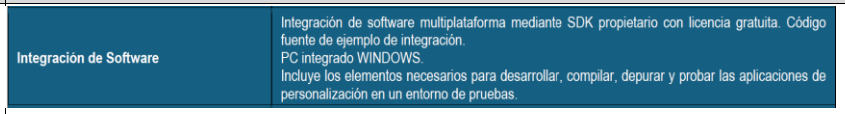
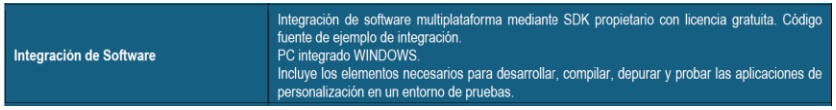
REQUISITOS QUE REQUIEREN ACLARACION (CEDULA 4.0 RD)		NUMERO DE PAGINA Y SECCION (PROPUESTA DOCUMENTO DIGITAL)	ACLARACION Y/O EXPLICACION TECNICA
1.7	**Características electrónicas y sistema operativo**		
1.7.1	Las funcionalidades electrónicas serán operativas una vez se haga una activación mediante la comparación 1:1 al recoger su tarjeta el ciudadano.	Página 49 – 55 Sección TARJETA CON CHIP SIN CONTACTO Página 82 - Sección CARACTERÍSTICAS ADICIONALES Página 193 Sección I.9 Características electrónicas y sistema operativo	Cumplimos este punto, tal y como se confirma en la propuesta con el chip ofrecido, NXP JCOP 4 Java Card v3.0.5 Edición Clásica, uno de los chips más poderosos disponibles en el mercado. Se puede dirigir a la sección 1.3.2 TARJETA CON CHIP SIN CONTACTO (páginas 49-53) donde se enumeran características y funcionalidades generales del Circuito Integrado, de su Sistema Operativo (lista no exhaustiva) y de los aplicativos incluidos. Asimismo, la sección 1.3.3 Middleware (páginas 53-55) describe las características y funcionalidades del Middleware propuesto. El chip contiene certificación CC EAL 6+ que garantiza la seguridad para el manejo de información biométrica. El chip propuesto, junto con la gama específica de aplicativos incluidos, permiten una activación mediante la comparación 1:1 al recoger su tarjeta el ciudadano, funcionalidad estándar dentro de estos tipos de dispositivos. Una de las opciones es mediante un flujo en el que la tarjeta sale de la etapa de personalización en un estado en el que la firma electrónica está desactivada, para ser activada por el ciudadano en el momento de la entrega, mediante un pin que se le proporciona en ese momento. Los métodos de activación serán definidos en conjunto con la JCE.
1.7.3	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	Página 49 – 55 Sección TARJETA CON CHIP SIN CONTACTO Página 82 - Sección CARACTERÍSTICAS ADICIONALES Página 193 Sección I.9 Características electrónicas y sistema operativo	Cumplimos este punto, tal y como se confirma en la propuesta con el chip ofrecido, NXP JCOP 4 Java Card v3.0.5 Edición Clásica, uno de los chips más poderosos disponibles en el mercado. Se puede dirigir a la sección 1.3.2 TARJETA CON CHIP SIN CONTACTO (páginas 49-53) donde se enumeran características y funcionalidades generales del Circuito Integrado, de su Sistema Operativo (lista no exhaustiva) y de los aplicativos incluidos. Asimismo, la sección 1.3.3 Middleware (páginas 53-55) describe las características y funcionalidades del Middleware propuesto. En la aplicación incluida en la propuesta de Firma Electrónica para el chip (página 50) es un requisito estándar poder actualizar los pares de claves y sus certificados para gestionar la situación en la que los certificados electrónicos caducarían antes que el documento físico u otros escenarios de vencimiento de certificado. Para ello, es necesario asociar las condiciones de acceso adecuadas para la actualización a estos pares de claves y a los certificados asociados en el momento de la creación en la personalización. Esto permitirá que una entidad externa se autentique en el aplicativo y realice las operaciones de mantenimiento.
1.7.6	**Funcionalidad de firma electrónica**		
1.7.6.5	Capacidad de almacenar, generar y usar claves RSA de, como mínimo, 4096 bits de longitud (autoridad raíz y Subordinada). Para el caso de los certificados de ciudadanos será de 2048 bits. Las claves que componen la "PKI de Firma Digital" y la "PKI de Firma de Documentos" deben estár basadas en los estándares X.509v3 y el RFC 5280. Se debe tener la capacidad de soportar curvas elípticas NIST P-256, BrainpoolP256r1, entre otras, conforme con los estándares: o BSI TR-03111 Elliptic Curve Cryptography (ECC) based on ISO 15946. Technical Guideline TR-03111, Version 2.0 o ISO15946-1 ISO/IEC. 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General. 2002. o ISO15946-2 ISO/IEC. 15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures. 2002. o ISO15946-3 ISO/IEC. 15946-3: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment. 2002. o El eID debe ser capaz de almacenar certificados x.509 que permitan a los ciudadanos gozar de los servicios de criptografía.	Página 28 - Sección SEGURIDAD Y PROTECCIÓN DE DATOS Página 90 - Sección GESTIÓN DEL ALMACÉN DE CLAVES Página 101 - Sección ALGORITMOS Página 432 - Sección PRODUCT FEATURES (Traducción en página 435) Página 52 - Sección CARACTERÍSTICAS DEL CHIP SIN CONTACTO Página 101 - Sección ALGORITMOS Página 103 - Sección PKI CIUDADANA – PKI SUBORDINADA X509	Cumplimos este punto, tal y como se confirma en la propuesta con el chip ofrecido, NXP JCOP 4 Java Card v3.0.5 Edición Clásica, uno de los chips más poderosos disponibles en el mercado. En la aplicación incluida en la propuesta de Firma Electrónica para el chip (página 50), este requerimiento se cumple de acuerdo con las páginas y secciones mencionadas en la columna de la izquierda. Por una parte, el sistema operativo JCOP4 y los aplicativos incluidos en la propuesta (página 50, documento nacional de identidad electrónico, ePKI, Firma Digital) dentro del circuito integrado (IC), permiten la importación o generación de pares de claves RSA directamente dentro del chip, con almacenamiento seguro y certificado de claves privadas. Las longitudes de clave pueden ser de 4096 bits (autoridad raíz y Subordinada) y 2048 bits (certificado ciudadano). Las claves que componen la PKI de Firma Digital y la PKI de Firma de Documentos pueden estar basados en los estándares X.509v3 y el RFC 5280. Estos certificados se almacenan en el chip y se recuperan según sea necesario, sujeto a las políticas de seguridad. La solución es compatible con ECDSA y ECDH, con compatibilidad para curvas ECC como NIST P-256 y BrainpoolP256r1, cumpliendo con los estándares indicados. Como se menciona en este documento https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-Cible-CC-2025_03en.pdf llamado Security Target de ChipDoc v3.2 (aplicativos), explica los objetivos del Common Criteria que NXP ha certificado para las firmas digitales, siendo ésta, la Security Target SSCD (Secure Signature Creation Device). En la sección de estándares (página 68), se hace referencia al ISO 15946. Este documento es el que está detrás del certificado EAL5+ SSCD (para firma digital) y que está incluido en nuestra propuesta (páginas 503-516 del documento Security Target)
2.1	**Especificaciones de maquinas de impresión**		
2.1.13	La máquina debe tener su propio PC integrado con su propio sistema operativo y software de la máquina.	Página 81 - Sección MÓDULO LÁSER CLM600 "Integración de Software" Página 81 - Sección MÓDULO LÁSER CLM600 "Integración de Software"	 Confirmamos que el equipo ofertado cuenta con su propio PC de acuerdo con lo referenciado en el Pliego y el cual es accesible mediante RDP.
2.1.14	El sistema operativo de la PC debe ser WINDOWS. Las impresoras pueden ser WINDOWS o LINUX.	Página 81 - Sección MÓDULO LÁSER CLM600 "Integración de Software"	 Confirmamos que el sistema operativo está de acuerdo con lo referenciado en el Pliego.

