Requisitos de experiencia (OBLIGATORIOS)

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

CM

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Magallanes Media

Buenos Aires, 11 de febrero de 2025

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

Junta Central Electoral
Comité de Compras y Contrataciones
República Dominicana

Asunto: Acreditación de experiencia - Proceso JCE-CCC-LPI-2024-0001

Estimados miembros del Comité de Compras y Contrataciones,

Por medio de la presente, me dirijo a ustedes en mi calidad de apoderado de Magallanes Media S.A., con el fin de dar cumplimiento a los requisitos de experiencia establecidos en el pliego de la contratación Ref: JCE-CCC-LPI-2024-0001, destinada a la contratación de la empresa que suministrará los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI) de la República Dominicana.

Somos proveedores del Registro Nacional de las Personas (RENAPER), organismo estatal responsable de la identificación y registro de las personas físicas domiciliadas en el territorio de la Republica Argentina.

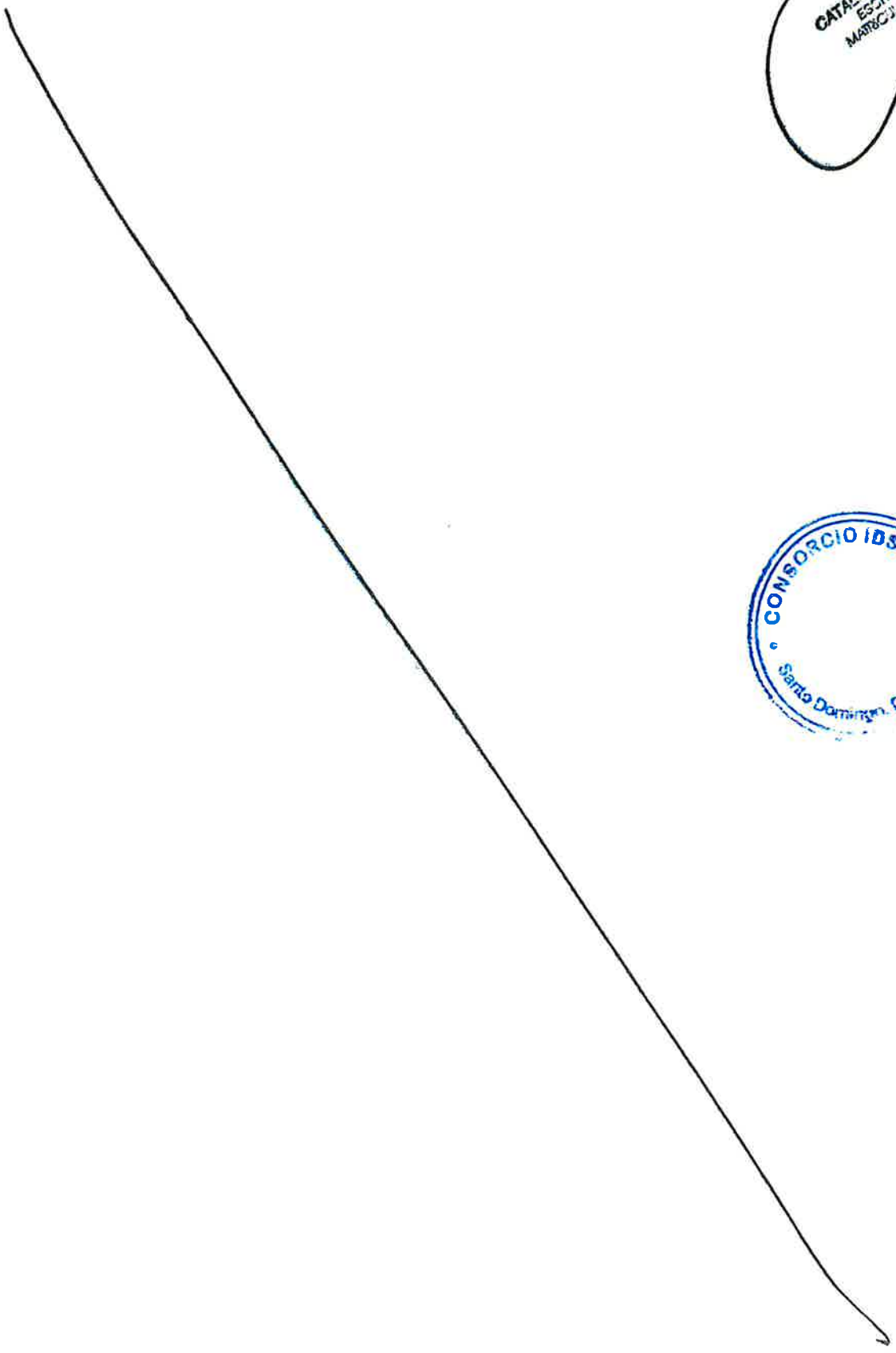
En este sentido, detallamos a continuación nuestra experiencia en proyectos relevantes que cumplen con los requisitos establecidos:

Punto 3.1.6.3 - Requisitos de experiencia (No obligatorios)

a) 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 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 referencia de clientes donde se muestre explícitamente la solicitud, las cuales deben estar dirigidas a la JCE. Al menos una de las referencias debe cumplir con la norma ISO 18013-5.

Presentamos:

- Nota emitida por el RENAPER con fecha 11 de junio de 2024, correspondiente al proceso 78-0012-LPU23, en la cual hemos sido proveedores de la tecnología utilizada para la emisión de la cédula nacional de identidad móvil denominada Smart DNI, alojada en la aplicación gubernamental argentina "Mi Argentina" (Orden de Compra Nro. 78-0013-OCA23). Los componentes suministrados por Magallanes Media S.A. cumplen totalmente con todas las normas ISO e ICAO, y la solución sigue los lineamientos establecidos en la norma ISO/IEC 18013-5.



- Nota emitida por el RENAPER con fecha 12 de julio de 2024, correspondiente al proceso 78-0006-LPU19, en el cual se llevó a cabo el Proyecto Smart DNI Argentina (Orden de compra 78-1054-OC19)

Punto 3.1.6.2 - Requisitos de experiencia (Obligatorios)

d) Al menos una (1) experiencia en la 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 una carta formulada a la JCE certificando la implementación del proyecto en una institución pública mediante declaración jurada o carta emitida directamente por la entidad de gobierno. La misma debe indicar claramente los puntos aquí requeridos, en papel timbrado, con nombre completo del firmante, cargo e institución, debidamente sellada y firmada, e incluir un teléfono de contacto y correo oficial para constatar la información.

Presentamos:

- Nota emitida por el RENAPER con fecha 3 de febrero de 2025, correspondiente al proceso 78-0016-LPU22, en la cual hemos sido proveedores de la tecnología de PKI de Firma Digital y de PKI para documentos de viaje ICAO (Órdenes de compra Nro. 78-0034-OC23 y 78-0051-OC24). Ambas soluciones han sido implementadas con integraciones a los sistemas existentes mediante interfaces definidas específicamente para tal fin.

