding directly applied pressure. This method accelerates fatigue due to imposed bending, especially in the area of the antenna and associated connections if present.

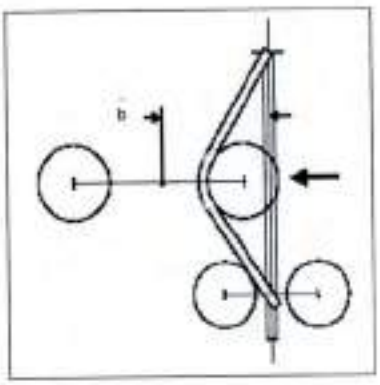
Test bench

Bending machine
PC/SC reader
Vector network analyzer
Height gage
(see chapter 6)

Procedure

Calibration:





Orientation = spine: b0 = 15 mm; b(40N) > b0+20, so b = 35 mm
Orientation = top: b0 = 13 mm; b(40N) = 28 mm, so b = 28 mm

Test:

Taking into account, the specified orientation, the MRP should be clamped at one extremity and allowed to freely move at the opposite edge.
Set up the apparatus to impose a maximum centerline deflection b0 + 20 mm, or a maximum applied force of 40 N (whichever occurs first).
Flex the book 1000 times at 0.5 Hz (orientation = spine).
Flex the book 1000 times at 0.5 Hz (orientation = top).

The current version supersedes and replaces all previous versions.
This report shall not be reproduced or communicated except in its full unmodified latest version

Criteria

Functional evaluation: samples shall comply with requirements of [R90] (see §8.1).
Physical Damage evaluation: samples shall comply with requirements of [R90] (see §8.2).
Datapage warpage evaluation: samples shall comply with requirements of [R90] (see §8.5).
Book warpage evaluation: samples shall comply with requirements of [R90] (see §8.6).

Results

Sample	Application functionality	Physical damage	Datapage warpage (mm)	Book warpage (mm)	Resonance frequency (before/after in MHz)
7P497	PASS	PASS	PASS	PASS	1% (16,65 / 16,75)
8P497	PASS	PASS	PASS	PASS	0% (16,70 / 16,75)
9P497	PASS	PASS	PASS	PASS	1% (16,70 / 16,80)

The current version supersedes and replaces all previous versions
This report shall not be reproduced or communicated except in its full unmodified latest version

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101886852
Santo Domingo, R.D.

10 DETAILED RESULTS: TEST SEQUENCE

10.1 Thermal cycling sequence

Reference

[R90] §10.11. This stress method subjects the MRP to cycling between two temperature extremes. This stress simulates the thermal shock the MRP could experience due to thermal expansion and contraction of each MRP component. The test is conducted over a short period of time for each stress cycle.

Test bench

Thermal shocks chamber (subcontractor's equipment)
PC/SC reader
Vector network analyzer
(see chapter 6)

Procedure

Place in a climate controlled chamber at temperature of 77 °C ± 3 °C for 15mn (Control of relative humidity in the climate controlled chambers is not required for this test).
Transfer the sample to a second climate controlled chamber held at a temperature of –32 °C ± 3 °C in less than 15 seconds. Cold exposure duration is 15 min, and then the sample is moved to the first chamber. The position of the sample in the holder should not be modified during the transfer process.
Repeat the process for 20 cycles.

Criteria

Functional evaluation: samples shall comply with requirements of [R90] (see §8.1).
Physical Damage evaluation: samples shall comply with requirements of [R90] (see §8.2).

Results

Sample	Application functionality	Physical damage	Resonance frequency (before/after in MHz)
4P497	PASS	PASS	1% (16,60 / 16,75)
5P497	PASS	PASS	0% (16,70 / 16,75)
6P497	PASS	PASS	0% (16,65 / 16,65)

Note

This exposure is subcontracted.
These samples have then been used for the following bending fatigue test

10.2 Bending fatigue sequence

Reference

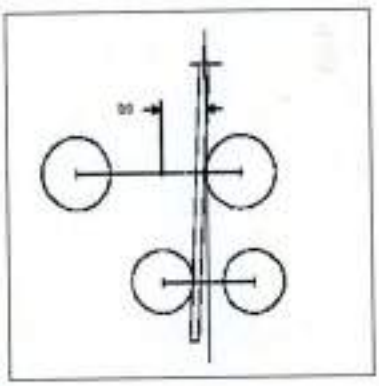
[R90] §10.10. The purpose of this test is to determine the bending fatigue resistance of the booklet construction to fully reversed loading. This method differs from the back pocket stress method by avoiding directly applied pressure. This method accelerates fatigue due to imposed bending, especially in the area of the antenna and associated connections if present.

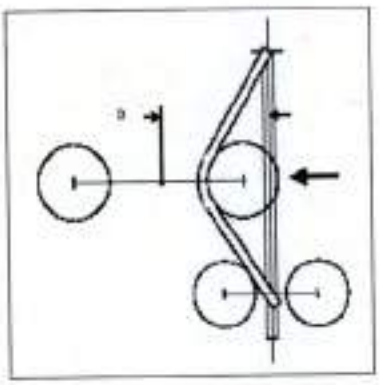
Test bench

Bending machine
PC/SC reader
Vector network analyzer
Height gage
(see chapter 6)

Procedure

Calibration:





Orientation = spine: b0 = 15 mm; b(40N) > b0+20, so b = 35 mm
Orientation = top: b0 = 13 mm; b(40N) = 28 mm, so b = 28 mm

Test:

Taking into account, the specified orientation, the MRP should be clamped at one extremity and allowed to freely move at the opposite edge.
Set up the apparatus to impose a maximum centerline deflection b0 + 20 mm, or a maximum applied force of 40 N (whichever occurs first).
Flex the book 1000 times at 0.5 Hz (orientation = spine).
Flex the book 1000 times at 0.5 Hz (orientation = top).

The current version supersedes and replaces all previous reports
This report shall not be reproduced or communicated except in its full unmodified latest version

Criteria

Functional evaluation: samples shall comply with requirements of [R90] (see §8.1).
Physical Damage evaluation: samples shall comply with requirements of [R90] (see §8.2).
Datapage warpage evaluation: samples shall comply with requirements of [R90] (see §8.5).
Book warpage evaluation: samples shall comply with requirements of [R90] (see §8.6).

Results

Sample	Application functionality	Physical damage	Datapage warpage (mm)	Book warpage (mm)	Resonance frequency (before/after in MHz)
4P497	PASS	PASS	PASS	PASS	0% (16,60 / 16,65)
5P497	PASS	PASS	PASS	PASS	0% (16,70 / 16,65)
6P497	PASS	PASS	PASS	PASS	0% (16,65 / 16,65)

Note

These samples have previously performed the Thermal Cycling test.

11 TERMS AND CONDITIONS

Disclaimers:
This test report contains only information about the tested samples. It is not an endorsement of the entire production of the product.
This test report doesn't constitute an official approval by the test authority.

Commitment:
We certify that the results included in this test report are the precise results of the tests performed on the tested samples.
Tests are performed on a qualified and accepted test bench at the time of test session.

Intellectual Property:
Refer to General Terms & Conditions of sales and supply given with the estimate.

Storage:
The test results are kept 10 years by the testing laboratory.
Samples are managed according to customer's request.

Complaint procedure:
The laboratory has a policy and appropriate procedures for the resolution of complaints from customers or other parties. This procedure includes an investigation and corrective actions if the problem is confirmed. An e-mail may be addressed directly to quality service at quality@fime.com. This procedure is available on request.

----------END of DOCUMENT----------

TRADUCCIÓN OFICIAL: Prueba ISO 18745-1 Resistencia

Fime

Una acción. Mil millones de transacciones.

INFORME DE PRUEBA

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg. 1ra Instancia D.N.
SANTO DOMINGO, R.D.

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC. 01[illegible]2
Santo Domingo, R.D.

OBJETO DE INFORME	**Sesión de prueba ISO 18745-1**
INFORME REFERENCIA	**C19REP02-060**

VERSIÓN DEL INFORME V1.0	FECHA DE EMISIÓN DEL INFORME 2019/12/11
NÚMERO DE PÁGINAS 16 páginas	FECHAS DE PRUEBAS Del 15/11/2019 al 05/12/2019
NOMBRE DEL VENDEDOR SELLO	AUTORIZADO POR
NOMBRE DEL PRODUCTO Y VERSIÓN Pasaporte electrónico	Luc Morcel Experto 2019-12-11 08:18+01:00

La versión actual reemplaza y reemplaza todas las versiones anteriores. Este informe no se reproducirá ni comunicará excepto en su última versión completa y sin modificaciones.

CUADRO DEL CONCURSO

1. HISTORIAL DE REVISIONES 4
2. RESUMEN DE RESULTADOS DE LA PRUEBA 4
   2.1 Codificación 4
   2.2 Resumen de las pruebas independientes según la norma ISO 18745-1 4
   2.3 Resumen de la secuencia de pruebas ISO 18745-1 4
   2.4 Conclusión 4
3. DOCUMENTOS DE REFERENCIA 5
4. INFORMACIÓN DE LABORATORIO 6
   4.1 Identificación del laboratorio de pruebas 6
   4.2 Personal 6
   4.3 Procedimientos operativos 6
   4.4 Subcontratación 6
5. INFORMACIÓN CLIENTE Y PRODUCTO 7
   5.1 Identificación del cliente 7
   5.2 Información de muestra 7
   5.3 Imagen de muestra 7
6. INFORMACIÓN SOBRE EL EQUIPO DE PRUEBA 8
7. INCERTIDUMBRES DE LA MEDICIÓN 8
8. MÉTODOS DE EVALUACIÓN 8
   8.1 Evaluación funcional 8
   8.2 Evaluación de daños físicos 9
9. RESULTADOS DETALLADOS: PRUEBAS INDEPENDIENTES 10
   9.1 Secuencia de ciclado térmico 10
   9.2 Secuencia de fatiga por flexión 11
10. RESULTADOS DETALLADOS: SECUENCIA DE LA PRUEBA 13
    10.1 Secuencia de ciclado térmico 13

10.2 Secuencia de fatiga por flexión

11. TÉRMINOS Y CONDICIONES

1 HISTORIAL DE REVISIONES

FECHA	VERSIÓN	AUTOR	COMENTARIO
11/12/2019	1.0	YBR	Versión inicial

2 RESUMEN DE RESULTADOS DE LA PRUEBA

2.1 Codificación

PASS: Aprobada

FAIL: Prueba fallida

N/A: No aplica

2.2 Resumen de las pruebas independientes según la norma ISO 18745-1

PRUEBA	VEREDICTO
Secuencia de ciclos térmicos	APROBADA
Secuencia de fatiga por flexión	APROBADA

2.3 Resumen de la secuencia de pruebas ISO 18745-1

PRUEBA	VEREDICTO
Secuencia de ciclos térmicos	APROBADA
Secuencia de fatiga por flexión	APROBADA

2.4 Conclusión

Los resultados de la sesión de prueba muestran que las muestras probadas cumplen los requisitos necesarios para pasar el plan de prueba definido con el cliente, como se detalla en este informe.

3 DOCUMENTOS DE REFERENCIA

REFERENCIAS		
[R20]	ISO/CEI 7810:2003	Fichas de identificación- Características físicas
[R60]	OACI (6ª edición, 2005)	Doc. 9303 Parte 1 Vol.2
[R90]	ISO/IEC 18745-1:2018	Tecnología de la información – Métodos de prueba para documentos de viaje legibles por máquina (MRTD) y dispositivos asociados – Parte 1: Métodos de prueba físicos para pasaportes (durabilidad).
[R91]	ISO/IEC 18745-2:2016	Tecnología de la información – Métodos de prueba para documentos de viaje de lectura mecánica (MRTD) y lectores asociados – Parte 2: Métodos de prueba para la interfaz sin contacto

4 INFORMACIÓN DE LABORATORIO

4.1 Identificación del laboratorio de pruebas

Nombre y dirección del laboratorio que realizó la prueba y emitió este informe de prueba:
FIME EMEA
8 calle Comodoro JH Hallet
14000 Caen, FRANCIA
Teléfono: +33(0)231 440 807

4.2 Personal

Las siguientes personas han colaborado en la preparación, ejecución o informe de las pruebas contenidas en este informe:

PRUEBAS	
G. Behue	Técnico de pruebas experimentado
Y. Briard	Técnico de pruebas experimentado
L. Morcel	Experto

INFORME		
Propiedad de	L. Morcel	Experto
Revisado por	Y. Briard	Técnico de pruebas experimentado
Autorizado por	Y. Linot	Administrador de actividades

4.3 Procedimientos operativos

Los procedimientos internos que se relacionan con la ejecución de las pruebas están disponibles en el Pasaporte Electrónico del Plan de Aseguramiento de la Calidad.
La plantilla utilizada para crear estos informes es rep_ISO18745-1 v3.0.

4.4 Subcontratación

Se han subcontratado las siguientes pruebas: secuencia de ciclado térmico.

4.5 Condiciones de funcionamiento

Las pruebas se han realizado bajo las siguientes condiciones ambientales durante toda la sesión:

Temperatura	20 °C a 26°C
Humedad relativa	40% HR a 60% HR

Las condiciones ambientales se registran con un termo-higrómetro (de forma continua para la sala de pruebas y durante el funcionamiento para las cámaras de pruebas).

5 INFORMACIÓN CLIENTE Y PRODUCTO

5.1 Identificación del cliente

Nombre de la empresa	SELP
Dirección	Rue Louis Pergaud, 16000-Angouleme, Francia
Contacto	con Brice Chaveroux
Teléfono	+33545251895
Correo electrónico:	b.chaveroux@selp.fr

5.2 Información de muestra

Nombre del producto:	Pasaporte electrónico
Versión:	con eDatapage
Factor de forma:	Folleto
Número de páginas:	32 páginas
Formato de las páginas de datos:	Plástico
Chip/Aplicación	MOB10/P60
Característica:	Estampado en caliente en la cubierta

Las muestras analizadas por el Laboratorio de Pruebas se identifican en la siguiente tabla:

PRODUCTOS	LOTE	IDENTIFICACIÓN INTERNA	FECHA DE RECEPCIÓN
Pasaporte electrónico	C19STN02-060	1P497 a 9P497	08/11/2019

5.3 Imagen de muestra

6 INFORMACIÓN SOBRE EL EQUIPO DE PRUEBA

TIPO	DESCRIPCIÓN	INFORMACIÓN ADICIONAL
Máquina de tensión de flexión	Referencia interna: 40/04 Marca: BGI Modelo o tipo: BIGI087	Verificado el: 29/04/2019 Tolerancia de deflexión: compatible con un MPE de 1 mm Tolerancia de frecuencia: compatible con un MPE de 0,025 Hz
Calibrar	Referencia interna: 20/01 Marca: Mitutoyo	Verificado el: 11/02/2019 Incertidumbre: 0,03 mm
Software: Interfaz de lector PC/SC	Nombre del software: Lector ATR Marca: FIME	Versión del software: V1.5
Termo-higrómetro (sala de pruebas)	Referencia interna: C09/33 Marca: ELPRO Modelo o tipo: Ecolog LH2	Verificado el: 21/05/2019 Incertidumbre: 0,2 °C; 2%
Analizador de redes vectoriales	Referencia interna: C07/01 Marca: Rohde & Schwarz Modelo o tipo: ZVL6 Kit de calibración: ZV-Z135(C07/01A)	Verificado el: 29/10/2018 Incertidumbre: 0,1 MHz

7 INCERTIDUMBRES DE LA MEDICIÓN

En este informe, las incertidumbres se dan en un nivel de confianza de k = 2.
Para la manifestación de cumplimiento no se han considerado incertidumbres de medición. Las manifestaciones establecidas sobre medición incluidas en el área de incertidumbre se identifican con un asterisco.

8 MÉTODOS DE EVALUACIÓN

8.1 Evaluación funcional
Referencia: [R90] 9.1, [R91] 5.6.2 y 5.6.3

- Compruebe si los datos obligatorios de la solicitud LDS del pasaporte electrónico se pueden recuperar de la muestra. Alternativamente, compruebe que la muestra puede responder a una solicitud ATR, utilizando un lector PC/SC. Para algunas pruebas subcontratadas, la evaluación funcional no se realiza 30 minutos después de la finalización de la prueba, contrariamente al requisito de [R90] 9.1.5.
- Se dan a título informativo las frecuencias de resonancia antes y después de la prueba.

8.2 Evaluación de daños físicos

Referencia: [R90] 9.2

- La imagen deberá ser reconocible
- La información escrita deberá ser legible, sin letras ni palabras faltantes.
- La ZLM deberá ser legible por máquina.
- El MRP deberá estar intacto: no se deberán separar páginas.
- Abrir el MRP en la página de datos (180°) no provocará más daños.
- Abrir el MRP en una página de visa (180°) no ocasionará ningún daño adicional.
- La parte que contiene el PIC (cubierta, página de datos, página de visa especial) no permite el acceso directo al chip ni a la antena.
- No deberá faltar ninguna parte de la página de datos.
- En el caso de las páginas de datos, más del 90 % del enlace deberá estar intacto.
- Para las demás páginas, más del 90% de la encuadernación deberá estar intacta.
- Al menos el 50% de la estampación en caliente de la cubierta deberá estar intacta.
- Cualquier agujero en cualquier lámina deberá tener un diámetro inferior a 2 mm.
- Las áreas de delaminación a lo largo de los bordes deberán tener menos de 3 mm de profundidad y 3 mm de longitud.
  La delaminación dentro de la hoja deberá tener una longitud inferior a 3 mm.

9 RESULTADOS DETALLADOS: PRUEBAS INDEPENDIENTES

9.1 Secuencia de ciclo térmico

Referencia

[R90] 10.11. Este método de estrés somete al MRP a ciclos entre dos extremos de temperatura. Este estrés simula el choque térmico que podría experimentar el MRP debido a la expansión y contracción térmica de cada componente del MRP. La prueba se realiza durante un corto período de tiempo para cada ciclo de estrés.

Banco de pruebas

Cámara de choque térmico (equipo subcontratista)
Lector de PC/SC
Analizador de redes vectoriales
(Ver capítulo 6)

Procedimiento

Colóquelo en una cámara con clima controlado a una temperatura de 77 °C ± 3 °C durante 15 minutos (no se requiere control de la humedad relativa en las cámaras con clima controlado para esta prueba).
Transfiera la muestra a una segunda cámara con clima controlado a una temperatura de -32 °C 3 °C en menos de 15 segundos. La duración de la exposición al frío es de 15 minutos y luego la muestra se traslada a la primera cámara. La posición de la muestra en el soporte no debe modificarse durante el proceso de transferencia. Repita el proceso durante 20 ciclos.

Criterios

Evaluación funcional: la muestra debe cumplir con los requisitos de [R90] (ver 8.1).
Evaluación del daño físico: la muestra deberá cumplir con los requisitos de [R90] (ver 8.2).

Resultados

Muestra	Funcionalidad de la aplicación	Daño físico	Frecuencia de resonancia (antes/después en MHz)
1P497	APROBADA	APROBADA	0% (16,70/16,70)
2P497	APROBADA	APROBADA	1% (16,75/16,65)
3P497	APROBADA	APROBADA	1% (16,75/16,85)

Nota

Esta exposición está sub-concentrada.

9.2 Secuencia de fatiga por flexión

Referencia

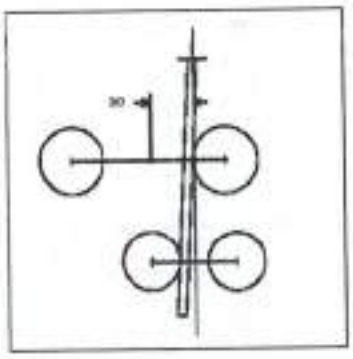
[R90] 10.10. El propósito de esta prueba es determinar la resistencia a la fatiga por flexión de la construcción del folleto ante una carga totalmente invertida. Este método se diferencia del método de tensión del bolsillo trasero al evitar la presión aplicada directamente. Este método acelera la fatiga debido a la flexión impuesta, especialmente en el área de la antena y las conexiones asociadas, si las hay.

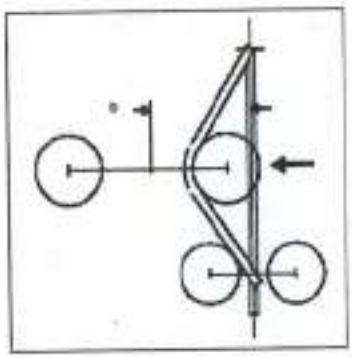
Banco de pruebas

Máquina dobladora
Lector PS/SC
Analizador de redes vectoriales
Medidor de altura
(Ver capítulo 6)

Procedimiento

Calibración





ORIENTACION: COLUMNA VERTEBRAL b0 = 15 mm; b(40N) > b0+20, por lo que b = 35 mm
ORIENTACION: ARRIBA b0 = 13 mm; b(40N) = 28 mm, por lo que b = 28 mm

Prueba:

Teniendo en cuenta la orientación especificada, el MRP debe sujetarse en un extremo y dejarse mover libremente en el borde opuesto.
Configure el aparato para imponer una desviación máxima en la línea central b0 + 20 mm, o una fuerza máxima aplicada de 40 N (lo que ocurra primero).
Flexione el libro 1000 veces a 0,5 Hz (orientación = lomo).
Flexione el libro 1000 veces a 0,5 Hz (orientación = arriba).

Criterios

Evaluación funcional: las muestras deberán cumplir con los requisitos de [R90] (ver 8.1).
Evaluación de daños físicos: las muestras deberán cumplir con los requisitos de [R90] (ver 8.2).
Evaluación de la deformación de la página de datos: las muestras deberán cumplir con los requisitos de [R90] (ver 8.5).
Evaluación de deformación de libros: las muestras deberán cumplir con los requisitos de [R90] (ver 8.6).

Resultados

Muestra	Solicitud funcionalidad	Físico daño	Página de datos Deformación (mm)	Deformación del libro (mm)	Frecuencia de resonancia (antes/después en MHz)
7P497	APROBADA	APROBADA	APROBADA	APROBADA	1% (16,65/16,75)
8P497	APROBADA	APROBADA	APROBADA	APROBADA	0% (16,70/16,75)
9P497	APROBADA	APROBADA	APROBADA	APROBADA	1% (16,70/16,80)

10 RESULTADOS DETALLADOS: SECUENCIA DE PRUEBA

10.1 Secuencia de ciclo térmico

Referencia

[R90] 10.11 Este método de estrés somete al MRP a ciclos entre dos extremos de temperatura. Este estrés simula el choque térmico que podría experimentar el MPR debido a la expansión y contracción térmica de cada componente del MPR. La prueba se realizó durante un período corto de tiempo para cada ciclo de estrés.

Banco de pruebas

Cámara de choque térmico (equipo del subcontratista)
Lector de PC/SC
Analizador de redes vectoriales
(ver capítulo 6)

Procedimiento

Colóquelo en una cámara con clima controlado a una temperatura de 77 °C ± 3 °C durante 15 minutos (no se requiere control de la humedad relativa en las cámaras con clima controlado para esta prueba).
Transfiera la muestra a una segunda cámara con clima controlado a una temperatura de -32 °C 3 °C en menos de 15 segundos. La duración de la exposición al frío es de 15 minutos y la muestra se traslada a la primera cámara. La posición de la muestra en el soporte no debe modificarse durante el proceso de transferencia. Repita el proceso durante 20 ciclos.

Criterios

Evaluación funcional: las muestras deberán cumplir con los requisitos de [R90] (ver 8.1).
Evaluación de daños físicos: las muestras deberán cumplir con los requisitos de [R90] (ver 8.2).

Resultados

muestra	Solicitud funcionalidad	Físico daño	Frecuencia de resonancia (antes/después en MHz)
4P497	APROBADA	APROBADA	1% (16,60/16,75)
5P497	APROBADA	APROBADA	0% (16,70/16,75)
6P497	APROBADA	APROBADA	0% (16,65/16,75)

Nota

Esta exposición está subcontratada.
Estas muestras se han utilizado luego para la siguiente prueba de fatiga por flexión.