2.1.19	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.	Página 82 - Sección CARACTERÍSTICAS ADICIONALES "El sistema de posicionamiento automático XY"	**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. 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. La definición es tanto automática como plausible para ser definida por los técnicos de la JCE.
2.1.22	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 las piezas 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.	Página 84 - Sección CONDICIONES DE GARANTÍA Página 84 – 86 Sección CLASIFICACIÓN DE REPUESTOS	En la Sección CONDICIONES DE GARANTÍA, se establece que ofrecemos un tiempo de garantía por 5 años posteriores a la entrega de equipos a la JCE. Adicionalmente, se explica que el tiempo de vida útil de los equipos es de 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. En la Sección CLASIFICACIÓN DE REPUESTOS, se indica que, de acuerdo con la clasificación de las piezas, se determina su vida útil.
2.1.24	El proveedor deberá incluir 230 lectores de chip sin contacto, y poner como opcional, la compra de lectores de forma individual. La características del lector de tarjetas debe ser Lector para NFC Compatible con ISO 14443 Tipo A, Tipo B y Tarjetas Mifare 1k&4k, ICAO 9303 con interoperabilidad OACI DOC 9303, ISO18013, PA, AA, BAC, EAC , SAC.	El lector NFC se suministró en el momento de la presentación de la oferta. Véase la confirmación adjunta (Ver Anexo A de esta subsanación). Se facilitó la marca y el modelo del lector NFC. Se adjunta una copia del paquete del producto entregado. Las especificaciones del lector NFC figuran en el paquete y cumplen con las especificaciones requeridas (Ver Anexo A de esta subsanación). En la pregunta del Grupo 1, Pregunta 25, de agosto de 2024, que establece este requisito, el texto completo indica: La impresora debe realizar un control de calidad. Las 230 unidades serán entregadas junto con las impresoras.	Queremos aclarar que el estándar ICAO 9303 (OACI- por sus siglas en español) corresponden al estándar que define los requisitos para documentos de viaje electrónicos, incluyendo el uso de tecnología RFID/NFC basada en el protocolo ISO/IEC 14443 (Tipo A y B) para comunicación sin contacto. Basado en las especificaciones del ACR1252U, se puede confirmar que este lector cumple con el estándar ICAO 9303, ya que soporta los protocolos ISO/IEC 14443 Tipo A y B y está diseñado específicamente para leer documentos de viaje electrónicos, como pasaportes electrónicos [JM1] [JM2]. 1.1 ACR1252U Reader III: • El ACR1252U es un lector NFC de marca ACS que cumple con el estándar ISO/IEC 14443 Tipo A y B, lo que lo hace compatible con tarjetas sin contacto utilizadas en pasaportes electrónicos. • Según la documentación de ACS, este lector está diseñado para aplicaciones de alta seguridad, como la lectura de e-Passports, y soporta los protocolos necesarios para interactuar con chips que cumplen con ICAO 9303, chips que son del mismo tipo del cual el CONSORCIO esta ofreciendo en la oferta (ver página 49 a 56 de nuestra oferta). • Además, el ACR1252U es certificado por estándares como PC/SC y CCID, y es compatible con aplicaciones que requieren autenticación segura, lo que refuerza su idoneidad para MRTD, requerimiento del OACI 9303. • Basado en las especificaciones del ACR1252U, confirmamos que este lector cumple con el estándar ICAO 9303, ya que soporta los protocolos ISO/IEC 14443 Tipo A y B y está diseñado específicamente para leer documentos de viaje electrónicos, como pasaportes electrónicos. Ahora, en relación con la compatibilidad del lector ofertado ACR1252U Reader III con el estándar ISO 18013, mencionamos: Según la documentación de ACS: • El ACR1252U es un lector NFC certificado por el NFC Forum, que opera a 13.56 MHz y soporta ISO/IEC 14443 Tipo A y B, ISO/IEC 18092 (NFC), MIFARE, FeliCa, y etiquetas NFC compatibles. • Es capaz de operar en los tres modos NFC: lector/escritor, emulación de tarjeta, y comunicación peer-to-peer, lo que lo hace versátil para aplicaciones como pagos, control de acceso, y lectura de documentos electrónicos. • Incluye un SAM (Secure Access Module) para autenticación mutua y diversificación de claves, proporcionando seguridad para transacciones sin contacto. • Es compatible con PC/SC y CCID, lo que asegura interoperabilidad con diversas aplicaciones y sistemas operativos (Windows, Linux, macOS, Android). • Se confirma que para ISO/IEC 18092 y ISO/IEC 14443 Tipo A y B el lector puede interactuar con dispositivos y etiquetas NFC que cumplen con los requisitos técnicos de ISO/IEC 18013-5, incluyendo smartphones que emulan mDL mediante HCE.
2.1.25	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. 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.	Página 78 - Sección BENEFICIOS DE LA SOLUCIÓN, último párrafo, "Capacidad de incluir componentes adicionales para controles de calidad". Página 81 – Sección MÓDULO LÁSER CLM600 Diagnóstico y Personalización	En el aparato mencionado, el orden en que se encuentra expuesto en nuestra propuesta agota el requisito solicitado de flujo de trabajo y diferentes criterios de control de calidad que podrán ser utilizados con los equipos propuesto, solución que también fue demostrada durante la prueba de concepto. Es decir, el párrafo mencionado contiene el flujo que puede ser usado la JCE para realizar el control de calidad deseado, en el mismo orden que se encuentra expuesto en nuestra propuesta. La impresora cuenta con un módulo de diagnóstico y personalización que permite la configuración y monitoreo para informes de producción.
2.2	**Personalización**		
2.2.21	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.	Página 81 - Sección MÓDULO LÁSER CLM600 – • Integración de Software • Diagnóstico y personalización	**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. Como se menciona en nuestra oferta, el equipo cuenta con un módulo de diagnóstico y personalización que incluye una aplicación de configuración y monitoreo basada en web (web-based). Esta aplicación también se utiliza para la personalización de datos personales, almacenando datos de manera temporal, acorde a configuración que se le realice. Este módulo es el que permite la integración con el sistema de emisión de la JCE.