Quedamos a disposición para brindar cualquier información adicional que sea requerida.

Atentamente,

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Licenciado Fabian Carlomagno
Apoderado
Magallanes Media S.A.

FIRMA/S CERTIFICADA/S EN SELLO/S
DE ACTUACION F 09130467 N° .....
Buenos Aires, 13/02/2025

CATALINA CARLOMAGNO
ESCRIBANA
MATRICULA 4728


CONSORCIO IDSECURE IDS
Santo Domingo, D. N.

COLEGIO DE ESCRIBANOS

ACTA DE CERTIFICACION DE FIRMAS

LEY 404

F 019130467

Buenos Aires, 13 de FEBRERO de 2025 . En mi carácter de escribano Subrogante del Registro Notarial número 2165 de esta Ciudad

CERTIFICO: Que la/s Firma que obra/n en el documento que adjunto a esta foja, cuyo requerimiento de certificación se formaliza simultáneamente por ACTA número 127 del LIBRO número 52 , es/son puesta/s en mi presencia por la/s persona/s cuyo/s nombre/s, documento/s de identidad y justificación de identidad se indican: Lisandro Fabián CARLOMAGNO, titular del Documento Nacional de Identidad número 21.402.683.- El compareciente EXPRESA actuar en nombre y representación y en su carácter de APODERADO de "MAGALLANES MEDIA S.A.", con con sede social en Magallanes 1.315 de esta Ciudad, lo que acredita con el Poder General Amplio otorgado por escritura 99 de fecha 26 de agosto de 2022, pasada ante la Escribana Yamila Damaris Peverelli, al folio 350 del presente Registro Notarial de su titularidad, documentación que he tenido a la vista para el acto y de la cual surgen facultades suficientes, y de la que surge que la sociedad acredita personería con: 1) Estatuto Social de la empresa otorgado por Escritura 48 del 1° de noviembre de 2007, pasada ante la escribana de esta Ciudad, Sara Norma Tobal, al folio 142 del Registro Notarial 1549 a su cargo, inscripta su primera copia en la Inspección General de Justicia con fecha 14 de noviembre de 2.007 bajo el número 18.979, libro 37 de sociedades por acciones; y 2) Cambio de objeto social y Reforma de Estatuto Social otorgado por Escritura 74 de fecha 11 de marzo de 2010, pasada ante mí, al folio 260 protocolo A del Registro Notarial 929 de esta Ciudad de mi adscripción, inscripta su primera copia en la Inspección General de Justicia con fecha 8 de abril de 2010, bajo el número 6306, libro 48 de sociedades por acciones.- Se deja constancia que el firmante justifica su identidad con la exhibición del citado documento, de

CONSORCIO IDSECURE 103 Santo Domingo, Q.N.

F 019130467

acuerdo al inciso a) del artículo 306 del Código Civil y Comercial; y que el documento consiste en Nota a la Junta Central Electoral – Comité de compras y contrataciones, de República Dominicana, fechada el 11/02/2025.-

CATALINA CARBONE
ESCRIBANA
MATRICULA 4728

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

250213000546

EL COLEGIO DE ESCRIBANOS de la Ciudad de Buenos Aires, Capital Federal de la República Argentina, en virtud de las facultades que le confiere la ley orgánica vigente, LEGALIZA la firma del escribano CARBONE, CATALINA obrantes en el documento anexo: Certificación de firmas firmada por dicho escribano en la foja de Certificación de Firmas F-19130467 respecto del acta 127 de fecha 13/02/2025 que obra en el libro 52. La presente legalización 250213000546, no juzga sobre el contenido y forma del documento y puede ser verificada en la página web del Colegio de Escribanos de la Ciudad de Buenos Aires. www.colegio-escribanos.org.ar

Firmado Digitalmente por Colegio de Escribanos de la Ciudad de Buenos Aires. Escribano Legalizador ROSATO DE DE PASCALE, NELIDA CRISTINA, Matrícula 3587. Buenos Aires, 13/02/2025 14:08.-

CONSORCIO IDSECURE IDS
Santo Domingo, D. N.

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA

Apostilla de La Haya

Número: CE-2025-16062622-APN-DTD#JGM

CIUDAD DE BUENOS AIRES
Jueves 13 de Febrero de 2025

Referencia: Apostilla. Verificar en| Verify at| Vérifier sur: www.argentina.gob.ar/legalizacion-internacional

APOSTILLE (Convention de la Haye du 5 de octobre 1961)	
1. País |*Country* |*Pays*: ARGENTINA	
El presente documento público |*This public document* |*Le présent acte public*	
2. Ha sido firmado por |*Has been signed by* |*A été signé par*: ROSATO DE DE PASCALE NELIDA CRISTINA	
3. Quien actúa en calidad de |*Acting in the capacity of* |*Agissant en qualité de*: FUNCIONARIO HABILITANTE	
4. Y está revestido del sello/timbre de |*Bears the seal/stamp of* |*Est revêtu du sceau/timbre de*: COLEGIO DE ESCRIBANOS DE LA CIUDAD DE BUENOS AIRES	
Certificado |*Certified*	*Attesté*	
5. En |*At* |*A*: CIUDAD AUTÓNOMA DE BUENOS AIRES	6. El día |*The* |*Le*: 13/02/2025
7. Por |*By* |*Par*: Colegio de Escribanos de la Ciudad de Buenos Aires	
8. Bajo el Número |*Nº* |*Sous Nº*: 190013/2025	9. Sello/Timbre |*Seal/Stamp* |*Sceau/Timbre*: 4500
10. Firma |*Signature* |*Signature*: URRESTI JOAQUIN ESTEBAN	

Esta Apostilla certifica únicamente la autenticidad de la firma, la calidad en que el signatario del documento haya actuado y, en su caso, la identidad del sello o timbre del que el documento público esté revestido.
Esta Apostilla no certifica el contenido del documento para el cual se expidió. No es válido el uso de esta Apostilla en la República Argentina.
This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears. This Apostille does not certify the content of the document for which it was issued. This Apostille is not valid for use anywhere within República Argentina.
Cette apostille atteste uniquement la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte public est revêtu. Cette apostille ne certifie pas le contenu de l'acte pour lequel elle a été émise. L'utilisation de cette Apostille n'est pas valable en/au Argentina.

Tipo de documento apostillado |*Type of document* |*Type de document*: CERTIFICADO CON FIRMA DIGITAL

Titular |*Holder* |*Titulaire*: MAGALLANES MEDIA S.A.