10.2 Secuencia de fatiga por flexión

Referencia

[R90] 10.10. El objetivo de esta prueba es determinar la resistencia a la fatiga por flexión de la construcción del folleto ante una carga totalmente invertida. Este método se diferencia del método de tensión posterior al evitar la presión aplicada directamente. Este método acelera la fatiga debido a la flexión impuesta, especialmente en el área de la antena y las conexiones asociadas, si las hay.

Banco de pruebas

Máquina dobladora
Lector de PC/SC
Analizador de redes vectoriales
Medidor de altura
(Ver capítulo 6)

Procedimiento

Imagen aquí

Prueba:

Teniendo en cuenta la orientación especificada, el MRP debe sujetarse en un extremo y dejarse mover libremente en el borde opuesto.

Configure el aparato para imponer una desviación máxima en la línea central b0 + 20 mm, o una fuerza máxima aplicada de 40 N (lo que ocurra primero).

Flexione el libro 1000 veces a 0,5 Hz (orientación = lomo).

Flexione el libro 1000 veces a 0,5 Hz (orientación = arriba).

Criterios

Evaluación funcional:	las muestras deberán cumplir con los requisitos de [R90] (ver 8.1).
Evaluación de daños físicos:	las muestras deberán cumplir con los requisitos de [R90] (ver 8.2).
Evaluación de la deformación de la página de datos:	las muestras deberán cumplir con los requisitos de [R90] (ver 8.5).
Evaluación de deformación de libros:	las muestras deberán cumplir con los requisitos de [R90] (ver 8.6).

Muestra	Solicitud funcionalidad	Físico daño	Página de datos Deformación (mm)	Deformación del libro (mm)	Frecuencia de resonancia (antes/después en MHz)
4P497	APROBADA	APROBADA	APROBADA	APROBADA	0% (16,60/16,65)
5P497	APROBADA	APROBADA	APROBADA	APROBADA	0% (16,70/16,65)
6P497	APROBADA	APROBADA	APROBADA	APROBADA	0% (16,65/16,65)

Nota

Estas muestras han realizado previamente la prueba de ciclado térmico.

11 TÉRMINOS Y CONDICIONES

Descargo de responsabilidad:

Este informe de prueba contiene únicamente información sobre las muestras analizadas. No constituye una garantía de la producción completa del producto.

Este informe de prueba no constituye una aprobación oficial por parte de la autoridad de pruebas.

Compromiso:

Certificamos que los resultados incluidos en este informe de prueba son los resultados precisos de las pruebas realizadas en las muestras analizadas.

Las pruebas se realizan en un banco de pruebas calificado y aceptado en el momento de la sesión de prueba.

Prosperidad intelectual:

Consulte las Condiciones Generales de Venta y Suministro que se entregan junto con el presupuesto.

Almacenamiento:

Los resultados de las pruebas se conservan durante 10 años en el laboratorio de pruebas.

Las muestras se gestionan según solicitud del cliente.

Procedimiento de reclamación:

El laboratorio cuenta con una política y procedimientos adecuados para la resolución de quejas de clientes u otras partes. Este procedimiento incluye una investigación y acciones correctivas si se confirma el problema. Se puede enviar un correo electrónico directamente al servicio de calidad a qualite@fime.com . Este procedimiento está disponible a pedido.

----------FIN DEL DOCUMENTO----------

Traducido a petición de la parte interesada y registrada en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Once (11)días del mes de Febrero del año Dos Mil Veinticinco (2025).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

S.C.S / DPE
5184-12-8-96

Carta jurada de realización de Prueba ISO 18745-1 Resistencia

SELP

Paris, 13 de junio del 2024

Junta Electoral Central

Ref: JCE-CCC-LPI-2024-0001 "Pliego de Condiciones especificas destinado a la contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)"

A quien corresponda:

Por la presente certifico que la empresa SELP S.A.S. llevó a cabo, a través del laboratorio externo internacional Fime, pruebas conforme al estándar ISO 18745-1. Anexo encontrarán el documento que describe dichas pruebas, así como los resultados obtenidos.

Atentamente,

Bastien Blanc
Representante
SELP S.A.S.

SELP SAS
187 Allée des Plagnes
24340 MAREUIL-EN-PERIGORD
Tél. : 05 53 60 84 44 - Fax : 05 53 60 84 45
SIRET : 351 667 928 00011

Me François MILLIER
Notaire à Paris, soussigné
Certifie la signature de
M. BLANC
apposée ci-dessus

COPY SOLUTIONS INTERNATIONAL, SA
CSI
RNC: 101898852
Santo Domingo, R.D.

APOSTILLE

(Convention de La Haye du 5 octobre 1961)

1. *République française*

REPUBLIQUE DOMINICAINE

Le présent acte public

2. a été signé par **Me**

3. agissant en qualité de **Notaire**

4. est revêtu du sceau /timbre de **Son étude**

Atteste

5. à Paris

6. le 19 JUIN 2024

7. par le Procureur général près la Cour d'appel de Paris

8. sous le n° 19 37 C

9. Signature

SYLVIE SCHLANGER
AVOCAT GENERAL

COUR D'APPEL DE PARIS

"L'apostille atteste seulement l'authenticité de la signature, du sceau ou timbre dont le document. Elle ne signifie pas que le contenu du document est correct ou que la République française approuve son contenu."

TRADUCCIÓN OFICIAL: Carta jurada de realización de Prueba ISO 18745-1 Resistencia

Yo **LIC. SANTO C. SIERRA,** intérprete judicial, debidamente juramentada para el ejercicio de mis funciones **CERTIFICO** que he procedido a traducir las partes centrales de un documento escrito originalmente en Francés, cuya versión en idioma Español de acuerdo a mí mejor el conocimiento es el siguiente:

LIC. SANTO C. SIERRA
Intérprete Judicial Juzg. 1ra Instancia D.N.
SANTO DOMINGO, R.D.

SELP

Paris, 13 de junio del 2024

Junta Electoral Central

Ref: JCE-CCC-LPI-2024-0001 "Pliego de Condiciones específicas destinado a la contratación de la empresa que se encargará de suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)"

COPYSCAN INTERNATIONAL, S.A. RNC: 101890852 Santo Domingo, R.D.

A quien corresponda:

Por la presente certifico que la empresa SELP S.A.S. llevó a cabo, a través del laboratorio externo internacional Fime, pruebas conforme al estándar ISO 18745-1. Anexo encontrarán el documento que describe dichas pruebas, así como los resultados obtenidos.

Atentamente,

Bastien Blanc
representante
SELP S.A.S.

SELP SAS
187 Avenida de las Plagnes
24340 MAREUIL-EN-PERIGORD
Tél.: 05 53 60 84 44 - Fax: 05 53 60 84 45
SIRET 351 667 928 00011

Sr. François MILLIER
Notario de París, abajo firmante
Certifica la firma de
M.BLANG
pegado arriba

APOSTILLA

(Convenio de La Haya del 5 de octubre de 1961)

1. República Francesa

REPUBLICA DOMINICANA

El presente acto público

2. ha sido firmado por: Me MILLER

3. actuando en calidad de: Notario

4. está revestido del sello estampado de: Su despacho

Atestiguado

5. en París

6. el 19 JUN 2023

7. por el Procurador General ante la Corte de Apelación de París

Sello

8. Nosotros

9. Sello

10. Firma

SYLVIE SCHLANGER

ABOGADA GENERAL

Sello en el documento. No significa que el contenido del documento sea "La Apostilla sólo confirma la autenticidad de la firma, el significado o corrección o que la República Francesa aprueba su contenido".

Traducido a petición de la parte interesada y registrada en mi protocolo en Santo Domingo, Distrito Nacional, Capital de la República Dominicana, a los Veintitrés (23) días del mes de Octubre del año Dos Mil Veinticuatro (2024).

LIC. SANTO C. SIERRA
INTERPRETE JUDICIAL
HELP

S.C.S / DPE
5184-12-8-96

Certificaciones ISO del Fabricante de las Impresoras, el Mobile ID y el PKI

ISO 18013 para iOS

fime

Global Enterprise Technologies Corp
230 2nd Avenue, Waltham, Massachusetts, 02451, USA

15th November 2024

Subject: Confirmation of conformity of iOS-based mDL - GET Mobile ID, v.5.4.8 with ISO/IEC 18013-5:2021

Dear Mr. Alexander,

This letter serves to confirm the conformity of the abovementioned mDL application ('the application') to ISO/IEC 18013-5:2021.

FIME tested v.5.5.1(13) of this mDL application in January 2023 and found it to be compliant with this standard. The test scope included testing the application on its interface to an mDL reader, by executing the test cases listed in the latest draft version of ISO/IEC 18013-6. Testing was limited to the features supported by the application, as indicated in the Implementation Conformance Statement in the Appendix to this letter. Details of the application under test, the test environment, and the test devices used for testing can be found on the next page. The number of the Test Report containing the full overview of executed test cases and all test results is UL_eID_GET_iOS_003.

In August 2024, GET provided Fime with release notes describing the changes between the tested version 5.4.8 and version 5.5.1(13). After reviewing these release notes, FIME concluded there is no need for re-testing version 5.4.8 since the described changes are not likely to impact the conformity to ISO/IEC 18013-5.

As a reminder, the correct functioning of the application is dependent on several factors in its operational environment. GET Group is solely and fully responsible for the conformity of the application to all applicable standards, specifications, and requirements.

This confirmation letter is valid for one year from the date of issuance.

Yours sincerely,

FIME

David Bakker
Technical Lead

Página/Folio No.748 de 843

mDL implementation scope

System Under Test

Application name and version	mDL - GET Mobile ID, v.5.5.1 (13)
Operating System	iOS
Application available through	TestFlight
Date of receipt of application	2023-01-09
Certification Type	Integrated Product Certification
Issuing Authority	Utah Driver License Division

Implementation Conformance Statement Summary

Device engagement technologies	QR code
Device retrieval technologies	BLE in mdoc central client mode BLE in mdoc peripheral server mode
Server retrieval technologies	WebAPI, OIDC
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc authentication, mdoc reader authentication

Test Environment

Standard	ISO/IEC 18013-5:2021
Test Case Specification	FIME mDL Test Case Specification
Test Suite	UL mDL Application Test Suite v1.1.12
mDL Test App	mdltestapp-1.1.4
Test device on which the mDL Test App is installed	Google Pixel 3a
OS version of the test device on which the mDL Test App is installed	Android 12

Test Devices and Platform

Device brand and type	iPhone 13	iPhone SE (2nd Gen)
OS version	iOS 16.2	iOS 13.5.1

Página/Folio No.749 de 843

A.1 Implementation conformance statement

The Implementation Conformance Statements below were provided to FIME by GET Group and have been used to determine which test cases to execute.

The ICS version used by GET Group is v1.5.

A.1.1 General information

mDL owner	
Application owner Name	GET Group
Address	230 2nd Avenue
City	Waltham
State	MA
Zip Code / Postal Code	02451
Country	USA
Contact Name	Alexander Kambanis
Contact Title	Managing Director
Contact Email Address	akambanis@getgroupna.com
Contact Phone Number	+1 (617) 901-1700

Issuing Authority General Information (Applicable for Integrated Product Certification Only)	
Issuing Authority Name	Utah Department of Public Safety, Driver License Division
Issuing Authority Address	Utah Department of Public Safety
City	Salt Lake City
State	Utah
Zip Code / Postal Code	84114-4501
Country	USA
Contact Name	Brittaney Akagi
Contact Title	IT / Quality Assurance Manager
Contact Email Address	bakagi@utah.gov

mDL Application General Information	
Certification Type	☐ Functional[1] ☒ Integrated Product[2]
Application name and version	GET Mobile ID, v.5.5.1 (13)
The minimum version of iOS supported	13.4
How many documents are present on the mDL under test?	1

[1] For functional certification, the mDL data set can be a sample data set that the mDL owner would like to personalize onto the mDL.

[2] Integrated product certification requires the mDL data set to be prepared and personalized by an Issuer System of Record (SoR) and the mDL data set shall be a representative of the mDL that will be used in production.

Página/Folio No.750 de 843

For each document, please specify the applicable DocType	org.iso.18013.5.1.mDL
For each document, please specify all data element namespaces used by the document	org.iso.18013.5.1, com.scytales.18013.5.1, org.aamva.us, org.iso.18013.5.1.aamva

For each namespace different from the mDL namespace ("org.iso.18013.5.1"), please specify the identifiers of all data elements present in the document	{
	"org.iso.18013.5.1.mDL" : {
	"com.scytales.18013.5.1" : [
	"status",
	"vehicle_category",
	"vehicle_category_list",
	"full_address",
	"email",
	"mobile_number"
	],
	"org.aamva.us" : [
	"real_id"
	],
	"org.iso.18013.5.1.aamva" : [
	"DHS_compliance"
	]
	}
	}

A.1.2 For mdl data model test cases

Note: all the data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

#	ICS statements for mDL Data Model test cases [3]	
1.	Data element administrative_number is present in the mDL data.	☒YES ☐NO
2.	Data element sex is present in the mDL data.	☒YES ☐NO
3.	Data element height is present in the mDL data.	☒YES ☐NO
4.	Data element weight is present in the mDL data.	☒YES ☐NO

[3] Note: all of the data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

Página/Folio No.751 de 843

5.	Data element eye_color is present in the mDL data.	☒YES ☐NO
6.	Data element hair_color is present in the mDL data.	☒YES ☐NO
7.	Data element birth_place is present in the mDL data.	☒YES ☐NO
8.	Data element resident_address is present in the mDL data.	☒YES ☐NO
9.	Data element portrait_capture_date is present in the mDL data.	☒YES ☐NO
10.	Data element age_in_years is present in the mDL data.	☒YES ☐NO
11.	Data element age_birth_year is present in the mDL data.	☒YES ☐NO
12.	Data element age_over_NN is present in the mDL data. In case you select YES, please provision the following age_over_NN data elements in the mDL data with the corresponding values (TRUE / FALSE) during personalization.	☒YES ☐NO
	NN	**Return Value**
	age_over_15	TRUE
	age_over_18	TRUE
	age_over_21	TRUE
	age_over_60	FALSE
	age_over_65	FALSE
	age_over_68	FALSE
13.	Data element issuing_jurisdiction is present in the mDL data.	☒YES ☐NO
14.	Data element nationality is present in the mDL data.	☒YES ☐NO
15.	Data element resident_city is present in the mDL data.	☒YES ☐NO
16.	Data element resident_state is present in the mDL data.	☒YES ☐NO
17.	Data element resident_postal_code is present in the mDL data.	☒YES ☐NO
18.	Data element resident_country is present in the mDL data.	☒YES ☐NO
19.	Data element biometric_template_face is present in the mDL data.	☐YES ☒NO

Página/Folio No.752 de 843

20.	Data element biometric_template_voice is present in the mDL data.	☐YES ☒NO
21.	Data element biometric_template_finger is present in the mDL data.	☐YES ☒NO
22.	Data element biometric_template_iris is present in the mDL data.	☐YES ☒NO
23.	Data element biometric_template_retina is present in the mDL data.	☐YES ☒NO
24.	Data element biometric_template_hand_geometry is present in the mDL data.	☐YES ☒NO
25.	Data element biometric_template_signature_sign is present in the mDL data.	☐YES ☒NO
26.	Data element biometric_template_keystroke is present in the mDL data.	☐YES ☒NO
27.	Data element biometric_template_lip_movement is present in the mDL data.	☐YES ☒NO
28.	Data element biometric_template_thermal_face is present in the mDL data.	☐YES ☒NO
29.	Data element biometric_template_thermal_hand is present in the mDL data.	☐YES ☒NO
30.	Data element biometric_template_gait is present in the mDL data.	☐YES ☒NO
31.	Data element biometric_template_body_odor is present in the mDL data.	☐YES ☒NO
32.	Data element biometric_template_dna is present in the mDL data.	☐YES ☒NO
33.	Data element biometric_template_ear is present in the mDL data.	☐YES ☒NO
34.	Data element biometric_template_finger_geometry is present in the mDL data.	☐YES ☒NO
35.	Data element biometric_template_palm_geometry is present in the mDL data.	☐YES ☒NO
36.	Data element biometric_template_vein_pattern is present in the mDL data.	☐YES ☒NO
37.	Data element biometric_template_foot_print is present in the mDL data.	☐YES ☒NO
38.	Data element family_name_national_character is present in the mDL data.	☒YES ☐NO

Página/Folio No.753 de 843

39.	Data element given_name_national_character is present in the mDL data.	☒YES ☐NO
40.	Data element signature_usual_mark is present in the mDL data.	☒YES ☐NO

COPY SOLUTIONS INTERNATIONAL S.A. RNC 101008852 Santo Domingo, R.D.

A.1.3 For technology test cases

#	ICS statements for Technology test cases	
41.	mDL supports device engagement using NFC Static Handover	☐YES ☒NO
42.	mDL supports device engagement using NFC Negotiated Handover [4]	☐YES ☒NO
43.	mDL supports device engagement using QR code	☒YES ☐NO
44.	mDL supports device retrieval using NFC	☐YES ☒NO
45.	mDL supports extended-length APDUs for device retrieval using NFC	☐YES ☒NO
46.	mDL supports BLE version 4.2 (or above) and LE Data Packet Length Extension	☒YES ☐NO
47.	mDL supports device retrieval using BLE in mdoc central client mode	☒YES ☐NO
48.	If BLE in mdoc central client mode is used for device retrieval, mdoc verifies the value of the Ident characteristic	☒YES ☐NO
49.	mDL supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE	☐YES ☒NO
50.	mDL supports device retrieval using BLE in mdoc peripheral server mode	☒YES ☐NO
51.	mDL supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE	☐YES ☒NO
52.	mDL supports device retrieval using Wi-Fi Aware	☐YES ☒NO
53.	mDL supports the NCS-PK-2WDH-128 cipher suite for Wi-Fi Aware [5]	☐YES ☒NO

[4] Note that NFC Static Handover and NFC Negotiated Handover cannot be supported simultaneously if an mDL supports both technologies

[5] Only applicable in case the mdoc supports Wi-Fi Aware for device retrieval and supports NFC Negotiated Handover for device engagement.

54.	mDL supports server retrieval using OIDC	☒YES ☐NO
55.	mDL supports server retrieval using WebAPI	☒YES ☐NO
56.	mDL supports transferring server retrieval information in the device engagement structure	☒YES ☐NO
57.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message	☐YES ☒NO
58.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	

A.1.4 For security mechanism test cases

	ICS statements for Security Mechanisms test cases	
59.	Which curves does the mDL support for session establishment? Tick all that are supported.[6]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
60.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	☐YES ☒NO
61.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	
62.	Which curves does the mDL issuing authority support for issuer data authentication? Tick all that are supported.[7]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

[6] If the mDL supports multiple curves for session establishment, then for the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.
[7] If multiple documents are present on the mDL, the issuing authority can in theory use a different curve for signing the MSO on each of them. However, please note that UL expects the same curve to be used

Página/Folio No.755 de 843

63.	The mDL supports mdoc MAC authentication.	☒YES ☐NO
64.	If yes, which curves does the mDL support for mdoc MAC authentication? Tick all that are supported [8]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
65.	The mDL supports mdoc ECDSA/EdDSA authentication	☒YES ☐NO
66.	If yes, which curves does the mDL use for mdoc ECDSA/EdDSA authentication? Tick all that are supported [9]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
67.	The mDL supports mdoc reader authentication	☒YES ☐NO

for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

[8] If multiple documents are present on the mDL, the mDL can, in theory, use a different mdoc MAC authentication curve for each of them. However, please note that UL expects the same curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

[9] Note that for each document on an mDL, there could potentially be multiple SDeviceKey pairs for mdoc authentication, each in a separate MSO. It is therefore theoretically possible that a single document uses MAC authentication and ECDSA/EdDSA authentication alternatingly or uses different curves for ECDSA/EdDSA alternatingly. However, please note that UL expects that the same mdoc authentication mechanism (either MAC or ECDSA/EdDSA) is consistently used for all documents on a given sample. Moreover, UL expects that the same ECDSA/EdDSA curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

Página/Folio No.756 de 843

68.	If yes, which curves does the mdoc support for mdoc reader authentication? Tick all that are supported[10].	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

69.	If yes, for which data elements is successful reader authentication required before the mdoc will release them[11]	{
		"org.iso.18013.5.1.mDL" : {
		"org.iso.18013.5.1" : [
		"administrative_number",
		"sex",
		"weight",
		"eye_colour",
		"hair_colour",
		"birth_place",
		"resident_address",
		"portrait_capture_date",
		"age_in_years",
		"age_birth_year",
		"age_over_15",
		"age_over_18",
		"age_over_21",
		"age_over_60",
		"age_over_65",
		"age_over_68",
		"issuing_jurisdiction",
		"nationality",
		"resident_city",
		"resident_state",
		"resident_postal_code",
		"resident_country",
		"family_name_national_character",
		"given_name_national_character",
		"signature_usual_mark
		]}}

70.	If yes, mdoc supports retrieving OCSP information, if available, when verifying a mdoc reader authentication certificate.	☐YES ☒NO

[10] UL assumes that all mDL samples provided to us will support all of the mdoc reader authentication curves selected (provided that the correct CA certificates are installed).

[11] UL assumes that if mdoc reader authentication is supported, there is at least one data element that will not be released if mdoc reader authentication is not performed or fails.

Página/Folio No.757 de 843

A.1.5 For use case test cases

#	ICS statements for Use Case test cases	
71.	The mDL allows the mDL holder to refuse consent for sharing the portrait data element if requested by the reader	☐YES ☒NO

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC: 10[illegible]2

TRADUCCIÓN OFICIAL: ISO 18013 para iOS

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membrete de FIME Services North America Inc., domiciliado en 1945 The Exchange, Suite 200 SE, Atlanta, GA 30339, Estados Unidos de América

Global Enterprise Technologies Corp
230 2nd Avenue, Waltham, Massachusetts, 02451, E.U.A.

15 de noviembre de 2024

Asunto: Confirmación de Conformidad de mDL basado en iOS - GET Mobile ID, v.5.4.8 con ISO/IEC 18013-5:2021

Estimado Sr. Alexander:

Esta carta sirve para confirmar la conformidad de la aplicación mDL mencionada más arriba ('la aplicación') con ISO/IEC 18013-5:2021.

FIME probó la versión v.5.5.1(13) de esta aplicación mDL en enero de 2023 y determinó que cumple con esta norma. El alcance de la prueba incluyó probar la aplicación en su interface con un lector mDL, ejecutando los casos de prueba enumerados en la última versión preliminar de ISO/IEC 18013-6. Las pruebas se limitaron a las características admitidas por la aplicación, como se indica en la Declaración de Conformidad de Implementación en el Apéndice de esta carta. Los detalles de la aplicación bajo prueba, el entorno de prueba y los dispositivos de prueba utilizados para la misma se pueden encontrar en la página siguiente. El número del Informe de Prueba que contiene la descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas es UL_eID_GET_iOS_003.

En agosto de 2024, GET proporcionó a Fime notas de la versión que describen los cambios entre la versión 5.4.8 probada y la versión 5.5.1(13). Después de revisar esas notas de la versión, FIME concluyó que no es necesario volver a probar la versión 5.4.8, ya que es poco probable que los cambios descritos afecten la conformidad con la norma ISO/IEC 18013-5.

Como recordatorio, el correcto funcionamiento de la aplicación depende de varios factores de su entorno operativo. GET Group es el único y total responsable de la conformidad de la aplicación con todas las normas, especificaciones y requisitos aplicables.

Esta carta de confirmación es válida por un año a partir de su fecha de emisión.

