4. INFRAESTRUCTURA PKI Y SEGURIDAD

La Junta Central Electoral (JCE) ha establecido la necesidad de contar con **dos infraestructuras de clave pública (PKI) separadas** para garantizar la autenticidad, integridad y seguridad de los documentos electrónicos y las firmas digitales en el nuevo sistema de cedulación. Estas **infraestructuras** permitirán una **gestión diferenciada** de los certificados utilizados por los ciudadanos y los documentos emitidos por la JCE, asegurando así una separación clara de responsabilidades y funciones dentro del ecosistema digital de identidad.

Las tres infraestructuras son las siguientes:

1. **PKI de FIRMA DE DOCUMENTOS:** Infraestructura dedicada a la autenticación y verificación de documentos oficiales emitidos por la JCE, asegurando que cualquier documento generado por la institución sea inalterable, verificable y confiable.
2. **PKI de FIRMA DIGITAL:** Diseñada para emitir y gestionar certificados digitales destinados a los ciudadanos, permitiéndoles firmar documentos electrónicamente con plena validez legal.
3. **PKI para DOCUMENTOS DIGITALES (IACA):** Infraestructura que actuará como la Autoridad Certificadora de la Autoridad de Emisión ISO 18013-5 (IACA) y será la CA raíz fuera de línea para la PKI utilizada en la emisión de los Documentos de Identidad Digital, **incluida en el CAPITULO DE IDENTIDAD DIGITAL.**

Cada una de estas infraestructuras opera bajo **normativas internacionales de seguridad**, como **X.509v3, RFC 5280, Common Criteria EAL4+ y FIPS 140-2 Nivel 3**, garantizando una gestión segura de claves criptográficas y certificaciones digitales.

4.1 PKI DE FIRMA DE DOCUMENTOS

Para garantizar la autenticidad, integridad y seguridad de los documentos electrónicos dentro del nuevo sistema de cédulas de identidad, el **Consorcio IDSecure IDS** ha seleccionado a **TOPPAN SECURITY SAS (antiguo HID Global)** como proveedor de la Infraestructura de Clave Pública (PKI). TOPPAN SECURITY SAS es una empresa líder en soluciones de seguridad digital y firma electrónica, con una sólida trayectoria en la implementación de PKI para gobiernos e instituciones públicas a nivel global. Su tecnología cumple con los estándares internacionales establecidos por la OACI (Doc 9303), ISO 15408 y eIDAS, asegurando la interoperabilidad, seguridad y confiabilidad del sistema. La solución PKI propuesta garantizará la emisión segura de certificados digitales, la gestión de claves criptográficas y la validación de identidad digital de los ciudadanos.

TOPPAN
TOPPAN Security

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

4.1.1 Características de la PKI

En esencia, la PKI utiliza la criptografía asimétrica, un concepto fundamental en la seguridad de la información moderna basado en un par de claves relacionadas matemáticamente: una clave pública y una clave privada. La clave pública se distribuye libremente y puede ser conocida por cualquier persona, mientras que la clave privada es mantenida de forma segura por el propietario de la clave.

Las soluciones PKI se basan en varios elementos que trabajan en conjunto, por ejemplo, la autoridad de registro, la emisión de certificados, la creación de firmas, la validación de estado y los servicios de revocación. Dado que todos estos servicios se respaldan mutuamente, la seguridad de cada uno es esencial, como los eslabones de una cadena.

La implementación debe diseñarse cuidadosamente, teniendo en cuenta las inevitables amenazas de seguridad. Cada tipo de amenaza debe ser listado y evaluado utilizando una técnica de evaluación de riesgos, donde los riesgos se miden en términos de la probabilidad de ocurrencia y el impacto que podrían causar. Posteriormente, se pueden seleccionar contramedidas para reducir el nivel general de riesgo a un grado aceptable; cabe señalar que es poco probable lograr una seguridad perfecta y siempre se deben tomar decisiones de costo-beneficio al asignar el presupuesto de seguridad.

TOPPAN SECURITY recomienda utilizar una metodología formal, como la ISO 2700x, al diseñar y operar infraestructuras de TI relacionadas con la identidad.

Las mejores prácticas incorporarán:

- **Zonas de seguridad** física concéntricas para proteger activos como servidores, redes y estaciones de trabajo.
- **Módulos de seguridad** de hardware (HSM) para proteger la integridad de las claves secretas y privadas.
- **Técnicas de protección** en internet para sitios web y servicios web.
- **Seguridad procedimental** para proteger al personal administrativo de compromisos.
- **Monitoreo continuo** y revisión de las medidas de seguridad.
- **Actualizaciones regulares** de seguridad del software.
- **Planificación de recuperación** ante desastres y continuidad del negocio.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

De acuerdo con el Pliego de Especificaciones, ITEM III - ESPECIFICACIONES TÉCNICAS DE LAS PKI – CA. Nuestra solución es diseñada para cumplir con los requisitos y criterios técnicos, asegurando cumplimiento con el Doc. 9303 de la OACI.

En esta sección, proponemos implementar la infraestructura de criptografía basada en claves públicas (PKI), para emitir y revocar certificados digitales que se utilizarán para firmar electrónicamente las tarjetas electrónicas y para verificar tarjetas electrónicas.
Nuestra propuesta incluye los elementos necesarios la provisión, configuración, integración y puesta en marcha de una Infraestructura de Clave Pública, con finalidad de autenticar la tarjeta electrónica que ofrece acceso de sólo lectura de Chip de Circuito Integrado (IC), que, por su vez, cumple con la norma ISO 15408, y posee certificación CC EAL 4+ en el sistema operativo provisto.
En resumen, proporcionamos componentes y servicios destinados a la emisión segura y eficiente de las tarjetas CI y CIE de próxima generación de República Dominicana.

4.1.2 Componentes de la PKI:

En el caso de ser adjudicados, estaremos coordinando y apoyando 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.

4.1.2.1 Infraestructura PKI - Integrale™ KMS

Integrale™ KMS está diseñado para gestión de las claves para documentos electrónicos seguros y en conformidad con ICAO Documento 9303. Integrale™ KMS proporciona una interfaz gráfica de usuario amigable para la instalación de las CA de ICAO (CSCA y CVCA) o las CA de los documentos digitales (IACA) con la generación y el mantenimiento de claves privadas y el certificado X.509 para la firma y autenticación de documentos.

Garantizando el cumplimiento con las especificaciones:

- El CSCA utiliza algoritmos criptográficos actuales y almacena las claves privadas en un HSM.
- El CSCA trabaja en un entorno sin conexión y será la autoridad encargada de firmar certificados para entidades gubernamentales o documentos de importancia nacional.
- El CSCA generará listas de revocación de certificados (CRL) según ICAO 9303.
- El acceso se da a través de una autenticación multifactorial para el inicio de sesión en la interfaz de administración.
- El CSCA es capaz de emitir los certificados VDS Signer, siendo también responsable de mantener la infraestructura de claves públicas y de gestionar la emisión y revocación de estos certificados

CONSORCIO IDSECURE IDS Santo Domingo, D.N.

- El CSCA es capaz de emitir certificados de firmante de lista maestra, así asegurando la confianza de todas las entidades.