Observaciones |*Observations* | *Observations*:

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.02.13 15:30:54 -03:00

COSSIO DOLORES ALEJANDRA COSSIO DOLORES ALEJANDRA -
en representación de
COLEGIO DE ESCRIBANOS - 30526499456

Digitally signed by URRESTI Joaquin Esteban
Date: 2025.02.13 15:41:49 ART
Location: Ciudad Autónoma de Buenos Aires

JOAQUIN ESTEBAN URRESTI
20273115928

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.02.13 15:41:52 -03:00

Buenos Aires, 3 de febrero del 2025

A quien pueda interesar,

Esta carta se entrega a solicitud de nuestro proveedor Magallanes Media S.A., quien ha cumplido y está cumpliendo satisfactoriamente con sus obligaciones contractuales con nosotros como proveedores de la tecnología de PKI de Firma digital y de PKI para documentos de viaje ICAO Número de proceso 78-0016-LPU22 denominado: "Provisión, configuración, integración y puesta en marcha de una Infraestructura de Clave Pública PKI",

Diferencias entre la PKI para Documentos de Viaje ICAO y Certificados X.509

La Infraestructura de Clave Pública (PKI) es un sistema criptográfico que permite la creación, gestión y verificación de certificados digitales. Si bien tanto los documentos de viaje ICAO como los certificados X.509 se basan en PKI, existen diferencias significativas en su implementación y propósito.

PKI para Documentos de Viaje ICAO

- **Propósito específico:** Diseñada específicamente para asegurar la autenticidad de los pasaportes electrónicos y otros documentos de viaje.
- **Estándares:** Cumple con los estándares de la Organización de Aviación Civil Internacional (OACI), que establecen requisitos rigurosos para la seguridad y la interoperabilidad de los documentos de viaje.
- **Certificados:** Los certificados utilizados en los documentos de viaje ICAO tienen una estructura y contenido específicos, diseñados para verificar la identidad del titular y la autenticidad del documento.
- **Autoridades de Certificación (CAs):** Las CAs que emiten certificados para documentos de viaje ICAO suelen ser entidades gubernamentales o designadas por el gobierno, y están sujetas a regulaciones y auditorías estrictas.
- **Aplicaciones:** Limitada a la verificación de la identidad en los puntos de control fronterizo y otros procesos relacionados con los viajes internacionales.

PKI para Certificados X.509 Genéricos

- **Propósito general:** Utilizada para una amplia variedad de aplicaciones, como el cifrado de comunicaciones, la firma de correo electrónico, la autenticación de servidores web (SSL/TLS), etc.
- **Estándares:** Se basa en el estándar X.509, que es un estándar abierto y ampliamente utilizado para la gestión de certificados digitales.
- **Certificados:** Los certificados X.509 tienen una estructura más flexible y pueden ser utilizados para diversas aplicaciones.
- **Autoridades de Certificación (CAs):** Las CAs que emiten certificados X.509 pueden ser públicas (como Let's Encrypt) o privadas (operadas por empresas o organizaciones).
- **Aplicaciones:** Amplia gama de aplicaciones, desde la seguridad en línea hasta la firma electrónica de documentos.

El proveedor Magallanes Media implemento ambas soluciones incluyendo integraciones con los sistemas existentes mediante interfaces definidas específicamente para tal fin.

Para la verificación de la información suministrada, o en caso de que necesiten detalles adicionales,

puede contactarnos a través de los siguientes datos

Nombre de la entidad contratante: Registro Nacional de las Personas (RENAPER)

Persona de contacto: Flavio Brocca

Designación: director IT Dirección: Calle Tte. General Juan Domingo Perón N° 664, CABA, Argentina

Números de contacto: +54 911 3181-6963

Dirección de correo electrónico: fbrocca@renaper.gob.ar

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2025-11698967-APN-DGTII#RENAPER

CIUDAD DE BUENOS AIRES
Lunes 3 de Febrero de 2025

Referencia: carta Magallanes PKI

El documento fue importado por el sistema GEDO con un total de 2 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.02.03 14:25:14 -03:00

Flavio Ramon Brocca
Director General
Dirección General de Tecnología e Innovación en Identidad
Dirección Nacional del Registro Nacional de las Personas

CONSORCIO iDSECURE ID3
Santo Domingo, D.N.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.02.03 14:25:15 -03:00

Pliego (RFP) PKI ReNaPer - 2022

Especificaciones Técnicas:

Renovación Integral de la Infraestructura de PKI del Registro Nacional de las Personas

CM

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

1. INTRODUCCIÓN

El presente documento describe la solución integral que se pretende realizar bajo la modalidad "llave en mano" solicitada por el Registro Nacional de las Personas para actualizar la infraestructura de hardware y software de su Sistema de Infraestructura de Clave Pública (PKI), incluyendo la migración de la CSCA existente y la integración de la solución a proveer con los servicios de la plataforma documentaria y equipos de personalización del organismo.

2. ESPECIFICACIONES TÉCNICAS OBJETO DE LA CONTRATACIÓN

Se requiere la provisión, configuración, integración y puesta en marcha de una Infraestructura de Clave Pública con la capacidad de descentralizar la firma de documentos en diversos centros de personalización, así como la migración de la PKI actualmente operativa para la emisión de pasaportes electrónicos y la integración con la plataforma DNI/Pasaporte y sus equipos de personalización.

3. DESCRIPCIÓN DE RENGLONES

La presente contratación tiene por objeto la provisión de los siguientes bienes y servicios asociados, en renglón único:

Renglón 1: Renovación Integral de la Infraestructura de PKI del Registro Nacional de las Personas

3.1 Bienes y servicios para proveer por el adjudicatario:

- Infraestructura PKI
- Firmador de Documentos
- N-PKD
- N-PKD con Sincronización OACI PKD
- Migración
- Integración con el sistema documentario del Registro Nacional de las Personas
- Soporte Integral

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

4. CARACTERÍSTICAS PRINCIPALES

- Los componentes de la PKI deberán cumplir con la funcionalidad para utilizar **BAC** (por sus siglas en inglés: Basic Access Control) y **SAC** (por sus siglas en inglés: Supplemental Access Control)
- El adjudicatario deberá contemplar la provisión de los productos de hardware y software, instalación, configuración, implementación, integración con los servicios y equipos de personalización, así como el mantenimiento y soporte de la infraestructura de PKI.
- El adjudicatario deberá apegarse a los lineamientos de operación y seguridad que el Registro Nacional de las Personas establezca con el objeto de preservar la confidencialidad, disponibilidad e integridad de la información institucional.
- El adjudicatario deberá dar atención y respuesta a incidentes o integración de ajustes o nuevas funcionalidades relacionados con la gestión y operación de la PKI, siguiendo procedimientos y metodologías basadas en mejores prácticas y documentando estos incidentes o cambios.
- El adjudicatario debe considerar prevenir, detectar y remediar oportunamente nuevas vulnerabilidades y amenazas que puedan comprometer los activos de infraestructura de la PKI.
- La solución de PKI propuesta debe garantizar la compatibilidad e integración con la plataforma documentaria del Registro Nacional de las Personas, así como con los equipos de personalización.
- El software que el proveedor utilizará en la PKI debe considerar manejo de APIs abiertas para integración con otros elementos necesarios para la producción del pasaporte, de manera enunciativa más no limitativa: la plataforma documentaria del Registro Nacional de las Personas para emisión de DNI, SmartDNI y pasaporte, entre otros.
- El sistema será administrado por RENAPER como el resto de la infraestructura y específicamente con la PKI, será igual a lo que sucede actualmente, el proveedor deberá intervenir solo si se requiere soporte de acuerdo al SLA y en las condiciones pactadas.

