EMDOC
CONSORCIO

ITEM III. Especificaciones Técnicas de las PKI CA y PKI Identidad Física y Digital

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

CONTENIDO

1. Especificaciones de la infraestructura de llave pública (PKI CA)

La **Infraestructura de Llave Pública** (PKI, por sus siglas en ingles *"Public Key Infrastructure"*) será la utilizada para garantizar la autenticidad, integridad y no repudio de documentos electrónicos mediante la firma digital. En la funcionalidad de firma electrónica para los ciudadanos se ha especificado que se requiere que dicha firma sea cargada al chip de la cedula de identidad y que se suministre una aplicación que maneje todo el ciclo de vida de dicha firma, es decir renovación, renovación, sellado de tiempo, etc. La **Infraestructura de Llave Pública** constará con su propia cadena de confianza completa, estando en línea o fuera de línea. Entre otras funcionalidades, permitirá a los ciudadanos la firma de documentos.

1.1 Propósito

Implementar una PKI para que la JCE esté en condiciones de gestionar todo el ciclo de vida de los certificados digitales que serán resguardados en la cédula de identidad que les será entregada a cada ciudadano. Mediante dichos certificados se dan elementos para verificar la autenticidad e integridad de los documentos de identidad ciudadana y al mismo tiempo los ciudadanos estarían en condiciones de firmar electrónicamente en procesos que implemente para tal fin el gobierno de la República Dominicana. Se incluye en este alcance los servicios profesionales para la integración de la firma electrónica en servicios públicos que señale la JCE, como por ejemplo en los ámbitos: electorales, del registro civil así se beneficien de los servicios de firma electrónica que facilitan validar la identidad de las personas. La interoperabilidad de la PKI se logra mediante APIs y Servicios web con tecnología API REST para verificar que los documentos sean auténticos e íntegros.

1.2 Objetivo general

Suplir los equipos, materiales y servicios para implementar una PKI que interoperará con la nueva "Cédula de Identidad y Electoral y Cédula de Identidad" para Incorporar nuevas tecnologías que aporten mayores niveles de seguridad, para de esa manera, dar seguimiento a la estrategia diseñada por las actuales autoridades de la Junta Central Electoral, vinculada a la modernización y mejoramiento de los servicios que ofrece a la ciudadanía, relacionados con la función electoral y las atribuciones que la Carta Magna le otorga, en materia del Registro Civil y de la Cédula de Identidad.

1.3 Objetivos principales

Son los siguientes:

- Implementar una PKI con redundancia en un sitio principal (producción) con el fin de tener continuidad en la operación.
- Implementar una PKI en un sitio alterno y alejado geográficamente del sitio principal, con el fin de reforzar el punto anterior, y que, en caso de algún contratiempo que interrumpa la operación del sitio principal se active este sitio alterno al que se denomina DRP (Disaster Recovery Plan).
- Implementar una PKI en un ambiente de pruebas, a fin de que el equipo de la JCE disponga de lo necesario para que pueda integrar la firma electrónica en todos

aquellos procesos y/o aplicaciones que el gobierno considere y que se traduzca en mejores servicios para la ciudadanía.

- Crear para la JCE su propia Autoridad Certificadora (AC), mediante la cual podrá controlar el ciclo de vida de los certificados digitales, esto coadyuva en garantizar la autenticidad y seguridad del documento de identidad. Se contempla crear una Autoridad Certificadora Raíz y una Autoridad Subordinada Operativa.
- Brindar los conocimientos a la JCE para que quede documentada el cómo se regirá la operación cotidiana de la AC.
- Implementar los componentes que acompañarán a la AC que permiten crear la PKI: una TSA (TimeStamp Authority) y un Motor de Firma.
- Realizar los servicios profesionales de nuestro personal especializado. En particular el acompañamiento del nacimiento operativo de la AC de la JCE, y en general puesta a punto, capacitación y arranque de la operación de la PKI, así como los servicios de soporte y mantenimiento de todos los componentes en los tres ambientes mencionados. En la siguiente sección (Componentes y servicios incluidos) se detallan estos.

1.4 Componentes y servicios incluidos

La presente propuesta considera la entrega de licencias, equipos criptográficos y servicios profesionales, para poner en operación y a punto una PKI con Autoridad Certificadora (AC), dentro de los plazos que señala el pliego petitorio.

Los componentes y servicios de la solución son los siguientes:

1.4.1 Licencias a perpetuidad

- SeguriServer (Autoridad Certificadora)
  - Ambiente Productivo
    - 1 instancia de servicio (1 Servidor [AC Raíz])
    - 2 instancias de servicio (2 Servidores [Activo - Pasivo]) para AC subordinada (operativa)
    - Licenciamiento cliente x procesador
  - Ambiente DRP
    - 1 instancia de servicio (1 Servidor) para AC Raíz
    - 1 instancia de servicio (1 Servidor) para AC subordinada (operativa)
    - Licenciamiento cliente x procesador
  - Ambiente Desarrollo
    - 1 instancia de servicio (1 Servidor)
- SeguriNotary (TSA - Autoridad De Sellos de Tiempo)
  - Ambiente Productivo
    - 2 instancias de servicio (2 Servidores [Activo - Pasivo])
    - Licenciamiento cliente x procesador
  - Ambiente DRP
    - 1 instancia de servicio (1 Servidor)
    - Licenciamiento cliente x procesador
  - Ambiente Desarrollo
    - 1 instancia de servicio (1 Servidor)
- SeguriSign (Motor de Firma Electrónica)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

- Ambiente Productivo
  - 2 instancias de servicio (2 Servidores [Activo - Pasivo])
  - Licenciamiento cliente x procesador
- Ambiente DRP
  - 1 instancia de servicio (1 Servidor)
  - Licenciamiento cliente x procesador
- Ambiente Desarrollo
  - 1 instancia de servicio (1 Servidor)

- Portal de Certificación (enrolamiento)
  - Ambiente Productivo
    - 2 instancias de servicio (2 Servidores [Activo - Pasivo])
    - Licenciamiento cliente x procesador
  - Ambiente DRP
    - 1 instancia de servicio (1 Servidor)
    - Licenciamiento cliente x procesador
  - Ambiente Desarrollo
    - 1 instancia de servicio (1 Servidor)
- Vertical de firma (incluye portales de: Administración, Agente y Firma)
  - Ambiente Productivo
    - 2 instancias de servicio (2 Servidores [Activo - Pasivo])
    - Licenciamiento cliente x procesador
  - Ambiente DRP
    - 1 instancia de servicio (1 Servidor)
    - Licenciamiento cliente x procesador
  - Ambiente Desarrollo
    - 1 instancia de servicio (1 Servidor)
- API
  - API con soporte a PKCS#11
    - Licencia corporativa para la JCE.

Las buenas prácticas indican estos vencimientos:

- Certificados de CA Raíz: Suelen tener una duración más larga (10-20 años) debido a la complejidad y la amplia distribución de la infraestructura que dependen de ellos.
- Certificados Intermedios: Duraciones moderadas (5-10 años) para asegurar un equilibrio entre seguridad y operatividad. Permiten un ciclo de renovación menos frecuente que minimiza las interrupciones.
- Certificados de Usuario Final y Servidor: Duraciones cortas (1-3 años) para maximizar la seguridad y la flexibilidad en la gestión. Son más fáciles de renovar y revocar en caso de compromisos.
- Se debe proveer la funcionalidad de revocación de certificados y la funcionalidad de sello de tiempo (Time Stamp).
- El vencimiento del certificado digital será estipulado dando cumpliento con la Ley de Comercio Electronico nacional y su reglamento

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.4.2 Equipos criptográficos (HSMs UTIMACO):

- 3 módulos de seguridad criptográfica CryptoServer CP5 Se 500 de Utimaco, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 2 equipos serán para ambiente productivo y 1 equipo para ambiente DRP.
- 2 módulos de seguridad criptográfica CryptoServer CP5 Se 12, con cumplimiento Common Criteria, eIDAS y FIPS 140-2 Nivel 3 o superior, que cumplen con las características descritas en el apartado Hardware Criptográfico, considerar impuestos, 1 equipo será para ambiente productivo y 1 equipo para ambiente DRP.
- 5 pólizas de Pólizas de Mantenimiento Premium para los 5 equipos: 3 CryptoServer CP5 Se 500 y 2 CryptoServer CP5 Se 12, con vigencia de 12 meses a partir de la firma del contrato.

