**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 ID SECURE IDS** | |
| **1.7.6** | **Funcionalidad de la 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 estar 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. |
| 1.7.6.10 | Condiciones de acceso independientes para cada clave/elemento. |
| **2.1** | **Especificaciones de máquinas 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. |
| 2.1.22 | 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 mantendrá́ 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. |
| 2.1.23 | Los equipos deberán disponer de un control de calidad y registrar los eventos identificados, garantizando: - Evaluación de funcionamiento del chip antes de su personalización. - Correcto grabado del chip después de su personalización. - Control de información grabada durante la personalización de la tarjeta de policarbonato. - Control de espesor, orientación de la tarjeta y referencia. - Control de MRZ (ZLM). - Control de texto. - Control de los datos del chip. - Control de los datos gráficos. |
| 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. |
| **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** |
| 3.1.10 | 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 Certificado en 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. |
| 3.1.26 | El DS que deberá utilizar una autenticación multifactorial para el inicio de sesión en la interfaz de administración debería avisar claramente antes de que finalice el tiempo de uso de la clave del certificado actualmente utilizado. |
| 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:  - Autenticación 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 comunicaciones - 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. |
| 3.2.5 | 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. |
| **3.2.11** | **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 ] |
| **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** |
| 4.7.2 | El ciudadano debe tener acceso a un portal donde pueda actualizar sus credenciales, cancelarlas, inspeccionar los accesos a su identidad. La solución debe permitir al ciudadano el acceso a un portal donde pueda actualizar sus credenciales, cancelar su aplicación, inspeccionar los accesos a su identidad y en general observar todas las transacciones que ha realizado con la misma. Se deben poder validar todas las operaciones realizadas con su identidad incluyendo la fecha y hora de las mismas. Debe tener la capacidad de mostrar el tipo de acceso aun si es hecho desde aplicaciones de terceros. Deben gestionarse todos los eventos del ciclo de vida y consultas. |