CONSORCIO IDSECURE IDS Santo Domingo D.N.

5. INFRAESTRUCTURA PKI

El PKI OACI SAC a proveer se compone de:

- Country Signing Certification Authority (CSCA), en conformidad con OACI 9303 Part 12, emitiendo el certificado CSCA auto firmado
- Certificados de enlace CSCA
- Firma de Documento (Document Signer (DS))

- Certificados de firma de MasterList (MasterList Signer (ML)), certificados de Firma de Listas de Desviaciones, y CRLs (Certificate Revocation List)

El adjudicatario debe garantizar que la infraestructura de PKI:

- Genere periódicamente certificados de firmantes de documentos conforme recomienda el Documento 9303 de la OACI.
- Firme y valide los datos (objetos de seguridad) para los documentos de identidad y viaje con el certificado de firmantes de documentos (Document Signer) que corresponda en cada caso.
- Implemente la funcionalidad de Firmante del Documento del Pasaporte Electrónico para cubrir toda la información de la personalización del pasaporte.
- Cuente con un esquema de recuperación inmediata ante desastres.
- Cumpla al menos con lo indicado por la OACI y las modificaciones mandatorias que la OACI establezca durante la vigencia del contrato.
- Incluya la entidad certificadora auto firmada (CSCA Country Signer Certificate Authority), y la certificación de firmantes de documentos (DS "Document Signer").

El hardware 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 las especificaciones funcionales de la OACI establecidas en el Doc 9303 vigente.

La infraestructura PKI debe incluir un módulo de seguridad de hardware (HSM) para la generación de la llave del Firmante del Documento. El hardware criptográfico centralizado utilizado para firmar los documentos deberá implementarse en alta disponibilidad (HA), en el ambiente de producción, con un dispositivo adicional fuera de línea para resguardo de las llaves CSCA.

Se requiere tener un dispositivo sin conexión adicional para hacer una copia de seguridad del CSCA principal. Los HSM de alta disponibilidad están destinados para los Firmantes de Documentos.

El adjudicatario instalará el hardware central de la PKI en el data center del Registro Nacional de las Personas para generar conjuntos de claves para diferentes períodos de tiempo que se utilizarán para procesar las Firmas Digitales que se aplicarán para la firma de los datos de acuerdo al modelo ICAO.

El adjudicatario deberá contar con un mecanismo de respaldo de las llaves públicas y privadas, de manera segura y debe de existir un método seguro de transferencia de llaves y certificados desde el

appliance criptográfico offline hacia el appliance criptográfico online, que no ponga en riesgo la integridad y confidencialidad de los pares de llaves y certificados en ningún momento.

La expedición de llaves y certificados, así como el transporte entre el ambiente offline y el online debe ser descrito por el adjudicatario en su propuesta técnica. Este proceso debe considerar que las claves y procesos de expedición, renovación y transporte no dependan de una sola persona y que se requieran al menos 2 participantes. Esta gestión de claves deberá estar en línea con lo establecido en el documento 9303 punto 4.

Los HSM propuestos deberán contar con certificación FIPS 140-2 Nivel 3 como mínimo para la CSCA.

Es importante recalcar que la infraestructura criptográfica offline, deberá permanecer aislada de manera lógica y física permanentemente.

Las llaves privadas no deberán de poder ser extraídas del HSM una vez creadas, esto se refiere a que la comunicación para el firmado del chip, entre la PKI con la plataforma documentaria del Registro Nacional de las Personas y/o el equipo de personalización, debe realizarse de manera segura, por ejemplo, mediante uso de comunicación cifrada.

La Infraestructura de Clave Pública (PKI) debe establecerse dentro del Data Center del Registro Nacional de las Personas, sito la calle Dr. Pedro Chutro 2798, CABA, y deberá contar con la capacidad de soportar la producción descentralizada de documentos.

Deberá considerarse la provisión y actualización permanente de un documento de Políticas de Certificación (CP) para definición de servicio y declaraciones de prácticas de certificación (CPS), así como también, soporte de la PKI que contenga procedimientos de instalación, procedimientos operativos y procedimientos administrativos.

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

6. FIRMA DE DOCUMENTOS

Un elemento clave para conformidad de las normas de la OACI con la seguridad de los documentos de viaje electrónicos, es garantizar que los datos no hayan sido manipulados durante o después del proceso de producción. La solución a proveer deberá gestionar la firma criptográfica del SOD (Security Object Data).

El adjudicatario deberá implementar una CA (Autoridad Certificante) 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 el pasaporte electrónico y DNI que ofrece acceso de solo lectura de Chip de Circuito Integrado (IC).

Conforme lo especifica la Parte 12 del Doc 9303, la Entidad Certificadora de la PKI es auto firmada, es decir, no se encuentra subordinada a ninguna autoridad certificante superior.

El adjudicatario deberá implementar la CS CSCA (clave privada de firma de país) que será utilizada para firmar y producir los DS (certificados de firmante de documento).

El adjudicatario deberá implementar el certificado DS, que será emitido por el CSCA.

El adjudicatario deberá implementar la CA que será responsable de la generación de claves/certificados de seguridad necesarios para el Control de acceso básico (BAC), el Control de acceso suplementario (SAC) y la autenticación activa (AA).

El adjudicatario deberá indicar en su propuesta técnica claramente la función de hashing, el algoritmo de firma y la longitud de la clave que respalda o planea respaldar en el futuro cercano.

El requisito mínimo para la función hash (es decir, SHA-256 o superior), algoritmo de firma (es decir, RSA-PKCS, RSA-PSS, ECDSA) y longitud de clave deberán cumplir con las especificaciones establecidas en el Doc 9303 de la OACI vigente respecto a la PKI.

El adjudicatario deberá expedir, firmar y validar el certificado de firmante de documentos de identidad y el certificado de firmante de pasaportes, con el certificado de autoridad de certificación de firma país.

El adjudicatario deberá expedir, firmar y validar los certificados de firmante de lista maestra, firmante de lista de desviaciones y la lista de certificados revocados (CRL) con el certificado de autoridad de certificación de firma país.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

El adjudicatario deberá implementar que tanto el CSCA como el DS almacenarán las llaves privadas en HSMs (hardware criptográfico) por razones de seguridad y eficiencia.

Los DSC (Document Singer Certificate) a utilizar para la emisión de Documentos serán distribuidos en TRECE (13) locaciones remotas, de las cuales SEIS (6) corresponden a aeropuertos y SIETE (7) a futuros centros de impresión. Las posibles locaciones son las que se detallan seguidamente, debiendo preverse la posibilidad de ampliar la cobertura a los distritos que oportunamente se determinen. El proveedor deberá detallar cómo se realizará la descentralización en base a las buenas prácticas, a las recomendaciones de OACI y a las evidencias que presente como experiencias anteriores. A su vez, debe garantizar un procedimiento seguro para garantizar la distribución de la clave privada, según los lineamientos establecidos por RENAPER y lo establecido por la OACI en el documento 9303 punto 5.