1.4.3 Servicios profesionales

- Instalación y configuración de la solución que se proponga para los tres ambientes:
  - Producción en alta disponibilidad.
  - DRP en disponibilidad simple.
  - Desarrollo en disponibilidad simple.
- Asistencia Técnica en Normatividad de la Autoridad Certificadora para la generación del sustento legal de la Autoridad Certificadora de la JCE. Estos servicios brindan todo lo necesario para acompañar a la JCE en el nacimiento operativo de su AC y se genera la documentación que reglamenta la operación de la misma. Incluye las actividades de realizar la ceremonia de atestiguamiento y la generación del script para llevar a cabo la ceremonia.
- Asistencia técnica de integración de 1(una) aplicación o un máximo de 40 horas para a la integración de firma digital a una aplicación o proceso propietaria que designe la JCE.
- Capacitación (transferencia de conocimientos). Para el personal de la JCE, la capacitación va dirigida tanto a desarrolladores como al personal designado por la JCE que operará la solución tecnológica.
- Pólizas de soporte técnico 7x24 y mantenimiento de todos los componentes de software de la PKI propuesta (Licenciamiento a perpetuidad) con vigencia por la duración del contrato.
- Mantenimiento premium para los equipos criptográficos de la marca Utimaco por el fabricante

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

- Servicios de desarrollo para ajustar componentes especializados que permitan integrar la firma electrónica con el uso de las cédulas. Estos componentes son los siguientes:

  - SeguriLib/Librería Criptográfica
  - SeguriServer
  - SeguriSign Core
  - Bibliotecas Propósito General
  - Extensión Navegador de Internet (Browser)
  - Portal Firma
  - Portal Administración Certificados
  - Documentación
  - API criptográfica para soportar PKCS#11

Las funcionalidades a habilitar en los componentes previos son:

- Soportar HSM de UTIMACO para los productos de la AC Raiz y AC Subordinada.
- Integración de PKCS11 de UTIMACO en software de Autoridad Certificadora
- Adecuaciones al software de las Autoridades Certificadoras (AC) , al Motor de firma, modificar los Web Services de generación de PDF con soporte a ECC
- Modificaciones al Portal de Admon de Certificados para recibir ECC para certificados de AC con ECC
- Consumir el PKCS11 para librerías de Firma y generación de llaves para integrar el Middleware que entregará Veridos Alemania
- Soporte de extensión Chrome para generación de llaves en la tarjeta, asociar el certificado instalado en la tarjeta y generar la firma
- Portal de Firma la nueva extensión de Chrome que incluye el middleware de Veridos
- Portal de Administración de Certificados para habilitar la interoperabilidad con soporte a las tarjetas de República Dominicana
- API para integración de firma en las Aplicaciones del cliente para las nuevas tarjetas

1.5 Propuesta de solución

Mediante la implementación de la PKI se logra lo siguiente:

- Autenticación Segura: La PKI permite que cada cédula emitida tenga un certificado digital único que autentica la identidad del portador de manera segura, haciendo uso de la criptografía de clave pública.

- Integridad de los Datos: Asegura que la información contenida en las cédulas no pueda ser alterada sin detección, mediante firmas digitales.
- Confianza en el Sistema: Al implementar una PKI, la Junta Central Electoral puede garantizar a los ciudadanos y a las entidades que requieren verificación de identidad, que el sistema es robusto y seguro.

Otros objetivos que nuestra solución cumple, son:

a) Actualiza la Información Personal y Biométrica:

- Certificación de la Autenticidad: Los certificados digitales gestionados por la PKI pueden ser utilizados para verificar que la actualización de los datos proviene de una fuente auténtica y autorizada.
- Control de Acceso Seguro: La PKI permite establecer controles de acceso basados en certificados digitales, asegurando que solo personal autorizado pueda acceder o modificar los datos biométricos y personales.

b) Garantiza la Autenticidad y Seguridad del Documento:

- Prevención de Fraudes: La PKI proporciona un mecanismo para que cada documento de identidad emitido sea único y verificable, lo que complica significativamente la falsificación y el uso fraudulento de documentos.
- Firma Digital: Los documentos pueden ser firmados digitalmente para verificar su autenticidad y verificar que no han sido modificados desde su emisión.

c) Facilita el Acceso a Servicios Mediante un Ecosistema Interoperable:

- Interoperabilidad: La PKI, al ser un estándar reconocido y ampliamente utilizado para la seguridad en las comunicaciones digitales, facilita la interoperabilidad entre diferentes sistemas y plataformas que utilizan API REST y otras tecnologías.
- Gestión del Ciclo de Vida de los Certificados: La PKI no solo emite certificados, sino que también los revoca y los renueva, gestionando todo el ciclo de vida de los certificados digitales, lo que es crucial para mantener la seguridad del sistema en el tiempo.

1.6 Funcionalidad de Firma Electrónica mediante la PKI propuesta

La PKI propuesta es totalmente compatible con la PKI ICAO de las cédulas para establecer un SOD activado en los datos del chip. Lo anterior lo logramos debido a que nuestra PKI es capaz de generar, gestionar y validar las firmas digitales y certificados que son utilizados para proteger y verificar la autenticidad de los datos almacenados en el chip de un documento electrónico, conforme a los estándares de la OACI. Esto asegura

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

que los datos biométricos y personales en el chip están protegidos contra modificaciones no autorizadas y pueden ser verificados de manera confiable a través de fronteras internacionales.

El acceso a la tarjeta está protegido mediante el uso de un Número de Identificación Personal (PIN) y una Clave Personal de Desbloqueo (PUK) para proteger el acceso a una tarjeta con chip es un enfoque estándar en la seguridad de tarjetas inteligentes.

Se soportan algoritmos de firma como RSA y ECDSA, asimismo, claves en formato CRT (Chinese Reminder Theorem) y en formato normal. Para el caso de RSA, para cada par de llaves, se generan números primos pseudoaleatorios p y q, dependiendo del tamaño de las claves se varía su tamaño, para más información ver la sección de Anexos [ver sección "Descripción técnica autoridad " (SeguriServer) y sección "Descripción técnica de Motor de Firma Electrónica" (SeguriSign)].

La PKI propuesta implementa PKCS#15, es decir, implementa el formato y organización específicos para los archivos de datos almacenados en tarjetas inteligentes que usan tecnología de chip integrado.

Se proveerán como parte de la solución, tarjetas con memoria suficiente para almacenar hasta 4 certificados, con sus correspondientes claves, incluyendo el caso de claves RSA 4096.

Cuando se generen los certificados digitales en las cédulas se soporta la autenticación de la información intercambiada; incorporando HMAC según ANSI X9.19 y DES. Sin embargo, proponemos el uso de AES en lugar de DES, dado que DES ya no es seguro.

El establecimiento del protocolo para generar claves de sesión basado en el esquema propuesto en ISO/IEC 9798-3 Authentication SASL Mechanism se plantea del siguiente modo, asumiendo que ya se tienen los certificados en las cédulas de identidad:

Intercambio de Claves y Autenticación

- Intercambio de Claves Públicas: Las entidades intercambian sus claves públicas, es decir sus certificados digitales.
- Generación de Claves de Sesión: Cada parte genera una clave de sesión, que puede ser una clave simétrica temporal para cifrar la comunicación durante una sesión.

Autenticación Utilizando Firmas Digitales

- Firma de la Clave de Sesión: Cada parte firma la clave de sesión generada utilizando su clave privada.
- Envío de la Clave de Sesión Firmada: La clave de sesión firmada se envía a la otra entidad junto con el certificado digital del emisor.