De ustedes sinceramente,
Firma ilegible
FIME
David Bakker
Líder Técnico

Alcance Implementación mDL

Sistema bajo Prueba

Nombre y Versión Aplicación	mDL – GET Mobile ID, v.5.5.1 (13)
Sistema Operacional	iOS
Aplicación disponible a través	Prueba de Vuelo
Fecha de Recibo Aplicación	2023-01-09
Tipo Certificación	Certificación Integrada del Producto
Autoridad Emisora	División Licencias de Conducir de Utah

Resumen Declaración de Conformidad de la Implementación

Tecnologías Interacción con Dispositivos	Código QR
Tecnologías Recuperación de Dispositivos	BLE en mdoc modo cliente central BLE en mdoc modo servidor periférico
Tecnologías Recuperación de Servidores	WebAPI, OIDC
Mecanismos Seguridad para la Recuperación Dispositivos	Cifrado de sesión, autenticación de datos del emisor, autenticación mdoc, autenticación del lector mdoc

Ambiente de la Prueba

Estándar	ISO/IEC 1803-5:2021
Especificación Caso Prueba	Especificación Caso Prueba FIME mDL
Conjunto de Pruebas	Conjunto Prueba v1.1.12 Aplicación UL mDL
Aplicación Prueba mDL	Mdltestapp-1.1.4
Dispositivo de Prueba donde se instala la Aplicación Prueba mDL	Google Pixel 3ª
Versión OS del Dispositivo de Prueba donde se instala la Aplicación de Prueba mDL	Android 12

Dispositivos y Plataforma de la Prueba

Marca y Tipo Dispositivo	Iphone 13	iPhone SE (2da. Generación)
Versión OS	iOS 16.2	iOS 13 5.1

A.1 Resumen Declaración de Conformidad de la Implementación

Las Declaraciones de Conformidad de la Implementación que aparecen más adelante fueron proporcionadas a FIME por el Grupo GET y se han usado para determinar qué casos de prueba se deben ejecutar.

La versión de ICS que utiliza el Grupo GET es la v1.5.

A.1.1 Información General

Propietario mDL	
Nombre Propietario de la Aplicación	GET Group
Dirección	230 2da Avenue
Ciudad	Waltham
Estado	MA
Código Postal	02451
País	EUA
Nombre del Contacto	Alexander Kambanis
Título del Contado	Director Gerente
Dirección correo electrónico de Contacto	akambanis@oelgroupna.com
Número de teléfono del Contacto	+1 (617) 901-1700

Información General Autoridad Emisora (Aplicable únicamente a la Certificación del Producto Integrada)	
Nombre Autoridad Emisora	Departamento de Seguridad Pública de Utah, División Licencia de Conducir
Dirección Autoridad Emisora	Departamento de Seguridad Pública de Utah
Ciudad	Ciudad Salt Lake
Estado	Utah
Código Postal	84114-4501
País	EUA
Nombre del Contacto	Brittaney Akagi
Título del Contado	IT / Gerente Aseguramiento de Calidad
Dirección correo electrónico de Contacto	bakagi@utah.gov

Información General Aplicación mDL	
Tipo Certificación	☐Funcional[1] ☒Producto Integrado[2]
Nombre y Versión de la Aplicación	GET Mobile ID, v. 5.5.1 (13)
La versión mínima de soporte iOS	13.4
¿Cuántos documentos están presentes en la prueba mDL?	1

Para cada documento, por favor especifique el DocType [Tipo de Documento] que aplique	org.iso.18013.5.1.mDL
Para cada documento, por favor especifique todos los espacios de nombres de los elementos usados en el documento.	org.iso.18013.5.1, com.scytales.18013.5.1, org.aamva.us, org.iso.18013.5.1.aamva
Para cada espacio de nombres diferente del nombre del espacio mDL ("org.iso.18013.5.1"), por favor, especifique los identificadores de todos los datos de los elementos presentes en el documento.	{ "org.iso.18013.5.1.mDL" : { "com.scytales.18013.5.1" : ["status", "categoria_vehiculo", "lista_categoria_vehiculo", "dirección_completa", "e-mail", "número_móvil"], "org.aamva.us" : ["real_id"], "org.iso.18013.5.1.aamva" : ["DHS_compliance"] } }

A.1.2 Modelo de Datos mDL para casos de prueba

Nota: todos los elementos de datos de esta sección se encuentran en el espacio predeterminado de nombres de datos mDL ("org.iso.18013.5.1"). Las declaraciones ICS de esta sección deben completarse solo para documentos que tengan DocType = "org.iso.18013.5.1.mDL".

[1] Para la certificación funcional, el conjunto de datos mDL puede ser un conjunto de datos de muestra que el propietario del mDL desea personalizar en el mDL.

[2] La certificación integrada de productos requiere que el conjunto de datos mDL sea preparado y personalizado por un Sistema de registro (SoR) del emisor y el conjunto de datos mDL debe ser representativo del mDL que se utilizará en producción

#	Declaraciones ICS para los casos de prueba del Modelo de Datos mDL[1]	
1.	El elemento de datos número_administrativo está presente en los datos mDL.	☒Si ☐No
2.	El elemento de datos sexo_ está presente en los datos mDL.	☒Si ☐No
3.	El elemento de datos altura_ está presente en los datos mDL.	☒Si ☐No
4.	El elemento de datos peso_ está presente en los datos mDL	☒Si ☐No
5.	El elemento de datos color de ojos_ está presente en los datos mDL	☒Si ☐No
6.	El elemento de datos color de pelo_ está presente en los datos mDL	☒Si ☐No
7.	El elemento de datos lugar de nacimiento_ está presente en los datos mDL	☒Si ☐No
8.	El elemento de datos dirección de residencia_ está presente en los datos mDL	☒Si ☐No
9.	El elemento de datos captura de imagen_ está presente en los datos mDL	☒Si ☐No
10.	El elemento de datos edad en años_ está presente en los datos mDL	☒Si ☐No
11.	El elemento de datos edad_año de nacimiento_ está presente en los datos mDL	☒Si ☐No
12.	El elemento de datos edad_mayor de_NN está presente en los datos mDL En caso de seleccionar SI, favor dar los elementos de datos edad_mayor de_NN en los datos mDL con su correspondiente valor (VERDADERO/FALSO) durante la personalización	☒Si ☐No
	NN	Valor Retorno
	Edad_mayor de_15	Verdadero
	Edad_mayor de_18	Verdadero
	Edad_mayor de_21	Verdadero
	Edad_mayor de_60	Falso
	Edad_mayor de_65	Falso
	Edad_mayor de_68	Falso
13.	El elemento de datos jurisdicción_emisora_ está presente en los datos mDL	☒Si ☐No
14.	El elemento de datos nacionalidad_ está presente en los datos mDL	☒Si ☐No
15.	El elemento de datos ciudad_de residencia_ está presente en los datos mDL	☒Si ☐No
16.	El elemento de datos estado_de residencia_ está presente en los datos mDL	☒Si ☐No
17.	El elemento de datos código_postal_de residencia_ está presente en los datos mDL	☒Si ☐No
18.	El elemento de datos país_ de residencia_está presente en los datos mDL	☒Si ☐No
19.	El elemento de datos plantilla_biométrica_cara_ está presente en los datos mDL	☒Si ☐No
20.	El elemento de datos plantilla_biométrica_voz_ está presente en los datos mDL	☒Si ☐No
21.	El elemento de datos plantilla_biométrica_dedo_ está presente en los datos mDL	☒Si ☐No
22.	El elemento de datos plantilla_biométrica_iris_ está presente en los datos mDL	☒Si ☐No
23.	El elemento de datos plantilla_biométrica_retina_ está presente en los datos mDL	☒Si ☐No
24.	El elemento de datos plantilla_biométrica_mano_ geométrica está presente en los datos mDL	☒Si ☐No
25.	El elemento de datos plantilla_biométrica_firma_ está presente en los datos mDL	☒Si ☐No
26.	El elemento de datos plantilla_biométrica_ pulsación de teclas_ está presente en los datos mDL	☒Si ☐No
27.	El elemento de datos plantilla_biométrica_movimiento de labios_ está presente en los datos mDL	☒Si ☐No
28.	El elemento de datos plantilla_biométrica_cara_térmica_ está presente en los datos mDL	☒Si ☐No
29.	El elemento de datos plantilla_biométrica_mano_térmica_ está presente en los datos mDL	☒Si ☐No
30.	El elemento de datos plantilla_biométrica_pasos_ está presente en los datos mDL	☒Si ☐No
31.	El elemento de datos plantilla_biométrica_olor_corporal_ está presente en los datos mDL	☒Si ☐No
32.	El elemento de datos plantilla_biométrica_adn_ está presente en los datos mDL	☒Si ☐No
33.	El elemento de datos plantilla_biométrica_oído_ está presente en los datos mDL	☒Si ☐No
34.	El elemento de datos plantilla_biométrica_geometría_dedo_ está presente en los datos mDL	☒Si ☐No
35.	El elemento de datos plantilla_biométrica_geometría_palma manos_ está presente en los datos mDL	☒Si ☐No

[1] Nota: todos los elementos de datos de esta sección se encuentran en el espacio predeterminado de datos mDL ("org.iso.18013.5.1"). Las declaraciones ICS de esta sección deben completarse solo para documentos que tengan DocType = "org.iso.18013.5.1.mDL".

36.	El elemento de datos plantilla_biométrica_patrón_venas_ está presente en los datos mDL	☒Si ☐No
37.	El elemento de datos plantilla_biométrica_huella_pié_ está presente en los datos mDL	☒Si ☐No
38.	El elemento de datos apellido_carácter_nacional_ está presente en los datos mDL	☒Si ☐No
39.	El elemento de datos nombre_carácter_nacional_ está presente en los datos mDL	☒Si ☐No
40.	El elemento de datos marca_usual_firma_ está presente en los datos mDL	☒Si ☐No

A.1.3. Para Casos de Prueba de Tecnología

#	Declaraciones ICS para los casos de prueba de Tecnología	
41.	mDL admite interacción con el dispositivo usando NFC Static Handover	☐Si ☒No
42.	mDL admite interacción con el dispositivo usando NFC Negotiated Handover[4]	☐Si ☒No
43.	mDL admite interacción con el dispositivo usando Código QR	☒Si ☐No
44.	mDL admite recuperación del dispositivo usando NFC	☐Si ☒No
45.	mDL admite APDU de longitud extendida para la recuperación del dispositivo usando NFC	☐Si ☒No
46.	mDL admite BLE versión 4.2 (o la que antecede) y Paquete de Datos LE de longitud extendida	☒Si ☐No
47.	mDL admite recuperación del dispositivo usando BLE modo cliente central	☒Si ☐No
48.	Si utiliza BLE en modo cliente central para la recuperación de dispositivos, verifique el valor de la característica Ident	☒Si ☐No
49.	mDL admite el perfil de transmisión L2CAP si actúa como cliente GATT para la recuperación del dispositivo usando BLE	☐Si ☒No
50.	mDL admite recuperación de dispositivos usando BLE en modo de servidor periférico	☒Si ☐No
51.	mDL admite el perfil de transmisión L2CAP si actúa como servidor GATT para la recuperación del dispositivo usando BLE	☐Si ☒No
52.	mDL admite recuperación del dispositivo usando Wi-Fi Aware	☐Si ☒No
53.	mDL admite el conjunto cifrado NCS-PK-2WDH-128 para Wi-Fi Aware[5]	☐Si ☒No
54.	mDL admite la recuperación del servidor usando OIDC	☒Si ☐No
55.	mDL admite la recuperación del servidor usando WebAPI	☒Si ☐No
56.	mDL admite la transferencia de información de recuperación desde la estructura de interacción del dispositivo	☒Si ☐No
57.	mDL implementa un tiempo de espera entre el tiempo de envío de datos de interacción del dispositivo y establecimiento de la recepción del mensaje	☐Si ☒No
58.	En caso afirmativo, ¿cuántos segundos es el período de espera para la finalización de la sesión implementada por el mDL?	

A.1.4 Para Casos de Prueba de los Mecanismos de Seguridad

	Declaraciones ICS para los casos de prueba de los Mecanismos de Seguridad	
59.	¿Cuáles curvas admite mDL para el establecimiento de sesiones? Marque todas las compatibles.[6]	☒Curva P-256 ☐Curva P-384 ☐Curva P-521 ☐X25519 ☐X448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
60.	mDL admite el intercambio de más de una solicitud y respuesta de mDOC para la recuperación del dispositivo con el lector mDOCen una sola sesión.	☐Si ☒No

[4] Tenga en cuenta que la transferencia NFC Static Handover y NFC Negotiated Handover no se pueden admitir simultáneamente si un mDL admite ambas tecnologías

[5] Solo se aplica en caso de que el mDOC admita Wi-Fi Aware para la recuperación del dispositivo y admita NFC Negotiated Handover para la interacción con el dispositivo

[6] Si mDL admite varias curvas para el establecimiento de sesiones, entonces, a los efectos de la prueba, el propietario de mDL debe proporcionar una muestra separada para cada una de las curvas admitidas

61.	Si es afirmativo, ¿cuántos segundos es el periodo de espera para la finalización de la sesión implementada por mDL?	
62.	¿Cuáles curvas admite la autoridad emisora mDL para la autenticación de los datos del emisor? Marque todas las compatibles[7]	☒Curva P-256 ☐Curva P-384 ☐Curva P-521 ☐Ed25519 ☐Ed448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
63.	El mDL admite la autenticación MAC de mDOC	☒Si ☐No
64.	Si afirmativo, ¿cuáles curvas admite el mDL para la autenticación MAC de mDOC? Marque todas las compatibles[8]	☒Curva P-256 ☐Curva P-384 ☐Curva P-521 ☐X25519 ☐X448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
65.	El mDL admite la autenticación ECDSA/EdDSA de mDOC	☒Si ☐No
66.	Si es así, ¿cuáles curvas utiliza el mDL para la autenticación ECDSA/EdDSA de mDOC? Marque todas las compatibles[9]	☒Curva P-256 ☐Curva P-384 ☐Curva P-521 ☐Ed25519 ☐Ed448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
67.	El mDL admite la autenticación de lectores mDOC	☒Si ☐No
68.	Si afirmativo, ¿cuáles curvas admite el mDOC para la autenticación del lector mDOC? Marque todas las compatibles[10]	☒Curva P-256 ☒Curva P-384 ☒Curva P-521 ☐Ed25519 ☐Ed448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
69.	Si es así, ¿para qué elementos de datos se requiere una autenticación	(

[7] Si hay varios documentos en la mDL, la autoridad emisora puede, en teoría, utilizar una curva diferente para firmar la MSO de cada uno de ellos. Sin embargo, tenga en cuenta que UL espera que se utilice la misma curva para todos los documentos de la muestra dada. Para pruebas, el propietario del mDL debe proveer una muestra independiente para cada una de las curvas admitidas.

[8] Si hay varios documentos en el mDL, el mDL puede, en teoría, utilizar una curva de autenticación MAC de mDOC diferente para cada uno de ellos. Sin embargo, tenga en cuenta que UL espera que se utilice la misma curva para todos los documentos de la muestra dada. Para pruebas, el propietario del mDL debe proveer una muestra independiente para cada una de las curvas admitidas.

[9] Tenga en cuenta que para cada documento de un mDL, podría haber varios pares de SDeviceKey para la autenticación mDOC, cada uno en un MSO independiente. Por tanto, es teóricamente posible que un solo documento utilice la autenticación MAC y la autenticación ECDSA/EdDSA de forma alternada o utilice diferentes curvas para ECDSA/EdDSA de forma alternada. Sin embargo, tenga en cuenta que UL espera que se utilice de forma constante el mismo mecanismo de autenticación mDOC (MAC o ECDSA/EdDSA) para todos los documentos de una muestra determinada. Además, UL espera que se utilice la misma curva ECDSA/EdDSA para todos los documentos de una muestra determinada. Para realizar pruebas, el propietario del mDL debe proporcionar una muestra independiente para cada una de las curvas admitidas.

[10] UL asume que todas las muestras de mDL que se nos proporcionan admitirán todas las curvas de autenticación de lectores mDOC seleccionadas (siempre que se instalen los correctos certificados CA).

69.	Si es así, ¿para qué elementos de datos se requiere una autenticación exitosa del lector antes de que mDOC los libere?[12]	{ "org.iso.18013.5.1.mDL": { "org.iso.18013.5.1.*": ["número_administrativo" "sexo", "peso", "color_ojos", "color_pelo", "lugar_nacimiento", "dirección_residencia", "fecha_captura_retrato", "edad_en_años", "edad_año_nacimiento", "edad_más de_15", "edad_más de_18", "edad_más de_21", "edad_más de_60", "edad_más de_65", "edad_más de_68", "jurisdicción_emisora", "nacionalidad", "ciudad_residencia", "estado_residencia", "código_postal_residencia", "país_residencia", "apellido_carácter_nacional", "nombre_carácter_nacional" "firma_marca_usual"]}}
70.	En caso afirmativo, mDOC admite la recuperación de la información de OCSP, si disponible, al verificar un certificado de autenticación del lector mDOC	☐Si ☒No

A.1.5 Para uso en los casos de Casos de Pruebas

#	Declaraciones ICS para Uso en los Casos de Casos de Pruebas	
71.	El mDL permite al titular de mDL rechazar el consentimiento para compartir el elemento de datos del retrato, si así lo solicita el lector	☐Si ☒No

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los doce (12) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 208/25.

Ana María Feria

[12] UL asume que si se admite la autenticación de lectores mDOC, hay por lo menos un elemento de datos que no se liberará si la autenticación de lectores mDOC no se realiza o falla.

ISO 18013 para Android

fime

COPY SOLUTIONS INTERNATIONAL, SA
CSI
RNC 101898852
Santo Domingo, R.D.

Global Enterprise Technologies Corp
230 2nd Avenue, Waltham, Massachusetts, 02451, USA

15th November 2024

Subject: Confirmation of conformity of Android-based mDL - GET Mobile ID, v.5.1.23 with ISO/IEC 18013-5:2021

Dear Mr. Alexander,

This letter serves to confirm the conformity of the abovementioned mDL application ('the application') to ISO/IEC 18013-5:2021.

FIME tested v5.5.0 of this mDL application in December 2022 and found it to be compliant with this standard. The test scope included testing the application on its interface to an mDL reader, by executing the test cases listed in the latest draft version of ISO/IEC 18013-6. Testing was limited to the features supported by the application, as indicated in the Implementation Conformance Statement in the Appendix to this letter. Details of the application under test, the test environment, and the test devices used for testing can be found on the next page. The number of the Test Report containing the full overview of executed test cases and all test results is UL_eID_GET Group_Android_002.

In August 2024, GET provided Fime with release notes describing the changes between the tested version 5.5.0 and version 5.1.23. After reviewing these release notes, FIME concluded there is no need for re-testing version 5.1.23, since the described changes are not likely to impact the conformity to ISO/IEC 18013-5.

As a reminder, the correct functioning of the application is dependent on several factors in its operational environment. GET Group is solely and fully responsible for the conformity of the application to all applicable standards, specifications, and requirements.

This confirmation letter is valid for one year from the date of issuance.

Yours sincerely,

FIME

David Bakker
Technical Lead

Página/Folio No.768 de 843

mDL implementation scope

System Under Test

Application name and version	mDL - GET Mobile ID, v.5.5.0
Operating System	Android
Application available through	Android Package File (APK) of the mDL Application was provided by the customer
Date of receipt of application	2022-10-26
Certification Type	Integrated Product Certification
Issuing Authority	Utah Driver License Division

Implementation Conformance Statement Summary

Device engagement technologies	QR code, NFC Static Handover
Device retrieval technologies	BLE in mdoc central client mode BLE in mdoc peripheral server mode NFC, WiFi-Aware[1]
Server retrieval technologies	WebAPI, OIDC
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc authentication, mdoc reader authentication

Test Environment

Standard	ISO/IEC 18013-5:2021
Test Case Specification	FIME mDL Test Case Specification
Test Suite	UL mDL Application Test Suite v1.1.11
mDL Test App	mdltestapp-1.1.4
Test device on which the mDL Test App is installed	Google Pixel 3a
OS version of the test device on which the mDL Test App is installed	Android 12

Test Devices and Platform

Device brand and type	Google Pixel 6	Samsung Galaxy S9
OS version	Android 13	Android 8

[1] Wi-Fi Aware was tested only on the Google Pixel 6 device running Android 13.

Página/Folio No.769 de 843

A.1 Implementation conformance statement

The Implementation Conformance Statements below were provided to FIME by GET Group and have been used to determine which test cases to execute.

The ICS version used by GET Group is v1.5.

A.1.1 General information

mDL owner	
Application owner Name	GET Group
Address	230 2nd Avenue
City	Waltham
State	MA
Zip Code / Postal Code	02451
Country	USA
Contact Name	Alexander Kambanis
Contact Title	Managing Director
Contact Email Address	akambanis@getgroupna.com
Contact Phone Number	+1 (617) 901-1700

Issuing Authority General Information (Applicable for Integrated Product Certification Only)	
Issuing Authority Name	Utah Department of Public Safety, Driver License Division
Issuing Authority Address	Utah Department of Public Safety
City	Salt Lake City
State	Utah
Zip Code / Postal Code	84114-4501
Country	USA
Contact Name	Brittaney Akagi
Contact Title	IT / Quality Assurance Manager
Contact Email Address	bakagi@utah.gov

mDL Application General Information	
Certification Type	☐ Functional[2] ☒ Integrated Product[3]
Application name and version	GET Mobile ID, v.5.5.0
The minimum version of iOS supported	Android 8.0 (API level 26)
How many documents are present on the mDL under test?	1

[2] For functional certification, the mDL data set can be a sample data set that the mDL owner would like to personalize onto the mDL.
[3] Integrated product certification requires the mDL data set to be prepared and personalized by an Issuer System of Record (SoR) and the mDL data set shall be a representative of the mDL that will be used in production.

Página/Folio No.770 de 843

For each document, please specify the applicable DocType	org.iso.18013.5.1.mDL
For each document, please specify all data element namespaces used by the document	org.iso.18013.5.1, com.scytales.18013.5.1, org.aamva.us, org.iso.18013.5.1.aamva

For each namespace different from the mDL namespace ("org.iso.18013.5.1"), please specify the identifiers of all data elements present in the document	[
	"org.iso.18013.5.1.mDL" : {
	"com.scytales.18013.5.1" : [
	"status",
	"vehicle_category",
	"vehicle_category_list",
	"full_address",
	"email",
	"mobile_number"
	],
	"org.aamva.us" : {
	"real_id"
	],
	"org.iso.18013.5.1.aamva" : {
	"DHS_compliance"
	}
	}
	}

A.1.2 For mdl data model test cases

Note: all the data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

#	ICS statements for mDL Data Model test cases [4]	
1.	Data element administrative_number is present in the mDL data.	☒YES ☐NO
2.	Data element sex is present in the mDL data.	☒YES ☐NO
3.	Data element height is present in the mDL data.	☒YES ☐NO
4.	Data element weight is present in the mDL data.	☒YES ☐NO

[4] Note: all of the data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

Página/Folio No.771 de 843

5.	Data element eye_color is present in the mDL data.	☒YES ☐NO
6.	Data element hair_color is present in the mDL data.	☒YES ☐NO
7.	Data element birth_place is present in the mDL data.	☒YES ☐NO
8.	Data element resident_address is present in the mDL data.	☒YES ☐NO
9.	Data element portrait_capture_date is present in the mDL data.	☒YES ☐NO
10.	Data element age_in_years is present in the mDL data.	☒YES ☐NO
11.	Data element age_birth_year is present in the mDL data.	☒YES ☐NO
12.	Data element age_over_NN is present in the mDL data. In case you select YES, please provision the following age_over_NN data elements in the mDL data with the corresponding values (TRUE / FALSE) during personalization.	☒YES ☐NO
	NN	**Return Value**
	age_over_15	TRUE
	age_over_18	TRUE
	age_over_21	TRUE
	age_over_60	FALSE
	age_over_65	FALSE
	age_over_68	FALSE
13.	Data element issuing_jurisdiction is present in the mDL data.	☒YES ☐NO
14.	Data element nationality is present in the mDL data.	☒YES ☐NO
15.	Data element resident_city is present in the mDL data.	☒YES ☐NO
16.	Data element resident_state is present in the mDL data.	☒YES ☐NO
17.	Data element resident_postal_code is present in the mDL data.	☒YES ☐NO
18.	Data element resident_country is present in the mDL data.	☒YES ☐NO
19.	Data element biometric_template_face is present in the mDL data.	☐YES ☒NO

Página/Folio No.772 de 843

20.	Data element biometric_template_voice is present in the mDL data.	☐YES ☒NO
21.	Data element biometric_template_finger is present in the mDL data.	☐YES ☒NO
22.	Data element biometric_template_iris is present in the mDL data.	☐YES ☒NO
23.	Data element biometric_template_retina is present in the mDL data.	☐YES ☒NO
24.	Data element biometric_template_hand_geometry is present in the mDL data.	☐YES ☒NO
25.	Data element biometric_template_signature_sign is present in the mDL data.	☐YES ☒NO
26.	Data element biometric_template_keystroke is present in the mDL data.	☐YES ☒NO
27.	Data element biometric_template_lip_movement is present in the mDL data.	☐YES ☒NO
28.	Data element biometric_template_thermal_face is present in the mDL data.	☐YES ☒NO
29.	Data element biometric_template_thermal_hand is present in the mDL data.	☐YES ☒NO
30.	Data element biometric_template_gait is present in the mDL data.	☐YES ☒NO
31.	Data element biometric_template_body_odor is present in the mDL data.	☐YES ☒NO
32.	Data element biometric_template_dna is present in the mDL data.	☐YES ☒NO
33.	Data element biometric_template_ear is present in the mDL data.	☐YES ☒NO
34.	Data element biometric_template_finger_geometry is present in the mDL data.	☐YES ☒NO
35.	Data element biometric_template_palm_geometry is present in the mDL data.	☐YES ☒NO
36.	Data element biometric_template_vein_pattern is present in the mDL data.	☐YES ☒NO
37.	Data element biometric_template_foot_print is present in the mDL data.	☐YES ☒NO
38.	Data element family_name_national_character is present in the mDL data.	☒YES ☐NO

39.	Data element given_name_national_character is present in the mDL data.	☒YES ☐NO
40.	Data element signature_usual_mark is present in the mDL data.	☒YES ☐NO

A.1.3 For technology test cases

#	ICS statements for Technology test cases	
41.	mDL supports device engagement using NFC Static Handover	☒YES ☐NO
42.	mDL supports device engagement using NFC Negotiated Handover [5]	☐YES ☒NO
43.	mDL supports device engagement using QR code	☒YES ☐NO
44.	mDL supports device retrieval using NFC	☒YES ☐NO
45.	mDL supports extended-length APDUs for device retrieval using NFC	☒YES ☐NO
46.	mDL supports BLE version 4.2 (or above) and LE Data Packet Length Extension	☒YES ☐NO
47.	mDL supports device retrieval using BLE in mdoc central client mode	☒YES ☐NO
48.	If BLE in mdoc central client mode is used for device retrieval, mdoc verifies the value of the Ident characteristic	☒YES ☐NO
49.	mDL supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE	☐YES ☒NO
50.	mDL supports device retrieval using BLE in mdoc peripheral server mode	☒YES ☐NO
51.	mDL supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE	☐YES ☒NO
52.	mDL supports device retrieval using Wi-Fi Aware	☐YES ☒NO
53.	mDL supports the NCS-PK-2WDH-128 cipher suite for Wi-Fi Aware [6]	☐YES ☒NO

[5] Note that NFC Static Handover and NFC Negotiated Handover cannot be supported simultaneously if an mDL supports both technologies

[6] Only applicable in case the mdoc supports Wi-Fi Aware for device retrieval and supports NFC Negotiated Handover for device engagement.