Infraestructura de Clave Pública (PKI) y Certificación de Seguridad

Nuestra propuesta cumple con los requisitos establecidos en el Pliego de Condiciones, incluyendo la implementación de una **PKI con CA Raíz y CA Subordinada** dentro de las instalaciones de la JCE, asegurando una infraestructura segura y confiable.

1.1 Seguridad y Redundancia

- La infraestructura estará protegida mediante **firewalls avanzados, segmentación de redes y autenticación multifactorial (MFA)**.
- **Redundancia y Alta Disponibilidad (Cluster):** Se implementará un sistema de **respaldo activo en premisas**, garantizando continuidad operativa, según normas internacionales como la ISO/IEC 270031 o la ISO 22301.
- **HSM Certificado**: Se integrará un **HSM FIPS 140-2 Nivel 3 o superior**, cumpliendo con los estándares internacionales de seguridad.
- **Certificación Common Criteria EAL4+**: Garantizando una evaluación de seguridad robusta.

1.2 Administración del Ciclo de Vida de Certificados

- **Portal Web para la Gestión de Certificados:** Se implementará un sistema que permitirá la emisión, renovación, revocación y auditoría de certificados digitales.
- **Sellos de Tiempo (TSA)**: Integración de una Autoridad de Sellos de Tiempo (Time Stamping Authority) sincronizada con la fuente oficial de la República Dominicana.
- **Cumplimiento Normativo**: Se garantizará la compatibilidad con **X.509, eIDAS CC EAL4+ e ISO 15408**.

1.3 Integración y Compatibilidad

- **Interoperabilidad con sistemas gubernamentales**: Se desarrollarán APIs REST para asegurar la integración con aplicaciones del gobierno y terceros.
- **Soporte para Infraestructura de Clave Pública (PKI)**: Implementación de soluciones criptográficas modernas, incluyendo **RSA 4096, ECDSA y AES-256**.
- **Mecanismos de Autenticación y Control de Acceso**: Se garantizará un modelo de autenticación basado en credenciales digitales con validaciones criptográficas.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Infraestructura PKI: Cumplimiento y Recomendaciones

Nuestra solución de PKI está diseñada para alinearse completamente con los requisitos de la JCE, proporcionando un ecosistema seguro y altamente disponible para la emisión de certificados digitales.

2.1 Refuerzo de Seguridad en la Infraestructura PKI

- **Asegurar la redundancia en la infraestructura de PKI**, especificando claramente la configuración en cluster.
- **Incluir una matriz de cumplimiento**, comparando los requisitos del pliego con las especificaciones de la propuesta.
- **Especificar claramente las certificaciones del HSM**, asegurando que cumple con **FIPS 140-2 Nivel 3 y Common Criteria EAL4+**.
- **Detallar la interoperabilidad de la solución**, asegurando que la PKI puede integrarse con otros sistemas gubernamentales a través de APIs.
- **Ampliar la sección de administración del ciclo de vida de certificados**, incluyendo detalles sobre la capacidad de emisión, revocación y auditoría en el portal web.

4.1.2.2 Firmante de Documentos - Integrale DPS

Integrale™ DPS se propone como el sistema de preparación de datos y firma para documentos electrónicos. Es el módulo específico para la firma de documentos digitales, garantizando su autenticidad e integridad. Integrale ™ DPS se ejecuta en un dispositivo de hardware especializado (HSM). Acepta solicitudes de preparación de datos entrantes de fuentes confiables a través de servicios web de una manera segura y prepara datos con el procesamiento de seguridad.

Para documentos conformes con la ICAO, el DPS ofrece la preparación del formato de Grupos de Datos de la ICAO, así como la ejecución de la operación de firma de documentos con la clave secreta del Firmante de Documentos.

- **Generación del Par de Claves DS**: Los pares de claves DS serán generados por Integrale DPS para la firma de documentos. Una vez generado, el par de claves DS se almacenará de forma segura dentro del HSM y no podrá exportarse. La solicitud de certificado del nuevo par de claves DS se enviará a la CSCA (es decir, KMS) para la emisión del certificado DS.
- **Preparación de Datos ICAO**: Al recuperar la información, el motor integrado agrupará los datos personales de acuerdo con la estructura especificada por los Grupos de

CONSORCIO IDSECURE IDS · Santo Domingo, D.N. ·

Datos (DG) de la ICAO. Esto incluye la generación de la firma digital, dentro del HSM, con las claves del Firmante de Documentos sobre los DG ya formateados.

Garantizando el cumplimiento con las especificaciones:

- El DS dispondrá de un servicio web SOAP al que llamar para la generación de SOD y creará un SOD conforme a la OACI 9303.
- El DS utiliza algoritmos criptográficos actuales y almacena las claves privadas en un HSM.
- El acceso se da a través de una autenticación multifactorial para el inicio de sesión en la interfaz de administración.

4.1.2.3 Hardware

El hardware cumple a todos los requerimientos para implementar una infraestructura de criptografía basada en claves públicas (PKI). Está incluido en esta propuesta, la provisión, instalación, configuración y puesta en marcha de los dispositivos HSM, certificados como mínimo FIPS 140-2, así como toda la infraestructura adicional para estos dispositivos (racks, cableado de conectividad local). El HSM de nuestra oferta, ofrece característica similares o superiores a las especificaciones proporcionadas.

Categoría	UTIMACO CryptoServer
APIS criptográficos	PKCS #11 Java, Microsoft CNG (evolución de la antigua CAPI),OpenSSL CXI (Utimaco's comprehensive Cryptographic eXtended services Interface)
Algoritmos criptográficos asimétricos	RSA, DSA, ECDSA (NIST y Brainpool curves), ECDH (NIST y Brainpool curves), Ed25519, ECC, ECIES. Diffie Hellman (DH) y más.
Algoritmos criptográficos simétricos	AES, AES-GCM, DES, 3DES, CMAC, HMAC, y más.
Condiciones de Operación	Voltaje: 100~220V, Temp: +10°C a +40°C, Humedad (No Condensada): 20% a 90%, supera las MTBF: 150,000 horas a 25°C.

Certificaciones de seguridad	FIPS 140-2 Nivel 3, Password and Multi-Factor (PED), eIDAS CC EAL4+, EN 419 221-5, UL, IEC/EN 60950-1, IEC/EN 62368-1, CE, FCC
Generación de números aleatorios reales (TNRG)	Cumple
Copia de seguridad de la tarjeta inteligente del material clave	Cumple
Doble conector de red	Cumple
Administración remota (vía red)	Cumple
Administración local	Cumple
Soportar interface gráfica del HSM	Cumple
Opciones múltiples para autentificación y control de acceso	Cumple
Múltiple integración para aplicaciones de PKI, servicios de encriptación	Cumple
Separación de tareas	Cumple
Sistemas operativos soportados: Windows y Linux	Cumple
Rendimiento nominal mínimo (firmas RSA /segundo, 2048 bit, modo Bulk): 25	Cumple
Habilitado para operación en cluster (alta disponibilidad)	Cumple
Debe permitir la importación / exportación de llaves internas a través de un método seguro, desde y hacia otro HSM	Cumple
El HSM deberá proveer mecanismos de detección de apertura llamados "Tamper Evidence" y ser resistentes al forzado, característica denominada "Intrusion Resistant"	Cumple

De acuerdo con los requisitos y siempre que resulte técnicamente beneficioso para el proyecto, se pueden implementar en el HSM Ultimaco algoritmos simétricos y asimétricos que no estén descritos explícitamente en el manual oficial. Este proceso se basa en la utilización del SDK, que permite la integración de algoritmos propietarios (por ejemplo, ECIES, ARIA, SEED, RC2, RC4, RC5 y CAST) y la personalización de derivaciones de claves, previa presentación de las necesidades específicas del cliente durante la ejecución. En todo momento, se mantendrán los estándares de seguridad y rendimiento que caracterizan el proyecto.