CM

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

Local	Tipo	Pasaporte (**)	DNI (**)
Salta	Aeropuerto	2	---
Córdoba	Aeropuerto	6	---
Mendoza	Aeropuerto	6	---
Rosario	Aeropuerto	5	---
Aeroparque	Aeropuerto	29	---
Ezeiza	Aeropuerto	15	---
Local	**Tipo**	**Pasaporte (**)**	**DNI (**)**
Centro	Centro de Impresión	2.728	19.881
NOA	Centro de Impresión	133	3.366
NEA	Centro de Impresión	102	3.012
CUYO	Centro de Impresión	175	2.222
Patagonia	Centro de Impresión	121	1.521
Santa Cruz	Centro de Impresión	Abastecido desde CABA	302
Tierra del fuego	Centro de Impresión	Abastecido desde CABA	165

* Producción actual diaria

** Producción futura diaria estimada

7. N-PKD

El N-PKD tiene un propósito similar al PKD de la OACI, replicando a nivel nacional lo que la PKD de la OACI hace internacionalmente. Por lo tanto, funciona como un agregador nacional para todos los elementos de confianza y seguridad necesarios, para verificar y validar documentos de viaje electrónicos en las fronteras.

El N-PKD es un repositorio para publicar información sobre la PKI, incluyendo:

- Certificados CSCA
- Certificado de enlaces CSCA
- Certificado de Firma de Documentos
- Certificados de Firma Masterlist
- Certificados de Firma de Lista de Desviación
- Lista Revocación de Certificados (CRL)
- Masterlists
- Listas de Desviación

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

El N-PKD podrá ejecutarse sobre un sistema LDAP. El LDAP se configurará con una estructura jerárquica siguiendo la estructura de las reglas de Nombre Distinguido de los certificados emitidos. El acceso público a LDAP se configurará de acuerdo con la política a definir dentro del proyecto, utilizando mecanismos estándares.

Para mayor comodidad y facilidad de operación se proporcionará una aplicación de interfaz gráfica de usuario nPKD.

Para automatizar las operaciones, especialmente en el escenario fuera de línea, los archivos anteriores se podrán exportar tanto en DER/PEM, como en formato LDIF (formato estándar LDAP).

Todos los procedimientos se deberán ajustar a lo establecido en el documento 9303, específicamente en el punto 5. MECANISMOS DE DISTRIBUCIÓN.

7.1 N-PKD CON SINCRONIZACIÓN OACI PKD

Además de las características básicas de almacenamiento y distribución de certificados internos, la solución nPKD deberá contar con un módulo para automatizar las comunicaciones con la PKD de la OACI, cargando y descargando regularmente los datos criptográficos pertinentes necesarios para la validación de documentos de viaje electrónicos en los Sistemas de Inspección. RENAPER asumirá los pagos a OACI para inscripción a PKD.

La solución nPKD a proveer deberá tener las siguientes características principales:

- Asegurar el almacenamiento de todos los certificados digitales y otros materiales emitidos en el ámbito de la CSCA nacional (Certificados de enlace y CSCA auto- firmados, certificados DS, certificados de Listas Maestras, certificados de Listas de Desviación, Listas de Desviación Maestra, CRLs)
- Asegurar el almacenamiento y la sincronización bidireccional de todos los materiales criptográficos entre nPKD y OACI PKD
- Gestionar la orquestación de procesos entre diferentes zonas de confianza y los principales componentes del sistema
- Segregar componentes y sistemas sensibles, limitando la necesidad de interacción directa entre ellos
- Contar con una interfaz de administración web para gestionar todas las operaciones, incluida la automatización de las operaciones de rutina
- Definir procesos y procedimientos técnicos y de operación para administrar y operar el servicio
- Contar con control de acceso basado en roles de administradores y operadores
- Generar registros de auditoría y registros históricos
- Mantener la trazabilidad de todas las transacciones
- Comunicaciones seguras
- Configuración en cluster

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

8. MIGRACIÓN DE LA PLATAFORMA ACTUAL

Esta actividad crítica consiste en la migración de la totalidad correspondiente desde la plataforma actual para la puesta en operación de la nueva PKI.

El adjudicatario deberá presentar un Plan de Migración, el cual incluirá la ruta a seguir, los requisitos previos, los roles, la responsabilidad y las tareas a desarrollar tanto por el personal del ReNaPer como por su parte.

Una vez instalado el equipamiento, se migrarán los certificados y datos necesarios de la plataforma actual a la que la reemplazará, realizándose una serie de pruebas que estarán definidas en el Plan de Migración.

Superadas las pruebas satisfactoriamente, la nueva Plataforma quedará en operación, dando de baja la actualmente operativa.

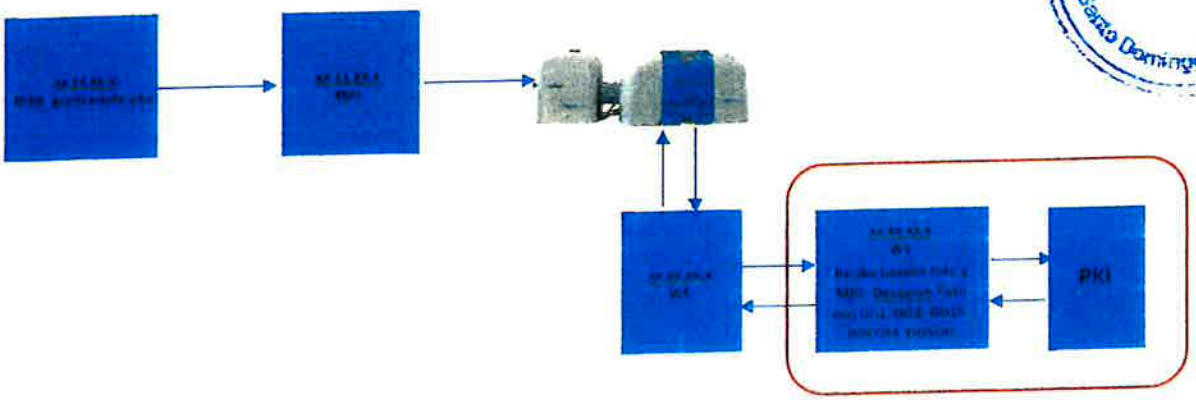
9. INTEGRACIÓN CON EL SISTEMA DOCUMENTARIO DEL REGISTRO NACIONAL DE LAS PERSONAS

La PKI debe considerar que la entidad certificadora raíz autofirmada y sus componentes de administración de llaves y certificados se encuentran resguardados por el Registro Nacional de las Personas fuera de línea (offline) en un appliance criptográfico.

El firmado y/o encriptado de información se realizará conforme a la normativa OACI, será definido e implementado en conjunto entre Adjudicatario y el Registro Nacional de las Personas, de manera no limitativa, podrá ser a través de Webservices para comunicar la PKI con el sistema del ReNaPer, los cuales deberán ser desarrollados conforme a los criterios que éste defina.