3.1	Características generales de la PKI		
3.1.5	El proveedor deberá proporcionar un portal para firma de documentos con el estándar ISO 32000-1, además de la integración a las aplicaciones de la JCE que permita firmar con certificados tanto en la cédula de identidad o externos .El portal para Firmar documentos debe manejar al menos tres tipos de roles: 1. Administrador, con todos los permisos, esta figura debe poder generar y/o enrolar Agentes Certificadores; 2. Agente Certificador con permisos para enrolar y/o generar certificados para los usuarios finales o firmantes; 3. Firmante, son los usuarios que podrán firmar los documentos.	Página 95 - Sección ADMINISTRACIÓN DE ACTORES Página 54 - Sección MIDDLEWARE	En nuestra propuesta, ante el requerimiento de la referencia se encuentra agotado en las páginas 54, apartado Middleware, se encuentra descrito la compatibilidad que posee el chip ofertado y el componente middleware, para interactuar con portales web y viabilizar la firma digital de documentos PDF, en cumplimiento del ISO 32000-1. Así mismo, el gráfico incluido en la página 55 de nuestra propuesta, presenta los componentes requeridos para que esta funcionalidad pueda ser implementada (Ver gráfico página 54). El estándar ISO 32000-1 es el estándar predeterminado utilizado por todos los emisores de documentos PDF (Ej.: Adobe, Nitro, Google, etc.) y nuestro software está configurado por defecto para procesar documentos PDF del estándar mencionado. En complemento de esta funcionalidad, en la página 99 de nuestra propuesta, se explica claramente la funcionalidad del firmador de documentos (Document Signer), el cual contiene un administrador web que incluye la administración de actores (página 95) que pueden ser configurados y utilizados para la gestión de los certificados. Este mismo componente, permitirá a la JCE integrar lo requerido para firmar con los certificados emitidos.
3.1.10	El oferente deberá incluir en su propuesta, toda la infraestructura física necesaria para la implantación, ejecución y mantenimiento de la PKI, el conjunto de hardware y software en las instalaciones que indique la dirección de informática. El contrato de mantenimiento a cotizar será de dos (2) años. A partir de los dos años, la JCE podrá renovar el mantenimiento con el precio establecido del proveedor de forma anual. Para la solución de la PKI el ambiente productivo debe habilitarse en alta disponibilidad con 2 nodos activos en balanceo de carga, un ambiente de DRP en disponibilidad simple (1 nodo) y un ambiente de desarrollo en disponibilidad simple (1 nodo).	Página 88 - 105 Sección GET TRUST – SOLUCIÓN DE PKI Página 102 - Sección INFRAESTRUCTURA GET TRUST 3.5. Infraestructura GET Trust Página 103 - Sección MÓDULO DE SEGURIDAD POR HARDWARE (HSM) - Según Punto a Punto Página 97 - Sección ADMINISTRACIÓN DE PARTICIONES	Nuestra propuesta contempla el cumplimiento y entrega de toda la infraestructura. En atención a la solicitud de especificaciones técnicas detalladas sobre la infraestructura tecnológica que dará soporte a la operación de la plataforma PKI y los sistemas de emisión de cédulas digitales, me permito presentar las siguientes consideraciones: 1. Enfoque de contratación basado en resultados Desde el análisis del Pliego de Condiciones, identifico con claridad una orientación hacia el cumplimiento de resultados funcionales medibles y verificables, con estándares internacionales y metas operativas bien definidas. Algunos ejemplos contenidos en el pliego incluyen: •La exigencia de certificación EAL4+ para los componentes del PKI (página 1 de la propuesta técnica), •La conformidad con normativas como eIDAS (página 2), •El cumplimiento de ISO/IEC 15408 en materia de seguridad (página 3), •La capacidad de emisión alineada a la demanda poblacional de la JCE, y •El aseguramiento de continuidad del negocio y niveles de servicio adecuados (ver capítulos 6.3, 6.4 y 8.4). Estos elementos reflejan que la contratación persigue la entrega de una plataforma integralmente funcional, segura y resiliente. 2. Integración explícita de la infraestructura en el plan de trabajo Desde la fase inicial del diseño del proyecto, incluimos en el cronograma de ejecución (página 168 de nuestra oferta) la entrega, instalación y validación completa de la infraestructura tecnológica necesaria para soportar el sistema PKI, con fechas definidas y tareas claramente secuenciadas. Entre las actividades incluidas en el cronograma del documento "Cronograma Proyecto CÉDULA 4.0 RD – Febrero 24, 2025", destaco: •Línea 23: Definición y entrega de requisitos para implementación PKI •Línea 24: Definición de Autoridades Certificadoras y dominios PKI •Línea 25: Plan de configuración del entorno •Líneas 26–28: Habilitación de área de cómputo y entrega de infraestructura física •Línea 29: Preparación de máquinas virtuales (VMs) •Línea 31: Instalación y configuración del entorno de preproducción •Línea 32: Pruebas de aceptación de la solución PKI •Líneas 34–35: Configuración de los entornos de producción y de recuperación ante desastres (DR) Estas tareas han sido planificadas para ejecutarse dentro de las primeras 20 semanas del proyecto, lo que demuestra una visión estructurada, responsable y técnicamente coherente con los objetivos de disponibilidad y resiliencia del sistema.
			3. Diseño de la infraestructura orientado a disponibilidad y resiliencia La infraestructura propuesta ha sido concebida para responder a los requerimientos del pliego y alinearse con las mejores prácticas descritas en los capítulos 6.3, 6.4, 8.4 y 8.5. Su diseño contempla: •Redundancia física y lógica en todos los niveles, incluyendo entornos productivos y de contingencia, •Separación de ambientes de preproducción y pruebas para asegurar estabilidad en los despliegues, •Medidas de cifrado, monitoreo continuo y control de acceso para garantizar conformidad con normativas de seguridad, •Arquitectura modular y escalable que soporta el volumen de emisión de certificados digitales exigido, permitiendo además adaptabilidad futura. 4. Detalle técnico complementario En respuesta al requerimiento puntual, desglosamos la infraestructura tecnológica considerada, la cual incluye: •Configuración de servidores físicos y virtuales por ambiente (Producción, Preproducción, DR), •Detalles de capacidad de procesamiento (núcleos de CPU), memoria RAM y tipo de almacenamiento, •Segmentación funcional: componentes de HSM, autoridades de certificación, bases de datos, interfaces administrativas y de validación, •Arquitectura de red, elementos de seguridad perimetral, y políticas de respaldo automatizado, •Procedimientos para recuperación ante incidentes, alineados con los tiempos máximos de recuperación definidos. Esta infraestructura ya forma parte de la planificación logística y técnica del proyecto, y ha sido seleccionada para asegurar niveles óptimos de respuesta.
3.1.12	En la Nube (compatible con los servicios en la nube de Azure): CMS, CRL/Protocolo de Estado del Certificadoen Línea, Repositorio PKI, y servicios adicionales no críticos	Página 89 - Sección GET AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA – CSCA Página 99 - Sección FIRMADO DE DOCUMENTOS GET TRUST (DOCUMENT SIGNER) Página 103 - Sección MÓDULO DE SEGURIDAD POR HARDWARE (HSM)	En la página 89, en la sección GET AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA – CSCA se encuentra listado el listado de componentes que componen la CSCA propuesta por el consorcio, incluyendo el sistema de gestión de credenciales, la lista de revocación y todos los demás componentes de la PKI. Así mismo, en la Página 102 se detalla el despliegue de componentes de la PKI (GET Trust PKI – Arquitectura principal) que se propone para el proyecto. De esta manera se cumple con los requerimientos solicitados, donde todos estos componentes se hospedarán en la infraestructura propuesta, dentro de las premisas de la JCE. También, haciendo relación a la respuesta dada por la JCE en el documento de Respuesta Técnicas a Oferentes de Agosto, Grupo 1, pregunta 12, donde se menciona "Algunos componentes críticos de la PKI deben permanecer alojados en las instalaciones (on-premise), mientras que otros componentes pueden ser alojados en la nube" Subrayado nuestro.

			Primero, la JCE puede utilizar el sitio web de acceso público indicado a continuación para verificar si una empresa está utilizando un producto con certificación EAL4+. Common Criteria permite al JCE confirmar qué productos han recibido la certificación completa EAL4+, listados por producto y proveedor. El sitio web es: https://www.commoncriteriaportal.org/products/index.cfm Tal como se detalla en nuestra oferta, y complementando mediante la presentación de la certificación EAL4+ mencionada, el software completo de la Infraestructura de Clave Pública está certificado con CC EAL4+. La misma solución de software se utiliza para crear las Autoridades de Certificación tanto para la PKI de Documentos como para la PKI de Firma Digital. https://commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/anssi-cc-2021_17fr.pdf El consorcio C4RD, mediante la solución de PKI GET Trust, a integrado un componente de la empresa Eviden. Consulte la página 102, donde GET proporciona la certificación de Eviden y la confirmación de que se integrará en nuestra solución. Se debe entender que una solución PKI con este tipo de certificación es una solución más costosa que una solución no certificada. El coste está relacionado con las importantes ventajas técnicas que ofrece la certificación EAL4+ para toda la solución PKI. La certificación únicamente del chip y el HSM no proporciona el mismo nivel de seguridad que la certificación EAL4+ de todos los componentes PKI. La JCE insistió correctamente en este requisito, ya que proporciona una garantía de seguridad integral para toda la solución. La principal ventaja de contar con la certificación EAL4+ para todo el sistema de firma PKI, en lugar de solo el HSM, reside en una garantía de seguridad integral:
3.1.13	Tanto la PKI de firma de documentos como la PKI de Firma Digital deben cumplir CC EAL 4+	Página 811 - Certificado Common Criteria EAL4+ Página 102 - Sección CARACTERÍSTICAS CLAVES	1. Seguridad Integral: oCuando solo se certifica el HSM, el hardware es seguro, pero el software que gestiona el proceso de firma podría presentar vulnerabilidades. Por ejemplo, un software defectuoso podría hacer un uso indebido de las claves, firmar datos incorrectos o ser explotado para eludir las protecciones del HSM. oCertificar todo el sistema de firma PKI garantiza la seguridad tanto del software (p. ej., la aplicación de creación de firmas o la autoridad de certificación) como del hardware, lo que reduce el riesgo de que vulnerabilidades comprometan el proceso de firma. 2. Cumplimiento Normativo: oEn contextos de alta seguridad, como las firmas electrónicas cualificadas según el reglamento eIDAS de la Unión Europea, un Dispositivo Cualificado de Creación de Firmas (QSCD) debe cumplir con estándares de seguridad específicos. Esto suele requerir la certificación de todo el sistema (hardware y software), no solo del HSM. oPor ejemplo, productos como el dispositivo ADSS SAM están certificados según EAL4+ en su conjunto para firmas remotas que cumplen con eIDAS, lo que garantiza un cumplimiento que una certificación de HSM independiente podría no satisfacer por completo.3. Reducción del Riesgo: Un sistema de firma PKI certificado garantiza que todo el flujo de trabajo, desde la gestión de claves en el HSM hasta la generación de firmas en el software, ha sido evaluado y reforzado contra ataques. Esto es fundamental para aplicaciones que requieren confianza, como documentos legales o transacciones financieras. Ejemplo práctico oNuestro HSM con certificación EAL4+ garantiza el almacenamiento seguro de claves y las operaciones criptográficas. Sin embargo, si se combina con software PKI no certificado, el sistema podría ser vulnerable a ataques que aprovechen vulnerabilidades de software. oPor el contrario, un sistema de firma PKI con certificación EAL4+ (por ejemplo, un dispositivo integrado o una solución de software y hardware) garantiza que todo el proceso cumpla con los mismos altos estándares, ofreciendo mayor confianza en las firmas generadas. PIE DE NOTA: Tras la revisión, ninguna de las empresas de los otros consorcios aparece listada como poseedora de un producto de firma PKI con certificación EAL4+. Es posible también que hubieran contratado a una empresa tercera, como ha hecho GET.
3.1.22	El CSCA debería ser capaz de emitir certificados de firmante de lista maestra.	Página 90 - Sección GET AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA – CSCA	En la página 90, GESTIÓN DE DEPOSITOS EN GARANTIA (Escrow management), se menciona la característica ofrecida para la creación de la llave maestra que se encuentra incluida en nuestra oferta de solución PKI.
3.1.27	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.	Página 99 - Sección FIRMADO DE DOCUMENTOS GET TRUST (DOCUMENT SIGNER)	En la página 108 de nuestra propuesta se hace mención a la manera como se propone realizar la firma de los documentos mID (según el estándar ISO 18013-5), el cual incluye una integración con la solución de PKI propuesta. Así mismo, la página 99, se menciona la posibilidad que tiene el sistema GET Trust de gestionar diferentes entidades firmantes (comúnmente denominadas “Firmantes de documentos” o DS), este será un DS independiente para el firmado digital de la Tarjeta Digital de la JCE. El sistema de Document Signer contiene un 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 (extracto de la pagina 99 de la oferta del consorcio C4RD). La solución de PKI propuesta esta preparada para realizar una implementación de DTC en el momento en que la JCE decida realizarla, en conjunto con la solución de GET Mobile ID para la Tarjeta Digital. Para complementar esta respuesta, por favor ver la respuesta a la pregunta 4.2 de esta subsanación, donde se explica la manera como la tecnología ofertada está preparada para el uso de DTC dentro de la aplicación de Tarjeta Digital y cómo se utiliza la solución de PKI para este fin.