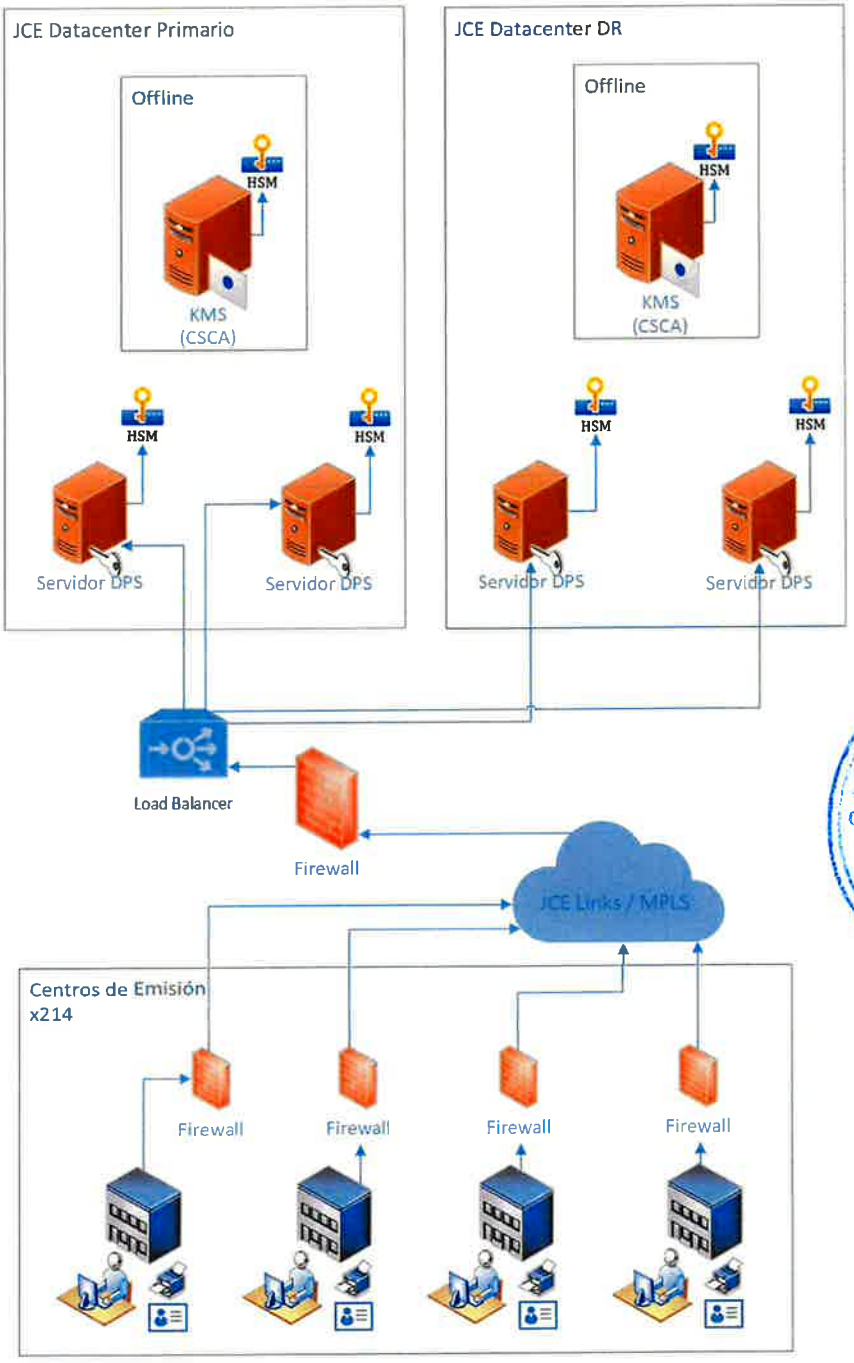
4.1.3 Integración con el sistema documentario del registro nacional

La solución propuesta considera integración de la plataforma de PKI con la solución de personalización con la que cuenta en la actualidad.

4.1.4 Soporte

La solución propuesta considera los niveles de soporte requeridos en el pliego de especificaciones técnicas. Se mantendrá la infraestructura actualizada anualmente y garantizamos su conformidad cuando sea requerida por una puesta al día de las normas y especificaciones contenidas en el Documento 9303, o cuando sea requerido por la JCE.

4.1.5 Arquitectura Propuesta



CM

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

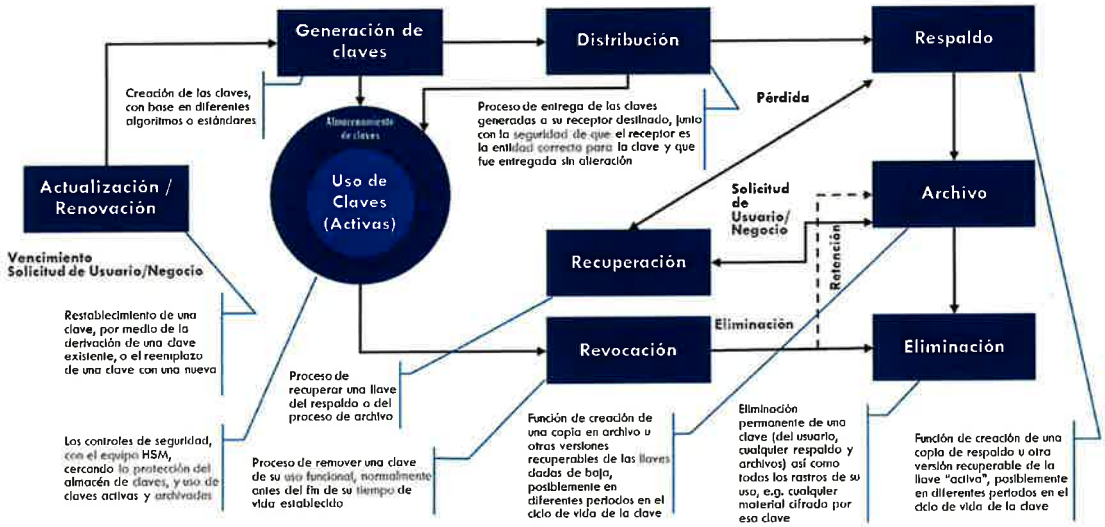
Detalles de los componentes

Gestión de las claves – Integrale™ KMS

Integrale™ KMS está diseñado para la gestión de las claves para documentos electrónicos seguros y en conformidad con ICAO. **Integrale™ KMS** proporciona una interfaz gráfica de usuario amigable para la instalación de la CA, con la generación y el mantenimiento de claves y el certificado X.509 para la firma y autenticación de documentos.