Página/Folio No.774 de 843

COPY SOLUTIONS INTERNATIONAL CSI RNC 101 * Santo Domingo R.D.

54.	mDL supports server retrieval using OIDC	☒YES ☐NO
55.	mDL supports server retrieval using WebAPI	☒YES ☐NO
56.	mDL supports transferring server retrieval information in the device engagement structure	☒YES ☐NO
57.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message	☐YES ☒NO
58.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	

A.1.4 For security mechanism test cases

	ICS statements for Security Mechanisms test cases	
59.	Which curves does the mDL support for session establishment? Tick all that are supported.[7]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
60.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	☐YES ☒NO
61.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	
62.	Which curves does the mDL issuing authority support for issuer data authentication? Tick all that are supported.[8]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

[7] If the mDL supports multiple curves for session establishment, then for the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.

[8] If multiple documents are present on the mDL, the issuing authority can in theory use a different curve for signing the MSO on each of them. However, please note that UL expects the same curve to be used

63.	The mDL supports mdoc MAC authentication.	☒YES ☐NO
64.	If yes, which curves does the mDL support for mdoc MAC authentication? Tick all that are supported [9]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
65.	The mDL supports mdoc ECDSA/EdDSA authentication	☒YES ☐NO
66.	If yes, which curves does the mDL use for mdoc ECDSA/EdDSA authentication? Tick all that are supported [10]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
67.	The mDL supports mdoc reader authentication	☒YES ☐NO

for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

[9] If multiple documents are present on the mDL, the mDL can, in theory, use a different mdoc MAC authentication curve for each of them. However, please note that UL expects the same curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

[10] Note that for each document on an mDL, there could potentially be multiple SDeviceKey pairs for mdoc authentication, each in a separate MSO. It is therefore theoretically possible that a single document uses MAC authentication and ECDSA/EdDSA authentication alternatingly or uses different curves for ECDSA/EdDSA alternatingly. However, please note that UL expects that the same mdoc authentication mechanism (either MAC or ECDSA/EdDSA) is consistently used for all documents on a given sample. Moreover, UL expects that the same ECDSA/EdDSA curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

Página/Folio No.776 de 843

68.	If yes, which curves does the mdoc support for mdoc reader authentication? Tick all that are supported[11].	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

69.	If yes, for which data elements is successful reader authentication required before the mdoc will release them[12]	{
		"org.iso.18013.5.1.mDL" : {
		"org.iso.18013.5.1" : [
		"administrative_number",
		"sex",
		"weight",
		"eye_colour",
		"hair_colour",
		"birth_place",
		"resident_address",
		"portrait_capture_date",
		"age_in_years",
		"age_birth_year",
		"age_over_15",
		"age_over_18",
		"age_over_21",
		"age_over_60",
		"age_over_65",
		"age_over_68",
		"issuing_jurisdiction",
		"nationality",
		"resident_city",
		"resident_state",
		"resident_postal_code",
		"resident_country",
		"family_name_national_character",
		"given_name_national_character",
		"signature_usual_mark
		]}}

70.	If yes, mdoc supports retrieving OCSP information, if available, when verifying an mdoc reader authentication certificate.	☐YES ☒NO

[11] UL assumes that all mDL samples provided to us will support all of the mdoc reader authentication curves selected (provided that the correct CA certificates are installed).

[12] UL assumes that if mdoc reader authentication is supported, there is at least one data element that will not be released if mdoc reader authentication is not performed or fails.

Página/Folio No.777 de 843

A.1.5 For use case test cases

#	ICS statements for Use Case test cases	
71.	The mDL allows the mDL holder to refuse consent for sharing the portrait data element if requested by the reader	☐YES ☒NO

Página/Folio No.778 de 843

TRADUCCIÓN OFICIAL: ISO 18013 para Android

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membrete de FIME Services North America Inc., domiciliado en 1945 The Exchange, Suite 200 SE, Atlanta, GA 30339, Estados Unidos de América

Global Enterprise Technologies Corp
230 2nd Avenue, Waltham, Massachusetts, 02451, E.U.A.

15 de noviembre de 2024

Asunto: Confirmación de Conformidad de Android basado en mDL - GET Mobile ID, v.5.1.23 con ISO/IEC 18013-5:2021

Estimado Sr. Alexander:

Esta carta sirve para confirmar la conformidad de la aplicación mDL mencionada más arriba ('la aplicación') con ISO/IEC 18013-5:2021.

FIME probó la versión v.5.5.0 de esta aplicación mDL en diciembre 2022 y determinó que cumple con esta norma. El alcance de la prueba incluyó probar la aplicación en su interface con un lector mDL, ejecutando los casos de prueba enumerados en la última versión preliminar de ISO/IEC 18013-6. Las pruebas se limitaron a las características admitidas por la aplicación, como se indica en la Declaración de Conformidad de Implementación en el Apéndice de esta carta. Los detalles de la aplicación bajo prueba, el entorno de prueba y los dispositivos de prueba utilizados para la misma se pueden encontrar en la página siguiente. El número del Informe de Prueba que contiene la descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas es UL_eID_GET Group_Android_002.

En agosto de 2024, GET proporcionó a Fime notas de la versión que describen los cambios entre la versión 5.5.0 probada y la versión 5.1.23. Después de revisar esas notas de la versión, FIME concluyó que no es necesario volver a probar la versión 5.1.23, ya que es poco probable que los cambios descritos afecten la conformidad con la norma ISO/IEC 18013-5.

Como recordatorio, el correcto funcionamiento de la aplicación depende de varios factores de su entorno operativo. GET Group es el único y total responsable de la conformidad de la aplicación con todas las normas, especificaciones y requisitos aplicables.

Esta carta de confirmación es válida por un año a partir de su fecha de emisión.

De ustedes sinceramente,
Firma ilegible
FIME
David Bakker
Líder Técnico

Alcance Implementación mDL

Sistema bajo Prueba

Nombre y Versión Aplicación	mDL – GET Mobile ID, v.5.5.0
Sistema Operacional	Android
Aplicación disponible a través	Paquete Archivo Android (APK) de la Aplicación mDL que fue provisto por el cliente
Fecha de Recibo Aplicación	2021-10-26
Tipo Certificación	Certificación Integrada del Producto
Autoridad Emisora	División Licencias de Conducir de Utah

Resumen Declaración de Conformidad de la Implementación

Tecnologías Interacción con Dispositivos	Código QR, NFS Static Handover
Tecnologías Recuperación de Dispositivos	BLE en mdoc modo cliente central BLE en mdoc modo servidor periférico NFC, WiFi-Aware[1]
Tecnologías Recuperación de Servidores	WebAPI, OIDC
Mecanismos Seguridad para la Recuperación Dispositivos	Cifrado de sesión, autenticación de datos del emisor, autenticación mdoc, autenticación del lector mdoc

Ambiente de la Prueba

Estándar	ISO/IEC 1803-5:2021
Especificación Caso Prueba	Especificación Caso Prueba FIME mDL
Conjunto de Pruebas	Conjunto Prueba v1.1.11 Aplicación UL mDL
Aplicación Prueba mDL	Mdltestapp-1.1.4
Dispositivo de Prueba donde se instala la Aplicación Prueba mDL	Google Pixel 3ª
Versión OS del Dispositivo de Prueba donde se Instala la Aplicación de Prueba mDL	Android 12

Dispositivos y Plataforma de la Prueba

Marca y Tipo Dispositivo	Google Pixel 6	Samsung Galaxy S9
Versión OS	Android 13	Android 8

A.1 Resumen Declaración de Conformidad de la Implementación

Las Declaraciones de Conformidad de la Implementación que aparecen más adelante fueron proporcionadas a FIME por el Grupo GET y se han usado para determinar qué casos de prueba se deben ejecutar.

La versión de ICS que utiliza el Grupo GET es la v1.5.

A.1.1 Información General

Propietario mDL	
Nombre Propietario de la Aplicación	GET Group
Dirección	230 2da Avenue
Ciudad	Waltham
Estado	MA
Código Postal	02451
País	EUA
Nombre del Contacto	Alexander Kambanis

[1] WiFi Aware fue probado solo con el dispositivo Google Pixel 6 funcionando con Android 13.

Título del Contado	Director Gerente
Dirección correo electrónico de Contacto	akambanis@gelgroupna.com
Número de teléfono del Contacto	+1 (617) 901-1700

Información General Autoridad Emisora (Aplicable únicamente a la Certificación del Producto Integrada)	
Nombre Autoridad Emisora	Departamento de Seguridad Pública de Utah, División Licencia de Conducir
Dirección Autoridad Emisora	Departamento de Seguridad Pública de Utah
Ciudad	Ciudad Salt Lake
Estado	Utah
Código Postal	84114-4501
País	EUA
Nombre del Contacto	Brittaney Akagi
Título del Contado	IT / Gerente Aseguramiento de Calidad
Dirección correo electrónico de Contacto	bakagi@utah.gov

Información General Aplicación mDL	
Tipo Certificación	☐Funcional[2] ☒Producto Integrado[3]
Nombre y Versión de la Aplicación	GET Mobile ID, v. 5.5.0
La versión mínima de soporte iOS	Android 8.0 (Nivel API 26)
¿Cuántos documentos están presentes en la prueba mDL?	1

Para cada documento, por favor especifique el DocType [Tipo de Documento] que aplique	org.iso.18013.5.1.mDL
Para cada documento, por favor especifique todos los espacios de nombres de los elementos usados en el documento.	org.iso.18013.5.1, com.scytales.18013.5.1, org.aamva.us, org.iso.18013.5.1.aamva
Para cada espacio de nombres diferente del nombre del espacio mDL ("org.iso.18013.5.1"), por favor, especifique los identificadores de todos los datos de los elementos presentes en el documento.	{ 'org.iso.18013.5.1.mDL' : { 'com.scytales.18013.5.1' : ["status", "categoria_vehiculo", "lista_categoria_vehiculo", "dirección_completa", 'e-mail', "número_móvil"], 'org.aamva.us' : ["real_id"], 'org.iso.18013.5.1.aamva' : ["DHS_compliance"] } }

A.1.2 Modelo de Datos mDL para casos de prueba

Nota: todos los elementos de datos de esta sección se encuentran en el espacio predeterminado de nombres de datos mDL
("org.iso.18013.5.1"). Las declaraciones ICS de esta sección deben completarse solo para documentos que tengan

[2] Para la certificación funcional, el conjunto de datos mDL puede ser un conjunto de datos de muestra que el propietario del mDL desea personalizar en el mDL.

[3] La certificación integrada de productos requiere que el conjunto de datos mDL sea preparado y personalizado por un Sistema de registro (SoR) del emisor y el conjunto de datos mDL debe ser representativo del mDL que se utilizará en producción

DocType = "org.iso.18013.5.1.mDL".

#	Declaraciones ICS para los casos de prueba del Modelo de Datos mDL[4]	
1.	El elemento de datos número_administrativo está presente en los datos mDL.	☒Si ☐No
2.	El elemento de datos sexo_ está presente en los datos mDL.	☒Si ☐No
3.	El elemento de datos altura_ está presente en los datos mDL.	☒Si ☐No
4.	El elemento de datos peso_ está presente en los datos mDL	☒Si ☐No
5.	El elemento de datos color de ojos_ está presente en los datos mDL	☒Si ☐No
6.	El elemento de datos color de pelo_ está presente en los datos mDL	☒Si ☐No
7.	El elemento de datos lugar de nacimiento_ está presente en los datos mDL	☒Si ☐No
8.	El elemento de datos dirección de residencia_ está presente en los datos mDL	☒Si ☐No
9.	El elemento de datos captura de imagen_ está presente en los datos mDL	☒Si ☐No
10.	El elemento de datos edad en años_ está presente en los datos mDL	☒Si ☐No
11.	El elemento de datos edad_año de nacimiento_ está presente en los datos mDL	☒Si ☐No
12.	El elemento de datos edad_mayor de_NN está presente en los datos mDL En caso de seleccionar SI, favor dar los elementos de datos edad_mayor de_NN en los datos mDL con su correspondiente valor (VERDADERO/FALSO) durante la personalización	☒Si ☐No
	NN	Valor Retorno
	Edad_mayor de_15	Verdadero
	Edad_mayor de_18	Verdadero
	Edad_mayor de_21	Verdadero
	Edad_mayor de_60	Falso
	Edad_mayor de_65	Falso
	Edad_mayor de_68	Falso
13.	El elemento de datos jurisdicción_emisora_ está presente en los datos mDL	☒Si ☐No
14.	El elemento de datos nacionalidad_ está presente en los datos mDL	☒Si ☐No
15.	El elemento de datos ciudad_de residencia_ está presente en los datos mDL	☒Si ☐No
16.	El elemento de datos estado_de residencia_ está presente en los datos mDL	☒Si ☐No
17.	El elemento de datos código_postal_de residencia_ está presente en los datos mDL	☒Si ☐No
18.	El elemento de datos país_de residencia_ está presente en los datos mDL	☒Si ☐No
19.	El elemento de datos plantilla_biométrica_cara_ está presente en los datos mDL	☐Si ☒No
20.	El elemento de datos plantilla_biométrica_voz_ está presente en los datos mDL	☐Si ☒No
21.	El elemento de datos plantilla_biométrica_dedo_ está presente en los datos mDL	☐Si ☒No
22.	El elemento de datos plantilla_biométrica_iris_ está presente en los datos mDL	☐Si ☒No
23.	El elemento de datos plantilla_biométrica_retina_ está presente en los datos mDL	☐Si ☒No
24.	El elemento de datos plantilla_biométrica_mano_ geométrica está presente en los datos mDL	☐Si ☒No
25.	El elemento de datos plantilla_biométrica_firma_ está presente en los datos mDL	☐Si ☒No
26.	El elemento de datos plantilla_biométrica_pulsación de teclas_ está presente en los datos mDL	☐Si ☒No
27.	El elemento de datos plantilla_biométrica_movimiento de labios_ está presente en los datos mDL	☐Si ☒No
28.	El elemento de datos plantilla_biométrica_cara_térmica_ está presente en los datos mDL	☐Si ☒No
29.	El elemento de datos plantilla_biométrica_mano_térmica_ está presente en los datos mDL	☐Si ☒No
30.	El elemento de datos plantilla_biométrica_pasos_ está presente en los datos mDL	☐Si ☒No
31.	El elemento de datos plantilla_biométrica_olor_corporal_ está presente en los datos mDL	☐Si ☒No
32.	El elemento de datos plantilla_biométrica_adn_ está presente en los datos mDL	☐Si ☒No
33.	El elemento de datos plantilla_biométrica_oído_ está presente en los datos mDL	☐Si ☒No
34.	El elemento de datos plantilla_biométrica_geometría_dedo_ está presente en los datos mDL	☐Si ☒No
35.	El elemento de datos plantilla_biométrica_geometría_palma manos_ está presente en los	☐Si ☒No

[4] Nota: todos los elementos de datos de esta sección se encuentran en el espacio predeterminado de datos mDL ("org.iso.18013.5.1"). Las declaraciones ICS de esta sección deben completarse solo para documentos que tengan DocType = "org.iso.18013.5.1.mDL".

	datos mDL	
36.	El elemento de datos plantilla_biométrica_patrón_venas_ está presente en los datos mDL	☐Si ☒No
37.	El elemento de datos plantilla_biométrica_huella_pié_ está presente en los datos mDL	☐Si ☒No
38.	El elemento de datos apellido_carácter_nacional_ está presente en los datos mDL	☒Si ☐No
39.	El elemento de datos nombre_carácter_nacional_ está presente en los datos mDL	☒Si ☐No
40.	El elemento de datos marca_usual_firma_ está presente en los datos mDL	☒Si ☐No

A.1.3. Para Casos de Prueba de Tecnología

#	Declaraciones ICS para los casos de prueba de Tecnología	
41.	mDL admite interacción con el dispositivo usando NFC Static Handover	☒Si ☐No
42.	mDL admite interacción con el dispositivo usando NFC Negotiated Handover[5]	☐Si ☒No
43.	mDL admite interacción con el dispositivo usando Código QR	☒Si ☐No
44.	mDL admite recuperación del dispositivo usando NFC	☒Si ☐No
45.	mDL admite APDU de longitud extendida para la recuperación del dispositivo usando NFC	☒Si ☐No
46.	mDL admite BLE versión 4.2 (o la que antecede) y Paquete de Datos LE de longitud extendida	☒Si ☐No
47.	mDL admite recuperación del dispositivo usando BLE modo cliente central	☒Si ☐No
48.	Si utiliza BLE en modo cliente central para la recuperación de dispositivos, verifique el valor de la característica Ident	☒Si ☐No
49.	mDL admite el perfil de transmisión L2CAP si actúa como cliente GATT para la recuperación del dispositivo usando BLE	☐Si ☒No
50.	mDL admite recuperación de dispositivos usando BLE en modo de servidor periférico	☒Si ☐No
51.	mDL admite el perfil de transmisión L2CAP si actúa como servidor GATT para la recuperación del dispositivo usando BLE	☐Si ☒No
52.	mDL admite recuperación del dispositivo usando Wi-Fi Aware	☐Si ☒No
53.	mDL admite el conjunto cifrado NCS-PK-2WDH-128 para Wi-Fi Aware[6]	☐Si ☒No
54.	mDL admite la recuperación del servidor usando OIDC	☒Si ☐No
55.	mDL admite la recuperación del servidor usando WebAPI	☒Si ☐No
56.	mDL admite la transferencia de información de recuperación desde la estructura de interacción del dispositivo	☒Si ☐No
57.	mDL implementa un tiempo de espera entre el tiempo de envío de datos de interacción del dispositivo y establecimiento de la recepción del mensaje	☐Si ☒No
58.	En caso afirmativo, ¿cuántos segundos es el periodo de espera para la finalización de la sesión implementada por el mDL?	

A.1.4 Para Casos de Prueba de los Mecanismos de Seguridad

	Declaraciones ICS para los casos de prueba de los Mecanismos de Seguridad	
59.	¿Cuáles curvas admite mDL para el establecimiento de sesiones? Marque todas las compatibles.[7]	☒Curva P-256 ☐Curva P-384 ☐Curva P-521 ☐X25519 ☐X448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
60.	mDL admite el intercambio de más de una solicitud y respuesta de mDOC para la recuperación del dispositivo con el lector mDOCen una	☐Si ☒No

[5] Tenga en cuenta que la transferencia NFC Static Handover y NFC Negotiated Handover no se pueden admitir simultáneamente si un mDL admite ambas tecnologías

[6] Solo se aplica en caso de que el mDOC admita Wi-Fi Aware para la recuperación del dispositivo y admita NFC Negotiated Handover para la interacción con el dispositivo

[7] Si mDL admite varias curvas para el establecimiento de sesiones, entonces, a los efectos de la prueba, el propietario de mDL debe proporcionar una muestra separada para cada una de las curvas admitidas

	sola sesión.	
61.	Si es afirmativo, ¿cuántos segundos es el período de espera para la finalización de la sesión implementada por mDL?	
62.	¿Cuáles curvas admite la autoridad emisora mDL para la autenticación de los datos del emisor? Marque todas las compatibles[8]	☒Curva P-256 ☐Curva P-384 ☐Curva P-521 ☐Ed25519 ☐Ed448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
63.	El mDL admite la autenticación MAC de mDOC	☒Si ☐No
64.	Si afirmativo, ¿cuáles curvas admite el mDL para la autenticación MAC de mDOC? Marque todas las compatibles[9]	☒Curva P-256 ☐Curva P-384 ☐Curva P-521 ☐X25519 ☐X448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
65.	El mDL admite la autenticación ECDSA/EdDSA de mDOC	☒Si ☐No
66.	Si es así, ¿cuáles curvas utiliza el mDL para la autenticación ECDSA/EdDSA de mDOC? Marque todas las compatibles[10]	☒Curva P-256 ☐Curva P-384 ☐Curva P-521 ☐Ed25519 ☐Ed448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1
67.	El mDL admite la autenticación de lectores mDOC	☒Si ☐No
68.	Si afirmativo, ¿cuáles curvas admite el mDOC para la autenticación del lector mDOC? Marque todas las compatibles[11]	☒Curva P-256 ☒Curva P-384 ☒Curva P-521 ☐Ed25519 ☐Ed448 ☐brainpoolP256r1 ☐brainpoolP320r1 ☐brainpoolP384r1 ☐brainpoolP512r1

[8] Si hay varios documentos en la mDL, la autoridad emisora puede, en teoría, utilizar una curva diferente para firmar la MSO de cada uno de ellos. Sin embargo, tenga en cuenta que UL espera que se utilice la misma curva para todos los documentos de la muestra dada. Para pruebas, el propietario del mDL debe proveer una muestra independiente para cada una de las curvas admitidas.

[9] Si hay varios documentos en el mDL, el mDL puede, en teoría, utilizar una curva de autenticación MAC de mDOC diferente para cada uno de ellos. Sin embargo, tenga en cuenta que UL espera que se utilice la misma curva para todos los documentos de la muestra dada. Para pruebas, el propietario del mDL debe proveer una muestra independiente para cada una de las curvas admitidas.