3.2	Autoridad de Certificación (CA) de firma de país (CSCA)		
3.2.3	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 y requerirá medidas de seguridad robustas, entre otras: - Atenticación multifactorial (MFA para acceso a la administración). Cifrado avanzado en todas las comunicaciones y datos almacenados, utilizando algoritmos criptográficos robustos y actuales. - Uso de Módulos de Seguridad por Hardware (HSMs) certificados (FIPS 140-2 nivel 2 o superior) para la generación y almacenamiento de claves privadas. - Implementación de sistemas avanzados de monitoreo y detección de intrusos (IDS/IPS). - El monitoreo debe incluir de infraestructura, de seguridad y de comuniciones - Segmentación de redes que aísle la infraestructura de PKI de otras redes corporativas. - Mantenimiento de todos los sistemas y software de la PKI actualizados con los últimos parches de seguridad. - Realización de auditorías regulares y evaluaciones de seguridad. - Capacitación del personal involucrado en la operación y gestión de la PKI sobre las mejores prácticas de seguridad y procedimientos de respuesta a incidentes.	MFA Página 28 - Sección SEGURIDAD Y PROTECCIÓN DE DATOS Página 149 - Sección SEGURIDAD Y CUMPLIMIENTO Página 825 - Sección PRINCIPALES CARACTERÍSTICAS HSM Página 104 - Sección MÓDULO DE SEGURIDAD POR HARDWARE (HSM) Página 139 - Sección ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA DEL PKI – CA Página 436 - Sección CARACTERÍSTICAS DEL PRODUCTO IDS/IDP Página 163 - Sección ANÁLISIS DE RIESGOS Monitoreo Página 97 - Sección ADMINISTRACIÓN DE AUDITORIA, REPORTES Y SUPERVISIÓN Página 139 - Sección ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA DEL PKI – CA Página 144 - Sección SEGURIDAD Y CUMPLIMIENTO Página 145 - Sección ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA Segmentación de redes: Página 102 - Sección - INFRAESTRUCTURA GET TRUST Página 163 - Sección ANÁLISIS DE RIESGOS Mantenimiento Página 139 - Sección PLAN DE MANTENIMIENTO PARA PKI Página 143 - Sección MANTENIMIENTO PREVENTIVO Y CORRECTIVO Auditorías: Página 139 - Sección ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA DEL PKI – CA Página 144 - Sección SEGURIDAD Y CUMPLIMIENTO Capacitación Página 154 - Sección PLAN DE CAPACITACION PARA PKI	Efectivamente todo en cuanto a proteccion ha sido contemplado en el diseño. La infraestructura propuesta para la plataforma de Infraestructura de Clave Pública (PKI) destinada a la Junta Central Electoral (JCE) ofrece sólidas garantías de seguridad y cumplimiento, integrando integralmente los requerimientos establecidos por la institución. Nuestra solución cumple con el estándar EAL4+ (tal como esta debidamente transparentado en nuestra propuesta) bajo el marco ISO/IEC 15408 (Criterios Comunes), así como con el reglamento europeo eIDAS, brindando un marco robusto y confiable para la protección de datos y la gestión de firmas electrónicas avanzadas. Las medidas de autenticación multifactorial (MFA) para el acceso administrativo están claramente detalladas en nuestra propuesta técnica (Páginas 28, 149 y 825), asegurando que solo personal autorizado tenga acceso a las operaciones críticas. Para la generación y almacenamiento seguro de claves privadas, la solución incorpora Módulos de Seguridad por Hardware (HSM) certificados según el estándar FIPS 140-2 nivel 2 o superior, lo cual está minuciosamente descrito en las páginas 104, 139 y 436 de la propuesta técnica. La infraestructura propuesta también incluye sistemas avanzados de monitoreo y detección de intrusiones (IDS/IPS), descritos explícitamente en la sección de Análisis de Riesgos (Página 163), reforzando la protección frente a amenazas externas. Asimismo, el monitoreo integral de infraestructura, seguridad y comunicaciones es abordado ampliamente en las páginas 97, 139, 144 y 145, permitiendo un control continuo y proactivo del entorno. En términos de segmentación de redes, nuestra solución garantiza el aislamiento de la infraestructura PKI respecto a redes corporativas externas, tal como se indica en las páginas 102 y 163. Esto reduce significativamente la superficie de ataque y fortalece la seguridad operacional. Adicionalmente, nuestro plan integral de mantenimiento preventivo y correctivo, detallado en las páginas 139, 143 y 168, contempla actualizaciones regulares de software y firmware cada seis meses, lo que asegura que todos los componentes críticos permanezcan protegidos frente a vulnerabilidades emergentes. Se realizarán auditorías regulares y exhaustivas, descritas en las páginas 139, 144 y 168 (incluyendo revisiones específicas de control de calidad), así como evaluaciones semestrales de seguridad mediante pruebas de penetración y vulnerabilidades, garantizando el cumplimiento continuo con los estándares más estrictos en materia de seguridad informática. Finalmente, la propuesta incluye un completo programa de capacitación técnica, detallado en las páginas 154 y 168, asegurando que el personal del JCE esté preparado para gestionar eficientemente la plataforma PKI, implementar mejores prácticas en seguridad digital y reaccionar adecuadamente frente a cualquier eventual incidente, fortaleciendo aún más la resiliencia institucional.
3.2.4	La solución debe de ser redundante y el oferente debe de explicar y detallar cómo. La aplicación de software que implementa CSCA y CVCA se desea que cumplan con el EAL 4+ pero no es obligatorio.	Página 102 – Sección INFRAESTRUCTURA GET TRUST Página 811 - 816: Certificado Common Criteria EAL4+ con su traducción	Como se menciona en la oferta, en el apartado 3.5 de la página 102, se describe la infraestructura que comprende componentes esenciales del sistema y la intercomunicación entre ellos. El gráfico en esta misma página muestra la alta disponibilidad (redundancia) diseñada donde incluso se menciona la cantidad de servidores por componente. La aplicación que implementa el CSCA, mismo CSCA que se requiere para ser CC EAL 4+ como lo establece el requisito para 3.1.13, se basa en el consumo de Servicios Web que se implementan con las mejores prácticas con interfaces SOAP y REST. Por lo tanto, aunque el software que implementa el CSCA puede no estar certificado EAL4+, el CSCA deben cumplir con la certificación EAL4+ según lo establecido en la Sección 3.1.13. De lo contrario, el JCE podría comprometer la seguridad integral de la solución PKI.