- Verificación de la Firma: Al recibir la clave de sesión firmada, la entidad receptora utiliza la clave pública del emisor, extraída de su certificado digital, para verificar la firma. Esto asegura la autenticidad de la clave de sesión y confirma la identidad del emisor.

Establecimiento de la Comunicación Segura

Una vez que ambas partes han verificado las claves de sesión:

- Cifrado de Comunicaciones: Utiliza las claves de sesión para cifrar y descifrar la comunicación entre las entidades, asegurando la confidencialidad y la integridad de los datos intercambiados.

- Re-autenticación: Pueden implementarse mecanismos de re-autenticación periódica para mantener la seguridad de la comunicación a lo largo del tiempo.

Mediante el empleo de criptografía de curvas elípticas (ECC), se generan la clave privada y de esta se deriva la correspondiente clave pública. el estándar ANSI X9.63 especifica cómo dos partes pueden cooperar para crear una clave compartida que puede ser usada para cifrar comunicaciones subsecuentes. Esta cooperación bien puede realizarse usando RSA o ECC.

1.7 Características de la PKI propuesta

Para mayor detalle de toda la funcionalidad de la PKI ofertada ver en la sección Anexos, (ver sección "Descripción técnica funcional de productos PKI"). En este apartado listamos algunos aspectos funcionales de la misma.

Mediante el uso de los certificados emitidos por el servidor de la Autoridad Certificadora (AC), los sellos de tiempo emitidos por el componente SeguriNotary (TSA) para dotar de certeza respecto al momento en que se plasma una firma y el componente SeguriSign (Motor de firma electrónica) que permite el uso de los del lado cliente (usuario) para que se ejecute la firma, se proveen todos los beneficios que otorga la firma electrónica a los documentos:

- **Integridad** (el documento firmado no ha sufrido alteraciones),
- **Autenticación** (quién firmó) y
- **No repudio** (no se puede negar haber firmado).

La PKI implementada gestiona el ciclo de vida de los certificados: emisión, revocación y renovación de los mismos que se utilizarán para firmar electrónicamente las tarjetas electrónicas (CSCA) y para verificar tarjetas electrónicas (CVCA). Al mismo tiempo la PKI permite las verificaciones de identidad que menciona el estándar ISO 18013-5.

La PKI es compatible con Common Criteria, en el caso del equipo criptográfico (HSM) cumple con las certificaciones de eIDAS, Common Criteria, FIPS 140-2 N3, entre otras especificaciones (Para más detalles ver en la sección de Anexos, la destinada a la

descripción técnica de Módulo nShield). El HSM resguardará las claves de la Autoridad Certificadora de la JCE, con las cuales se firmarán los certificados digitales que estarán en las cédulas de identidad.

En la sección de Anexos podrá consultarse todos los aspectos relacionados al software y hardware necesarios para dejar implementada la PKI que se propone. Por ejemplo, toda la gestión de las firmas la llevará SeguriSign, asimismo todo el ciclo de vida de los certificados lo cubre SeguriServer, en particular las listas de certificados revocados (CRL), conforme a las especificaciones funcionales de la OACI.

SeguriServer (Autoridad Certificadora de la PKI):

- Permite firmar certificados para entidades gubernamentales o documentos de importancia nacional.
- Utiliza algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante, en particular el que proponemos es de la marca Utimaco.
- Permite verificar certificados revocados mediante la publicación periódica de una lista de revocación de certificados (ICAO 9303).
- Puede trabajar en un entorno sin conexión.
- Puede utilizar autenticación multifactorial para el inicio de sesión en la interfaz de administración, por ejemplo, la combinación de contraseña y el uso de certificados digitales.
- Puede firmar un VDS (Visible Digital Seal), que es una especie de "sello digital visible" que se utiliza en documentos de viaje y otros documentos de identidad. SeguriServer al firmar estos sellos, se asegura que la entidad que firma el VDS es legítima y que los datos contenidos en el sello son auténticos y no han sido alterados desde su emisión.
- Permite asegurar que los certificados incluidos en la lista maestra sean legítimos y estén bien gestionados, lo que incluye la emisión, renovación y revocación de los mismos.
- Puede ser configurado para que firme (Document Signer) documentos digitales de manera masiva, por ejemplo, los certificados de de las cédulas de identidad o los VDS. Lo anterior con las llaves estando resguardadas en un HSM para el control de la seguridad.
- El SOD (Signed Object Directory) es un componente crucial en los documentos de viaje electrónicos. Contiene datos digitales críticos como información biográfica y biométrica, que pueden ser firmados digitalmente por el componente SeguriServer (Document Signer).

- El componente SeguriServer posee una capa de Servicios web tipo REST para la firma del SOD.
- Utiliza algoritmos criptográficos actuales y almacenará las claves privadas en un HSM de cualquier fabricante, en particular de un HSM Utimaco propuesto.
- Permite el control de acceso en la interfaz de administración mediante el uso de la autenticación multifactorial, dando aviso antes de que expire el tiempo de uso de la clave del certificado actualmente utilizado.
- Se pueden configurar un par de claves destinadas resguardas en el HSM para un DS exclusivo que firme los DTC (Digital Travel Credential. Estándar ICAO de documento de viaje en móvil) para la aplicación Tarjeta Digital de la JCE. Se requerirá implementar una interfaz que permita acceder al sistema back-end de la JCE.

1.8 Otras consideraciones para la CSCA

EMDOC implementará una CA con especificaciones y un marco que cumplan con el Documento 9303 de la OACI vigente sobre el esquema de Firmas Digitales PKI propuesto para autenticar la tarjeta electrónica que ofrece acceso de sólo lectura de Chip de Circuito Integrado (IC).

EMDOC proveerá el licenciamiento, equipos criptográficos y servicios profesionales para instalar y configurar la PKI de la JCE, en particular la CA 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. La arquitectura que se propone es multicapa, siendo los datos y equipos criptográficos situados en la red interna de la JCE con todas las medidas de seguridad apropiadas, tanto físicas como lógicas. La ubicación de los sistemas o instalaciones propuestos será proporcionada por la JCE.

Los certificados de CA de firma del país se generarán en una infraestructura de CA sin conexión, altamente protegida. La solución cumple con estándares internacionales de criptografía y de las mejores prácticas de arquitectura de soluciones. Los certificados digitales están codificados de acuerdo al estándar X509. Asimismo, como parte de la solución se considera la implementación, configuración y puesta en operación de equipos criptográficos HSM, certificados con FIPS 140-2 N3, que serán instalados en las instalaciones de la JCE.

Toda la infraestructura adicional (racks, cableado, etc.), será provista con las características señaladas en las secciones: 6.1.4 Descripción técnica de Módulo CryptoServer CP5 SE 500 Utimaco y 5.1.7 Descripción técnica de Módulo CryptoServer CP5 SE 12 de Utimaco.

El certificado DS será emitido por la CSCA (SeguriServer). Para el caso de procesos de firma masiva, la PKI (SeguriServer) será responsable de la generación de claves/certificados de seguridad requeridos, no así las de los ciudadanos, serán estos

los que en completa privacidad generarán su par de claves y requerimiento de certificación, siendo la CSCA la encarga de emitir el certificado correspondiente mediante un agente certificador.

Tola la infraestructura propuesta de la PKI de la JCE se prevé este actualizada anualmente y garantizando 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.