[10] Tenga en cuenta que para cada documento de un mDL, podría haber varios pares de SDeviceKey para la autenticación mDOC, cada uno en un MSO independiente. Por tanto, es teóricamente posible que un solo documento utilice la autenticación MAC y la autenticación ECDSA/EdDSA de forma alternada o utilice diferentes curvas para ECDSA/EdDSA de forma alternada. Sin embargo, tenga en cuenta que UL espera que se utilice de forma constante el mismo mecanismo de autenticación mDOC (MAC o ECDSA/EdDSA) para todos los documentos de una muestra determinada. Además, UL espera que se utilice la misma curva ECDSA/EdDSA para todos los documentos de una muestra determinada. Para realizar pruebas, el propietario del mDL debe proporcionar una muestra independiente para cada una de las curvas admitidas.

[11] UL asume que todas las muestras de mDL que se nos proporcionan admitirán todas las curvas de autenticación de lectores mDOC seleccionadas (siempre que se instalen los correctos certificados CA).

69.	Si es así, ¿para qué elementos de datos se requiere una autenticación exitosa del lector antes de que mDOC los libere?[12]	{
		"org.iso.18013.5.1.mDL": {
		"org.iso.18013.5.1.": {
		"número_administrativo",
		"sexo",
		"peso",
		"color_ojos",
		"color_pelo",
		"lugar_nacimiento",
		"dirección_residencia",
		"fecha_captura_retrato",
		"edad_en_años",
		"edad_año_nacimiento",
		"edad_más de_15",
		"edad_más de_18",
		"edad_más de_21",
		"edad_más de_60",
		"edad_más de_65",
		"edad_más de_68",
		"jurisdicción_emisora",
		"nacionalidad",
		"ciudad_residencia",
		"estado_residencia",
		"código_postal_residencia",
		"país_residencia",
		"apellido_carácter_nacional",
		"nombre_carácter_nacional"
		"firma_marca_usual"
		]}}

70.	En caso afirmativo, mDOC admite la recuperación de la información de OCSP, si disponible, al verificar un certificado de autenticación del lector mDOC	☐Si ☒No

A.1.5 Para uso en los casos de Casos de Pruebas

#	Declaraciones ICS para Uso en los Casos de Casos de Pruebas	
71.	El mDL permite al titular de mDL rechazar el consentimiento para compartir el elemento de datos del retrato, si así lo solicita el lector	☐Si ☒No

EN FE DE LO CUAL, firmo y sello la presente **Certificación,** a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los doce (12) días del mes de febrero del año dos mil veintiecinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 224/25.

Ana María Feria

[12] UL asume que si se admite la autenticación de lectores mDOC, hay por lo menos un elemento de datos que no se liberará si la autenticación de lectores mDOC no se realiza o falla.

ISO/IEC DIS 18013-5. (UL)

Global Enterprise Technologies Corp.
Mr. Alex Kambanis
230 3Rd Ave
Waltham, MA 02451-7528
United States

UL Verification Services Inc.
333 Pfingsten Road
Northbrook, IL 60062-2096
USA

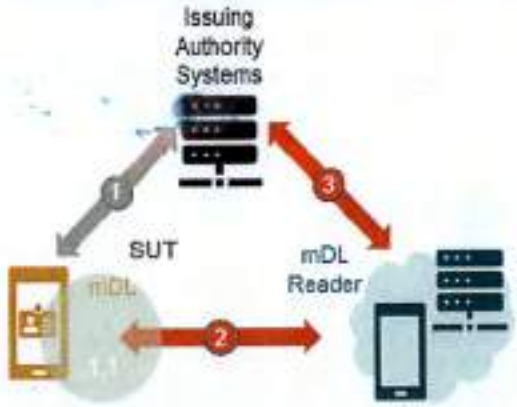
Date of Issuance: 16 November 2020
UL Order Number: 13515921

Subject: GET Group NA mDL (holder) application – Conformity Assessment Summary

Dear Mr. Kambanis,

We are pleased to hereby provide you with the Conformity Assessment Summary, following the successful conformity assessment of Global Enterprise Technologies Corp. North America (GET Group NA) mDL (holder) applications for iOS and Android.

The system under test (SUT) for this conformity assessment is GET Group NA mDL Application, whereby the mDL test data and the functional behavior of the mDL application have been evaluated on its interface to the mDL Reader against the requirements of ISO/IEC DIS 18013-5.



The detailed test results are described in the Conformity Test Report. These findings are valid for the evaluated version of the product, configuration, implementation, and system and version of the standard.

We congratulate you with the successful evaluation of your product, and thank you for your trust in UL.

Warm regards,

Henk van Dam
mDL Global Operations Manager
Identity Management & Security, UL

Página/Folio No.788 de 843

Global Enterprise Technologies Corp.
Mr. Alex Kambanis
230 3Rd Ave
Waltham, MA 02451-7528
United States

UL Verification Services Inc.
333 Pfingsten Road
Northbrook, IL 60062-2096
USA

Date of Issuance: 16 November 2020
UL Order Number: 13515921

Conformity Assessment Summary

The product listed below has been tested by UL and found to be in compliance with the indicated Test Procedure, as detailed in the referenced Test Report.

System Under Test

mDL App name and version	GET mID (STAGING) 3.8 (4) for iOS	GET mID (CT) 3.8 (17) for Android
Operating System	iOS	Android
App Available through	TestFlight	MS App Center
Release date	13 November 2020	12 November 2020

Implementation Conformance Statement

Device engagement	QR code	QR code	NFC (static handover)	NFC (static handover)
Data transfer (offline)	BLE (peripheral mode)	Wi-Fi Aware	BLE (peripheral mode)	Wi-Fi Aware
Platform	iOS + Android	Android	Android	Android

Security mechanisms (offline)	Session Encryption (ECDH)	Issuer Data Authentication	mDL Authentication (MAC)
Data transfer (online)*	WebAPI (default, configurable)	Open ID Connect (OIDC)	
Security mechanisms (online)**	JSON Web Signature (JWS)	Transport Layer Security (TLS)	

*) Data transfer (online) concerns the interaction between an mDL Reader and Issuing Authority Systems. The interaction of the mDL on its interface to the mDL Reader to enable online data transfer is in scope for this assessment. The actual online data transfer is out of scope for this assessment.
**) Security mechanisms (online) concern the interaction between an mDL Reader and Issuing Authority Systems (out of scope for this assessment)

Test Environment

mDL Standard	ISO/IEC DIS 18013-5:2020(E) (https://www.iso.org/standard/69084.html) (ISO WG10N1818)
mDL Test Case Specification	UL mDL Test Cases v0.5
mDL Test Suite	UL mDL Test Suite v0.5.2
mDL Test App	UL mDL Test App v0.5.1

Test Devices

Device	iPhone SE	iPhone 11	iPhone 5S	OnePlus 8	Samsung Galaxy S10
OS	iOS 14.0.1	iOS14.2	iOS 12.4	Android 10	Android 10

Test Scope

The test scope for this conformity assessment concerns protocol and interface testing of the System Under Test (mDL apps) as installed on the specified Test Devices, on its interface to an mDL Reader. The test coverage is limited to the requirements of ISO/IEC DIS 18013-5. Regarding Device Engagement and Data Transfer technologies, ISO/IEC DIS 18013-5 builds on existing standards for QR code, NFC, BLE, and Wi-Fi Aware. The correct functioning of these technologies are assessed implicitly. Exhaustive conformity assessment against those standards is out of scope. In scope are Data Model tests, Message Structure and Content tests, and Transaction tests, covering the different Device Engagement and Data Transfer technologies.

Test Procedure

For test execution, qualified UL Test Analysts 1) installed the mDL Apps on the specified Test Devices, 2) entered the configuration of the System Under Test in the mDL Test Suite, according to the Implementation Conformance Statement provided by the app developer and loaded the provided Issuing Authority CA test certificate, 3) operated the UL mDL Test Suite with its associated UL mDL Test App interacting with the System Under Test and performed user interaction with the System Under Test, 4) performed all applicable test cases as implemented in the mDL Test Suite, based on the mDL Test Case Specification, for each Test Device with mDL App, 5) analyzed the test results of each test case, 6) reported intermediate test results and observations to the app developer throughout test execution, 7) reported final test results in the UL mDL Application Conformity Test Report.

Test Result

For the specified System Under Test, as installed on the specified Test Devices, all applicable tests performed have successfully passed. Detailed test results are reported in the UL mDL Application Conformity Test Report. The mDL test data and the functional behavior of the System Under Test observed in the test environment is conformant to ISO/IEC DIS 18013-5.

Dependencies

Correct functioning of an mDL app is dependent on several factors in its operational environment, including but not limited to the availability and proper functioning of the supported technologies by the mobile device on which the app is installed, network connectivity in case of online data transfer, ISO/IEC DIS 18013-5 conformant behavior of the mDL Reader it interacts with, and availability of a correctly structured, ISO/IEC DIS 18013-5 conformant mDL data set provisioned by the Issuing Authority or its agent.

The test results are valid for the evaluated configuration of the system under test. The client provided all of the application software for testing by UL. UL has not established Follow-Up Service or other surveillance of the product. The client is solely and fully responsible for conformity of all products to all applicable standards, specifications or requirements. UL Logo and Marks shall not be used in connection with the above UL Statement. This UL Statement of Test Results does not indicate compliance with any UL certification program requirements.

Página/Folio No.789 de 843

TRADUCCIÓN OFICIAL: ISO/IEC 18013 (UL)

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membrete de UL Verification Services Inc., domiciliados en 333 Pfingsten Road, Northbrook, IL 60062-2096, Estados Unidos de América

Global Enterprise Technologies Corp.
Sr. Alex Kambanis
230 3Rd Ave
Waltham, MA 02451-7528
Estados Unidos de América

UL Verification Services Inc
333 Pfingsten Road
Northbrook, IL 60062-2096
Estados Unidos de América

Fecha emisión: 16 noviembre 2020
Número Orden UL: 13515921

Asunto: Solicitud GET Group NA mDL (titular) – Resumen Evaluación Conformidad

Estimado Sr. Kambanis,

Nos complace brindarle en el presente el Resumen de Evaluación de Conformidad, luego de la exitosa evaluación de conformidad a las aplicaciones mDL (titular) de Global Enterprise Technologies Corp. North America (GET Group NA) para iOS y Android.

El sistema bajo prueba (SUT, por sus siglas en inglés) para esta evaluación de conformidad es la aplicación mDL de GET Group NA, mediante la cual los datos de prueba mDL y el comportamiento funcional de la aplicación mDL se han evaluado en su interfaz con el lector de mDL, según los requisitos de ISO/IEC DIS 18013-5.

Sistema Emisor Autorización

Los resultados detallados de la prueba se describen en el Informe de Prueba de Conformidad. Estos hallazgos son válidos para la versión evaluada del producto, configuración, implementación y sistema y versión de la normativa.

Los felicitamos por la exitosa evaluación de su producto y les agradecemos su confianza en UL.

Con un cordial saludo,
Firma ilegible
Henk van Dam
Gerente mDL Global Operations
Gestión & Seguridad Identidad, UL

Global Enterprise Technologies Corp.
Sr. Alex Kambanis
230 3Rd Ave
Waltham, MA 02451-7528
Estados Unidos de América

UL Verification Services Inc
333 Pfingsten Road
Northbrook, IL 60062-2096
Estados Unidos de América

Fecha emisión: 16 noviembre 2020
Número Orden UL: 13515921

COPY SOLUTIONS INTERNATIONAL S.A. CSI RNC 101898652 Santo Domingo, R.D.

Resumen Evaluación de Conformidad

El producto detallado más abajo ha sido probado por UL y encontrado en cumplimiento con el Procedimiento de Prueba indicado, como detallado en el Reporte de Prueba referido.

Sistema Bajo Prueba

Nombre/Versión Aplicación mDL	GET mID (Staging) 3.8 (4) para iOS	GET mID (CT) 3.8 (17) para Android
Sistema Operativo	iOS	Android
Disponible a través Aplicación	TestFlight	MS App Center
Fecha Liberación	13 de noviembre de 2020	12 de noviembre de 2020

Implementación Declaración Conformidad

Dispositivo Involucrado	Código QR	Código QR	NFC (entrega estática)	NFC (entrega estática)
Fecha Transferencia (fuera línea)	BLE (modo periférico)	Wi-Fi Aware	BLE (modo periférico)	Wi-Fi Aware
Plataforma	iOS + Androide	Androide	Androide	Androide

Mecanismo Seguridad (fuera línea)	Sesión Encriptación (ECDH)	Emisor Autenticación Datos	Autenticación mDL (MAC)
Fecha Transferencia (en línea)*	WebAPI (falla configurable)	Conector ID Abierto (OIDC)	
Mecanismo Seguridad (en línea)**	JSON Firma Web (JWS)	Capa Transporte Seguridad (TLS)	

*)La transferencia de la datos (en línea) se refiere a la interacción entre un Lector mDL y los Sistemas Emisores de Autorización. La interacción del mDL en sus interfases en el Lector mDL permiten que la transferencia de la datos en línea esté dentro del alcance de esta evaluación. La transferencia real de datos en línea está fuera del alcance de esta evaluación.

**)Los mecanismos de seguridad (en línea) se refieren a la interacción entre un lector mDL y los Sistemas Emisores de Autorización (fuera del alcance de esta evaluación).

Ambiente de la Prueba

Normativa mDL	ISO/IEC DIS 18013-5-2020(E) (https://www.iso.org/standard/69084.html) (ISO WG 10N1818)
Especificación Caso Prueba mDL	UL mDL Casos Pruebas v0.5
Conjunto Pruebas mDL	UL mDL Conjunto Pruebas v0.5.2
Aplicación Prueba mDL	UL mDL Aplicaciones Pruebas v0.5.1

Dispositivos de la Prueba

Dispositivo	iPhone SE	iPhone 11	iPhone 5S	OnePlus 8	Samsung Galaxy S10
OS	iOS 14.0.1	iOS 14.2	iOS 12.4	Android 10	Android 10

Alcance de la Prueba

El alcance de la prueba para esta evaluación de conformidad se refiere a las pruebas de protocolo e interfaz del Sistema bajo Prueba (aplicaciones mDL) instalado en los dispositivos de prueba especificados, en su interfaz, con un lector mDL. La cobertura de la prueba se limita a los requisitos de ISO/IEC DIS 18013-5. En cuanto a las tecnologías de interacción de dispositivos y transferencia de datos, ISO/IEC DIS 18013-5 se basa en las normativas existentes para códigos QR, NFC, BLE y Wi-Fi Aware. El correcto funcionamiento de estas tecnologías se evalúa implícitamente. La evaluación exhaustiva de la conformidad con respecto a esas normas está fuera de alcance. El alcance incluye Pruebas de Modelo de Datos, Estructura de Mensajes y

INTERPRETE JUDICIAL DE JUZGADO LICDA. ANA MARIA DE LA CRUZ MAT. SANTO DOMINGO D.N.

Pruebas de Contenido y Pruebas de Transacciones, que cubren las diferentes tecnologías de interacción con dispositivos y transferencia de datos.

Procedimiento de Prueba

Para la ejecución de la prueba, los analistas de pruebas calificados de UL 1) instalaron las aplicaciones mDL en los dispositivos de prueba especificados, 2) ingresaron la configuración del sistema bajo prueba en mDL Conjunto Prueba, de acuerdo con la Declaración de Implementación de Conformidad proporcionada por el desarrollador de la aplicación y cargaron la Prueba de CA, 3) de la Autoridad Emisora del Certificado que operó el conjunto de pruebas UL mDL con su aplicación de prueba asociada UL mDL que interactuó con el Sistema bajo Prueba y realizó la interacción del usuario con el Sistema bajo Prueba, 4) realizaron todos los casos de prueba aplicables según lo implementado en el Conjunto de Pruebas mDL, basado en la Especificación de Casos de Prueba de mDL, para cada Dispositivo de Prueba con la aplicación mDL, 5) analizaron los resultados de las pruebas de cada caso de prueba, 6) informaron los resultados de las pruebas intermedias y las observaciones al desarrollador de la aplicación durante la ejecución de la prueba, 7) reportando los resultados finales de la prueba en el Informe de Prueba de Conformidad de la aplicación mDL de UL.

Resultado de la Prueba

Para el Sistema bajo Prueba especificado, tal como instalado en los Dispositivos de Prueba indicados, todas las pruebas aplicables realizadas han pasado con éxito. Los resultados detallados de las pruebas se reportan en el Informe de Prueba de Conformidad de las aplicaciones mDL de UL. Los datos de prueba mDL y el comportamiento funcional del sistema bajo prueba observado en el entorno de prueba cumplen con las ISO/IEC DIS 18013-5.

Dependencias

El correcto funcionamiento de una aplicación mDL depende de varios factores en su entorno operativo, incluidos, entre otros, la disponibilidad y el funcionamiento adecuado de las tecnologías admitidas por el dispositivo móvil sobre las que está instalada la aplicación, la conectividad de la red en caso de transferencia de datos en línea, el comportamiento conforme a las ISO/IEC DIS 18013-5 del lector mDL con el que interactúa y la disponibilidad de un conjunto de datos mDL correctamente estructurado y conforme con la ISO/IEC DIS 18013-5 proporcionado por la autoridad emisora o por su agente.

Los resultados de la prueba son válidos para la configuración evaluada del sistema bajo prueba. El cliente proporcionó todo el software de aplicación para que UL lo probara. UL no ha establecido un servicio de seguimiento ni ningún otro tipo de vigilancia del producto. El cliente es el único y total responsable de la conformidad de todos los productos con todas las normativas, especificaciones o requisitos aplicables. El logotipo y las marcas de UL no se utilizarán en relación con la declaración UL precedente. Esta Declaración de Resultados de Pruebas UL no indica el cumplimiento con ningún requisito del programa de certificación de UL.

EN FE DE LO CUAL, firmo y sello la presente **Certificación,** a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los diez (10) días del mes de junio del año dos mil veinticuatro (2024), habiéndola inscrito en el registro a mi cargo, bajo el No. 908/24.

Ana María Feria

LICDA. ANA MARIA FERIA
INTERPRETE JUDICIAL DE JUZGADO DE 1ra INSTANCIA
DEL DIST. NAC. SANTO DOMINGO, R.D.

Carta Jurada de Certificación CMMI DEV5

The Commonwealth of Massachusetts

William Francis Galvin - Secretary of the Commonwealth

Apostille

(Convention de la Haye du 5 Octobre 1961)

1. Country: United States Of America

This Public Document

2. Has been signed by: Caitlyn E. Burns

3. Acting in the capacity of: Notary Public

4. Bears the seal/stamp of: Caitlyn E. Burns

Whose commission expires on: 12/29/2028

Certified

5. At: Boston, Massachusetts 6. The: January 27, 2025

7. By: The Secretary of Commonwealth

8. No.: 2670492

9. Seal/Stamp: *(Great Seal of the Commonwealth)*

10. Signature:

William Francis Galvin
Secretary of the Commonwea

Prepared By: EPanico

GET Group Holdings Ltd.
Office No. 1701,1702,1703,1704,17
Level 17, Emirates Financial Towers, S
Dubai International Financial Centre
P.O. Box: 95703, Dubai, UAE
T: +971 (4) 388 87 79
F: +971 (4) 379 50 14
www.getgroup.com

GET GROUP

Company Limited by Shares Registered No. CL1024 T.R.N.: 100044551800003

January 14, 2025
14 de enero de 2025

To Whom It May Concern:
A quien pueda interesar:

I, Maysoon Jamal, am the CEO and sole shareholder of GET Group Holdings LTD, a Dubai, UAE company ("GET Group"). GET Group is the parent company to multiple entities that are part of its Passport & ID and Smart Solutions Business Units.

Yo, Maysoon Jamal, soy la directora ejecutiva y única accionista de GET Group Holdings LTD, una empresa de Dubái, Emiratos Árabes Unidos ("GET Group"). GET Group es la empresa matriz de varias entidades que forman parte de sus unidades de negocio de Pasaporte e Identificacion y Soluciones Inteligentes.

By this letter, I confirm that GET Group and its Passport & ID and Smart Solutions Business Units have been awarded the CMMIDEV/5 certification, as evidenced in the Certificate of Achievement attached as Exhibit A (the "Certificate").

Mediante esta carta, confirmo que GET Group y sus Unidades de Negocios Pasaporte e Identificacion y Soluciones Inteligentes han obtenido la certificación CMMIDEV/5, como se evidencia en el Certificado de Logro adjunto como Anexo A (el "Certificado").

I further certify that G.E.T. Secure ID Corp., a Delaware, USA company, and GET International FZCO, a Dubai, UAE company, are members of GET Group's Passport & ID Business Unit and, as such, has been awarded CMMIDEV/5 under the Certificate.

Además certifico que G.E.T. Secure ID Corp., una empresa de Delaware, EE. UU., y GET International FZCO, una empresa de Dubai, UAE, son miembros de la Unidad de Negocios de Pasaportes e Identificación de GET Group y, como tal, ha recibido CMMIDEV/5 bajo el Certificado.

COMMONWEALTH OF MASSACHUSETTS
COUNTY OF Middlesex

On this 14th day of January, 2025, before me, the undersigned notary public, Maysoon Jamal personally appeared, proved to me through satisfactory evidence of identification, which were lebanese passport, to be the person whose name is signed on the preceding or attached document in my presence.

Caitlyn E. Burns
Notary Public's Signature
My Commission Expires December 29, 2028

Sincerely,
Sinceramente,

Maysoon Jamal
GET Group CEO
CEO del GET Group

GET GROUP HOLDINGS Ltd.
P.O. Box 95703, Dubai - UAE, No.: CL1024

CAITLYN E. BURNS
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
December 29, 2028

COPY SOLUTIONS INTERNATIONAL S.A.
RNC 101899852
Santo Domingo, R.D.

Exhibit A
Anexo A

CMMIDEV/5 Certificate dated March 31, 2022
Certificado CMMIDEV/5 fechado el 31 de marzo de 2022

CERTIFICATE
OF ACHIEVEMENT

GET GROUP

GET Group Holdings LTD

Passport & ID and Smart Solutions Business Units

were appraised at **CMMI MATURITY LEVEL 5**

CMMIDEV/**5**

of the CMMI DEV Ver 2.0 of the CMMI Institute, USA.
Following Benchmark Appraisal Method v2.0 for Process Improvement

Appraisal ID Number 58300

March 31, 2022

DATE

CyberQ

SIGNATURE

Dr. Rajiv Nag (CyberQ)

(Certified High Mat Lead Appraiser, CMMI ID # 0000262-01)

CERTIFICADO
DE LOGRO

GET GROUP HOLDINGS LTD

Unidad De Negocios De Pasaporte e Identificacion y Soluciones
Inteligentes fue otorgado en CMMI Nivel Maduro 5
CMMIDEV /5

DE CMMI DEV VER 2.0 DE CMMI INSTITUDE, EE. UU. SIGUIENDO EL MÉTODO DE EVALUACIÓN DE REFERENCIA V2.0 PARA LA MEJORA DE PROCESOS
TASACIÓN NÚMERO DE ID 58300

31 de marzo,2022

TRADUCCIÓN OFICIAL: Carta Jurada de Certificación CMMI DEV5

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membreté de GET Group Holdings Ltd., con domicilio en Office No. 1701, 1702, 1703, 1704, 1705, Level 17 Emirates Financial Towers, South Tower, Dubai, International Financial Centre • Apartado Postal 95703, Dubai, Emiratos Árabes Unidos • T+971 (4) 388 87 78 • F +971 (4) 379 99 14 •. www.getgroup.com • Compañía Limitada por Acciones, Registrada bajo el No. CL 1024 • T.R.N.: 100044551800003

14 de enero de 2025

A quien pueda interesar:

La suscrito, Maysoon Jamal, soy la directora ejecutiva y única accionista de GET Group Holdings LTD, una empresa de Dubái, Emiratos Árabes Unidos ("GET Group"). GET Group es la empresa matriz de varias entidades que forman parte de sus unidades de negocio de Pasaportes e Identificacion y Soluciones inteligentes.

Mediante esta carta, confirmo que GET Group y sus Unidades de Negocios de Pasaportes e Identificacion y Soluciones Inteligentes han obtenido la certificación CMMIDEV/5, como se evidencia en el Certificado de Logro adjunto como Anexo A (el "Certificado").