Es muy importante garantizar que el secreto criptográfico para el sistema se genere, almacene y transporte de manera segura. **Integrale™ KMS** se ejecuta en un HSM certificado FIPS-140-2 Nivel 3 (Módulo de seguridad de hardware) para garantizar la calidad de la clave generada, así como el almacenamiento seguro de claves. **Integrale™ KMS**, además, proporciona un mecanismo seguro de transporte de clave, de modo que la clave de autenticación maestra se puede exportar desde **Integrale ™ KMS** de manera segura.

Gestión del ciclo de vida clave en Integrale™ KMS



4.1.6 Operaciones Para Documentos electrónicos

Autoridad de Certificación de Firma de País (CSCA)

Esto incluye la generación de la CSCA, Firmante de Documentos (DS), el par de claves criptográficas y los certificados digitales correspondientes, exportación de los certificados auto-firmados de la CSCA y la generación de la Lista de Revocación de Certificados (CRL).
Autoridad de Certificación de Verificación de País (CVCA)

Esto incluye la generación del par de claves criptográficas Root CVCA y los correspondientes Certificados de Verificación de Tarjetas (CVC). También es compatible con la generación y emisión de certificados para Verificadores de Documentos (DV) y Sistemas de Inspección (IS) nacionales.

Generación y transporte de claves simétricas y asimétricas.

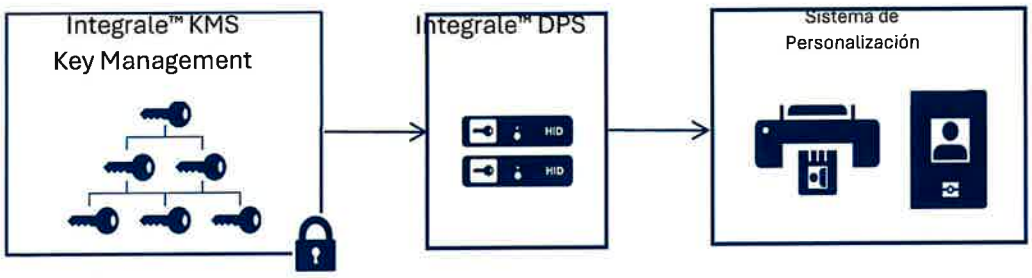
Copia de seguridad y restauración de claves: Se admiten dos modos de copia de seguridad, el formato de 3 componentes y el envoltorio de claves mediante la Clave de Zona Maestra (ZMK).

El formato de 3 componentes consiste en descomponer la llave en 3 piezas separadas para permitir el transporte de la llave en 3 rutas diferentes. La clave original podría reconstruirse solo cuando las 3 piezas se combinen juntas. Este mecanismo proporciona un alto nivel de seguridad y, por lo general, se usará para transportar la Clave de Zona Maestra (ZMK) que se utiliza para transportar otras claves secretas entre los sistemas o el dominio de seguridad. Cuando la ZMK ha sido transportada e importada con éxito, el transporte subsecuente de la llave se puede hacer envolviendo la clave en un formato cifrado por la ZMK.

- **Listado de Claves:** para mostrar todas las claves almacenadas dentro del HSM.
- **Pruebas de Cifrado y Descifrado:** para verificar la integridad de la clave.
- **Auditoría Completa de Rastreo:** en todas las operaciones en **Integrale ™ KMS** para fines de auditoría.

4.1.7 Sistema de Gestión de llaves - Integrale™ KMS

Interacción con la firma de documentos / Sistema de personalización



Integrale™ KMS: Generación de certificado CSCA y Firma de Certificados DS

Integrale™ DPS: Generación de certificados DS, almacenamiento de PMK y certificados DS firmados, preparación y provisión de datos de la aplicación en forma de script de codificación de chip junto con las claves necesarias para el sistema de personalización para la impresión y codificación de las tarjetas.

Sistema de Personalización: actualmente el sistema de personalización de la JCE.

4.1.8 Configuración - Integrale™ KMS

Esta propuesta de configuración de seguridad para el KMS incluye medidas estrictas de control de acceso, operatividad restringida y resiliencia mediante la separación de ubicaciones y administración de claves seguras.

Equipos y Control de Acceso

Infraestructura:

- 2 equipos KMS mantenidos en una habitación segura:
  - 1 x Principal
  - 1 x Respaldo
- 1 equipo KMS adicional para pruebas / desarrollo / capacitación.

Control de Acceso Físico:

- Acceso restringido a personal autorizado.

Operación y Conectividad

Operatividad:

- Operativos únicamente durante la generación y renovación de claves.
- Seguridad adicional: CSCA sin conexión a la red.

Ubicación y Resiliencia

Ubicaciones Separadas:

- Los dos equipos KMS (principal y respaldo) deben mantenerse en ubicaciones separadas para asegurar la resiliencia en caso de incidentes.
- Se instalará en las instalaciones de la JCE, los sistemas y equipos necesarios para generar conjuntos de claves para diferentes períodos de tiempo que se utilizarán para computar las Firmas Digitales que se aplicarán para la firma de los Certificados.

Administración y Control

Tarjetas de Administración:

- Operaciones administradas por tarjetas seguras:
  - Tarjetas de Administrador (Admin)
  - Tarjetas de Operador (Op)
- Cada tarjeta viene con sus propias claves / contraseñas.

CH

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Asignación de Titulares de Llave

Designación de Altos Directivos:

- Asignación de 5 altos directivos como titulares de la llave/tarjeta.

Requerimientos para Generación de Certificados

Generación Inicial:

- 5 poseedores de claves necesarios para la primera generación de certificados.

Generaciones Posteriores:

- Se requieren al menos 3 titulares de tarjeta / clave Admin / Op para cada ceremonia de generación de clave posterior.

Recuperación en Caso de Falla

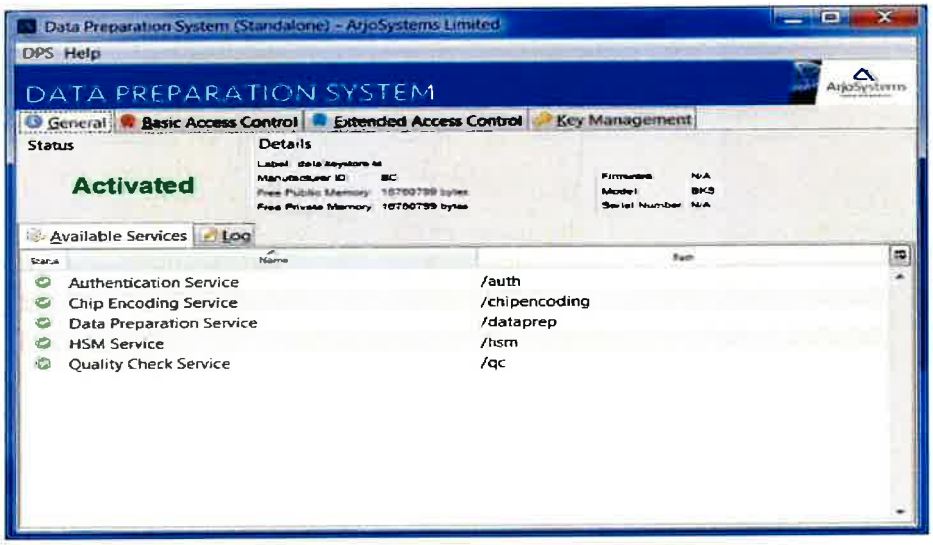
Procedimientos de Recuperación:

- El KMS será recuperable solo con las tarjetas de administración en caso de falla del sistema.