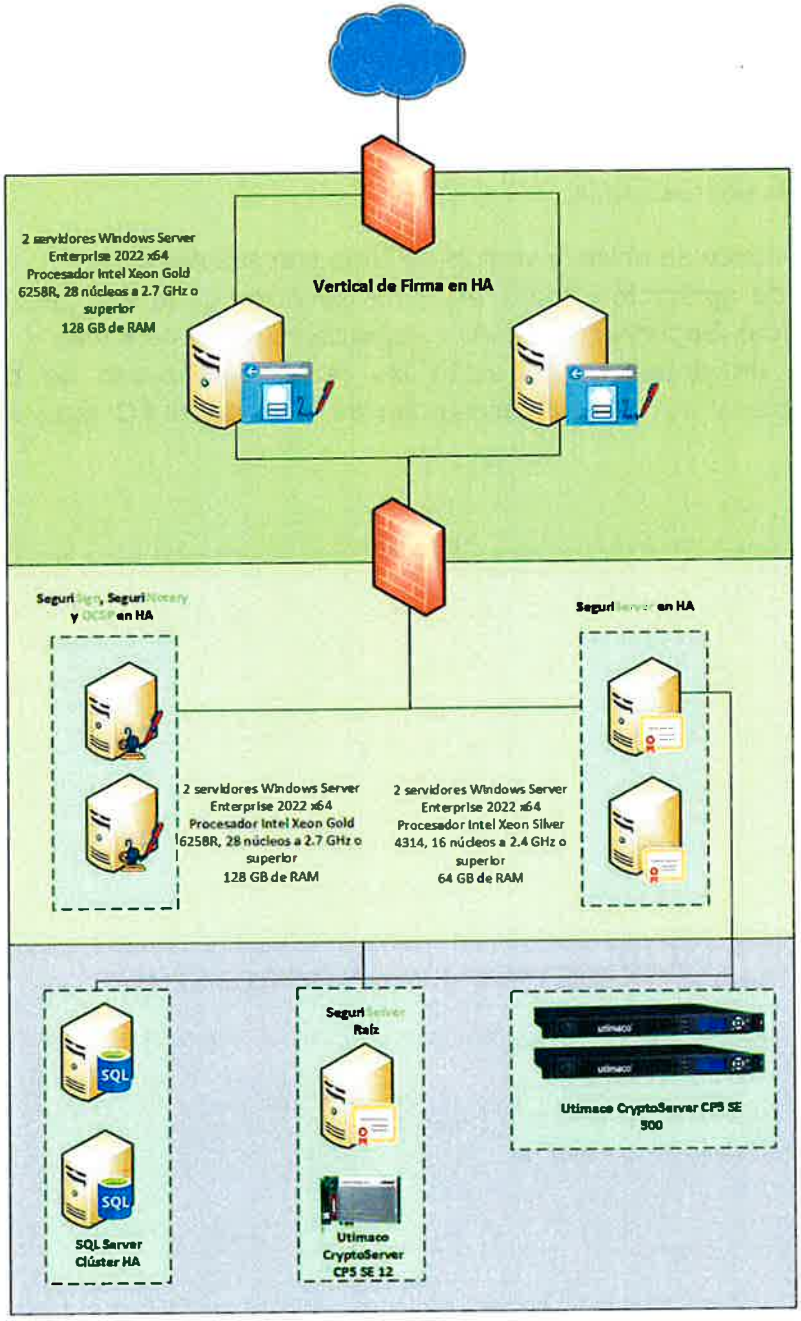
Especificaciones técnicas tarjeta de identidad digital y la Autoridad Certificadora

La tarjeta digital podrá ofrecer (si las leyes lo permiten) las mismas garantías jurídicas al titular que el CEI o CI. Los datos entregados y asociados a la tarjeta misma, al dueño de la tarjeta (ciudadano) podrán 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 serán firmados electrónicamente con las claves criptográficas de la JCE, que estarán resguardadas en el HSM. 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 CA de la JCE, con la figura de Autoridad Certificadora descrita en el apartado Infraestructura de clave pública (PKI).

1.9 Descripción funcional de los componentes de la PKI

1.9.1 Arquitectura de la PKI (conceptual)

Arquitectura para el ambiente de producción



Se provee redundancia en todos los componentes con el objeto de tener continuidad en la operación, el esquema será de conmutación por falla (failover) o por balanceo de cargas. Para este dispondremos de un balanceadora carga (ver descripción de la infraestructura).

Asimismo, puede observarse que la AC raíz es el único componente que no tiene redundancia, ya que, en realidad, este componente no tiene la misma demanda que la AC subordinada que es la encargada de certificar a los ciudadanos y por eso las llavees están en los HSM grandes, los CryptoServer CP5 SE 500. Mientras que la AC raíz solo emite certificados de AC, en este caso a las subordinadas y por lo mismo sus llaves están resguardadas en un HSM de poca capacidad, el CryptpServer CP5 SE12.

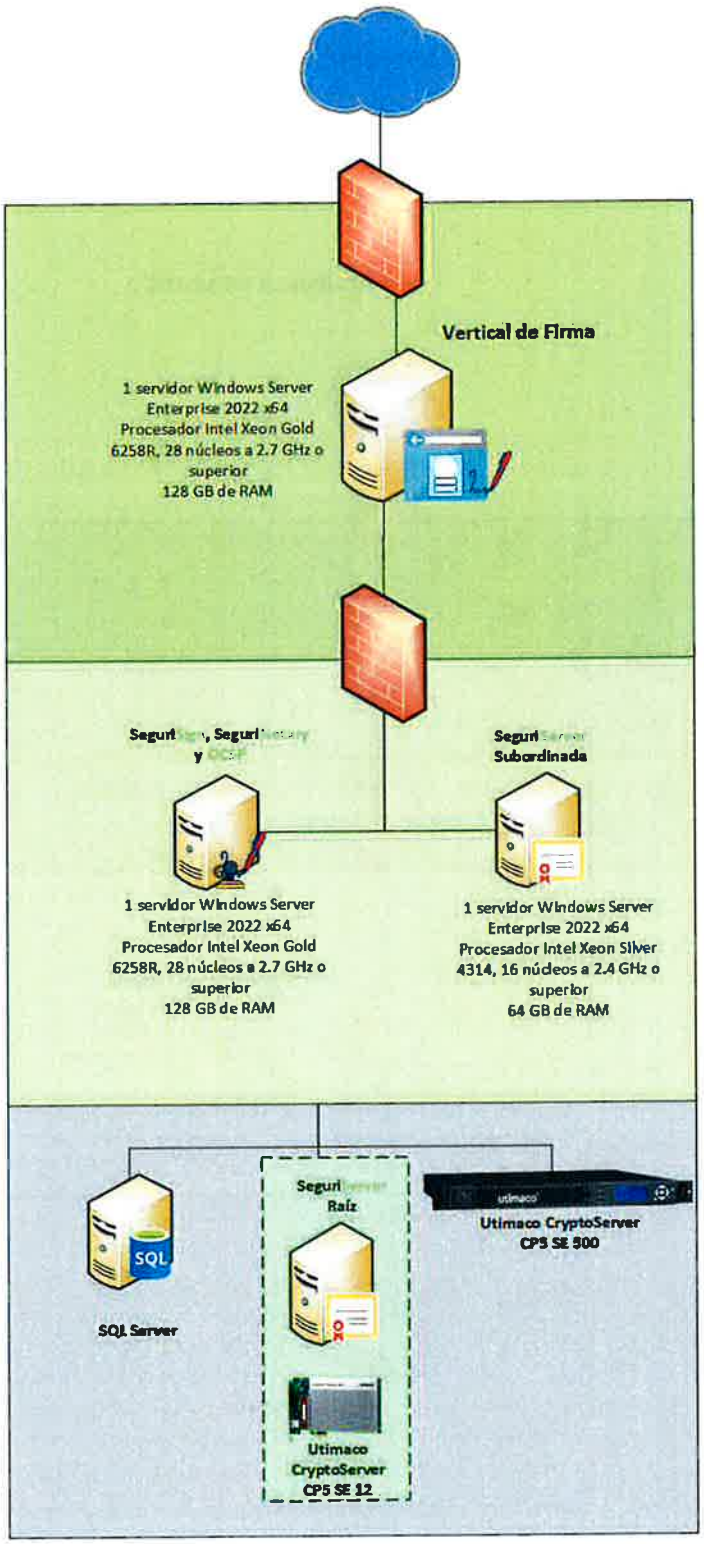
La arquitectura es en tres capas:

- **El Front**, donde se ubica la vertical de firma con sus portales;
- **La capa de aplicación** donde están los servicios de la PKI: SeguriServer (AC subordinada), SeguriNotary (TSA) y SeguriSign (motor de firma); y
- **La capa de datos** donde están las respectivas bases de datos de los componentes y los HSM que resguardan las llaves de las AC: raíz y subordinadas.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

EMDOC CONSORCIO

Arquitectura para el ambiente de DRP



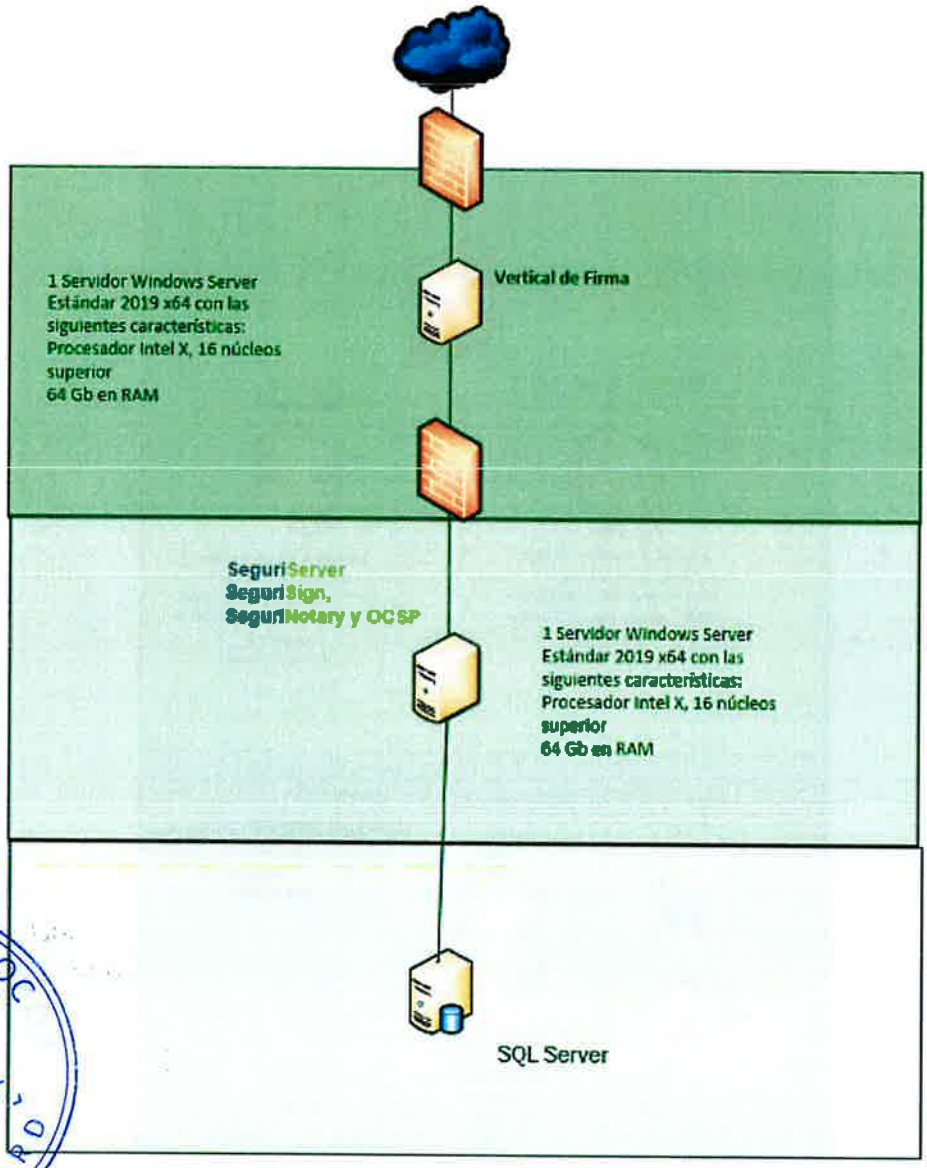
CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

Es la misma configuración que para el ambiente de producción, solamente que el esquema es en disponibilidad simple de los componentes.

Arquitectura para el ambiente de Desarrollo

Misma configuración que para el DRP, sin embargo, aquí no hay HSM y los requisitos del equipo son menores.

Ambiente Desarrollo



1.10 Autoridad Certificadora Raíz

La AC Raíz es el componente más confiable en una PKI, actuando como la fuente principal de verificación y confianza. Esta autoridad es la encargada de emitir certificados digitales a otras autoridades certificadoras (llamadas Autoridades Certificadoras Subordinadas) o a entidades finales u operativas, dependiendo de la estructura de la PKI, esto aplica a lo que estamos planteando que es como dictan las buenas prácticas.

1.10.1 Funcionalidad:

Emisión de Certificados: La AC Raíz emite certificados que verifican la identidad de las Autoridades Certificadoras Subordinadas. Estos certificados sirven como un voto de confianza, asegurando que las subordinadas son entidades confiables.

Creación de Llaves: Genera su propio par de llaves (una pública y una privada) porque es la raíz. La llave privada se utiliza para firmar los certificados de las autoridades subordinadas, mientras que la llave pública se distribuye para verificar esas firmas. Es importante señalar que esta autogeneración de llaves se realiza dentro del módulo criptográfico (HSM), es aquí donde ya encontramos la interoperación entre SeguriServer en su carácter de AC raíz y el HSM. El HSM que empleará la AC raíz es el modelo CryptoServer CP5 SE 12 de Utimaco, ver el respectivo anexo.

Raíz de Confianza: Funciona como el punto más alto de confianza en la PKI. Todos los certificados emitidos pueden ser rastreados hasta este punto, asegurando una cadena de confianza continua.

1.10.2 Beneficios:

Seguridad Mejorada: Al ser la autoridad más alta y centralizada, permite un control estricto de las políticas de seguridad y la emisión de certificados, minimizando la posibilidad de fraude o mal uso de las identidades digitales.

Interoperabilidad: Facilita la comunicación segura entre diferentes sistemas y organizaciones al proporcionar un estándar común de autenticación y cifrado.

Confianza Centralizada: Al ser el punto más alto de confianza, facilita la verificación de identidades y la validación de certificados a lo largo de toda la organización o sistema, sin necesidad de verificar cada conexión de manera individual.

La AC Raíz en una PKI es fundamental para establecer y mantener la integridad, la seguridad y la confianza en las comunicaciones digitales dentro de una organización o entre varias entidades.

Este proyecto considera la implementación de una AC raíz para la JCE.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.11 Autoridad Certificadora Subordinada (operativa o ciudadana)

1.11.1 Funcionalidad:

Emisión de Certificados: Las Autoridades Certificadoras Subordinadas son responsables de emitir certificados a entidades finales, como usuarios (ciudadanos) o dispositivos (cédulas de identidad), o a otras AC subordinadas. Estos certificados están firmados digitalmente por la AC subordinada, asegurando así la autenticidad e integridad de la información.

Verificación de Identidades: Antes de emitir un certificado, la AC subordinada verifica la identidad del solicitante, es lo que llamamos el proceso de enrolamiento y que liga la identidad real física) con la identidad electrónica. Este proceso es crucial para mantener la confiabilidad y seguridad de la red.

Gestión de Revocaciones: También manejan las listas de revocación de certificados (CRLs), que son esenciales para mantener actualizado el estatus de los certificados emitidos, identificando aquellos que han sido revocados y no deben ser confiados. Otro mecanismo que es más usado para verificar la revocación es el uso del protocolo OCSP acrónimo Inglés que significa Online Certificate Stauus Protocol, que a diferencia de la CRL con el OCSP se valida en línea, este protocolo lo implementan prácticamente todas las AC, en términos operativos se traduce en un puerto y una dirección IP donde la AC "escucha" peticiones para saber si un certificado está revocado y/o expirado.