3.2.5	Es obligatorio implementar planes de recuperación ante desastres y continuidad del negocio para la infraestructura PKI. Es importante que el plan de continuidad y recuperación ante desastres esté alineado con las normas internacionales, como la ISO/IEC 27031, que establece directrices para la preparación en tecnologías de la información, y la ISO 22301, que cubre los sistemas de gestión de continuidad del negocio.	<table><tr><th colspan="2">Estrategia de Recuperación ante Desastres y Continuidad del Negocio – Plataforma PKI</th><th colspan="2">Capítulo / Subcapítulo / Pagina</th></tr><tr><td>1</td><td>Certificaciones aplicadas a la plataforma: EAL4+</td><td colspan="2">páginas # 51,90,103,104,139,194, 208, 212, 433, 436, 467, 470, 475, 811, 812, 815, 816 y 826</td></tr><tr><td>2</td><td>Certificaciones aplicadas a la plataforma: eIDAS</td><td colspan="2">páginas # 53, 99, 103, 104, 139, 212, 401, 403 y 436</td></tr><tr><td>3</td><td>Certificaciones aplicadas a la plataforma: ISO/IEC 15410</td><td colspan="2">páginas # 7, 185, 208, 467, 468, 469, 471 y 472</td></tr><tr><td>4</td><td>Inclusión de tareas DRP en el cronograma (instalación sitio de contingencia, pruebas, estabilización)</td><td>Cronograma del Proyecto</td><td>Página 168</td></tr><tr><td>5</td><td>Inclusión explicita del DRP en el SLA contractual</td><td>SLA General – Propuesta Técnica</td><td>Página 130-150</td></tr><tr><td>6</td><td>Modelo de soporte técnico multinivel (L1-L3) y protocolo de atención</td><td>6.1.3 –Modelos de Servicio y SLA</td><td>Página 130-150</td></tr><tr><td>7</td><td>Tiempos de respuesta por criticidad (P1 a P4)</td><td>6.1.4 –SLA y Tiempos de Respuesta</td><td>Página 130-150</td></tr><tr><td>8</td><td>Protocolo formal para la apertura y atención de incidentes por parte de la JCE</td><td>6.1.5 –Procedimiento de Incidentes</td><td>Página 130-150</td></tr><tr><td>9</td><td>Escalamiento técnico y ejecutivo ante fallos</td><td>6.2 – Matriz de Escalamiento</td><td>Página 130-150</td></tr><tr><td>10</td><td>Mantenimiento preventivo y correctivo sobre la plataforma PKI</td><td>6.3 – Mantenimiento Preventivo/Correctivo</td><td>Página 130-150</td></tr><tr><td>11</td><td>Auditorías, monitoreo continuo, control de accesos y seguridad operativa</td><td>6.4 – Seguridad y Cumplimiento</td><td>Página 130-150</td></tr><tr><td>12</td><td>KPIs de desempeño: disponibilidad, MTTR, cumplimiento de SLA, incidentes de seguridad</td><td>6.5 – KPIs y Métricas</td><td>Página 130-150</td></tr><tr><td>13</td><td>Estrategia de continuidad: redundancia tecnológica, centros alternos, fábrica de respaldo</td><td>8.4.1 – Infraestructura de Respaldo</td><td>Página 164</td></tr><tr><td>14</td><td>Protocolos de respaldo de información y recuperación rápida</td><td>8.4.2 –Protocolos de Respaldo de Información</td><td>Página 164</td></tr><tr><td>15</td><td>Plan de recuperación ante crisis, tiempos máximos de recuperación (RTO), comité coordinador</td><td>8.4.4 –Plan de Recuperación Ante Crisis</td><td>Página 164</td></tr><tr><td>16</td><td>Procedimientos de simulación, pruebas ante fallos, y auditorías de resiliencia</td><td>8.5 – Procedimientos de Respuesta y Recuperación</td><td>Página 164</td></tr></table>	Tal cual como se demuestra, el plan de Recuperacion contra Desestres y Continidad de los servicios esta contemplado. En ese contexto, el Consorcio Cédula 4.0 R.D. ha diseñado una estrategia específica y robusta de recuperación y continuidad de la plataforma PKI, sustentada en los principios y directrices de tres pilares normativos fundamentales: •ISO/IEC 27031: Proporciona un marco detallado para la preparación en tecnologías de la información y las comunicaciones (TIC), orientado a asegurar que las capacidades tecnológicas que respaldan los procesos críticos puedan ser recuperadas dentro de los tiempos aceptables para el negocio. •ISO 22301: Estándar internacional de gestión de continuidad del negocio que define cómo una organización debe planificar, implementar, monitorear y mantener un sistema eficaz para asegurar la resiliencia operativa y la recuperación oportuna de funciones esenciales. •Capítulos 8.4 y 8.5 de esta propuesta técnica: Reafirman que el Consorcio ha concebido una estrategia integral de continuidad del servicio, aplicable directamente a los servicios críticos de emisión digital, dentro de los cuales la infraestructura PKI-CA juega un rol neurálgico. Esta estrategia incorpora medidas de redundancia tecnológica, centros de respaldo, protocolos de recuperación y simulacros periódicos, alineados con los estándares antes mencionados. El diseño de nuestra plataforma contempla mecanismos preventivos, reactivos y de mejora continua que aseguran la *resiliencia de la infraestructura PKI, su capacidad de recuperación ante incidentes y la restauración completa de los servicios de certificación digital, todo ello con un enfoque sistémico, probado y documentado. A lo largo de los capítulos 6 y 8 de la propuesta técnica se evidencia cómo esta estrategia se traduce en acciones técnicas, logísticas y contractuales específicas que blindan la operación de la JCE ante cualquier evento de alto impacto. *Estrategia DRP/BCP de la Plataforma PKI basada en el Cronograma y Certificaciones El consorcio ha estructurado un plan robusto y alineado con las mejores prácticas internacionales para garantizar la continuidad del servicio y una eficiente recuperación ante desastres (DRP/BCP). Este enfoque se sustenta en cuatro pilares fundamentales: 1. *Experiencia Técnica Especializada La presencia del experto Joel Pérez (PMP), con trayectoria demostrada en diseño de soluciones seguras, implementación de sistemas PKI y recuperación de desastres, aporta una dirección técnica de primer nivel al proyecto, validando su resiliencia.
			2. *Diseño Proactivo en el Cronograma de Implementación El cronograma del proyecto contempla: •Configuración de entornos de recuperación (Disaster Recovery) para la plataforma PKI (línea 35), •Ejecución de ceremonias de llaves separadas para producción y contingencia, y •Tareas de estabilización, validación técnica y continuidad del negocio planificadas entre las semanas 20-25. 3. *Contratos SLA con Cláusulas de Recuperación ante Desastres En la página 369 de la propuesta técnica, se explicita que dentro de los compromisos de soporte, se incluye la atención y gestión de recuperación ante desastres como parte del servicio ofrecido. 4. *Certificaciones de Seguridad y Fiabilidad La solución contempla: •EAL4+: seguridad operacional validada, •eIDAS: cumplimiento legal y técnico de identidad digital, •ISO/IEC 15408: gestión confiable y segura de componentes criptográficos. Estas certificaciones fortalecen la robustez de la infraestructura PKI, validando su alineación con entornos críticos de certificación digital y continuidad operativa. *Estrategia DRP/BCP de la Plataforma PKI basada en los Capítulos 6.1 a 6.5 de la Propuesta Técnica 1. *Soporte Multinivel y Escalamiento (Capítulos 6.1.3 a 6.2) •Modelo de soporte L1–L3 con tiempos de respuesta definidos. •Escalamiento progresivo desde técnicos operativos hasta la presidencia del consorcio. •Respuesta en < 2 horas para fallos críticos (P1), incluyendo caída total de servicios PKI-CA. 2. *Mantenimiento Preventivo y Correctivo del Entorno PKI (Capítulo 6.3) •Simulacros de incidentes, auditorías de seguridad, verificación de HSM, y actualización programada de software. •Atención inmediata a fallos imprevistos, restauración de claves, y sustitución de hardware comprometido. •Pruebas de penetración periódicas que permiten anticipar debilidades antes de que afecten la operación. 3. *Seguridad y Monitoreo Continuo (Capítulo 6.4) •Auditorías internas y de terceros. •Control de acceso basado en roles y monitoreo en tiempo real. •Procedimientos activos de notificación, análisis y recuperación ante incidentes de seguridad en el entorno PKI.
			4. *Indicadores Clave de Desempeño (KPIs) (Capítulo 6.5) •Disponibilidad del sistema > 99.9%. •Cumplimiento de SLA > 95%. •Seguimiento de incidentes de seguridad y eficiencia en tiempos de recuperación (MTTR). •Evaluaciones mensuales y revisión trimestral para mejora continua. *Estrategia de Continuidad del Servicio Aplicada a la Infraestructura PKI (Capítulos 8.4 y 8.5) Los capítulos 8.4 y 8.5 de la propuesta técnica reafirman que el Consorcio Cédula 4.0 R.D. ha concebido una estrategia integral de continuidad del servicio, aplicable directamente a los servicios críticos de emisión digital, dentro de los cuales la infraestructura PKI-CA juega un rol neurálgico. Esta estrategia se alinea con los principios de resiliencia operativa, redundancia tecnológica y recuperación ágil, tal como requieren las normas ISO/IEC 27031 e ISO 22301. 1. *Infraestructura de Respaldo (Capítulo 8.4.1) •Servidores redundantes y almacenamiento seguro para garantizar la disponibilidad de los servicios certificados. •Centros de producción secundarios y una fábrica de respaldo internacional en Francia, habilitada para producción de emergencia. •Seis sucursales como nodos alternos de operación ante fallos críticos. 2. *Protocolos de Respaldo de Información (Capítulo 8.4.2) •Copias automatizadas de las bases de datos de identidad con cifrado. •Mecanismos de recuperación rápida para restaurar servicios tecnológicos. 3. *Plan de Recuperación ante Crisis (Capítulo 8.4.4) •Pruebas periódicas de recuperación. •Tiempo Máximo de Recuperación (RTO): 24 a 48 horas para restablecer operaciones esenciales. •Comité de Seguridad y Continuidad como órgano coordinador estratégico. 4. *Simulaciones, Roles y Auditorías (Capítulo 8.5) •Simulacros periódicos, ensayos ante amenazas y auditorías anuales. •Roles claramente definidos que integran a los equipos de seguridad, tecnología y logística.