4.1.9 Preparación y Firmante de documentos (DS) – intégrale™ DPS

Integrale ™ DPS se propone como el sistema de preparación de datos para documentos electrónicos.

Integrale ™ DPS se ejecuta en un dispositivo de hardware. Acepta solicitudes de preparación de datos entrantes de fuentes confiables a través de servicios web de una manera segura y prepara datos con el procesamiento de seguridad. Para garantizar la seguridad de datos y los requisitos de privacidad durante la preparación de datos, todos los pasos de procesamiento criptográfico (p. Ej. Generación de **LDS de la OACI**, **firma de documentos** y scripts de codificación) se realizarán en un entorno de hardware seguro **Integrale ™** con un módulo de seguridad de hardware integrado (**HSM**).



A continuación, se muestran las operaciones admitidas por Integrale™ DPS en detalle.

4.1.10 Operaciones relacionadas con la OACI

Para los documentos compatibles con la OACI, Integrale™ DPS realiza la preparación del formato del grupo de datos de la OACI, así como para realizar la operación de firma de documentos con la clave secreta del firmante de documentos.

- **Generación de pares de claves DS**: El **DPS de Integrale™** generará pares de claves DS para habilitar la firma de documentos. El par de claves DS, una vez generado, se almacenará de forma segura dentro del HSM y no se podrá exportar. La solicitud de

certificado del par de claves DS recién generada se enviará al Integrale™ KMS para la emisión de certificados DS.

- **Preparación de datos de la OACI**: Al recibir la información, el motor integrado agrupará la información personal de acuerdo con la estructura de datos especificada por los Grupos de Datos (DG) de la OACI. Esto también incluye la generación de firma digital con las Claves del Firmante de Documentos dentro del HSM sobre los DG formateados.
- **Preparación de datos de chip**: los DGs firmados digitalmente se formatearán en un formato cargable específico para el chip y el sistema operativo de chip utilizado en la tarjeta electrónica. El archivo cargable se devolverá al sistema de llamadas.

4.1.11 Operaciones relacionadas con la Personalización

Clave de transporte de personalización de chip: la clave de transporte para "abrir" el chip para la personalización se transporta de forma segura al cliente final y se almacena en el HSM de Integrale™ DPS. Durante la personalización del chip, se realizará una autenticación mutua exitosa entre el chip y el DPS antes de que se puedan cargar los datos del chip.

Configuración - Integrale™ DPS

Esta propuesta de configuración de seguridad para el DPS asegura que los datos del chip estén protegidos durante la personalización y que el acceso no autorizado sea prevenido mediante el uso de HSM. La operación controlada mediante tarjetas de administrador y operador, así como la necesidad de altos directivos para la configuración inicial y recuperación del almacén de claves, garantiza un entorno seguro y bien administrado para la gestión de personalización de chips.

Equipos y Balanceo de Carga

- 4x DPS y 4 x HSM instalados en servidores de aplicaciones con equilibrio de carga.
- 1 x HSM de repuesto.

Protección y Almacenamiento de Datos

- DPS preparará los datos del chip protegidos por **autenticación pasiva y activa** durante la personalización.
- La **clave de personalización y administración del chip (PMK)** se almacenará en el **HSM** del DPS para evitar el acceso no autorizado.

Activación y Operación del DPS

- DPS debe activarse con la **tarjeta de operación** configurada para admitir la personalización del chip.

- Si el servidor de aplicaciones se reinicia, el operador debe **iniciar sesión** en el servidor y **reactivar el DPS** antes de cualquier personalización del chip.

Asignación de Titulares de Llave

Designación de Altos Directivos:

- Asignación de **5 altos directivos** como titulares de la llave/tarjeta.
- Estos directivos tendrán **tarjetas de administrador y operador**.

Requerimientos para la Configuración Inicial

Configuración Inicial:

- Se necesitarán los **5 altos directivos** para la configuración inicial.

Recuperación de Claves:

- El almacén de claves en el **DPS HSM** solo será recuperable con la **tarjeta de administrador configurada** cuando estén presentes al menos **3 titulares de claves/tarjetas**.

Operación y Activación del DPS

Se asignará **1 administrador** para **operar / activar** el DPS durante la **ceremonia de generación de claves** o después del **reinicio del servidor**.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

4.2 PKI DE FIRMA DIGITAL

La PKI de Firma Digital se utiliza para garantizar la autenticidad, integridad y no repudio de documentos electrónicos. Se utiliza para firmar electrónicamente documentos como contratos, formularios, transacciones financieras, entre otros. El objetivo es proporcionar una forma segura de verificar la identidad del firmante y asegurar que el documento no haya sido alterado después de ser firmado.

Este sistema es fundamental para asegurar que **las cédulas de identidad electrónicas (CIE), certificados de nacimiento, documentos de identificación y otros registros oficiales** sean confiables y resistentes a falsificaciones.

Sera un sistema y solución integral que habilitará a los ciudadanos y demás organismos del país a gozar de los principales beneficios de la criptografía. El objetivo principal es proporcionar a los ciudadanos un medio para generar firmas digitales seguras a través de su tarjeta de identidad, garantizando validez legal y seguridad. Esto implica la generación de certificados digitales de firma avanzada.

La PKI de Firma Digital emitirá **certificados digitales** de firma que estarán destinados a ser alojados dentro de las nuevas CI y CIE, con chip sin contacto (contactless) con funcionalidad de firma electrónica. Además de la emisión de certificados digitales de firma avanzada, el Sistema de PKI de Firma Digital dispone la posibilidad de integrar servicios de validación de certificados en línea, sellados de tiempo, portales de gestión del ciclo de vida de los certificados digitales para la JCE, portales de firma de documentos y demás servicios de validación para ciudadanos y otros organismos.

En este contexto, **MAGALLANES MEDIA**, como especialista en identidad digital, infraestructura de clave pública y autenticación remota dentro del consorcio, desempeñará un papel clave en el desarrollo y gestión de esta infraestructura, asegurando su integración con plataformas de validación en línea, sistemas gubernamentales y aplicaciones móviles. La experiencia de **MAGALLANES** en la interoperabilidad de credenciales electrónicas e infraestructura de clave pública fortalecerá la **PKI de Firma Digital**, garantizando su cumplimiento con los estándares internacionales y optimizando su operatividad en entornos digitales y físicos.