El esquema de personalización y firma de datos en el chip actual responde al siguiente diagrama:

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.



Un artefacto genera el XML, un servidor los almacena y el equipo de personalización toma el XML de ese repositorio. Luego, en el proceso de personalización propiamente dicho , el equipo invoca a la primera interfaz.

La primera interfaz es la que ejecuta en la IP local correspondiente y devuelve los archivos generados para que los equipos de personalización puedan firmar los datos en el chip.

Servicio: http://webservice.idear.gov.ar/EPASS_grupo_de_archivosEDNI.php?wsdl

Objeto: Este servicio tiene como objeto que la impresora pueda obtener los siguientes archivos:
dg1.bin - dg2.bin - dg15.bin - dgcom.bin - dgsod.bin

Para lograrlo el servicio solicita como datos de entrada:

1. Fotografía (Base64)
2. MRZ (Base64)
3. IDTRAMITE (Base 64)

La devolución del servicio será path donde se accede para descargar los archivos:

http://xx.xx.xx.xx:xxxx/Datos/carpeta/dg1.bin
http://xx.xx.xx.xx:xxxx/Datos/carpeta/dg2.bin
http://xx.xx.xx.xx:xxxx/Datos/carpeta/dg15.bin
http://xx.xx.xx.xx:xxxx/Datos/carpeta/dgcom.bin
http:/xx.xx.xx.xx:xxxx/Datos/carpeta/dgsod.bin

La segunda interfaz fue desarrollada por el proveedor actual y es la que devuelve los path enunciados en la interfaz anterior. Esta es la que deberá resolver el nuevo proveedor. Según el esquema es lo recuadrado en color rojo. La forma de resolverlo no está especificada, sólo está especificado la devolución de esa API o Servicio Web.

10. SOPORTE INTEGRAL

El objetivo de estas tareas es prestar apoyo especializado frente a cualquier contingencia que se pueda presentar en cualquier componente de la Plataforma dentro del contexto de servicio, incluyendo todo el equipamiento de hardware, software y nueva funcionalidad desarrollada.

El servicio de soporte tendrá una duración de 24 meses corridos desde la puesta en operación del nuevo equipamiento.

10.1 ALCANCE

Soporte Reactivo de la Plataforma (análisis, seguimiento y coordinación de todas las actividades relacionadas con la gestión de un incidente o problema, hasta que se dé solución al mismo).

Los incidentes de soporte se gestionarán por Portal Web, correo electrónico o por teléfono. Una vez generado el incidente de soporte por cualquiera de los medio disponibles, será asignado de manera automática un número ID de caso, con el cual se podrá realizar el seguimiento respectivo.

En caso de ser requerido se podrá modificar el nivel de severidad y el nivel de escalamiento que corresponda, mientras que el adjudicatario deberá determinar la cantidad y perfil de recursos a asignar para la resolución de cada incidente.

Cabe aclarar que, dado que el adjudicatario deberá adquirir el equipamiento, deberá incluirse en el servicio de soporte un esquema de escalamiento con los distintos fabricantes (tanto de Software como de Hardware), y presentar los esquemas de garantías de hardware adquirido, incluyendo el soporte del fabricante onsite por tres años (fallas de servidor, rotura de discos, fuentes de servidor, etc.), y la actualización de garantía básica por instalación in situ de todas las piezas de repuesto. En todos los casos en que se reemplacen discos por fallas, el contratante retendrá los defectuosos.

CONSORCIO IDSECURE IOS

10.2 SOPORTE EVOLUTIVO

Tareas de tecnología preventiva, capacitaciones (4 personas), transferencia de conocimiento, asesoramiento sobre temas puntuales y evaluación de alternativas sobre nuevas aplicaciones. Todas estas tareas excluyen la implementación que requiera el desarrollo del diseño de una solución específica, y la implementación de ningún tipo de tecnología que requiera un diseño específico para una solución particular.

10.3 CONTINUIDAD DE LA PLATAFORMA

El adjudicatario deberá proveer los manuales y procedimientos necesarios para que el ReNaPer pueda poner en funcionamiento el servicio y resolver los posibles errores comunes.

Todos los incidentes indicados por el área requirente y resueltos por el proveedor, deben ser documentados, de manera de permitir a futuro al área requirente la resolución del incidente en caso de que vuelva a surgir.

El adjudicatario se compromete a realizar los mejores esfuerzos técnicos y profesionales que tiene a su disposición, a fin de asegurar la transferencia de conocimiento al área requirente para operar la infraestructura, de manera que una vez que finalice el soporte técnico, el ReNaPer pueda mantener el nivel de servicio en los valores requeridos.

11. DIMENSIONAMIENTO

El adjudicatario deberá dimensionar la solución propuesta de manera tal que cuente con la capacidad de respuesta a **la volumetría promedio diaria** esperada:

DNI Virtual 10.000

Pasaporte 3.000

DNI 35.000

Se debe tener en cuenta que en el caso de los DNI Virtuales el DS del mismo no será requisito de este pliego.

12. ACUERDO DE NIVEL DE SERVICIO (SLA)

Los incidentes de soporte se registran vía web, correo electrónico y telefónico, con seguimiento web de la respuesta. Será responsabilidad del adjudicatario determinar la cantidad y perfil de recursos a asignar para la resolución de dicho incidente. El proveedor deberá disponer de un correo electrónico y un número telefónico destinado al reporte de incidentes, con disponibilidad 24 x 7. El proveedor debe cumplir con el acuerdo SLA para la totalidad de las locaciones descritas en la presente especificación técnica.

12.1 TIEMPO DE RESPUESTA

Tiempo transcurrido entre la comunicación al adjudicatario de la existencia del mal funcionamiento del/los componentes/s (llamada de servicio) hasta que él mismo toma contacto a los efectos de iniciar el tratamiento del incidente.

12.2 TIEMPO DE REPARACIÓN

Tiempo transcurrido entre la toma de contacto entre el cliente y el proveedor ante una incidencia hasta la corrección de la misma y puesta en funcionamiento a satisfacción del cliente.

12.3 REPARACIÓN

Se entiende que el componente reparado funcione y opere en las mismas condiciones previas al incidente.

Para el cumplimiento de lo estipulado, se entenderá como incidente: a cualquier desperfecto, funcionamiento anormal, o fuera de servicio parcial o total; a cualquier tipo y clase de evento que no permita que se pueda cumplir con el desempeño deseado según las especificaciones técnicas y/o funcionales realizadas.

A su vez, estos se dividen según su criticidad:

- **Criticidad Alta**: esta condición de servicio es válida cuando todos lo usuarios son afectados o, dada la caída de un sistema crítico para el organismo, el impacto organizacional es alto.

- **Criticidad Media**: condición válida cuando existe una degradación significativa en el rendimiento del servicio productivo.