Además, certifico que G.E.T. Secure ID Corp., una empresa de Delaware, Estados Unidos de América y GET International FZCO, una empresa de Dubái, Emiratos Árabes Unidos, son miembros de la Unidad de Negocios de Pasaportes e Identificación de GET Group, y, como tal, se le ha otorgado el CMMIDEV/5 bajo el Certificado.

Sinceramente,
Firma ilegible
Maysoon Jamal
CEP de GET Group
Lleva impreso el sello gomígrafo de la empresa

COMUNIDAD DE MASSACHUSETTS
CONDADO DE MIDDLESEX

A los 14 días de enero de 2025, compareció ante mí, notario público que suscribe, el Sr. Maysoon Jamal, a quien conozco personalmente, y quien probó ante mí mediante evidencia de identificación satisfactoria, que era el pasaporte libanés, ser la persona cuyo nombre firma el documento precedente o anexado en el mismo ante mi presencia.

Firma de Caitlyn E. Burns
Notario Público
Mi comisión expira el 29 de diciembre de 2028

CAITLYN E. BURNS
Notario Público
COMUNIDAD DE MASSACHUSETSS
Mi comisión expira el
29 de diciembre de 2028

Anexo A
Certificado CMMIDEV/5 fechado el 31 de marzo de 2022

CERTIFICADO DE LOGRO

GET GROUP HOLDINGS LTD

Unidad de Negocios de Pasaportes e Identificación y Soluciones Inteligentes
Le fue otorgado un CMMI NIVEL 5 DE VENCIMIENTO

CMMIDEV / 5

De CMMI DEV Versión 2.0 de CMMI Institute, USA
Siguiendo el Método de Evaluación v2.0 para la Mejora en los Procesos

Número ID Evaluación 58300

31 de marzo de 2022
Fecha

Logo CyberQ

Firma ilegible
Dr. Rajiv Nag (CyberQ)
(Certificado Alto Evaluador Jefe,
CMMI ID #0300282-01)

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los cuatro (4) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 147/25.

Ana María Feria

facetec

MANUFACTURER'S AUTHORIZATION

To: Junta Central Electoral of the Dominican Republic

Tender No.: JCE-CCC-LPI-2024-0001

THE PRINTING OF THE NEW IDENTITY AND ELECTORAL CARD (CIE) AND IDENTITY CARD (CI) (the "Project")

WHEREAS **FaceTec, Inc.**, who is the official producer of the *FaceTec ZoOm authentication software solution* and having production facilities at 10001 Park Run Drive, Summerlin, NV 89145, USA, does hereby exclusively authorize ***G.E.T. Secure ID Corp.***, located at *230 3rd Avenue, Waltham, MA 02451 USA* (hereinafter, together with the consortium in which it participates, the "Proposer"), to submit a proposal and subsequently negotiate and sign a contract with you for the above-referenced tender for resale of the following Product produced by us that Proposer will incorporate into its mobile identification solution:

- *FaceTec ZoOm authentication software solution (the "Product").*

Additionally, we confirm the facial liveness component used in the Product, which will be incorporated into Proposer's mobile identification solution, complies with ISO 30107-3, as is demonstrated by the ISO 30107-3 Confirmation Letter for the relevant Product component attached as Exhibit A.

We further authorize the Proposer to use our ISO 30107-3 certification and to directly provide development and integration services for the Product and hereby confirm that, in case the request for proposals process results in a contract between you and the Proposer, the above-listed Product will come with our full standard warranty.

The exclusive authority of the Proposer shall be limited to the Product for use for the Project in the Dominican Republic, and such exclusivity shall terminate on December 31, 2025, unless the Proposer is awarded the Project. If the Proposer is awarded a contract for the Project, the exclusivity and this authorization shall be automatically extended for the life of such contract.

Name: Satya Yenigalla, in the capacity of COO

Signed _____

Duly authorized to sign the authorization for and on behalf of: FaceTec, Inc.

Dated on this ~~31st day of January, 2025~~ February 7, 2025

© 2025 FaceTec, Inc. All Rights Reserved. Please visit www.FaceTec.com for additional information.

Exhibit A

ISO 30107-3 Confirmation Letter

(next page)

© 2025 FaceTec, Inc. All Rights Reserved. Please visit www.FaceTec.com for additional information.

BixeLab

Biometric Identity Experience & Evaluation Laboratory

Letter of Confirmation

for test report issued on the 27th of June 2023 for,

ISO/IEC 30107-3 compliant Presentation Attack Detection (PAD) Level 2 evaluation of,

BRYK.ID with FaceTec Server v9.6.30

To whom it may concern,

BixeLab is a biometric testing laboratory accredited by NIST (National Institute of Standards and Technology) under the National Voluntary Laboratory Accreditation Program (NVLAP testing Lab code: 600301-0) that conforms to the requirements of ISO/IEC 17025:2017 (General Requirements for Competence of Testing and Calibration laboratories).

Between April and May 2023, BixeLab evaluated the Item Under Test (IUT) in compliance with the applicable specifications of the ISO/IEC 30107-1 and ISO/IEC 30107-3 Presentation Attack Detection (PAD) testing and reporting standards.

The PAD evaluation was completed to a Level 2 sophistication in a secure laboratory testing environment using 8 Level A and 8 Level B Presentation Attack Instrument (PAI) species. 4 out of 8 Level B PAI species were tailored to the underlying technology based on pretesting. The PAIs were created for 15 conformant and consenting test subjects.

The evaluation consisted of 900 Level A attack presentations, 1200 Level B attack presentations, and 150 bona fide presentations. The following metrics were measured after original and supplementary testing. Testing resulted in the following metrics:

1. Attack Presentation Classification Error Rate (ACPER)
    a. 0% for Level A attacks
    b. 0% for Level B attacks
2. Attack Presentation Non-Response Rate (APNRR)
    a. 0% for Level A attacks
    b. 0.83% for Level B attacks
3. Bona fide Presentation Classification Error Rate (BPCER) of 0%
4. Bona fide Presentation Non-Response Rate (BPNRR) of 0%

This letter confirms that the IUT - BRYK.ID with Facetec Server v9.6.30 has been tested to the applicable ISO/IEC 30107-3 specifications for Presentation Attack Detection testing and reporting.

A detailed test and analysis report was generated to support the findings.

Ms. Somya Singh
Operations Manager
BixeLab Pty Ltd
info@bixelab.com

Dr. Ted Dunstone
Senior Responsible Officer
BixeLab Pty Ltd
info@bixelab.com

TRADUCCIÓN OFICIAL: ISO 30107-3 (Facetec)

058-2025

Yo, **Virginia Wall Guerra**, Intérprete Judicial de la República Dominicana, debidamente juramentada por el Consejo del Poder Judicial, titular de la cédula de identidad y electoral número 001-1637246-7, matrícula 47144, certifico que he traducido un documento cuyo original se encuentra en el idioma INGLÉS, marcado en mi protocolo con número 058-2025, cuyo texto en el idioma ESPAÑOL se leería de la forma siguiente:

[página 1]

[logo]

Autorización del fabricante

A la: Junta Central Electoral

N.° de licitación: JCE-CCC-LPI-2024-0001
LA IMPRESIÓN DE LA NUEVA TARJETA DE IDENTIDAD Y ELECTORAL (CIE) Y LA TARJETA DE IDENTIDAD (CI) ("el Proyecto")

CONSIDERANDO QUE, **FaceTec, Inc.**, es el productor oficial de la solución de software de autenticación FaceTec ZoOm y tiene instalaciones de producción en 10001 Park Front Drive, Summerlin, Nevada 89145, EE. UU., autoriza exclusivamente a G.E.T. Secure ID Corp., ubicada en 230 3rd Avenue, Waltham, MA 02451 EE. UU. (en adelante, junto con el consorcio en el que participa, el "Proponente"), a presentar una propuesta y posteriormente negociar un contrato con ustedes para la licitación de referencia anterior para la reventa del siguiente producto producido por nosotros que el proponente incorporará a su solución de identificación móvil:

• Solución de software de autenticación FaceTec ZoOm (el "Producto").

Además, confirmamos que el componente de vivacidad facial utilizado en el Producto, que se incorporará a la solución de identificación móvil del Proponente, cumple con la norma ISO 30107-3, como lo demuestra la Carta de Confirmación ISO 30107-3 para el componente del Producto correspondiente adjunta como Anexo A.

Autorizamos además al Proponente a utilizar nuestra certificación ISO 30107-3 y a proporcionar directamente servicios de desarrollo e integración para el Producto y por la presente confirmamos que, en caso de que el proceso de solicitud de propuestas dé como resultado un contrato entre usted y el Proponente, el Producto mencionado anteriormente vendrá con nuestra garantía estándar completa.

La autoridad exclusiva del Proponente se limitará al Producto para su uso en el Proyecto en la República Dominicana, y dicha exclusividad terminará el 31 de diciembre de 2025, a menos que el Proponente obtenga el Proyecto. Si el Proponente obtiene un contrato para el Proyecto, la exclusividad y esta autorización se extenderán automáticamente durante la vigencia de dicho contrato.

Virginia Wall Guerra
Intérprete Judicial de la República Dominicana
Alemán e Inglés

Nombre: Satya Yenigalla, en calidad de director de operaciones

Firmado: _____*[firma ilegible]*_____
Debidamente atuorizada para firmar por y en nombre de FaceTec, Inc.
Fechado en este día ~~31 de enero de 2025~~
Febrero 7, 2025

[pie de página]

FaceTec, Inc. 10001 Park Run Drive, Summerlin, NV 89145, USA
© 2025 FAceTec, Inc. Todos los derechos reservados. Por favor visite www.FaceTec.com para información adicional

[página 2]

Anexo A
Carta de confirmación ISO 30107-3
(próxima página)

[página 3]

[logo] BixeLab
Laboratorio de Experiencia y Evaluación de Identidad Biométrica

Carta de confirmación
del informe de prueba emitido el 27 de junio de 2023
para la evaluación de nivel 2 de detección de ataques de presentación (PAD)
conforme a la norma ISO/IEC 30107-3 de
BRYK.ID con FaceTec Server v9.6.30

A quien pueda interesar:

BixeLab es un laboratorio de pruebas biométricas acreditado por el NIST (Instituto Nacional de Normas y Tecnología) conforme al Programa Nacional Voluntario de Acreditación de Laboratorios (código de laboratorio de pruebas NVLAP: 600301-0) que cumple con los requisitos de la norma ISO/IEC 17025:2017 (Requisitos generales para la competencia de los laboratorios de prueba y calibración).

Entre abril y mayo de 2023, BixeLab evaluó el elemento bajo prueba (IUT) de conformidad con las especificaciones aplicables de las normas de prueba e informes de detección de ataques de presentación (PAD) ISO/IEC 30107-1 e ISO/IEC 30107-3.

La evaluación de PAD se completó hasta una sofisticación de Nivel 2 en un entorno de prueba de laboratorio seguro utilizando 6 especies de Instrumentos de Ataque de Presentación (PAI) de Nivel A y 8 de Nivel B. 4 de las 8 especies de PAI de Nivel B se adaptaron a la tecnología subyacente en función de pruebas previas. Los PAI se crearon para 15 sujetos de prueba conformes y que dieron su consentimiento.

La evaluación consistió en 900 presentaciones de ataques de Nivel A, 1200 presentaciones de ataques de Nivel B y 150 presentaciones auténticas. Se midieron las siguientes métricas después de las pruebas originales y complementarias. Las pruebas dieron como resultado las siguientes métricas:

1. Tasa de error de clasificación de presentación de ataques (ACPER)
a. 0 % para ataques de Nivel A
b. 0 % para ataques de Nivel B

2. Tasa de no respuesta a la presentación de ataques (APNRR)
a. 0 % para ataques de Nivel A
b. 0,83 % para ataques de nivel B

3. Tasa de error de clasificación de presentación (BPCER) de buena fe del 0 %

4. Tasa de falta de respuesta de presentación (BPNRR) de buena fe del 0 %

Esta carta confirma que el IUT - BRYK.ID con Facetec Server v9.6.30 se ha probado según las especificaciones ISO/IEC 30107-3 aplicables para pruebas e informes de detección de ataques de presentación.

Se generó un informe detallado de pruebas y análisis para respaldar los hallazgos.

[firma ilegible]
Srta. Somya Singh
Gerente de Operaciones
BixeLabPty Ltd
info@bixelab.com

[firma ilegible]
Dr. Ted Dunstone
Oficial Responsible Senior
BixeLab Pty Ltd
info@bixelab.com

-----Fin del documento traducido. Firma y sello al reverso-----

Virginia Wall Guerra
Intérprete Judicial de la República Dominicana
Alemán e inglés

Este documento se ha emitido a solicitud de parte interesada, en la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana, a los veintidós (22) días del mes de febrero del año 2025.

Virginia Wall Guerra
Intérprete Judicial en los
idiomas Alemán e Inglés
(809) 754-4979

Virginia Wall Guerra
Intérprete Judicial de la República Dominicana
Alemán e Inglés

MINISTERIO PÚBLICO
CENTRO DE ATENCIÓN AL CIUDADANO DISTRITO NACIONAL

Procuraduría General de la República
Confirme la validez de este documento ingresando el código CIS en portal.servicios.pgr.gob.do
Código CIS: 801-9202-7441947-2

EVIDEN
an atos business

To: Junta Central Electoral of the Dominican Republic

COPY SOLUTIONS INTERNATIONAL S.A. RNC 101698852 Santo Domingo, R.D.

MANUFACTURER'S AUTHORIZATION

Tender No.: JCE-CCC-LPI-2024-0001 THE PRINTING OF THE NEW IDENTITY AND ELECTORAL CARD (CIE) AND IDENTITY CARD (CI)

WHEREAS **KEYNECTIS SA**, who are, together with its business **CV Cryptovision GmBH** (jointly doing business under the commercial name "EVIDEN"), official producers of the IDnomic ID CA software solution and having production facilities at 5 RUE BELLINI TOUR ERIA, 92800 PUTEAUX France, do hereby exclusively authorize **G.E.T. Secure ID Corp.**, located at 230 3rd Avenue, Waltham, MA 02451 USA (hereinafter, together with the consortium in which it participates, the "Proposer"), to submit a proposal and subsequently negotiate and sign a contract with you for the above-referenced tender for resale of the following Product produced by us that Proposer will incorporate into its PKI solution:

- IDnomic ID CA, together with its respective components, maintenance and professional services (the "Product").

Additionally, we confirm the Product has Common Criteria EAL4+ certification, as is demonstrated in the attached **Exhibit A**. We further authorize the Proposer to use the CC EAL4+ certification and to directly provide development and integration services for the Product and hereby confirm that, in case the request for proposals process results in a contract between you and the Proposer, the above-listed Product will come with our full standard warranty.

Name: Simon Ulmer, in the capacity of Group VP/Head of Digital ID

Signed on Simon Ulmer
Group VP - Head of Digital ID – B2B Cybersecurity
M: +49 (0) 175 58 65 364
Tour Eria 5 rue Bellini 92800 Puteaux - France
evidian.com

Duly authorized to sign the authorization for and on behalf of: Keynectis SA/CV Cryptovision GmbH
Dated on this 13th day of February, 2025

Référence du rapport de certification	**ANSSI-CC-2021/17**
Nom du produit	**IDnomic ID CA**
Référence/version du produit	**Version 1.3.7**
Critère d'évaluation et version	**Critères Communs version 3.1 révision 5**
Niveau d'évaluation	**EAL 4 augmenté** ALC_FLR.3
Développeur	**IDNOMIC** 175 rue Jean-Jacques Rousseau 92138 Issy-les-Moulineaux Cedex, France
Commanditaire	**IDNOMIC** 175 rue Jean-Jacques Rousseau 92138 Issy-les-Moulineaux Cedex, France
Centre d'évaluation	**OPPIDA** 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables	**CCRA** Ce certificat est reconnu au niveau EAL2 augmenté de FLR.3. **SOG-IS** Ce certificat est reconnu au niveau EAL4 augmenté de FLR.3.

Página/Folio No.812 de 843

TRADUCCIÓN OFICIAL: EAL4+ (IDnomic)

059-2025

Yo, **Virginia Wall Guerra**, Intérprete Judicial de la República Dominicana, debidamente juramentada por el Consejo del Poder Judicial, titular de la cédula de identidad y electoral número 001-1637246-7, matrícula 47144, certifico que he traducido un documento cuyo original se encuentra en el idioma INGLÉS, marcado en mi protocolo con número 059-2025, cuyo texto en el idioma ESPAÑOL se leería de la forma siguiente:

[logo] EVIDEN
Un negocio atos

A la: Junta Central Electoral de la República Dominicana

AUTORIZACIÓN DEL FABRICANTE

N.º de licitación: JCE-CCC-LPI-2024-0001 IMPRESIÓN DE LA NUEVA TARJETA DE IDENTIDAD Y ELECTORAL (CIE) Y DE LA TARJETA DE IDENTIDAD (CI)

CONSIDERANDO QUE **KEYNECTIS SA**, que junto con su empresa **CV Cryptovision GmbH** (que operan conjuntamente bajo el nombre comercial "EVIDEN"), son productores oficiales de la solución de software IDnomic ID CA y tienen instalaciones de producción en 5 RUE BELLINI TOUR ERIA, 92800 PUTEAUX Francia, autorizan exclusivamente a G.E.T. Secure ID Corp., con domicilio en 230 3rd Avenue, Waltham, MA 02451 EE. UU. (en adelante, junto con el consorcio en el que participa, el "Proponente"), para presentar una propuesta y posteriormente negociar y firmar un contrato con usted para la licitación antes mencionada para la reventa del siguiente Producto producido por nosotros que el Proponente incorporará a su solución PKI:

• IDnomic ID CA, junto con sus respectivos componentes, mantenimiento y servicios profesionales (el "Producto").

Además, confirmamos que el Producto cuenta con la certificación Common Criteria EAL4+, como se demuestra en el **Anexo A**. Además, autorizamos al Proponente a utilizar la certificación Common Criteria EAL4+ y a proporcionar directamente servicios de desarrollo e integración para el Producto y por la presente confirmamos que, en caso de que el proceso de solicitud de propuestas dé como resultado un contrato entre usted y el Proponente, el Producto mencionado anteriormente vendrá con nuestra garantía estándar completa.

Nombre: Simon Ulmer, en calidad de vicepresidente de grupo/director de DI digital cast.

Virginia Wall Guerra
Intérprete Judicial de la República Dominicana
Alemán e Inglés

[firma ilegible] Firmado por Simon Ulmer
VP de Grupo + Jefe de ID Digital – BDS Cyberproducts
Cel: +49 (0) 175 58 65384
Tour Eria 5 rue Bellini 92800 Puteaux – Francia
Eviden.com

Debidamente autorizado para firmar la autorización en nombre y representación de: Keynectis SA/CV Cryptovision GmbH
Fechado el 13 de febrero de 2025

Keynectis SA
5 Rue Bellini, Tour Eria
92800
Francia

idnomic.com

478 217 318
R.C.S. Nanterre

[página 2]

Anexo A
Certificado IDnomic ID CA CC EAL4+

[página 3]

Informe de Certificación
ANSSI-CC-2021/17

IDnomic ID CA
(Version 1.3.7)

Referencia de informe de certificación **ANSSI-CC-2021/17**
Nombre del producto **IDnomic ID CA**
Referencia/versión del producto **Version 1.3.7**
Criterio de evaluación y versión **Criterios comunes versión 3.1, revisión 5**
Nivel de evaluación **EAL 4 aumentada** ALC_FLR.3
Desarrollador **IDNOMIC** 175 rue Jean-Jacques Rousseau 92138 Issy-les-Moulineaux Cedex, Francia

Virginia Wall Guerra
Intérprete Judicial de la República Dominicana
Alemán e Inglés

Comanditario	**IDNOMIC** 175 rue Jean-Jacques Rousseau 92138 Issy-les-Moulineaux Cedex, Francia
Centro de evaluación	**OPIDDA** 4-6 avenue du vieil étang, Edificio B, 78180, Montigny le Bretonneux, Francia
Acuerdos de reconocimiento aplicables	
[logo] **CCRA** Este certificado está reconocido para el nivel EAL2 aumentado de FRL.3.	*[logo]* **SOG-IS** Este certificado está reconocido para el nivel EAL4 aumentado de FLR.3.

[logo]

Este documento se ha emitido a solicitud de parte interesada, en la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana, a los veintidós (22) días del mes de febrero del año 2025.

Virginia Wall Guerra
Intérprete Judicial en los idiomas Alemán e Inglés
(809) 754-4979

Página/Folio No.816 de 843

Brochures

GET GROUP CLM600

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852

CLM600

PERSONALIZACIÓN POR GRABADO LÁSER

CLM600 es un sistema de personalización de tarjetas integrado, diseñado para funcionar de manera opcional con la impresora de retransferencia CP500. Cuenta con grabado láser de alta precisión para gráficos y funciones avanzadas de seguridad grabadas con láser para impresión en blanco y negro. Con su tamaño ultracompacto, el CLM600 combina a la perfección el grabado láser y ofrece un rendimiento potente sin concesiones.

www.getgroup.com

Página/Folio No.818 de 843

La CLM600 es una solución de vanguardia que incorpora un láser de fibra de 20W flexible y confiable, que ofrece la misma calidad de grabado de alto rendimiento de toda nuestra gama de productos.

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC 101898852
Santo

Características

- Posibilidad de personalización segura.
- Grabado láser de alta precisión y calidad.
- Diseño compacto y ligero.
- Manipulación automatizada de tarjetas.
- Fuente láser de larga duración.
- Apilador de salida seguro y bandeja de rechazos.

Especificaciones del CLM600

Tipo de láser	Fuente láser de fibra de 20W
Resolución	hasta 600 dpi
Material de la tarjeta	PC, PVC-L aprobado para documentos ID1
Velocidad de marcado	La velocidad de marcado de texto es de 900 m/s. Velocidad de marcado de imágenes es: 900m/s Rendimiento CPH: 60 tarjetas por hora
Lado de marcado	Doble cara
Características de marcado	Grabado de foto, datos, códigos de barras, elementos gráficos, CLI/MLI y táctil.
Cámara de autoposicionamiento	Cámara en blanco y negro para ajuste XY
Bandeja de salida	Capacidad: más de 100 tarjetas
Opciones	Sistema de visión Módulo CLI/MLI Lectura de códigos de barras Apilador de tarjetas de entrada opcional: Disponible para 100 a 300 tarjetas. Control de calidad para HW y SW opcionales para calidad total en un solo paso. Accesible a través de SDKs.
Conectividad	LAN Ethernet
Sistema operativo	Windows® 10, Windows® 11 (32/64bit).
Fuente de alimentación	110/220 V CA 50/60 Hz
Consumo eléctrico	0.3 KW
Condiciones ambientales	Temperatura ambiente de 20 a 25°C 60% de humedad relativa
Peso	Aprox. 29 kg
Dimensiones	340mm x 310mm x 540mm (ancho x fondo x alto)

700+
2B+
14+
35+
CMMI DEV /5

La identificación se digitaliza. Las licencias de conducir o documentos de identidad móviles ofrecen comodidad, seguridad e interoperabilidad como alternativa instantánea a los documentos de identidad físicos de plástico, al tiempo que ayudan a prevenir el fraude. Las identificaciones móviles también sientan las bases para una amplia gama de servicios digitales en línea. Los ciudadanos quieren que su documento de identidad sea aceptado en todas partes, y la norma ISO/IEC 18013-5 lo permite.

Con GET Mobile Verify, las empresas pueden transformar su manera de prestar servicios en persona y en línea.

La autenticación de datos y usuarios es instantánea, y las especificaciones de seguridad de las identidades almacenadas cumplen las normas ISO y AAMVA, sentando así las bases para una amplia gama de servicios de identidad.

SOLUCIONES GET MOBILE ID

MOSIP INTEGRATED

ISO 18013-5

CERTIFIED

MOBILE ADMINISTRATOR

Aplicaciones y servicios web que permiten a las autoridades emisoras integrar rápidamente los SOR existentes para emitir mID y mDL firmados digitalmente.