4.2.1 Características generales de la PKI de Firma Digital

El sistema de PKI de Firma Digital contempla tanto un Servicio de Autoridad de Certificación (CA) como un Servicio de Protocolo de Estado de Certificados en Línea (OCSP), que pueden ser implementados por la JCE para satisfacer una variedad de casos de uso en negocios digitales, incluida la generación de certificados digitales de firma avanzada. La PKI propuesta proporciona una Autoridad de Certificación (CA) y una Autoridad de Validación OCSP de alto rendimiento, robusta y confiable, que cumple con los estándares RFC 5280, RFC 6960 y RFC 5019. El sistema de PKI de Firma Digital cuenta con la certificación Common Criteria EAL 4 y cumple con los requisitos del Perfil de Protección Aprobado por el Gobierno para Autoridades de Certificación v.2.1 (2017) de la National Information Assurance Partnership. Esto significa que el Servidor PKI está certificado según el perfil de protección más reciente para CA y con un alto nivel de seguridad.

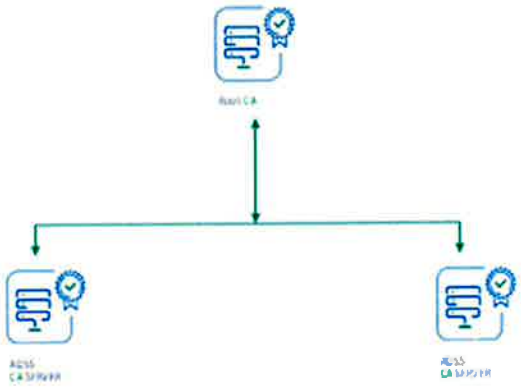
El Servicio de Certificación, la Autoridad de Certificación (CA), permite que las aplicaciones cliente soliciten la generación de claves y la emisión de certificados en nombre de los usuarios finales. En esta oportunidad específica, las claves de firma se generarán directamente en las nuevas CI y CIE, con chip sin contacto (*contactless*), y el Servicio de Certificación solo recibirá una solicitud de firma de certificado (CSR).

4.2.1.1 Generación de certificados digitales de firma avanzada x.509. CA dedicada de firma digital

La Autoridad de Certificación (CA), permite que las aplicaciones cliente soliciten la generación de claves y la emisión de certificados en nombre de los usuarios finales o clientes.

En esta oportunidad específica, las claves de firma se generarán directamente en la nueva tarjeta CI y CIE, y el Servicio de Certificación solo recibirá una solicitud de firma de certificado (CSR) de la Autoridad de Registro.

Estamos proponiendo, al menos, una estructura de PKI de dos niveles, que consta de una Autoridad de Certificación raíz (CA) y CAs subordinadas emisoras en alta disponibilidad, como se muestra en la siguiente figura.

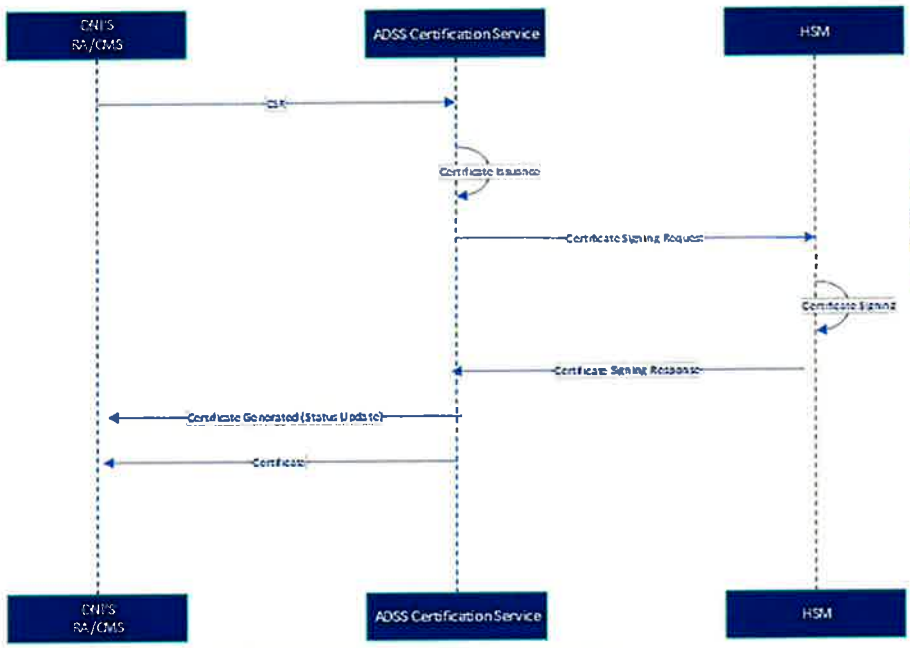


De esta manera, La **PKI** establecerá un dominio y cadena de confianza compuesto por los siguientes elementos:

- **Autoridad de Certificación Raíz (Root CA):** También llamada **CA Raíz**, esta CA estará fuera de línea y actúa como el ancla de confianza para la PKI de Firma Digital. Firma los certificados de su autoridad de certificación subordinada y las listas de revocación de autoridad asociadas (**CRLs**).
- Dispondrá de un HSM para almacenar de manera segura las llaves de la CA raíz.
- **CA Emisora:** Una CA en línea y de alta disponibilidad con dos nodos, responsable de firmar y crear los certificados x.509 de los usuarios finales y las listas de revocación de certificados (**CRLs**) asociadas.
- Según las necesidades de la JCE y la demanda de certificados es posible escalar el sistema y comisionar nodos y Cas emisoras adicionales.
- Cada nodo y CA emisora contará con su propio HSM dedicado.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

A la hora de la generación de los certificados de firma x.509, el siguiente diagrama secuencial ilustra la interacción a alto nivel entre los diversos componentes involucrados en el caso de uso de generación de certificados.



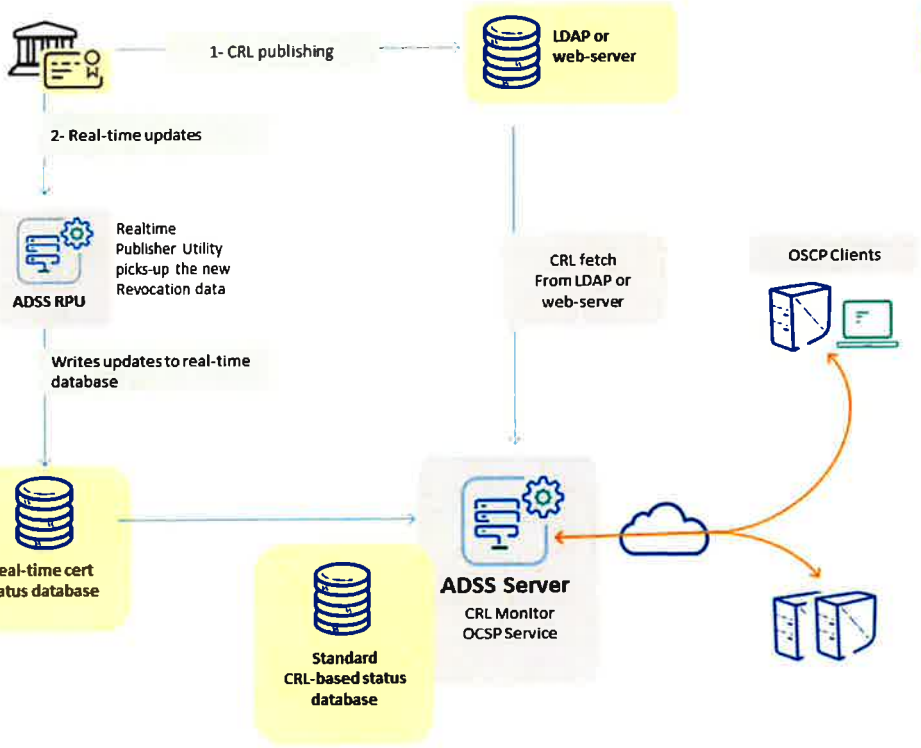
4.2.2 Servicio de validación de certificados (OCSP)

El servicio de protocolo de Estado de Certificados en Línea (OCSP) ayudará a las partes confiables a verificar el estado de un certificado y determinar si es válido o ha sido revocado, basándose principalmente en la lista de revocación de certificados (CRL) de la CA correspondiente.