- **Criticidad Baja**: válida para casos en que no se presentan usuarios afectados, y se asocia a un requerimiento de cambios de configuración con el fin de aumentar la performance o para seguir una normativa establecida.

12.4 NIVELES DE SERVICIO

Los niveles de servicio se definen por los tiempos de respuesta máximos acordados de acuerdo a la criticidad de los incidentes que pudieran surgir:

- **Criticidad Alta.** Tiempo máximo de respuesta: UNA (1) hora, con disponibilidad de lunes a domingo (7 x 24). Tiempo de resolución máximo: SEIS (6) horas corridas

- **Criticidad Media.** Tiempo máximo de respuesta: SEIS (6) horas, con disponibilidad 5 x 9 en el horario comprendido entre las 9:00 y las 18:00. Tiempo de resolución máximo: CUARENTA Y OCHO (48) horas corridas

- **Criticidad Baja.** Tiempo máximo de respuesta a programar con el contratante, con disponibilidad 5 x 9 en el horario comprendido entre las 9:00 y las 18:00. Tiempo de resolución máximo: SIETE (7) días corridos.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

13. LUGAR DE INSTALACIÓN:

- Centro de datos del RENAPER de la calle Pedro Chutro Nº 2780 - CABA
- Locaciones descritas en el punto 1.2

14. Pruebas de aceptación para la recepción definitiva:

La aceptación definitiva será cuando la infraestructura implementada devuelve los datos necesarios para realizar de manera efectiva las siguientes tareas:

14.1. Que se puedan firmar digitalmente en la línea de producción los pasaportes generados en los equipos de personalización en todos los modelos existentes en la planta

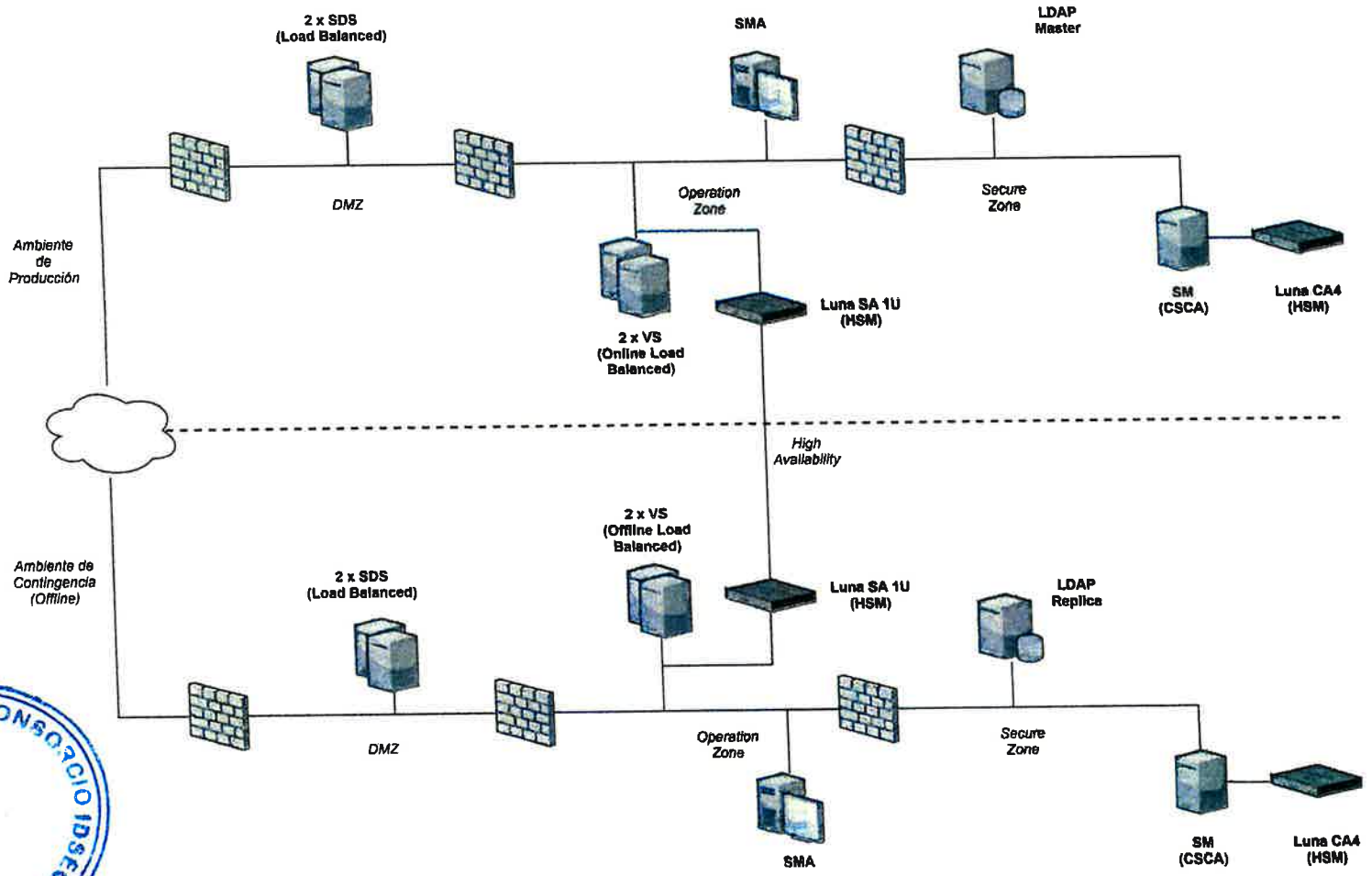
de producción como en los aeropuertos , usando la interfaz actual de servicio web que recibe como dato de entrada a la fotografía y a la MRZ en formato base64 y devuelve todos los grupos de datos para producir a la grabación y forma de datos en el chip.
Que pueda devolver durante un día de manera satisfactoria 3.000 invocaciones simuladas de datos para firmar pasaportes de acuerdo al procedimiento descrito.

14.2. Que pueda devolver al DS de los DNI en el móvil el set de datos necesarios para producir la firma estos dentro del SDK del teléfono donde residirá el DNI.
Que pueda devolver durante un día de manera satisfactoria 10.000 invocaciones simuladas de datos para firmar DNIs en el móvil de acuerdo al procedimiento descrito con las interfaces que RENAPER determine.

14.3. Que devuelva a la interfaz de firma de DNI luego de ingresar la fotografía y los datos de la MRZ los mismos grupos de datos del ítem 1).

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Anexo I – Diagrama Infraestructura Actual



Nota: En la figura se especifica la marca del hardware actual, no necesariamente requerida en la presente especificación técnica.