3.2.6	El proveedor adjudicado debe de coordinar y apoyar la implementación de la CA con las disposiciones legales establecidas en la Ley 126-02 sobre Comercio Electrónico, Documentos y Firma Digital y su reglamento contenido en el Decreto 335-03. Debe apoyar el proveedor adjudicado con su personal experto, en los pasos a seguir para establecer la CA en el país, y en los documentos que debe de generar. Pero la presentación y la autorización dependerá de la JCE ante las entidades gubernamentales.	Página 251 - Sección MATRIZ DE CUMPLIMIENTO (Entendemos y Aceptamos)	Como se menciona en la oferta presentada por el consorcio C4RD, página 251, entendemos y aceptamos que la JCE requerirá de nuestro apoyo y coordinación con el personal experto de nuestro consorcio, para presentar la documentación necesaria en cumplimento a la Ley 126-02 sobre Comercio Electrónico, Documentos y Firma Digital y su reglamento contenido en el Decreto 335-03, para la implementación de la CA.
3.2.8	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 JCE.eIDAS CC EAL4+ debe ser parte de las características de los HSM. La combinación de eIDAS con la certificación CC EAL4+ se refiere a productos o servicios de identificación electrónica y de confianza que cumplen con los altos estándares de seguridad definidos por Common Criteria y que también cumplen con los requisitos del reglamento eIDAS.	Página 104 - Sección MÓDULO DE SEGURIDAD POR HARDWARE (HSM) Página 811 - 816: Certificado Common Criteria EAL4+ con su traducción	Los siguientes enlaces disponibles publicamente proveen el reporte detallado completo de como el fabricante logra ela certirficacion EAL 4+ Tal como se muestra en la página 103 de la oferta del consorcio, el HSM ofertado, Marca Eviden, Referencia Crypt2pay, es: -Certificado en FIPS 140-2 Level 3: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4149 -Cumplimiento de Common Criteria EAL4+ en cumplimiento con CWA 14167-2-PP: https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-CC-2024_32fr.pdf https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-cible-CC-2024_32.pdf -Cumple con eIDAS -Estará instalado en las instalaciones de la JCE, como lo grafica la propuesta de implementación de la página 102.
3.2.11	**Algoritmos criptográficos asimétricos (podrá soportar)**		
3.2.11.1 - 3.2.11.9	[RSA, DSA, ECC, ECDSA, ECDH, Ed25519, ECIES, Brainpool curves (nombrados y definidos por el usuario), Diffie Hellman (DH)]	Página 104 - MÓDULO DE SEGURIDAD POR HARDWARE (HSM)	El HSM Trustway Crypt2pay ofertado (página 104) soporta una amplia gama de algoritmos criptográficos modernos y estandarizados, como RSA (claves de hasta 4096 bits con intercambio de claves DH), Firma 5 & PPS (más rápida y segura que RSASSA), DSA, ECC, ECDSA, ECDH, Ed25519 (EdDSA), ECIES (con la implementación de las primitivas ECDH, AES, HMAC, SHA-2, SHA-3), curvas ANSI y Brainpool. Estos algoritmos están diseñados para cumplir con los más altos niveles de garantía criptográfica. Al basarse en esta sólida base criptográfica moderna, Crypt2pay garantiza un rendimiento superior, una mayor protección de datos y la alineación con las mejores prácticas regulatorias y de la industria actuales Nuestra oferta está basada en la aclaración entrega por la JCE, en el documento RESPUESTAS TÉCNICAS A OFERENTES de Agosto – Grupo 4 – Pregunta 215 – Página 67, donde se indica que se deben seleccionar algoritmos que sean seguros, compatibles y eficientes para garantizar la robustez de las operaciones criptográficas realizadas por los HSMs.
3.2.12	**Algoritmos criptográficos simétricos (podrá soportar)**		
3.2.12.1 - 3.2.12.10	[AES, AES-GCM, DES, 3DES, ARIA, SEED, RC2, RC4, RC5, CAST]	Página 104 - MÓDULO DE SEGURIDAD POR HARDWARE (HSM) Página 50 - Sección TARJETA CON CHIP SIN CONTACTO	El HSM Trustway Crypt2pay es compatible con un conjunto completo de algoritmos criptográficos modernos y estandarizados, como AES (con modos como GCM y más rápidos y seguros que CAST), CHACHA y Poly1305 (más rápidos que AES-GCM), DES, 3DES, funciones hash SHA-1, SHA-2 y SHA-3; ampliamente reconocidos por su robustez y cumplimiento de los estándares internacionales de seguridad. Estos algoritmos están diseñados para cumplir con los más altos niveles de seguridad criptográfica y reemplazar eficazmente algoritmos antiguos tales como RC2, RC4, RC5, CAST, ARIA, o específicos de la región, como SEED. Al basarse en esta moderna base criptográfica, Crypt2pay garantiza un rendimiento superior, una mayor protección de datos y la conformidad con las mejores prácticas regulatorias y del sector. Nuestra oferta está basada en la aclaración entregada por la JCE, en el documento RESPUESTAS TÉCNICAS A OFERENTES de Agosto – Grupo 4 – Pregunta 215 – Página 67, donde se indica que se deben seleccionar algoritmos que sean seguros, compatibles y eficientes para garantizar la robustez de las operaciones criptográficas realizadas por los HSMs.
3.2.13	**Condiciones de operación**		
3.2.13.3	Humedad relativa no condensada: 20% a 90%	Página 104 - Sección MÓDULO DE SEGURIDAD POR HARDWARE (HSM)	Se adjunta la carta del fabricante del HSM que confirma esta especificación. Cualquier producto fabricado en la UE debe contar con las certificaciones CE y PCI. Ambas certificaciones exigen el rango de humedad especificado. Tenga en cuenta que el rango de temperatura original son las condiciones ideales para un rendimiento óptimo y duradero del HSM. Como se indica en la carta: el HSM Crypt2pay está diseñado con una tolerancia para desviaciones, permitiendo su funcionamiento a niveles de humedad relativa de hasta el 90 %, siempre que el ambiente interno permanezca sin condensación. Esta resiliencia en el diseño asegura un funcionamiento confiable incluso en condiciones variables, reduciendo el riesgo de degradación relacionada con la humedad.
3.2.13.4	MTBF mínimo 150,000 horas a 25°C /77°F	Página 103 - 104 - Sección MÓDULO DE SEGURIDAD POR HARDWARE (HSM)	Se adjunta carta del Fabricante confirmando el cumplimiento de este requisito. Ver Anexo B.
3.2.14	**Certificaciones de seguridad**		
3.2.14.2	eIDAS CC EAL4+	Página 103 - 104 - Sección MÓDULO DE SEGURIDAD POR HARDWARE (HSM)	Tal como se muestra en la página 103 de la oferta del consorcio, el HSM ofertado, Marca Eviden, Referencia Crypt2pay, es: -Certificado en FIPS 140-2 Level 3: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4149 -Cumplimiento de Common Criteria EAL4+ en cumplimiento con CWA 14167-2-PP. https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-CC-2024_32fr.pdf https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/ANSSI-cible-CC-2024_32.pdf -Cumple con eIDAS

