**LISTA DE REQUISITOS A CONSULTAR POR CONSORCIO**

En el marco del proceso de evaluación técnica y como parte de la verificación de las propuestas recibidas, a continuación, se presenta el listado de requisitos para los cuales **se requiere que los oferentes proporcionen las aclaraciones y/o explicaciones técnicas que, para cada requisito, permitan verificar, validar y comprender que se satisfacen de conformidad con lo ofertado.**

|  |  |
| --- | --- |
| **CONSORCIO CEDULA 4.0** | |
| **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. |
| 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 deberá́ prever la administración de todo el ciclo de vida de los mismos (generación, actualización y revocación) en la electrónica de los documentos |
| **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 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. |
| **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. |
| 2.1.14 | El sistema operativo de la PC debe ser WINDOWS. Las impresoras pueden ser WINDOWS o LINUX. |
| 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. |
| 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. |
| 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 caracteristicas 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. |
| 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. |
| **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. |
| **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. |
| 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). |
| 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 |
| 3.1.13 | Tanto la PKI de firma de documentos como la PKI de Firma Digital deben cumplir CC EAL 4+ |
| 3.1.22 | El CSCA debería ser capaz de emitir certificados de firmante de lista maestra. |
| 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. |
| **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. |
| 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. |
| 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. |
| 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. |
| 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. |
| **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) ] |
| **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 ] |
| **3.2.13** | **Condiciones de operación** |
| 3.2.13.3 | Humedad relativa no condensada: 20% a 90% |
| 3.2.13.4 | MTBF mínimo 150,000 horas a 25°C /77°F |
| **3.2.14** | **Certificaciones de seguridad** |
| 3.2.14.2 | eIDAS CC EAL4+ |
| **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” |
| 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. |
| **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. |