A continuación, se describe el mecanismo clásico de funcionamiento del Servicio OCSP:

- Un usuario final firma utilizando su clave de firma almacenada en su tarjeta inteligente.
- La aplicación de la parte confiable desea delegar la complejidad de la verificación del estado del certificado al *backend* de la PKI de Firma Digital, por lo que realiza una solicitud OCSP al Servicio OCSP e incluye el identificador del certificado digital en la solicitud.
- El Servicio OCSP realiza todas las verificaciones estándar del estado del certificado y devuelve la respuesta OCSP a la aplicación cliente.

Dependiendo de las necesidades y restricciones del DNI, el servidor OCSP debe implementarse de manera que revele el estado del certificado en tiempo real. Para ello, se puede proponer fortalecer el servicio OCSP con Real-Time Publishing Utility (RPU).



Con respecto a la Lista de Revocación de Certificados (CRL), el DNI tiene varias opciones para su almacenamiento, incluyendo LDAP, un servidor web o una base de datos. La elección específica del método de almacenamiento dependerá de los requisitos de infraestructura y accesibilidad de la JCE y los organismos que precisen realizar este tipo de consultas.

Además, los detalles de implementación tanto del OCSP (Protocolo de Estado de Certificados en Línea) como de la CRL serán discutidos y finalizados en las etapas posteriores del proyecto para garantizar un sistema sólido y seguro de verificación del estado de los certificados.

De todas maneras todos los sistemas necesarios para realizar OCSP, generar y publicar listas de revocación de certificados están incluidos dentro del alcance de esta propuesta.

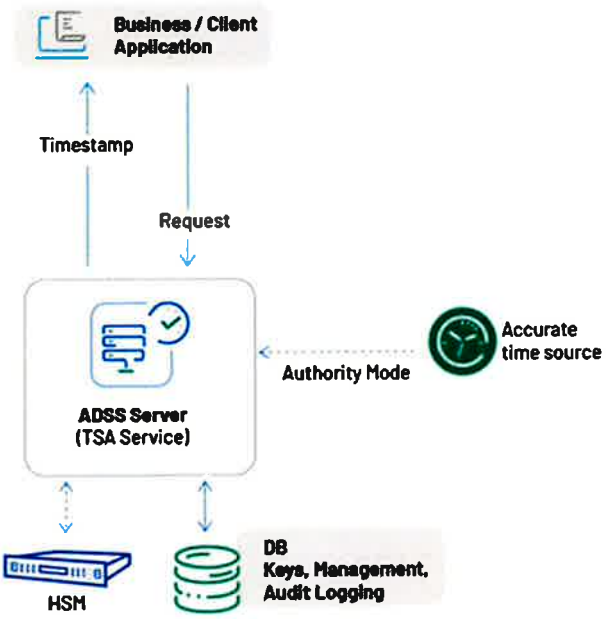
4.2.2.1 Servicio de autoridad de sellos de tiempo, TIME STAMPING AUTHORITY (TSA).

El módulo de servicio TSA producirá principalmente tokens de marca de tiempo para documentos firmados, para demostrar la existencia de los datos de origen de entrada o el hash seguro de los datos en un momento y fecha específicos.

El módulo TSA produce tokens de marca de tiempo RFC 3161 y RFC 5816 para cualquier dato electrónico, para demostrar la existencia de los datos de origen de entrada (o el hash seguro de los datos) en un momento y fecha específicos. El servidor TSA cumple con los requisitos ETSI EN 319 422 y EN 319 421 para servicios TSA.

Existen dos formas diferentes en las que se puede utilizar el servicio TSA para producir tokens de marca de tiempo:

- TSA local: Utilizar el servicio TSA local y las claves locales de firma de marca de tiempo; o
- TSA externa: Enviar la solicitud de marca de tiempo a otro TSA externo. En este caso, el servicio TSA actúa como un concentrador de solicitudes de marca de tiempo, las cuales son atendidas por uno o más TSAs en el backend.



El TSA se utiliza para sellar temporalmente documentos, firmas digitales y mensajes de respuesta de verificación / OCSP para confirmar su validez en un momento específico.

Fortalecer la PKI de Firma Digital con un TSA le permitirá asegurar lo siguiente:

- **Emisión de marcas de tiempo:** El TSA utiliza su certificado confiable para crear un token de marca de tiempo que registra de manera segura el momento exacto en que se creó el documento o la firma digital.
- **No repudio:** La marca de tiempo asegura que la firma no pueda ser fechada de forma retroactiva ni adelantada, evitando cualquier reclamo de que el documento fue firmado en un momento diferente.
- **Validación a largo plazo:** Los TSAs son cruciales para la validación a largo plazo de las firmas, ya que permiten verificar la validez de un documento mucho después de que haya caducado o sido revocado el certificado utilizado para firmarlo.

El módulo de servicio TSA podrá ser sincronizado con la hora oficial de la República Dominicana y las llaves del servicio podrán estar almacenadas en software o hardware. Asimismo, las timestamps podrán ser parta de los elementos que tiene cada firma electrónica.

4.2.3 Portal de gestión del ciclo de vida de los certificados digitales de firma avanzada.

Gestionar certificados digitales de manera efectiva es un requisito clave para cualquier equipo de seguridad informática. El portal de gestión del ciclo de vida de certificados lo hace de manera rápida, simple y segura. Los administradores de seguridad autorizados de la JCE pueden monitorear, revisar y aprobar solicitudes de emisión de certificados, renovar certificados antes de que caduquen y revocar certificados desde una interfaz intuitiva y segura en un navegador web. El portal de gestión del ciclo de vida proporciona notificaciones automáticas de estos eventos críticos en tiempo.

El portal es una aplicación de autoridad de registro de interfaz frontal que aprovecha el poder de la CA de la PKI de Firma Digital para emitir y gestionar directamente el ciclo de vida de los certificados. El portal ofrece una experiencia de usuario intuitiva tanto para administradores como para usuarios finales. Los administradores pueden crear fácilmente flujos de trabajo de inscripción para la obtención de certificados de usuario final o la inscripción de certificados de servidor basados en solicitudes de firma de certificados PKCS#10.