4	**Especificaciones de la tarjeta de identidad digital**		
4.2	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"	Página 748 - Sección ISO 18013 IOS Página 768 - Sección ISO 18013 Android Página 788 - Sección UL Verification Services Inc. 18013 Parte 5	Los DTC son credenciales de viaje digitales que cumplen con las especificaciones de ICAO (publicadas en los Reportes Técnicos de DTC y eventualmente incorporadas en Doc 9303). Un DTC es una representación digital de la identidad del viajero, diseñada para complementar o sustituir temporalmente un pasaporte físico. Los DTC están vinculados a una infraestructura de clave pública (PKI) gestionada por la autoridad emisora de documentos de viaje, garantizando seguridad y verificación offline. Existen tres formatos de DTC: eMRTD-bound (vinculado a un ePassport), smart-device-bound (vinculado a un dispositivo móvil) y temporary (emitido para un solo uso) El ISO/IEC 18013-5 se diseñó originalmente para licencias de conducir móviles, su marco técnico (mdoc) es lo suficientemente flexible para aplicarse a otros tipos de documentos de identidad digitales, incluidos los DTC. Los DTC pueden adoptar tecnologías y protocolos de ISO 18013-5, como el almacenamiento en dispositivos móviles y la verificación segura mediante criptografía, para garantizar que sean interoperables con sistemas de viaje internacionales. Por ejemplo, un DTC puede usar el formato mdoc para representar datos de identidad de manera segura en un dispositivo móvil, alineándose con los requisitos de ICAO para interoperabilidad y seguridad. Uso de PKI: Tanto ICAO 9303 como ISO 18013-5 emplean infraestructuras de clave pública para garantizar la autenticidad e integridad de los datos. En ICAO 9303, los DTC usan la PKI de la autoridad emisora para validar la identidad del titular, mientras que en ISO 18013-5, el modelo VICAL (Verified Issuer Certificate Authority List) asegura la confianza en las credenciales móviles. Aunque el VICAL es opcional en ISO 18013-5, su función es análoga al sistema de certificados de ICAO. Este DTC, emitido por una autoridad de pasaportes, cumple con ICAO 9303 para garantizar que sea aceptado en fronteras internacionales. El formato de datos y la seguridad (como el uso de un chip virtual o una billetera digital) pueden basarse en ISO 18013-5, permitiendo que el DTC sea presentado y verificado de manera segura desde un dispositivo móvil, similar a una licencia de conducir móvil. La autoridad de frontera puede verificar el DTC utilizando la PKI de ICAO, mientras que el formato mdoc de ISO 18013-5 asegura que los datos sean legibles y seguros en el dispositivo. La certificación en ISO/IEC 18013-5 proporciona una base sólida para implementar DTC, ya que cubre aspectos clave como el formato mdoc, la criptografía y la interoperabilidad en dispositivos móviles. Así mismo, teniendo en cuenta que la oferta del consorcio C4RD incluye la implementación de una solución de PKI en cumplimiento al estándar ICAO 9303, demuestra una preparación idónea para la implementación de los DTC.
4.5	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.	Página 99 - Sección FIRMADO DE DOCUMENTOS GET TRUST (DOCUMENT SIGNER) Página 748 – Certificación ISO 18013-5 para iOS. Página 768 – Certificación ISO 18013-5 para Android.	Como se menciona en la pagina 111 de la oferta del Consorcio C4RD, la solución de GET Mobile ID puede ser integrada con una solución de PKI. Sumado a lo anterior, y teniendo en cuenta que la oferta del consorcio incluye una solución de PKI robusta, y a raíz de esta integración propuesta, la Tarjeta digital podrá ser verificada por terceros para validar la integridad y procedencia original de los datos del ciudadano. Esto hace referencia al cumplimiento del estándar ISO 18013-5, específicamente al dar cumplimiento a la autenticación ECDSA/EdDSA que mencionan los certificados presentados. El hecho de obtener la certificación ISO 18013-5 significa que todos los datos entregados son firmados electrónicamente, como requisito primordial para obtener la certificación.
4.7	**Aspectos generales de la tarjeta digital**		
4.7.38	Análisis de Interfaces: Se deberá presentar un plan de análisis y pruebas para el ajuste de interfaces de comunicación propuestas por el JCE. Se deben incluir igualmente a definición de escenarios de prueba.	Página 108 - 109 - Sección GET MOBILE ADMINISTRATOR Página 160 – Sección Plan de Capacitación para Tarjeta Digital Página 168 – Cronograma de implementación.	Tal como se muestra en las páginas 108, GET Mobile Administrator, y el párrafo mencionado "Servicios prestador por GET Mobile Administrator", se menciona la fácil integración con los sistemas de registro, que este caso será el sistema de JCE. También, desde la pagina 109 a la 111, se hace la explicación de los diferentes modelos de integraciones disponibles en el GET Mobile Administrator, los cuales la JCE podrá decidir utilizar de acuerdo con la mejor decisión técnica que tome durante el proceso de implementación. Y como esta mencionado, en la página 168, donde se detalla todo el plan de implementación del modulo GET Mobile ID, tareas desde la 36 a las 61, se encuentran planificadas tareas relacionadas a este requerimiento, como lo son Revisión del plan de implementación, Definición de diccionario de datos, Guía de interacciones / integraciones y Requerimientos de seguridad, UAT – GET Mobile Administrator UAT, son tareas planificadas por el CONSORCIO para agotar el requerimiento solicitado. De igual forma, en la pagina 160 se encuentra el plan de capacitación para la implementación de la tarjeta digital, donde uno de los cursos a realizar por parte del consorcio hace relación a la forma de realizar el flujo de emisiones, componentes e integraciones, con las interacciones y pruebas necesarias para una implementación exitosa.

Anexo A

FORMULARIO DE ENTREGA DE MUESTRAS

CONSORCIO CÉDULA 4.0 RD

SNCC.F.056

Junta Central Electoral

JUNTA CENTRAL ELECTORAL
COMPRAS Y CONTRATACIONES

No. EXPEDIENTE
JCE-CCC-LPI-2024-0001

25 de febrero de 2025

Página 1 de 1

FORMULARIO DE ENTREGA DE MUESTRAS

Nombre del Oferente : COPY SOLUTIONS INTERNATIONAL, S.A

Renglón No.	Código	Descripción	Unidad de medida	Muestra Entregada[1]	Observaciones[2]
N/A	9704B007AB	Scanner Canon P208	Und	x	
N/A	2727C002CERT7	Cámara Canon T7	Und	x	
N/A	STU-540	Lector de Firma Wacom STU540	Und	x	
N/A	LIVETOUCH	Scanner Biométrico de Huellas Dermalog Live Touch Quattro	Und	x	
N/A	50013-001-104	Lector de Huellas Dactilares HID 4500	Und	x	
N/A	COMP000628	Impresora Punto de Venta	Und	x	
N/A	ACR1252U-M1	Lector de Tarjetas Inteligentes NFC	Und	x	

Firma _____

Sello

RNC 101898852

Recibido 25/2/2025

JUNTA CENTRAL ELECTORAL · Comité de Compras y Contrataciones ·

[1]Marcar con una x.
[2]Uso exclusivo de la Entidad Contratante.