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2022-55379770-APN-DGTII#RENAPER

CIUDAD DE BUENOS AIRES
Jueves 2 de Junio de 2022

Referencia: PET PKI v2.0 ONTI

El documento fue importado por el sistema GEDO con un total de 16 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.06.02 12:14:13 -03:00

Flavio Ramon Brocca
Director General
Dirección General de Tecnología e Innovación en Identidad
Dirección Nacional del Registro Nacional de las Personas

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Digitally signed by Gestion Documental Electronica
Date: 2022.06.02 12:14:13 -03:00

/Default.aspx)

Miércoles 8 de Mayo, 10:30:37

Ver documento contractual

Gobierno de la República Argentina
— Año 2023

Datos de la Orden de compra

Número Orden de compra:
78-0035-OC23

Tipo:
Original

Descripción:
Orden de compra generada por Proceso Nº 78-0016-LPU22

Ejercicio:
2023

Fecha autorización:
30/06/2023

Fecha perfeccionamiento:
30/06/2023

Fecha inicio:
30/06/2023

Fecha finalización:
30/12/2025

Duración del contrato:
30 Meses a partir del Inicio del documento contractual

Datos del proceso

Número expediente:
EX-2022-56817430- -APN-DAYF#RENAPER

Número procedimiento:

1288

Localidad:

Ciudad Autónoma de Buenos Aires

Provincia:

Ciudad Autónoma de Buenos Aires

Teléfono:

43032305

Fax:

No definido

Email:

lisandro.carlomagno@ipesa.net

Detalle del Documento Contractual

Renglón	Alternativa	Código catálogo	Descripción	Cantidad	Unidad medida	Precio unitario	Moneda	Total	Acciones
1	1	3.4.9-7480.1	INFRAESTRUCT. P/FIRMA DIGITAL; DESCRIPCION: INFRAESTRUCT.P/FIRMA DIGITAL	1,00	SERVICIO	918.500,00	Dolar Estadounidense	$ 918.500,00	

Renglón	Alternativa	Código catálogo	Descripción	Cantidad	Unidad medida	Precio unitario	Moneda	Total	Acciones
2	1	3.4.6-2139.1	SERV. DE SOPORTE TECNICO; DESCRIPCION: SERV. DE SOPORTE TECNICO	1,00	SERVICIO	751.500,00	Dolar Estadounidense	$ 751.500,00	

Total documento contractual

Importe total

1.670.000,00

Importe bonificado

0,00

Importe neto

1.670.000,00

Moneda

Dolar Estadounidense

Detalle de entrega

Secretaría de
Innovación Pública
Oficina Nacional de
Contrataciones
Presidencia de la nación

PRDFINMSAPPB05 v 1.1.836_COMPRAR

Avisos sobre Navegadores
Términos y Condiciones de Uso
Preguntas Frecuentes

Envíenos por favor un ticket aquí (https://incidencias.innovacion.gob.ar/servicedesk/customer/portal/6)

Certificación en foja de Reproducciones Nº V0001253SE
Bs. As., 4 de junio de 2024

Yamila Daniaris
CONSORCIO IDSECURE ID3
Santo Domingo, D.N.

PM

COLEGIO DE ESCRIBANOS
CIUDAD DE BUENOS AIRES
CAPITAL FEDERAL - REPUBLICA ARGENTINA

CERTIFICACION DE REPRODUCCIONES
LEY 404

CERTIFICACION DE REPRODUCCIONES V 000825358

En la Ciudad de Buenos Aires, a **CUATRO de JUNIO de DOS MIL VEINTICUATRO**; en mi carácter de Escribana titular del Registro Notarial número 2.165 de la Ciudad Autónoma de Buenos Aires, **CERTIFICO** que la reproducción anexa, extendida en **TRES** fojas, que sello y firmo, es **COPIA FIEL** de su original que tengo a la vista.- Se expide la presente autenticación de reproducciones para su presentación ante quien corresponda, sin que ello implique juzgar sobre el contenido y forma de la documentación exhibida al efecto.- El documento que se certifica consiste en ORDEN DE COMPRA Numero 78-0035-OC23, fecha de inicio 30 de junio de 2023, y su correspondiente legalización, perteneciente a Magallanes Media SA C.U.I.T 30-71037547-6.-

CONSORCIO 13 SECURE
Santo Domingo Q.N.

240604000484

EL COLEGIO DE ESCRIBANOS de la Ciudad de Buenos Aires, Capital Federal de la República Argentina, en virtud de las facultades que le confiere la ley orgánica vigente, LEGALIZA la firma del escribano PEVERELLI, YAMILA DAMARIS obrantes en el documento anexo: CERTIFICACIÓN DE REPRODUCCIONES firmada por dicho escribano en la foja de Certificación de Reproducciones V-825358 con fecha 04/06/2024. La presente legalización 240604000484, no juzga sobre el contenido y forma del documento y puede ser verificada en la página web del Colegio de Escribanos de la Ciudad de Buenos Aires. www.colegio-escribanos.org.ar

Firmado Digitalmente por Colegio de Escribanos de la Ciudad de Buenos Aires. Escribano Legalizador ANDREOLI, VERONICA BEATRIZ, Matrícula 5647. Buenos Aires, 04/06/2024 13:40.-

República Argentina - Poder Ejecutivo Nacional

AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Apostilla de La Haya

Número: CE-2024-58813631-APN-DTD#JGM

CIUDAD DE BUENOS AIRES
Miércoles 5 de Junio de 2024

Referencia: Apostilla. Verificar en | Verify at | Vérifier sur: www.argentina.gob.ar/legalizacion-internacional

APOSTILLE (Convention de La Haye du 5 octobre 1961)	
1. País | Country | Pays: ARGENTINA	
El presente documento público | This public document | Le présent acte public	
2. Ha sido firmado por | Has been signed by | A été signé par: ANDREOLI VERONICA BEATRIZ	
3. Quien actúa en calidad de | Acting in the capacity of | Agissant en qualité de: FUNCIONARIO HABILITADO	
4. Y está revestido del sello/timbre de | Bears the seal/stamp of | Est revêtu du sceau/timbre de: COLEGIO DE ESCRIBANOS DE LA CIUDAD DE BUENOS AIRES	
Certificado | Certified | Attesté	
5. En | At | A: CIUDAD AUTÓNOMA DE BUENOS AIRES	6. El día | The | Le: 04-06-2024
7. Por | By | Par: Colegio de Escribanos de la Ciudad de Buenos Aires	
8. Bajo el número | Nº | Sous nº: 15519/2024	9. Sello/timbre | Seal/stamp | Sceau/timbre: 4200
10. Firma | Signature | Signature: GRIECO MARIA TERESA	

[illegible]

Tipo de documento apostillado | Type of document | Type de document: CERTIFICADO CON FIRMA DIGITAL

Titular | Holder | Titulaire: MAGALLANES MEDIA SA

Observaciones | Observations | Observations:

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.06.04 15:28:39 -03:00

COSSIO DOLORES ALEJANDRA COSSIO DOLORES ALEJANDRA -
en representación de
COLEGIO DE ESCRIBANOS - 30526499456

Digitally signed by GRIECO Maria Teresa
Date: 2024.06.05 08:44:53 ART
Location: Ciudad Autónoma de Buenos Aires

MARIA TERESA GRIECO
27136561982
-

CONSORCIO ... Q N ... IOS

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.06.05 08:44:56 -03:00