GET MOBILE

MOBILE ID

Aplicaciones móviles para los ciudadanos, disponibles para Android e iOS, que permiten a los ciudadanos compartir su ID de forma segura y proteger su privacidad

GET

MOBILE VERIFY

Aplicaciones, y APIs para verificadores, para aceptar mIDs y mDLs con confianza, disponibles para Android, iOS, Windows y Web

GET

Página/Folio No.820 de 843

GET MOBILE

GET GROUP

COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

GET MOBILE ID

TU ID DE CONFIANZA EN CUALQUIER LUGAR

www.getgroup.com

MECANISMOS DE CONFIANZA - ISO 18013-5

Casos de uso de mID

Página/Folio No. 822 de 843

CUMPLIMIENTO Y SOPORTE DE NORMAS

- Cumple las directrices de AAMVA
- Cumple con la certificación ISO/IEC18013
- Comunicación peer to peer NFC nativa

COPY SOLUTIONS INTERNATIONAL S.A.
RNC: 101894752
Santo Domingo, R.D.

MODOS DE COMUNICACIÓN

- TLS 1.3 y versiones posteriores
- NFC peer mode
- Bluetooth peer to peer mode
- Wifi Aware Neighbor Awareness
- Código QR

CARACTERÍSTICAS DE CONTROL DE SEGURIDAD

- Seguridad redundante mediante almacenes de claves respaldados por hardware
- Cifrado de datos en reposo y transmisión cifrada basada en sesiones
- Los datos de mID están firmados por la autoridad emisora de confianza a prueba de manipulaciones
- La ofuscación de aplicaciones significa que el código ejecutable no se puede piratear
- OAuth habilitado para autorización de agentes del orden
- Seguridad revisada para el nivel de garantía de identidad

Por qué GET Group

MSECB MSECB

CMMIDEV/5

Copyright © 2023 GET Group. All rights reserved.

GET TRUST

GET GROUP

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC 101898852
Santo Domingo, R.D.

INSPIRANDO CONFIANZA

INFRAESTRUCTURA AVANZADA DE LLAVE PÚBLICA

www.getgroup.com

GET Trust es una solución avanzada de Infraestructura de Llave Pública (PKI) desarrollada para afirmar la seguridad de los datos y garantizar la autenticidad del remitente detrás de los datos. La solución esencial para todos los sectores gubernamentales, instituciones financieras y ecosistemas jurídicos para los que la garantía de primer nivel de la identidad electrónica y digital es obligatoria para las transacciones diarias.

GET Trust incorpora procesos de seguridad optimizados con varios mecanismos para garantizar la seguridad, facilitar el intercambio de información privada y ayudar a proteger los datos, sistemas, dispositivos y redes, de ataques maliciosos y fraudulentos.

PRINCIPALES CARACTERÍSTICAS:

Simplificar la Gestión de Certificados

GET Trust ha sido dotado de un proceso optimizado de automatización de la emisión, revocación y renovación de certificados digitales, lo que reduce el esfuerzo manual requerido para la gestión de certificados y disminuye el riesgo de interrupciones relacionadas con los mismos.

Altamente Escalable

GET Trust es una solución completamente escalable construida con la modularidad en mente, capaz de manejar un gran número de certificados digitales y usuarios, sin afectar el rendimiento o la seguridad. Adicionalmente es capaz de soportar varios tipos de certificados digitales, incluyendo SSL/TLS, S/MIME, y certificados de firma de código.

Gestión segura de Llaves

GET Trust garantiza la confidencialidad, integridad y disponibilidad de los certificados y llaves digitales para salvaguardar los activos digitales sensibles mediante mecanismos adecuados de cifrado y autenticación, incluida la autenticación basada en certificados, la revocación de certificados en caso de estar comprometidos o por uso indebido, la autenticación multifactor y varios métodos de recuperación en caso de pérdida o corrupción de llaves.

PKI personalizada

Con GET Trust, las organizaciones pueden diseñar jerarquías y perfiles de certificados, así como herramientas de supervisión e informes en tiempo real que se ajusten a sus necesidades. Además, permite una integración perfecta con la infraestructura de TI existente.

Orientado a Servicio

Los servicios de GET Trust son autónomos y modulares; la implantación del software es más flexible y ágil porque se pueden introducir o ajustar nuevos servicios sin afectar todo el sistema. Los servicios fomentan la reutilización porque pueden ser utilizados por numerosas aplicaciones o sistemas.

Cumplimiento

GET Trust cumple plenamente las normas y reglamentos del sector, como la norma X.509 para certificados digitales. Certificación Common Criteria EAL4+ opcional

VENTAJAS DEL SISTEMA:

Autenticación:

Permite a las empresas autenticar de forma segura y confiable la identidad de usuarios y dispositivos, garantizando que sólo el personal y los sistemas autorizados tengan acceso a la información crítica.

Confidencialidad:

Utilizando GET Trust las organizaciones pueden operar con confianza, sabiendo que su información sensible está segura y protegida.

No repudio

Mejora la confiabilidad y la credibilidad. Esto contribuye a aumentar la confianza entre clientes, socios y reguladores.

REST API

Proporciona a las empresas un poderoso conjunto de herramientas para crear aplicaciones seguras y confiables, lo que lo convierte en un componente esencial de cualquier stack de desarrollo de software moderno.

Interoperabilidad

Proporciona una manera fluida y confiable para intercambiar certificados digitales, llaves y cualquier otra información de seguridad crítica. Esto permite a las organizaciones establecer confianza y garantizar la confidencialidad, integridad y disponibilidad de sus datos y sistemas.

COPY SOLUTIONS INTERNATIONAL, S.A.
CSI
RNC: 101898852
Santo Domingo, R.D.

COMPONENTES DEL SISTEMA:

GET Trust Autoridad de certificación
Permite a las empresas gestionar de forma sencilla sus infraestructuras de seguridad y simplifica el mantenimiento de llaves y certificados digitales.

01

GET Trust Repositorio de certificados
Proporciona un enfoque seguro y escalable para gestionar certificados digitales, simplificando a las organizaciones la emisión, revocación y actualización de certificados según sea necesario.

02

GET Trust Autoridad de registro
Proporciona una gestión segura y eficiente de las identidades de usuarios y dispositivos, así como la emisión de certificados digitales que autentican sus identidades.

03

GET Trust Autoridad de Validación
Una sofisticada herramienta para verificar la autenticidad de los certificados digitales emitidos por las Autoridades de Certificación (CA) antes de que se utilicen.

04

GET Trust Descubrimiento de certificados
Ofrece a las empresas un destino centralizado para descubrir, gestionar y supervisar sus certificados digitales. Proporcionando visibilidad de todos los certificados en uso.

05

COMO FUNCIONA:

GET Trust aborda el reto del acceso seguro a las empresas, aprovechando tecnologías avanzadas de cifrado y certificados digitales. Nuestros completos servicios de seguridad dan soporte a casos de uso críticos en múltiples dominios, ayudando a las empresas a proporcionar un acceso seguro a servicios y aplicaciones, al tiempo que se protege frente a amenazas sofisticadas.

Firmas digitales:

Más seguras que las firmas en papel. Asegura la validez e integridad de los documentos y transacciones electrónicas, garantizando que no han sido manipulados ni alterados.

Compatible con soluciones de identificación de pasaportes electrónicos:

Solución de seguridad de última generación que proporciona una identificación segura y confiable a los ciudadanos.

Redes privadas y seguridad VPN

Garantiza la confidencialidad, integridad y disponibilidad de los datos permitiendo el uso de certificados digitales para la autenticación, cifrando las transmisiones de datos y proporcionando controles de acceso eficaces.

Autenticación de usuarios y dispositivos

Gestiona las identidades de todos los usuarios y dispositivos de su empresa desde una única plataforma para simplificar la shadow IT y aprovechar sus ventajas.

Seguridad de correo electrónico

Gracias a las completas funciones de cifrado de correo electrónico estándar del sector, la seguridad de las comunicaciones se hace más sencilla.

Sitios web y servicios

Facilita el uso de funciones de seguridad como la gestión de permisos, la firma electrónica, el recibo digital y el cifrado en toda una gama de aplicaciones para el lugar de trabajo.

Firmado de código

Asegura la reputación del software y garantiza la autenticidad, integridad y el no repudio del código para salvaguardarlo contra la inyección de Malware.

POR QUÉ GET GROUP

CMMI DEV/5

Copyright © 2025 GET Group. All rights reserved.

EOS REBEL T7

CARACTERÍSTICAS

- Resolución: 24.1 megapíxeles.
- Procesador: DIGIC 4+.
- Compatibilidad inalámbrica Wi-Fi y NFC.
- Tipo de sensor: CMOS APS-C (22.3 mm x 14.9 mm).
- Sensibilidad ISO AUTO (100-6,400). Expandible hasta (12,800).
- LCD: 3.0" (7.5 cm) tipo/pantalla aumentó y (920,000 píxeles).
- Disparo en ráfaga: Máx. 3fps para aprox. 69 imágenes JPEG, 6 imágenes RAW.
- Balance de blancos: AUTO. Activado fotografía menos rojos.
- Visor óptico: Visor luminoso con aprox. 95% de cobertura. Magnification aprox. 0.8x.
- Mini salida HDMI.
- Flash incorporado.
- Tarjetas de memoria: SD, SDHC & SDXC.
- Sensores AF: 9 (9 cruz), 1 tipo cruz al centro.
- Modos de disparo: Modos de Escena: Automático inteligente, Sin Flash, Auto creativo, Retrato, Paisaje, Deporte, Retrato nocturno y el mismo modo de disparo Cámara.
- EOS video: -Full HD 1920 x 1080 (MOV: 30p/25p/24p). -HD 1280 x 720 (MOV: 60p/50p). -SD 640 x 480 (MOV: 30p/25p).
- Dimensiones aproximadas: (W) x (H) x (D) = (mm/pulg/pulg/profundidad).

CONTENIDO DEL KIT

- EOS Rebel T7 cuerpo.
- Lente EF-S 18-55 mm.
- Cargador LC-E10.
- Batería LP-E10.
- Correa de mano EW-4000.
- Tapa de lente.
- Ocular EF.

ACCESORIOS

La EOS Rebel T7 es compatible con toda la línea de Flash Speedlite, Lentes EF y EF-S de Canon y una gran variedad de accesorios.

/canonmexicano @CanonMexicano canon.com.mx

6220B458

ZOOM iN

La comunidad fotográfica exclusiva de Canon Mexicana te da la bienvenida por haber adquirido tu kit fotográfico.

Disfruta de los beneficios exclusivos que ZOOM iN tiene para ti, así como:

- Seminarios y cursos de fotografía
- Mantenimiento preventivo gratuito
- Descuentos en escuelas de fotografía

Sólo regístrate en www.canonzoomin.com

CONOCE LAS FUNCIONES DE TU NUEVA CÁMARA EN UNA SOLA CLASE CORTESÍA DE CANON MEXICANA

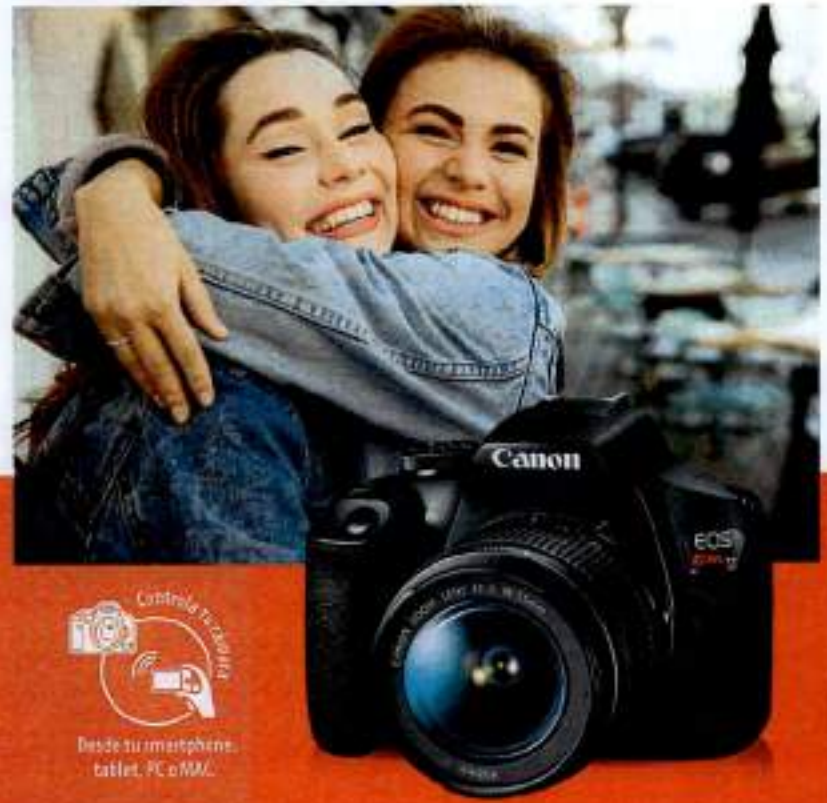
Canon

Canon

EOS REBEL T7

COPY SOLUTIONS CSI RNC: 101868352 Santo Domingo, R.D.

COMPARTE TUS MEJORES MOMENTOS



Controla tu cámara desde tu smartphone, tablet, PC o MAC.

9 Puntos AF · Wi Fi CERTIFIED · NFC · 24.1 MEGA PIXELS CMOS · Filtro Creativo · FULL HD 1080

Canon

Canon

Comparte tus mejores fotos

La **EOS Rebel T7** cuenta con la más alta calidad que tus fotografías y videos merecen. Es ideal para las personas con cámaras digitales ó teléfonos inteligentes que desean obtener imágenes aún más asombrosas. Equipada con un sensor de imagen CMOS de 24.1 megapixeles y un procesador de imagen DIGIC 4+ para obtener fotos y videos con detalles precisos y colores brillantes, aún en condiciones de poca luz.

No te olvides de compartir tus mejores fotos en redes sociales, gracias a la conectividad **Wi-Fi y NFC** integrada en la EOS Rebel T7.

Captura y comparte

Con la **EOS Rebel T7** que incorpora la tecnología Wi-Fi y NFC ahora podrás, compartir imágenes y disparar de forma remota desde tu smartphone, tablet, PC o Mac.

Todas las imágenes son con Fines Ilustrativos

EOS REBEL T7

Sensor CMOS de 24.1 megapixeles y Procesador DIGIC 4+

24.1 MEGA PIXELS CMOS

Gracias al sensor de alta resolución se pueden capturar fotografías y videos con detalles más nítidos, mientras que el procesador de imagen DIGIC 4+ convierte la luz recibida por el sensor en detalles más finos y de alta calidad.

Sensibilidad ISO

ISO 6400 6400

El rango de ISO parte del 100 al 6,400 y puede ser expandible hasta 12,800. Con estas sensibilidades podrás realizar tomas fotográficas y videos desde un interior, al aire libre o fotografía nocturna sin problema.

Video FULL HD

FULL HD 1080

Gracias al sensor CMOS y a la compatibilidad con toda la línea de lentes es posible grabar películas de bajo ruido con grandes efectos a una alta definición. Utiliza ISO 6,400 en video para grabar escenas nocturnas.

9 Puntos de autoenfoque

La nueva cámara **EOS Rebel T7** cuenta con 9 puntos de autoenfoque y con 1 punto tipo cruz al centro, lo cual permite un enfoque más preciso.
El AF Servo mantiene continuamente un seguimiento de los objetos en movimiento para obtener las mejores tomas, incluyendo deportes, autos y parque de diversiones.

Compatible con la línea de lentes intercambiables

EF Lenses EF-S Lenses

Además la **EOS Rebel T7** es totalmente compatible con la amplia variedad de lentes intercambiables EF y EF-S en video y fotografía.

Utilice lentes desde un gran angular para obtener fotos o videos de paisajes, hasta un telefoto para capturar objetos a larga distancia.

Filtros Creativos

Diviértete cambiando por completo el ambiente con los 5 tipos de filtros creativos con los que cuenta.

Todas las imágenes son con Fines Ilustrativos

COPY SOLUTIONS INTERNATIONAL, S.A. RNC. 101893522 Santo Domingo, R.D.

SOLUCIONES BIOMÉTRICAS

Lector DigitalPersona® 4500

APLICACIONES

- Seguridad de PC de escritorio
- Seguridad de PC móvil
- Aplicaciones personalizadas

LECTOR ÓPTICO DE HUELLAS DACTILARES CON CONEXIÓN USB

El lector de huellas dactilares DigitalPersona 4500 es un dispositivo periférico, con conexión USB, ideal para usuarios únicos de computadores de escritorio, así como para varios usuarios en entornos compartidos. Su diseño compacto permite liberar espacio en los escritorios de las compañías, mientras que su aspecto profesional y moderno lo hace ver elegante en entornos de punto de venta. El lector DigitalPersona 4500 utiliza tecnología óptica de escaneo de huellas dactilares para lograr una excelente calidad de imagen, una amplia área de captura y una confiabilidad óptima. Tiene un revestimiento de silicona que le permite leer un amplio rango de huellas dactilares con rapidez y precisión, sin importar el ángulo en que se ubique el dedo. La carcasa de metal de alta calidad es resistente al desplazamiento involuntario.

Para usarlo, simplemente ubique un dedo en la pantalla del lector y este capturará y codificará, rápida y automáticamente, la imagen de la huella dactilar antes de enviarla al motor biométrico de DigitalPersona® FingerJet™ para su verificación. El usuario tendrá una retroalimentación óptma gracias a una luz intermitente roja que le indica que la imagen de la huella dactilar ha sido capturada.

El diseño del lector de huellas dactilares DigitalPersona 4500 permite su uso con una amplia variedad de programas de software, incluyendo nuestras soluciones de autenticación así como con la mayoría de nuestros kits de desarrollo de software DigitalPersona. Independientemente de si usted es un cliente corporativo o un integrador de sistemas, las soluciones de verificación de identidad biométrica de DigitalPersona son una extensión lógica de su sistema y aplicaciones de seguridad.

Página/Folio No.830 de 843

CARACTERÍSTICAS

- LED azul
- Tamaño compacto
- Excelente calidad de imagen
- Resistencia óptima contra descargas electrostáticas
- Datos de huellas dactilares cifrados
- Rechazo de huella dactilar latente
- Rechazo de huella dactilar falsificada
- Rotación invariable
- Robusto
- Funciona bien con huellas dactilares secas, húmedas o ásperas
- Compatible con la mayoría de los SDK de DigitalPersona

ESPECIFICACIONES

Voltaje de suministro	5,0 V ±5 % suministrado mediante USB
Corriente de alimentación: escaneo	< 100 mA (típico)
Corriente de alimentación: en reposo	120 mA (típico)
Corriente de alimentación: modo suspensión	< 0,5 mA (máximo)
Inmunidad contra descarga electrostática (ESD, por sus siglas en inglés)	>15 kV, montado en la caja
Temperatura de operación	0 - 40 °C
Humedad de almacenamiento	20 % - 90 % sin condensación
Información escaneada	Escala de grises de 8 bits
Cumplimiento de normas	FCC Clase B, CE, ICES, BSMI, MIC, USB, WHQL
Peso	105 gramos
Interfaz	Dispositivo USB 2.0 de velocidad máxima, de alta potencia

Datos sujetos a cambio sin notificación previa

hidglobal.com

Norteamérica: +1 512 776 9000
Línea gratuita: 1 800 237 7769
Europa, Medio Oriente, África: +44 1440 714 850
Asia Pacífico: +852 3160 9800
Latinoamérica: +52 55 5081 1650

© 2012 HID Global Corporation/ASSA ABLOY AB. Todos los derechos reservados. HID, HID Global, el logotipo del ladrillo azul de HID, DigitalPersona, Finger Jet y el diseño de cadena son marcas comerciales o marcas comerciales registradas de HID Global o de sus licenciantes y proveedores en EE. UU. y otros países y no se deben utilizar sin la correspondiente autorización. Todas las demás marcas comerciales, marcas de servicio y nombres de productos o servicios son marcas comerciales o marcas comerciales registradas de sus respectivos propietarios.
2012-05-14-eol-digitalpersona-4000-reader-ds-es PLT-04538

An ASSA ABLOY Group brand

ASSA ABLOY

Página/Folio No.831 de 843

Serie BSC-10

NUEVA Impresora accesible de calidad y alta velocidad

COPY SOLUTIONS INTERNATIONAL, S.A.
RNC. 101558052
Santo Domingo, R.D.

Star Micronics se enorgullece en anunciar el lanzamiento de la BSC-10. La BSC-10 de Star es una impresora económica de alta velocidad y de impresión térmica directa. Disponible con conexión LAN, ya puedes conectar facilmente la BSC-10LAN a su red.

Con su diseño simple y carga fácil de papel, esta impresora fue diseñada para superar a la competencia en los entornos de retail y hospitalidad. Su alta velocidad de procesamiento de recibos (250mm/segundo), su interface dual y habilidad de soportar rollos de papel de 10cm, la hace la primera opción para los vendedores de retail y operadores globales de la industria de la hospitalidad. La BSC-10 está disponible en 3 modelos facilitándole al cliente el trabajo de selección del modelo adecuado según la aplicación.

Modelos USB/Serial, USB/Paralela y Ethernet están disponibles. La BSC-10 también cuenta con emulación de impresión ESC/POS con la utilidad de configuración Star, incluyendo OPOS y compatibilidad con cajones de dinero ESC/POS. La BSC-10 viene con adaptador de corriente.

- **Ultra rápida a 250mm/seg**
- **Compatible con ESC/POS**
- **Viene con fuente de poder**
- **Alta resolución de 203 dpi**
- **Fácil instalación y mantenimiento**

Serie BSC-10

NUEVA Impresora accesible de alta calidad y velocidad
Diseñada específicamente para satisfacer las necesidades básicas de impresión de recibos.

Utilitario "StarPRNT Intelligent"

Compacta y de fácil cargado de papel "Drop-In & Print"
Sin palanca de apertura de la tapa a umentando así la confiabilidad.

Interfaz dual
Serial/USB
Paralelo/USB o
Ethernet

BSC10UC gris – Gris USB / Paralelo
BSC10UD gris – Gris USB / RS232
BSC10E gris – Gris Ethernet

Con emulación ESC / POS™ y utilidad de configuración STAR que incluye compatibilidad con OPOS™ y Cajón de dinero Epson.

No hay interruptores de configuración, todo es configurable por software.

Todo incluido, impresora, fuente de alimentación y el conjunto de utilidades StarPRNT con certificación WHQL.

Incluido en la caja
CD y Fuente de alimentación PS-60.

Fácil Reposición
del cabezal de impresión, cortador automático y PCB. Basta con quitar la tapa frontal de la impresora para acceder al cabezal de impresión, el cortador automático o a la placa principal (PCB).

Especificaciones de la Impresora BSC-10

Características	**Hardware** Rápida: Hasta 250mm/s Fácil cargado de papel "Drop-In & Print" Cortador Automático de Guillotina. Ocupa poco espacio. Conexión de cables empotrados. **Software** (Incluido en Windows® Drivers) Utilidad para la impresión de Logos (Logos de la tienda, cupones y artes gráficas) Capacidad de compresión de recibos Búsqueda de texto inteligente 'STAR' y función de impresión de cupones.
Conectividad	**Serial/USB** **Paralelo/USB** **Ethernet**
Controladores	Windows® XP SP3 Vista (32 bit / 64 bit) SP2 Windows® 7 (32 bit / 64 bit) SP1 OPOS driver
Qué está Incluido	**Impresora BSC-10** **CD con driver, manual y utilidades** **Fuente de alimentación**
Accesorios Opcionales	Timbre / Buzzer (BU01-24-A)
Especificaciones Técnicas	Método de Impresión : Térmico Directo Velocidad de Impresión : 250mm/segundo Ancho de Papel : 80mm / 58mm Espesor/Peso : 0.06 – 0.085mm Diámetro de papel : Max 102mm Emulación : ESC/POS™ Circuito Controlador de Periféricos 2 circuitos (24V Máx. 1A), 1 Entrada de compulsión Resolución de Impresión: 203 dpi MCBF: 60 Millones de Líneas Cortador Automático: Un Millón de Cortes Dimensiones: 142 (An) x 212 (L) x 149 (Al) mm
Garantía	2 años de Garantía
Para Mayor Información	Ventas: +1 732-623-5500 ext. 648 Sitio Web: http://espanol.starmicronics.com http://www.starmicronics.com.mx/

10 cm de diámetro del rollo de papel de capacidad

10cm único fuera de la capacidad de rollo de papel de diámetro, con un 60% más de papel en un rollo de lo que significa menos cambios de rollo de papel, disminución del costo por la recepción, el transporte reduce el rollo de papel y los requisitos de almacenamiento.