/UR.03.2012

DISTRIBUCIÓN Y COPIAS
Original 1 – Expediente de Compras
Copia 1 – Agregar Destino

LECTOR NFC ACS – ARC1252U Reader III	REFERENCIA - S/N
	

ANEXO B

EVIDEN
an atos business

Environmental Compliance and Reliability of the Trustway Crypt2pay HSM

The Trustway Crypt2pay Hardware Security Module (HSM) complies with the CE (Conformité Européenne) marking requirements, including those related to environmental conditions. As stated in the official technical documentation and compliance reports, the product has been validated to operate within a relative humidity range of 30% to 70%, which is aligned with CE environmental standards for electronic equipment.

This humidity range ensures **optimal performance and long-term reliability**. However, the **Crypt2pay HSM is engineered with a tolerance** for deviations, **allowing operation at relative humidity levels up to 90%**, provided that the internal environment remains non-condensing. This design resilience ensures dependable functioning even in variable conditions, reducing the risk of moisture-related degradation.

At the lower end of the spectrum, the device can safely function at relative humidity levels as low as 20%, assuming moderate temperature fluctuations. This helps avoid issues such as thermal shock or electrostatic discharge (ESD), both of which are mitigated by the device's robust electronic design.

Reliability and MTBF Considerations

The **Trustway Crypt2pay HSM** is designed with long-term operational reliability in mind. The product achieves a **minimum Mean Time Between Failures (MTBF) of 150,000 hours at 25°C (77°F)**, demonstrating its robustness in continuous use under standard conditions.

This high MTBF value is a result of careful component selection and architectural design. The Crypt2pay HSM integrates **low-power, solid-state components**, which significantly reduce thermal stress and energy consumption. Additionally, the device features a **fanless design**, eliminating the need for mechanical cooling systems and thus avoiding common failure points associated with moving parts.

By removing these mechanical elements, the Crypt2pay HSM enhances both **longevity and reliability**, ensuring stable operation in critical infrastructure environments. Its **passive cooling and low power profile** also contribute to silent performance and energy efficiency, making it suitable for deployment in secure, high-availability installations.

Security Assurance through Trustway IP Protect Platform – Common Criteria EAL4+

The **Trustway Crypt2pay HSM** is built upon the **Trustway IP Protect platform**, a security architecture developed and certified by Eviden (an Atos Group company) to meet rigorous international standards. This underlying platform has been independently evaluated and certified under the **Common Criteria (CC) at Evaluation Assurance Level 4 augmented (EAL4+)**, which is recognized globally for its high level of assurance in the design, development, and testing of IT security products.

By leveraging the **Trustway IP Protect platform**, the Crypt2pay benefits from a **proven and certified security foundation**. This ensures that the cryptographic operations, key management, and secure processing environments adhere to internationally recognized security best practices, providing confidence in the **robustness, integrity, and reliability** of the system.

The use of a **CC EAL4+ certified platform** enables Trustway Crypt2pay to support secure implementations in **regulated industries such as finance, government, and critical infrastructure**, where compliance with strict security standards is mandatory.

Fermín Vázquez
Solution Manager – E BDS AME Specialized Sales
T: +49 (0) 2 09 1 67 24 50
M: +52 (81) 11 22 02 49
F: +49 (0) 2 09 1 67 24 61
Munscheidstr. 14 – 45886 Gelsenkirchen – Germany
eviden.com

EVIDEN
an atos business

Digitally signed by Fermín Vázquez
DN: 2.5.4.97=NTRFR-323623603, o=Eviden, sn=Vázquez, givenName=Fermín, cn=Fermín Vázquez, email=fermin-teuctzintli.vazquez@eviden.com
Date: 2025.05.20 14:56:21 -05'00'

EVIDEN
an atos business

Cumplimiento medioambiental y fiabilidad del HSM Trustway Crypt2pay

El Hardware Security Module (HSM) Trustway Crypt2pay cumple los requisitos de marcado CE (Conformité Européenne), incluidos los relativos a las condiciones medioambientales. Como se indica en la documentación técnica oficial y en los informes de conformidad, el producto ha sido validado para funcionar dentro de un rango de humedad relativa del 30% al 70%, que se ajusta a las normas medioambientales de la CE para equipos electrónicos.

Este rango de humedad garantiza un **rendimiento óptimo y fiabilidad a largo plazo**. Sin embargo, el HSM **Crypt2pay se ha diseñado con desviaciones de tolerancia**, lo que permite su **funcionamiento con niveles de humedad relativa de hasta el 90%**, siempre que el entorno interno se mantenga sin condensación. Esta resistencia de diseño garantiza un funcionamiento fiable incluso en condiciones variables, reduciendo el riesgo de degradación relacionada con la humedad.

En el extremo inferior del espectro, el dispositivo puede funcionar con seguridad a niveles de humedad relativa tan bajos como el 20%, suponiendo fluctuaciones moderadas de temperatura. Esto ayuda a evitar problemas como los choques térmicos o las descargas electrostáticas (ESD), ambos mitigados por el robusto diseño electrónico del dispositivo.

Consideraciones sobre fiabilidad y MTBF

El HSM Trustway Crypt2pay se ha diseñado pensando en la fiabilidad operativa a largo plazo. El producto alcanza un **tiempo medio entre fallos (MTBF) mínimo de 150.000 horas a 25 °C (77 °F)**, lo que demuestra su robustez en uso continuo en condiciones estándar.

Este alto valor de MTBF es el resultado de una cuidadosa selección de componentes y diseño arquitectónico. El HSM Crypt2pay **integra componentes de estado sólido de bajo consumo**, que reducen significativamente el estrés térmico y el consumo de energía. Además, **el dispositivo presenta un diseño sin ventilador**, lo que elimina la necesidad de sistemas de refrigeración mecánicos y, por tanto, evita los puntos de fallo habituales asociados a las piezas móviles.

Al eliminar estos elementos mecánicos, el HSM Crypt2pay mejora tanto la **longevidad como la fiabilidad**, garantizando un funcionamiento estable en entornos de infraestructuras críticas. Su **refrigeración pasiva y su perfil de baja potencia** también contribuyen a un rendimiento silencioso y a la eficiencia energética, lo que lo hace adecuado para su despliegue en instalaciones seguras y de alta disponibilidad.

Garantía de seguridad a través de la plataforma Trustway IP Protect - Common Criteria EAL4+

El HSM **Trustway Crypt2pay** se basa en la plataforma **Trustway IP Protect**, una arquitectura de seguridad desarrollada y certificada por Eviden (empresa del Grupo Atos) para cumplir rigurosos estándares internacionales. Esta plataforma subyacente ha sido evaluada de forma independiente y certificada bajo **Common Criteria (CC) at Evaluation Assurance Level 4 augmented (EAL4+)**, que es reconocido mundialmente por su alto nivel de garantía en el diseño, desarrollo y pruebas de productos de seguridad de TI.

Al aprovechar **la plataforma Trustway IP Protect**, Crypt2pay se beneficia de una **base de seguridad probada y certificada**. Esto garantiza que las operaciones criptográficas, la gestión de claves y los entornos de procesamiento seguro se adhieren a las mejores prácticas de seguridad reconocidas internacionalmente, proporcionando **confianza en la solidez, integridad y fiabilidad** del sistema.

El uso de una plataforma certificada **CC EAL4+** permite a Trustway Crypt2pay soportar implementaciones **seguras en sectores regulados como el financiero, el gubernamental y el de infraestructuras críticas,** donde el cumplimiento de estrictas normas de seguridad es obligatorio.

EVIDEN
an atos business

Digitally signed by Fermín Vázquez
DN: 2.5.4.97=NTRFR-323623603, o=Eviden, sn=Vázquez, givenName=Fermín, cn=Fermín Vázquez, email=fermin-teuctzintli.vazquez@eviden.com
Date: 2025.05.20 14:57:03 -05'00'