El portal y sistema global de gestión de ciclo del vida de los certificados digitales de firma avanzada permite a desarrolladores integrar la emisión de certificados de manera programática al exponer una API Rest, lo que facilita la integración de la gestión del ciclo de vida de certificados en otras aplicaciones. Este sistema también proporciona protocolos de inscripción estándar de la industria, lo que habilita integraciones de dispositivos y aplicaciones. Las organizaciones pueden emitir y gestionar certificados sin problemas utilizando protocolos estándar del mercado como SCEP.

Para acceder al portal cada usuario autorizado por la JCE deberá tener un certificado de autenticación.

4.2.4 Portal de firma de documentos

Dentro del alcance de esta propuesta estamos incluyendo el uso y acceso a un portal de firma de documentos con el estándar ISO 32000-1 y más avanzado para documentos portátiles PDF.

El portal de firma es un portal web que permite la aprobación en línea rápida y eficiente de cualquier documento empresarial, acuerdo, informe, solicitud o paquete. En este caso será configurado para poder utilizar el certificado digital de firma avanzada x.509 que emitirá el sistema de PKI de Firma Digital y se alojará en la nueva cédula física. Además el portal de firma es compatible con otros productos y servicios de terceros.

El portal web permite firmas electrónicas básicas, firmas electrónicas avanzadas y firmas electrónicas cualificadas del estándar de la Unión Europea. La mejor manera de demostrar que un documento no ha cambiado desde su firma es mediante firmas digitales criptográficas.

El portal web de firma se enfoca en el mercado de alta confianza, permitiendo el uso de esquemas PKI, así como otros certificados de alta confianza, incluidos aquellos reconocidos por Adobe Reader y Word para la seguridad persistente de documentos.

La interfaz web facilita la firma para cualquier usuario. Los documentos pueden compartirse, visualizarse y firmarse en cualquier dispositivo, en cualquier lugar y en cualquier momento, adaptándose a cualquier proceso de aprobación. Se admiten más de 20 idiomas, y otros pueden agregarse o personalizarse fácilmente. Utiliza firmas de larga duración estándar PDF PAdES y Word XAdES. Esto significa que los documentos firmados pueden verificarse de forma independiente, sin necesidad del portal, mediante cualquier lector de documentos compatible, como Adobe Reader, lectores de PDF de terceros, Microsoft Word, Office 365 u otro software compatible.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

4.2.5 Otras características del portal de firma:

✓ Compatible con **firmas remotas cualificadas** con **Nivel 2 de Control Exclusivo.**

Compatibilidad con formatos de documentos estándar:

- **PDF**
- **PDF/A-1** (a, b)
- **PDF/A-2** (a, b, u)
- **PDF/A-3** (a, b, u)
- **Documentos de Word**

✓ Todos los documentos están protegidos mediante **cifrado AES-256 bits.**

✓ Ofrece múltiples opciones de autenticación, incluyendo:

- **Microsoft Active Directory**
- **OAuth**
- **SAMLv2**
- **Freja eID**
- **BankID**
- **eID Easy**
- **Office 365**
- **Salesforce**, entre otros.

CONSORCIO IDSECURE IDS
Santo Domingo, D.N.

Evidencia firmada digitalmente:

Todas las operaciones realizadas por los usuarios quedan registradas en un **informe firmado digitalmente**, detallando todas las interacciones con el documento y el flujo de trabajo.

Dentro del alcance estamos incluyendo acceso a este portal para 100 usuarios de la JCE por año para satisfacer los roles de: 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.

1. Características adicionales del sistema PKI de Firma Digital

- Se contempla una **ceremonia de llaves** y creación de una CA raíz para todo el ecosistema de PKI de Firma Digital.
- **El vencimiento del certificado raíz será configurado a 10-20 años** o a convenir con la JCE.
- **Los vencimientos de los certificados intermedios serán configurados a 5-10** años o a convenir con la JCE.
- **Los vencimientos de los certificados de usuario final y servidor serán configurados a 1-3 años** o a convenir con la JCE.
- Se incluyen los **manuales de operación** de todos los componentes, ceremonia de llaves, procedimientos (CA raíz, renovación de certificados de CA subordinadas, recuperación de desastres)
- Se incluye toda la documentación del sistema de PKI de Firma Digital para definir las **características del certificado digital** de firma electrónica avanzada x.509, la definición de perfiles, sellado de tiempo, protocolos OCSP, y la referencia de todas las APIs para interactuar el sistema e integrarlo con distintas aplicaciones.
- Se incluye el **mantenimiento** de todo el ecosistema de firma digital a dos años.
- Se contempla **la generación, manejo y almacenamiento seguro** de claves criptográficas.
- La oferta incluye toda **la infraestructura física y software necesario** para la implementación, ejecución y mantenimiento de la PKI de Firma Digital, el conjunto de hardware y software en las instalaciones que indique la dirección de informática. El contrato de mantenimiento a cotizar es 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.
- Se incluye para la solución de la PKI de Firma Digital un ambiente productivo en **alta disponibilidad** con al menos 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).

CONSORCIO IDSECURE IDS
Santo Domingo, D. N.

- Toda la infraestructura de PKI de Firma Digital utilizará **módulos de seguridad por hardware (HSMs)** certificados (FIPS 140-2 nivel 2 o superior) para la generación y almacenamiento de claves privadas. La PKI de Firma Digital utilizará los mismos módulos HSM que la PKI de Firma de Documentos que cumplen con todos los requisitos de esta licitación y están detallados en la sección de PKI de Firma de Documentos.

- Para el caso del tamaño de llaves de la Autoridad ciudadana, tanto la **Autoridad Raíz como la Autoridad Subordinada** deberán tener un tamaño de llaves de 4096 bits. Para el caso de los certificados de usuario (ciudadanos) será de 2048 bits o a convenir previo al lanzamiento del proyecto.

- Se contempla que **las nuevas cedulas CI y CIE** puedan cambiar o ampliar su funcionalidad una vez se hayan entregado al ciudadano, en particular hablando de los certificados de firma digital que podrán tener un vencimiento diferente al documento físico en cuyo. En este caso se proveerá la administración de todo el ciclo de vida de estos (generación, actualización y revocación) en la electrónica de los documentos.

- La oferta incluye la generación de certificados digitales de firma dentro del **ambiente de pruebas**.

- Se incluye todo el **software y middleware** necesario para que la JCE desarrolle la integración entre la PKI y el Chip *contacless*.

- La oferta incluye la emisión de 1,000 certificados x.509 por año no acumulable y no prorrogable, por los primeros dos años, para permitirle a la JCE integrar y configurar correctamente todo el ecosistema de firma digital.

- Se provee la funcionalidad de **revocación de certificados** y sello de tiempos.

- El sistema propuesto estará bien **protegido** de cualquier acceso externo o no autorizado a través del diseño inherente y las instalaciones de seguridad de hardware y tendrá medidas de seguridad robustas, entre otras:

  - Se incluye la implementación de sistemas avanzados de monitoreo y detección de intrusos (IDS/IPS). El monitoreo incluye de infraestructura, de seguridad y de comunicaciones

  - Autenticación multifactorial (MFA para acceso a la administración). Cifrado avanzado en todas las comunicaciones y datos almacenados, utilizando algoritmos criptográficos robustos y actuales.

- Segmentación de redes que aísle la infraestructura de PKI de otras redes.
- 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.