1.11.2 Beneficios:

Descentralización del Riesgo: Al distribuir la emisión de certificados a múltiples AC subordinadas, se reduce el riesgo de un punto único de falla que podría comprometer toda la infraestructura de la PKI. En esta propuesta estamos implementando dos AC subordinadas en producción y una en DRP.

Escala y Flexibilidad: Las AC subordinadas permiten a la PKI escalar eficientemente, ya que pueden adaptarse y responder a las necesidades específicas de seguridad de distintos departamentos o sectores dentro de una organización.

Eficiencia en la Gestión: Facilitan la administración de certificados a nivel local (estatal, por ejemplo) o a nivel país, permitiendo una gestión más rápida y cercana a las necesidades específicas de los usuarios finales.

Las Autoridades Certificadoras Subordinadas juegan un papel crítico en la expansión y administración efectiva de una PKI, proporcionando seguridad y confianza en la autenticación y comunicación dentro de redes extensas. Al igual que la AC raíz estas AC subordinadas tendrán resguardadas sus llaves criptográficas en el módulo criptográfico (HSM), a diferencia de la AC raíz las AC subordinadas emplearán el HSM CryptoServer CP5 SE 500, esto debido a que la demanda operativa será mucho mayor.

1.12 Portal de Certificación (enrolamiento) empleando las cédulas de identidad

1.12.1 Funcionalidad:

Almacenamiento Seguro de Certificados y Llaves: El chip criptográfico en una tarjeta inteligente permite almacenar de manera segura certificados digitales y llaves criptográficas. Este chip está diseñado para ser resistente a ataques físicos y lógicos, protegiendo la información confidencial.

Autenticación y Firma Digital: Las tarjetas inteligentes con chip criptográfico pueden utilizarse para procesos de autenticación robusta y firma digital de documentos, estos documentos serían el resultado de algún proceso y/o trámite de la JCE que tenga cierto grado de automatización y que requiera firma digital. El chip realiza operaciones criptográficas directamente en la tarjeta, lo que mejora la seguridad al no exponer la llave privada fuera de la tarjeta.

Emisión y Gestión de Certificados: A través del portal de certificación (enrolamiento), los ciudadanos (usuarios) pueden solicitar la emisión o renovación de certificados que se almacenan directamente en el chip de la tarjeta inteligente. Esto puede incluir la generación de pares de llaves donde la llave privada nunca abandona el chip seguro.

1.12.2 Beneficios:

Seguridad Mejorada: La integración de certificados en un chip criptográfico aumenta significativamente la seguridad, dado que las llaves privadas están protegidas contra extracción. Esto minimiza el riesgo de duplicación o uso indebido de las credenciales.

Portabilidad: Las tarjetas inteligentes son dispositivos portátiles que permiten a los usuarios llevar sus credenciales criptográficas de forma segura y utilizarlas en diferentes sistemas, manteniendo la misma identidad digital segura.

Conveniencia y Acceso Controlado: Con las cédulas es posible, por ejemplo, facilitar un acceso controlado a edificios, sistemas de la JCE y otros recursos, combinando seguridad física y lógica en un solo dispositivo.

Cumplimiento de Normativas: Cumplen con estrictas normativas de seguridad y privacidad, lo que las hace adecuadas para industrias reguladas como la financiera, salud y gobierno. Es decir, es muy grande la cantidad de usos que pueden dársele al uso de las cédulas de identidad con chip criptográfico.

Nuestro portal de certificación (enrolamiento) que emite certificados para tarjetas inteligentes con chip criptográfico ofrece una solución robusta y segura para la gestión de identidades y accesos, optimizando tanto la seguridad como la operatividad en diversos entornos.

1.13 Portal Web de Firma

1.13.1 Funcionalidad:

Firma de Documentos PDF: El portal permite a los usuarios firmar digitalmente documentos en formato PDF, cumpliendo con el estándar PDF Signature (ISO 32000-1). Este estándar garantiza que la firma digital sea válida y reconocida a nivel nacional en este caso, o al menos en el ámbito de la JCE. Sin embargo, decimos a nivel nacional porque las cédulas tendrán validez en todo el país.

Integración con Tarjetas Inteligentes (Smartcards) con chip: Las llaves criptográficas de los usuarios están almacenadas de manera segura en tarjetas inteligentes con chip criptográfico. Cuando un usuario necesita firmar un documento, el portal interactúa con la tarjeta a través de un lector de tarjetas inteligentes para realizar la firma utilizando la llave privada que nunca sale del chip criptográfico.

Autenticación Segura: El acceso al portal requiere autenticación, que puede ser reforzada mediante el uso de la tarjeta inteligente, ya que el portal pide las llaves y la contraseña que protege a la llave privada, proporcionando un nivel adicional de seguridad antes de permitir la firma de documentos.

Gestión de Documentos Firmados: Además de permitir la firma, el portal de firma también ofrece servicios de almacenamiento, seguimiento y verificación de documentos firmados, facilitando la gestión de documentos legales y oficiales.

1.13.2 Beneficios:

Seguridad Avanzada: Al almacenar las llaves criptográficas en tarjetas inteligentes, se protege la identidad y las credenciales del usuario, minimizando el riesgo de robo o abuso de llaves privadas.

Conformidad Legal: Las firmas realizadas cumplen con los estándares legales para firmas digitales, lo que las hace jurídicamente vinculantes y aceptadas en procesos judiciales y administrativos.

Accesibilidad y Conveniencia: Los usuarios pueden firmar documentos desde cualquier lugar donde tengan acceso a Internet y un lector de tarjetas inteligentes, ofreciendo flexibilidad sin comprometer la seguridad.

Integridad del Documento: El uso del estándar PDF Signature asegura que cualquier alteración del documento después de su firma sea detectable, lo que aumenta la confianza en la validez de los documentos firmados.

El portal de firma proporciona una solución eficiente y segura para la firma digital de documentos, aprovechando la tecnología de tarjetas inteligentes para garantizar la seguridad y la autenticidad en general de las transacciones digitales.

1.14 PKI (Infraestructura de Llave Pública)

1.14.1 Componentes de la Infraestructura de Llave Pública (PKI):

SeguriServer (Autoridad Certificadora, AC raíz y subordinada):

- ***Funcionalidad***: Esta AC es responsable de emitir y administrar los certificados digitales almacenados en tarjetas inteligentes con chips criptográficos. SeguriServer genera el par de llaves (pública y privada), donde la llave privada se almacena de forma segura en el chip de la tarjeta inteligente y nunca se expone externamente. Lo anterior a través del portal de certificación (enrolamiento).
- ***Beneficios***: Aumenta la seguridad de las credenciales de identificación, minimizando el riesgo de duplicación o compromiso de las llaves privadas. Facilita el cumplimiento de normativas estrictas de seguridad y privacidad.

SeguriNotary (TSA):

- ***Funcionalidad***: SeguriNotary es una Autoridad de Sellado de Tiempo (TSA) que genera sellos de tiempo (timestamps) para cada firma digital realizada. Esto certifica el momento exacto en que se efectuó la firma, lo cual es crucial para procesos legales y de auditoría.
- ***Beneficios***: Proporciona pruebas irrefutables del momento de la firma, lo que es vital para la validez y la integridad a largo plazo de los documentos firmados digitalmente.