Ningún otro fabricante puede ofrecer todo esto!

10CM ROLLO DE PAPEL DE AHORRO DE VENTAJAS DE STAR		
Ancho del papel	80mm	80mm
Diámetro exterior	79.5mm	102mm
Tamaño de núcleo	12.7mm	12.7mm
Grosor del papel	65 micras	65 micras
Longitud de papel en un rodillo	74m	119m
Aumentar con el rollo estándar	0%	60%

9/27/13

Canon

imageFORMULA P-208II

ESCÁNER DE DOCUMENTOS PERSONAL ULTRACOMPACTO Y FÁCIL DE USAR

El escáner de documentos personal imageFORMULA P-208II es de tamaño ultracompacto y cuenta con características poderosas que lo hacen ideal para el uso en casa, oficina o en cualquier lugar que se encuentre. El cambiarlo de ubicación es tan fácil como su capacidad para llevar la información desde el papel hacia dispositivos Windows® y Mac®, y más allá.

AMPLIA VARIEDAD DE APLICACIONES

El escáner P-208II es ideal para usuarios que se mantienen en un lugar fijo y para los "guerreros del camino" que trabajan en las áreas de servicios profesionales, servicios financieros, servicios de salud, entre otros. Permite el escaneo de distintos tipos de documentos como por ejemplo: tarjetas de presentación, fotografías, facturas, contratos, informes, cartas, tarjetas de ID plásticas, licencias de conducir y muchos más. Ya sea que lo utilice en casa, en la oficina o mientras se traslada de un lugar a otro, el dispositivo puede ayudarle a mejorar su productividad, organización y eficiencia personal.

PORTÁTIL Y CONVENIENTE

Activado mediante un cable USB cuando está conectado a una computadora, el escáner P-208II ayuda a reducir el exceso de cables para permitir un proceso de escaneo rápido. Los usuarios se pueden beneficiar de su tamaño compacto, peso ligero y flexibilidad para escanear documentos con facilidad ya que se puede guardar en un maletín o en una bolsa para transportarlo sin complicaciones.

FACILIDAD DE USO

Al conectarse a una computadora, el escáner P-208II les permite a los usuarios "conectar y escanear" sin la necesidad de instalar software controladores ni aplicaciones. Además, con un solo clic puede ajustar automáticamente varias configuraciones de características para brindar fácilmente la mejor imagen escaneada. El software CaptureOnTouch de Canon integrado les permite a los usuarios configurar los trabajos de rutina para un acceso de un toque rápido y fácil. También permite enviar imágenes escaneadas directamente hacia aplicaciones en la nube de otros fabricantes,* como Evernote™, Microsoft® SharePoint®, Google Drive™, SugarSync, OneDrive y Dropbox. Este escáner también incluye los software controladores ISIS® y TWAIN para lograr una fácil integración con los sistemas de administración de contenido y de captura de otros fabricantes.

OPERACIÓN FLEXIBLE

El escáner P-208II puede escanear ambos lados de un documento al mismo tiempo, en color o en blanco y negro. Puede manejar una gran variedad de tipos de documentos, incluyendo documentos gruesos o delgados y tarjetas plásticas o tarjetas con relieve. Este escáner también puede manejar documentos largos y detectar cuando ocurre una alimentación doble para ayudar a garantizar que no se pierdan datos. Una capacidad inalámbrica opcional** aumenta las opciones de conectividad. Cuando se combina con el Adaptador Inalámbrico y Paquete de Baterías opcional WU10*, el escáner no solo funciona de forma inalámbrica en los entornos de Windows y Mac, sino también con los dispositivos iPad®, iPhone®, iPod touch® y Android™ mediante la aplicación descargable Canon CaptureOnTouch Mobile.*

imageFORMULA

P-208II

CARACTERÍSTICAS PODEROSAS

Para una máxima calidad de imagen, el escáner P-208II incluye características para ayudarle a mejorar la legibilidad de documentos difíciles de escanear. La configuración de Resolución Automática es útil para escanear tandas combinadas de documentos y fotografías ya que ajusta automáticamente la resolución para mejorar la calidad de la imagen y reducir el tamaño de los archivos. Otras características incluyen la capacidad de optimizar las imágenes de las fotografías escaneadas y el Reconocimiento Óptico de Caracteres (OCR), además de ayudarle a convertir los documentos que están originalmente en papel en información digital en la que puede realizar búsquedas, puede almacenar y compartir fácilmente.

CONCIENCIA AMBIENTAL

El escáner P-208II cumple con los lineamientos de ENERGY STAR® en cuanto al consumo eficiente de energía y cumple con las directivas WEEE y RoHS de la Unión Europea para la reducción de sustancias peligrosas y productos de desechos.**

ESPECIFICACIONES

Tipo:	Escáner de Documentos Personal
Alimentación de documentos:	Automática o manual
Tamaño de los documentos:	
Anchura:	De 2.0" a 8.5"
Longitud:	De 2.8" a 14.4"
Peso del documento:	Papel Común de 14 a 34 lb
Capacidad del alimentador:	10 hojas
Escala de grises:	8 bits
Color:	24 bits
Fuente de luz:	LED RGB
Elemento de escaneo: (CMOS)	Sensor de imagen por contacto
Modos de escaneo:	Color, escala de grises, blanco y negro
Resolución óptica:	600 ppp
Resolución de salida:	150/200/300/400/600 ppp

Velocidades de escaneo	**Unilateral**	**Bilateral**
Blanco y Negro:	Hasta 8 ppm	Hasta 16 ipm
Escala de grises:	Hasta 8 ppm	Hasta 16 ipm
Color:	Hasta 8 ppm	Hasta 16 ipm

Interfaz:	Hi-Speed USB 2.0
Sistemas operativos compatibles:	Windows XP [32 bits SP3 y 64 bits SP2 (WOW)], Vista [32 bits SP2 y 64 bits SP2 (WOW)], Windows 7 [32 bits y 64 bits (WOW)], Windows 8 [32 bits y 64 bits (WOW)], Windows 8.1 [32 bits y 64 bits (WOW)]. Mac OS X 10.6-10.10
Dimensiones (Al. x An. x Pr.):	1.5" x 12.3" x 2.2"
Peso:	1.3 lb
Consumo de energía:	2.5 W o menos (Modo Dormir: 1.5 W o menos)
Volumen diario sugerido:	100 escaneos†
Software de Windows incluido:	Software controlador ISIS/TWAIN, CaptureOnTouch, CaptureOnTouch Lite (integrado), Presto! BizCard, Evernote
Software de Mac incluido:	Software controlador TWAIN, CaptureOnTouch, CaptureOnTouch Lite (integrado), Presto! BizCard, Evernote
Opciones:	Adaptador Inalámbrico y Paquete de Baterías WU10, CaptureOnTouch Mobile de Canon (disponible a través de App Store℠ o Google Play Store), estuche portátil, Almohadilla de Separación.
Otras características:	Detección Automática de Color, Detección Automática de Tamaño de Página, Resolución Automática, Suavizamiento de Fondo, Corrección de Desviación, Énfasis de Borde, Reducción del Efecto Muaré, Corrección de Fotografía, Prevención de Sangrado/Eliminación de Fondo, Recorte del Sombreado, Omisión de Página en Blanco, Mejoramiento del Texto, Reconocimiento de la Orientación del Texto, Corrección de Color Tridimensional, Detección de Alimentación Doble, Preferencias del Usuario
Número de ítem:	9704B007

* Se requiere la suscripción a un servicio en la nube. Sujeta a los términos y condiciones de los proveedores de servicios en la nube de otros fabricantes.

** El escaneo inalámbrico requiere una red que funcione con la característica 802.11 b/g/n inalámbrica. El funcionamiento inalámbrico podría variar según el área y la distancia entre el escáner y los clientes de la red inalámbrica.

℠ CaptureOnTouch Mobile está disponible en App Store℠ o Google Store. CaptureOnTouch Mobile funciona con iOS 4.3 o posterior, Android 2.3.3 o posterior.

** Los hechos y las estadísticas de productos acerca de WEEE y RoHS de la Unión Europea se obtuvieron de Canon Electronics Inc. en el año 2015.

+ No está disponible en todos los países.

Los ejemplos se basan en configuraciones comunes, medidos en páginas/imágenes por minuto con documentos en tamaño Carta y orientaciones de alimentación tipo retrato, hasta 200 ppp, con un cable USB y un adaptador de CA, un cable USB 3.0 o dos cables USB 3.0 . Es posible que existan variaciones en las velocidades reales de procesamiento según el rendimiento de la PC y el software de aplicación.

El consumo de energía varía dependiendo de las configuraciones de USB/adaptador de CA utilizadas.

† Los cálculos se basan en la velocidad de escaneo y en el tiempo de uso diario asumido.

CANON U.S.A., INC.- LATIN AMERICA GROUP

Como socio de ENERGY STAR®, Canon U.S.A., Inc. certificó que este modelo cumple con los criterios de eficiencia energética de ENERGY STAR mediante un organismo de certificación reconocido por la EPA. ENERGY STAR y la marca ENERGY STAR son marcas registradas en los Estados Unidos de América. Canon es una marca registrada de Canon Inc. en los Estados Unidos de América y también podría ser una marca registrada o marca de fábrica en otros países. imageFORMULA es una marca registrada de Canon Electronics, Inc. Todos los demás nombres de productos y marcas a los que se hace referencia son marcas de fábrica de sus respectivos propietarios. Las especificaciones y la disponibilidad podrían cambiar sin previo aviso. No nos hacemos responsables por errores tipográficos.

©2015 Canon U.S.A., Inc. Todos los derechos reservados. Reproducción total o parcial sin autorización está prohibida

0193W083

Canon

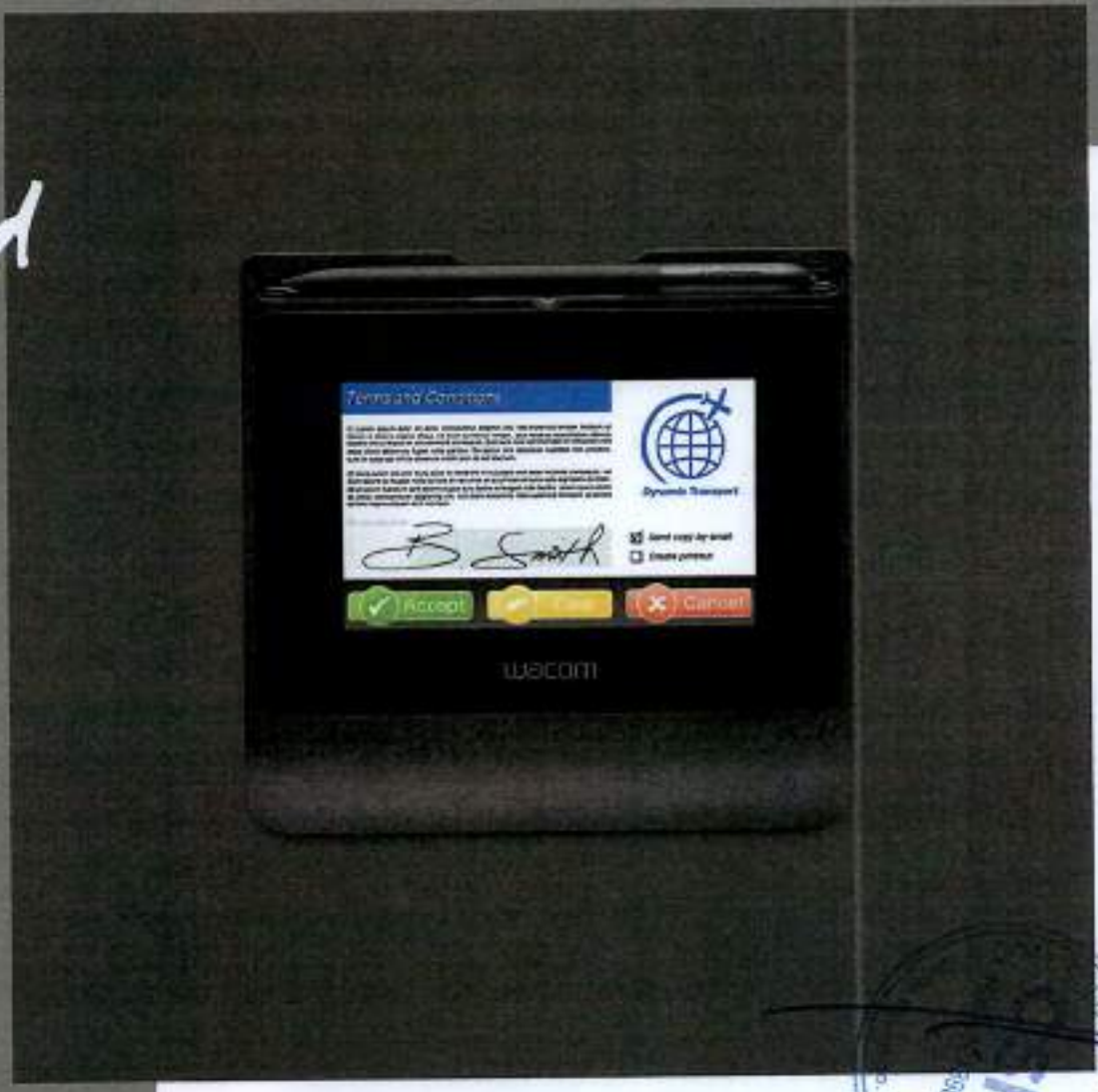
Canon USA - Latin America Group
One Canon Park
Melville, NY 11747
U.S.A.

www.cla.canon.com

Data Sheet

STU-540

5-inch color Signature Pad



wacom for Business

Página/Folio No.836 de 843

STU-540

The premium eSignature solution

Product Overview

The STU-540 signature pad is Wacom's most advanced and robust premium electronic signature device. It is ideal for high-traffic environments where in-person handwritten electronic signatures are required to confirm transactions, such as at bank teller desks, hotel check-ins, shop purchases or clinic registrations. The 5-inch high-resolution color LCD screen with hardened glass provides an attractive point of sale signing area with a paper-like feel and superb durability. When not in signature mode, it can also be used for displaying advertising, promotions or branding. A broad range of connectivity options ensure maximum deployment flexibility, including multiple alternatives for virtualized desktop environments. Transaction security is supported with advanced encryption built-in.

Key Features & Benefits

- **Low maintenance** costs thanks to high durability and the patented cordless, battery-free digital pen
- **Biometrically accurate signatures** using the digital pen with 1024 levels of pressure sensitivity
- **High durability and a natural, paper-like feel** enabled by the hardened glass with anti-glare screen treatment
- **Secure transactions** enabled by state-of-the-art AES256 / RSA2048 encryption
- **Support for virtualized environments** through the Virtual COM Port (VCP) for compatibility with Citrix XenDesktop and XenApp v6.5 and later
- **Customizable key pad and PIN pad** enabling input using graphic images or numerals
- **Attractive signature rendering** through the use of WILL™ (Wacom Ink Layer Language) technology that renders the best and most authentic-looking representation of handwritten electronic signatures
- **Enhanced signature traceability** through a UID (Unique hardware ID) for identifying the exact signature pad unit used for a particular signature and other inputs
- **Straightforward integration of signature pad support** into applications through the WILL™ SDK (Software Development Kit) for Signature
- **Ability to display promotional material** through an upgraded USB protocol and internal image storage that enables ads to be shown at natural speeds with no delays

wacom for Business

Página/Folio No.837 de 843

General Specifications

Dimensions (W x H x D)	6.41 x 6.18 x 0.39 inches / 163 x 157 x 10 mm
Weight (including stand)	0.6 lbs / 275 g
Main body color	Black
Power supply	USB bus powered
Power consumption	2.5 W maximum
Communication interface	USB/VCP/RS-232

LCD Display

Display Type	Amorphous TFT LCD
Cover plate surface	AG etched glass
Native resolution	800 x 480 pixels

Pad and Pen

Reading Technology	Electromagnetic Resonance (EMR)
Active area size	4.25 x 2.56 inches / 108 x 65 mm
Coordinate resolution	2540 lpi / 0.01 mm/pt (non-interpolated)
Coordinate accuracy	±0.02 inches / ±0.5 mm (center)
Report rate	200 points per second (non-interpolated)
Pressure levels	1024 (non-interpolated)
Encryption	AES256 / RSA2048

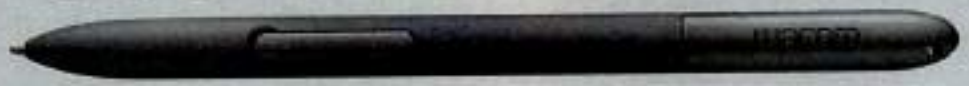
wacom for Business

Miscellaneous

Pen storage	Pen compartment
Connectivity security	USB cable locking system
Data security	Real time image capture without data storage. Internal memory for images only.
Security lock slot	Yes, Kensington
Operating temperature, relative humidity	+41° F to +104° F (+5° C to +40° C). (humidity 30 % to 80 % RH, no condensing)
Storage temperature, relative humidity	-4° F to +140° F (-20° C to +60° C). (humidity 30% to 90% RH, no condensing)
Signature software compatability	Compatible with Windows signature / eSign software and Wacom 's sign pro PDF and sign pro PDF Plug-in for Adobe Acrobat. For Windows, C++, .Net and Java development libraries available for developers (contact us for library and software availability in other development languages and platforms)
Package content	Signature pad, cordless and battery-free pen, USB cable (9.84 ft / 3 m), quick start guide, pen tether (nylon fiber, 19.7 inch / 50 cm)

COPY SOLUTIONS INTERNATIONAL S.A. ISO 9001:2015 Santo Domingo R.D.

More human



More digital

For more information or to discuss a potential project, please contact Wacom for Business sales at:

1-503-525-3100 /// esign@wacom.com

Wacom for Business leverages decades of leadership in digital pen technology to help organizations digitize processes that require in-person interaction. We enhance Wacom and third-party pen-enabled devices with software that stores and displays biometrically accurate digital ink. These integrations empower our global network of partners to seamlessly incorporate handwritten electronic signatures and annotation into organizational workflows. The result: Paperless processes with a familiar yet digital pen and paper feel.
Moreover, our WILL™ 3.0 (Wacom Ink Layer Language) standard for universal ink is powering new applications that will ensure the next generation of customer experiences are more human, and more digital.

wacom for Business

businesswacom.com
© 2019 Wacom Technology Corporation. For more information please contact:
Wacom Technology Corporation · 1455 NW Irving Street, Suite 600 | Portland, OR 97209 USA
esign@wacom.com · 1-503-525-3100

DERMALOG
JENETRIC

LIVETOUCH QUATTRO

The most easy-to-use tenprint scanner

Outstanding Features

- Integrated user guidance
- Captures flat and rolled fingerprints
- Captures hand signatures
- Rugged protection for durability
- FBI and BSI certified image quality

Key Benefit

LIVETOUCH QUATTRO combines unmatched user friendliness with high-quality fingerprint images

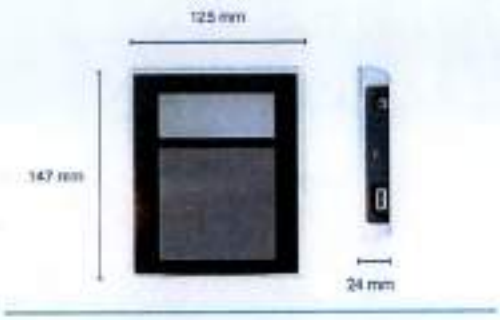
Página/Folio No.840 de 843

LIVETOUCH QUATTRO: The Most Easy-To-Use Tenprint Scanner

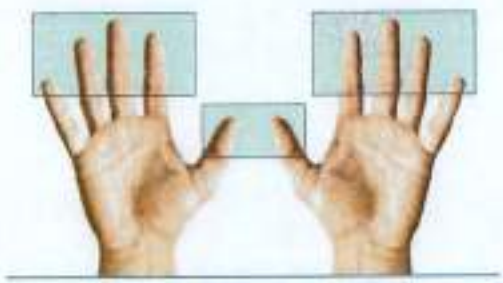
COPY SOLUTIONS INTERNATIONAL S.A.
CSI
RNC 101858852
Santo Domingo, R.D.

A compact and flexible solution for capturing fingerprints

LIVETOUCH QUATTRO combines unmatched user friendliness with high-quality fingerprint images. Whether you capture single, dual or four fingerprints, its integrated touchscreen provides easy to understand instructions that reduce failure-to-enroll rates and shorten the capture process. With its super compact design, LIVETOUCH QUATTRO integrates easily into enrollment systems in any operation environment.



Compact Design
With compact dimensions of 125 mm x 147 mm x 24 mm and a total weight of only 360 g, the LIVETOUCH QUATTRO easily integrates into existing applications. The device also features a USB power supply and IP54 protection, making it ideal for portable use.



Multiple Fingerprint Capture Options
In addition to single flat and rolled fingerprint enrollment, the LIVETOUCH QUATTRO can capture tenprints using the 4-4-2 method. It is the most convenient and efficient way to capture complete sets of fingerprints and ensures outstanding recognition accuracy.

Interactive User Guidance
For fast and convenient fingerprint capture, the LIVETOUCH QUATTRO features a graphical display that clearly and efficiently guides users through each step of the process. If the enrollment is incorrect, the device displays corrective instructions.

Product Features

- Resolution: 500 dpi
- Captures rolled and flat fingerprints (4-4-2)
- Captures hand signatures
- Integrated graphical user guidance
- Integrated colored resistive touchscreen
- Scratch resistance
- Certifications: FBI, BSI, CE, FCC, UL, RoHS
- IP54 protection class according to DIN EN 60529

Signature Capture
LIVETOUCH QUATTRO captures not only fingerprints but also hand signatures. High-quality digital signatures are generated using a stylus to sign on the integrated touchscreen. As a result, there is no longer any need for a separate signature pad.

Rugged Protection
The LIVETOUCH QUATTRO features a strong glass layer that covers the device's fingerprint sensor to protect it from scratches caused by objects such as rings, pens or keys. It also makes the scanner very resistant to abrasion from heavy use.

Certified Image Quality
The German Federal Office for Information Security has certified the LIVETOUCH QUATTRO fingerprint scanner according to "BSI TR-03121" standard. The fingerprint scanner also meets the image quality specification Appendix F by the Federal Bureau of Investigation (FBI).

Specifications **LIVETOUCH** QUATTRO

COPY SOLUTIONS INTERNATIONAL SA
CSI
RNC: 10 [illegible]352
Santo Domingo R.D.

Technical Features	
User Interface	On device touchscreen with graphical, real-time, dynamic user feedback
Capture Modes	Flat (4-4-2) and rolled fingerprints, electronic signatures
Image resolution	500 dpi
Scan Area (W x H)	81.3 mm x 76.2 mm (3.2" x 3.0")
Image Quality Certification	FBI EBTS Appendix F, BSI TR-03121, ID Flats, tenprint and Mobile ID FAP 60
Ingress Protection	IP54
Infection Prevention (optional)	Antimicrobial coating (AMC) tested for abrasion and washability
Scratch Restistance	Glass protection layer against scratches tested for hardness (DIN EN ISO 6507-1:2018-4:2018) and for abrasion (DIN 55654:2015-08)
Operating Temperature	-10 °C – 55 °C (14 °F – 131 °F)
Dimensions (W x H x D)	125 mm x 147 mm x 24 mm (4.9" x 5.8" x 0.94")
Weight	0.36 kg (0.8 lbs)
Scanner Interface	USB 3.0 / 2.0
Power Supply	Through the USB 3.0 interface (5 V, 900 mA) or external power supply for USB 2.0 operation
Operating System	Windows 7 / 8.1 / 10 (all 32- and 64-bit editions)
Certifications	FBI, BSI, WHQL, CE, FCC, UL, RoHS

© 2023 All content and images are owned by DERMALOG JENETRIC GmbH and are actively protected by copyright.