SeguriSign (Motor de firma electrónica):

- ***Funcionalidad***: Este servicio actúa como el núcleo operativo de la plataforma, encargándose de las interacciones entre los usuarios y los componentes tecnológicos. Gestiona la solicitud de sellos de tiempo (timestamps) a SeguriNotary, también se encarga de "preguntar" al servicio de validación en línea de la SeguriServer (OCSP) si un certificado de un usuario está revocado y/o expirado. Almacena en su base de datos los documentos firmados usando el estándar PDF Signature, junto con las respectivas evidencias que acompañan a cada firma: OCSP y sellos de tiempo por cada firma. Además, proporciona APIs y servicios web para que los usuarios puedan firmar documentos directamente desde un portal web o mediante aplicaciones de terceros. Otra gran característica es que SeguriSign puede configurarse para que reconozca a otras AC como de confianza, es decir, lo que se traduce en que pueda reconocer firmas digitales que están empleando certificados que no fueron emitidos por la AC de la JCE.
- ***Beneficios***: Asegura una gestión eficiente de las firmas digitales, permitiendo una fácil integración en diferentes plataformas y aplicaciones mediante sus APIs y Servicios Web. Mejora la accesibilidad y la flexibilidad para los usuarios finales, permitiéndoles firmar y gestionar documentos desde cualquier lugar.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

1.14.2 Beneficios Generales de la PKI:

- ***Seguridad Robusta*:** La combinación de tarjetas inteligentes, emisión segura de certificados, y sellado de tiempo asegura un alto nivel de seguridad en todo el proceso de firma.
- ***Integridad y Confiabilidad*:** La plataforma garantiza que las firmas son válidas, verificables y legalmente vinculantes, gracias a los procesos de validación y certificación que respaldan cada firma.
- ***Cumplimiento de Normativas*:** Cumple con normativas internacionales sobre la firma digital y la gestión de identidades digitales, lo que la hace adecuada para su uso en sectores regulados como el financiero, legal y gubernamental.
- **Interoperabilidad y Escalabilidad:** Gracias a las APIs y servicios web, la plataforma puede integrarse fácilmente con otras aplicaciones y sistemas, permitiendo una escalabilidad eficaz conforme crecen las necesidades del negocio.

1.15 Integración de la firma digital con las aplicaciones de la JCE empleando las cédulas de identidad (smartcards con chip)

Antes de describir el proceso general de integración de la firma digital, recordemos que quien orquesta o gestiona las firmas es SeguriSign. A su vez, por cada firma que se ejecuta SeguriSign interopera con Seguriserver para "preguntar" vía el OCSP, si un certificado está revocado o expirado, con SeguriNotary para pedir el sello de tiempo. La realización de la firma del lado del cliente (usuario) desde el navegador de internet se ejecuta por medio de un API y todo el flujo de firma se va tejiendo al invocar de manera propia los servicios web pertinentes.

Entonces ¿Cuáles son los componentes que actúan entre sí para lograr la firma? Estos son:

- **SeguriSign** (motor de firma) como el que orquesta y gestiona la ejecución del proceso de firma, tanto del lado cliente como del lado servidor.
- **SeguriServer**, que mediante su servico de OCSP emite la respuesta hacias SeguriSign de si un certificado (unas llaves criptográficas) no está revocado y/o expirado.
- **SeguriNotary** que emite un sello de tiempo pora cada firma ejecutada, quien se la solicita es SeguriSign.
- **Portal Web** o aplicación que implementa o integra la firma digital, este sería el cliente, para el caso de la solución presentada quién hace esto es nuestro portal de firma, es decir, es un ejemplo de cómo implementar firma desde un portal web.
- Desde luego los **servicios web de SeguriSign**.

- **API criptográfico** que se usa en el browser para gestionar la interacción entre la aplicación web y el lector de tarjetas para acceder a las llaves contenidas en la cédula de identidad, es decir, la smartcard.

Ahora procedemos a explicar el proceso de cómo sucede la integración de la firma digital y una aplicación por ejemplo de la JCE con los componentes mencionados, que forman parte de la PKI.

1.15.1 Proceso de Integración de la Firma Digital con Llaves en Smartcard:

Nota: cuando se lea "el cliente", se debe entender la aplicación de la JCE.

1. Inicialización del Proceso de Firma:

- ***Desde el cliente***: La aplicación cliente inicia el proceso de firma interactuando con un servicio web de SeguriSign. Esta solicitud inicial especifica quiénes firmarán, qué documento se va a firmar y el estándar de firma digital a aplicar.
- ***Respuesta de SeguriSign***: SeguriSign asigna un identificador único al proceso de firma y guarda los detalles pertinentes. Este identificador se usará para gestionar todo el proceso de firma.

2. Solicitud de Hash del Documento:

- ***El cliente solicita el hash***: La aplicación cliente, mediante la invocación a otro servicio web, solicita a SeguriSign el hash del documento que se va a firmar. Este paso requiere autenticación para asegurarse de que sólo los participantes autorizados obtengan el hash. En este caso los ciudadanos enrolados.
- ***Respuesta con el hash***: SeguriSign proporciona el hash del documento, que es esencial para la firma digital.

3. Firma del Hash con la Llave Privada:

- ***El API criptográfico*** *interactúa con la cédula de identidad (smartcard)*: El API criptográfico gestiona la interacción con la cédula de identidad (smartcard) para acceder a la llave privada del usuario, que está protegida y nunca sale del chip criptográfico. El usuario proporciona la contraseña para desbloquear su llave privada, y el API utiliza esta llave para firmar el hash del documento.
- ***Proceso seguro en la smartcard***: La operación de firma se realiza dentro del entorno seguro del chip criptográfico, asegurando que la llave privada no sea expuesta ni comprometida.

4. Envío de la Firma Digital a SeguriSign:

- ***El cliente envía la firma***: Tras obtener la firma digital, el cliente usa un servicio web para enviar esta firma a SeguriSign.

CONSORCIO EMDOC Santo Domingo, RD

- ***Recopilación de firmas*:** SeguriSign recopila y asocia cada firma recibida con el proceso de firma correspondiente, es decir, va recopilando las firmas de cada uno de los firmantes, si es que son 2 o más, o también si solo es uno, aquí podemos suponer que son dos o más.

Nota: Los pasos 2, 3 y 4 se repetirán por cada usuario que participe en el flujo de firma lanzado en el paso 1.

5. Finalización y Notificación:

- ***Cierre del proceso*:** Cuando todos los firmantes han completado sus firmas, SeguriSign finaliza el proceso de firma.
- ***Notificaciones a los participantes*:** SeguriSign notifica a todos los firmantes que el documento ha sido completamente firmado y que el proceso ha concluido con éxito. Con lo cual pueden descargar el documento ya firmado por todos, se invoca otro servicio web para esto.

Beneficios Clave de Usar Smartcards y el API de JavaScript:

- ***Protección avanzada de llaves privadas*:** Las llaves almacenadas en chips criptográficos de smartcards ofrecen un nivel superior de seguridad contra robos o exposición.
- ***Integridad y Autenticidad*:** La firma realizada en el chip garantiza que el documento firmado no pueda ser alterado sin detectarse, proporcionando una robusta evidencia de integridad y autenticidad.
- ***Conformidad y Validez Legal*:** Las firmas realizadas cumplen con normativas de seguridad y autenticación digital, haciéndolas legalmente vinculantes.
- ***Accesibilidad y Flexibilidad*:** Los servicios web y el API de JavaScript permiten una integración fácil y segura en cualquier aplicación, proporcionando a los usuarios la capacidad de firmar documentos de manera eficiente y segura desde cualquier lugar.

Este enfoque no solo maximiza la seguridad durante el proceso de firma digital, sino que también asegura que la solución sea escalable, accesible y cumpla con los más altos estándares de conformidad legal y seguridad informática.

1.16 Mantenimiento del licenciamiento de la PKI

Se incluye el mantenimiento del licenciamiento de los componentes de la solución para dar el servicio cubriendo los siguientes elementos:

- Software SeguriServer
- Software SeguriNotary

- Software SeguriSign
- Vertical de Firma
- Software Portal de Certificación (enrolamiento)
- API criptográfica con soporte a PKCS#11

Se entiende por mantenimiento la actualización a los productos de ***SeguriData*** (SeguriServer, SeguriNotary, SeguriSign, Vertical de Firma, Portal de Certificación, API con soporte a PKCS#11, en los ambientes de producción, DRP y desarrollo que la JCE tendrá, a fin de conservarlos en condiciones óptimas de funcionamiento, de acuerdo a sus propias especificaciones técnicas.

Upgrades

Son adecuaciones mayores que consisten en nuevas funcionalidades de los productos y tienen las siguientes características:

- Actualización para cumplir con los estándares de seguridad.
- Incorporación de nuevos módulos y protocolos de comunicación.
- Adecuaciones para cubrir con reglamentos y leyes Nacionales e Internacionales.
- Soporte a nuevos sistemas operativos y nuevas versiones de sistemas operativos ya existentes.

Las nuevas versiones serán enviadas a la JCE, en un plazo no mayor de 30 días hábiles, después de su liberación formal.

Updates

Son adecuaciones menores y consisten en el arreglo de problemas detectados en versiones anteriores o bien en modificaciones a la interfaz gráfica. Los updates serán enviados a la JCE, en plazo no mayor de 15 días hábiles, después de su liberación formal.

1.17 Servicios de soporte técnico 7x24 de los productos y componentes

La vigencia de la póliza de soporte técnico remoto será 7x24, durante la vigencia del contrato, con las siguientes características:

- 160 (ciento sesenta) horas anuales vía remota, correo electrónico o telefónico.
- Horario de atención de 24 (veinticuatro) horas, los 7 (siete) días de la semana, los 365 (trescientos sesenta y cinco) días del año.
- Se incluyen los servicios de soporte a los productos de software: SeguriServer, SeguriNotary, SeguriSign, Vertical de Firma, Portal de Certificación, API con soporte a PKCS#11, de acuerdo con lo siguiente, descrito de manera enunciativa mas no limitativa:

CONSORCIO EMDOC Santo Domingo, R.D.

- Brinda asesoría técnica y asistencia sobre el funcionamiento, operación y administración.
- Proporciona los parches a la JCE en caso de alguna falla del producto.
- Atención y resolución de incidencias presentadas en el software: SeguriServer, SeguriNotary, SeguriSign, Vertical de Firma, Portal de Certificación, API con soporte a PKCS#11, conforme al acuerdo de nivel de servicios de soporte técnico del pliego de requisitos, mismo que se señala a continuación:

1.17.1 Soporte Técnico del HSM

La propuesta incluye una Póliza de Mantenimiento Premium para el equipo criptográfico marca Utimaco, directamente del fabricante, además del respaldo para brindar soporte de primer nivel

Las características de la póliza de soporte de mantenimiento Premium incluye:

- Acceso 24x7 al equipo de soporte Helpdesk vía portal web, teléfono y email
- Respuesta inicial en menos de 2 horas
- Reemplazo de hardware en caso de ser necesario.
- Software, firmware y documento de actualizaciones

1.18 Duración del Servicio

Por tratarse de un documento de seguridad y para mantener la homogeneidad o igualdad, tanto en la impresión, como en las características técnicas que habrán de emplearse en la elaboración de la nueva Cédula de Identidad y Electoral y la Cédula de Identidad, el contrato para la producción será por el período de vigencia de la nueva Cédula de Identidad y Electoral y Cédula de Identidad, diez (10) años, por lo que cada Oferente propondrá su mejor programa de producción o entrega y la Junta Central Electoral evaluará en función de su máximo interés.

1.19 Lugar y Programa de Suministros

Los pedidos se librarán en el lugar designado por la JCE dentro del ámbito territorial de la República Dominicana y conforme al cronograma de entrega que se establezca. En caso de no especificarse, se entenderá que el lugar de entrega será la sede principal de la Junta Central Electoral.

1.20 Entregables del Proyecto

No.	Entregables	Descripción
		Licenciamiento perpetuo para:

1	**Licenciamiento perpetuo**	• Software SeguriServer:3 instancias x procesador y 1 instancia servidora • Software SeguriNotary:3 instancias x procesador y 1 instancia servidora • Software SeguriSign:3 instancias x procesador y 1 instancia servidora • Software Vertical de Firma:3 instancias por procesador y 1 instancia servidora • Software Portal de Certificación:3 instancias por procesador y 1 instancia servidora • API con soporte a PKCS#11
2	**Póliza de soporte técnico remoto 7x24 al software de la PKI**	Póliza de soporte técnico remoto 7x24 con vigencia por la duración del contrato y ampara a todos los componentes de software de la PKI.
3	**Póliza de mantenimiento al software de la PKI**	Póliza de mantenimiento para tener las versiones más recientes y en óptimas condiciones de los componentes de software de la PKI, durante la vigencia del contrato.
4	**Módulos criptográficos**	3 módulos criptográficos con las especificaciones del apartado 5.1.6 Descripción técnica de Módulo CryptoServer CR5 SE 500 de Utimaco. 2 módulos criptográficos con las especificaciones del apartado 5.1.7 Descripción técnica de Módulo CryptoServer CR5 SE 12 de Utimaco. 5 pólizas de mantenimiento Premium para los 5 equipos criptográficos durante la vigencia de la contratación.
5	**Instalación y configuración de la PKI de la JCE**	• Orden de Servicio firmada por el responsable del proyecto, con la descripción de las actividades realizadas en el servicio de instalación y configuración. • Memoria técnica con el detalle de la instalación y configuración de los

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

		componentes de la PKI, tanto los de software como los módulos criptográficos para los tres ambientes.
6	**Acompañamiento y Asistencia técnica a la Normatividad de la Autoridad Certificadora.**	• Script de creación de llaves de la Autoridad Certificadora de la JCE. • Plantillas para la generación de las Políticas de Certificación y Declaración de Prácticas de Certificación (CP y CPS según RFC 3647).
7	**Capacitación (Transferencia de conocimientos)**	• Autorización firmada por el responsable del proyecto, con la descripción de las actividades realizadas en el servicio. • Material de capacitación digital • Lista de asistencia del personal capacitado
8	**Acompañamiento y Asistencia técnica a la Integración.**	• Orden de Servicio firmada por el responsable del proyecto, con la descripción de las actividades realizadas en el servicio.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

1.21 Anexos a Solución PKI

1.21.1 Descripción técnica funcional de productos PKI

Descripción técnica autoridad certificadora (SeguriServer)

Software encargado de facilitar la administración del ciclo de vida de los certificados digitales, desde la emisión hasta la revocación de los certificados, para facilidad de operación SeguriServer cuenta con los siguientes componentes:

A. MÓDULO DE AUTORIDAD CERTIFICADORA

- Soporta su instalación en equipos con sistema operativo Microsoft Windows Server 2019 64 bits o superior.
- Cuenta con una consola gráfica de configuración para facilitar al administrador su operación y configuración.
- Puede establecer el puerto TCP de operación del servicio para comunicación de aplicaciones de acuerdo a las definiciones del contratante.
- Soporta los servidores de Base de Datos siguientes, para almacenamiento y administración de la información:
  - Microsoft SQL Server 2012 o superior
  - Oracle
- Cuenta con soporte para integración con el protocolo SMTP para comunicaciones con servidores de Correo Electrónico, para el envío de notificaciones de certificación.
- Permite la personalización del mensaje de notificaciones de correo electrónico de acuerdo a las necesidades de la institución.
- Soporta la emisión y administración ilimitada de Certificados Digitales.
- Soporta al menos 2 formatos de números de serie para los certificados digitales, secuenciales o extendidos.
- Cuenta con un módulo de auditoría de operaciones de la Autoridad Certificadora, este funciona a través de la emisión de recibos criptográficos (bajo el estándar RFC3161), garantizando la integridad de las operaciones y de la base de datos para todo el ciclo de vida de los certificados:
  - Emisión
  - Verificación de estado
  - Revocación
- Las transacciones entre la autoridad registradora, los servicios de validación y la autoridad certificadora están cifradas electrónicamente de

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

acuerdo a los algoritmos utilizados LFFEA para la generación de certificados en caso de requerirse.

- Soporta varios servicios de Autoridad Certificadora en el mismo equipo, cada servicio es independiente y puede configurarse individualmente.
- Soporta al menos 3 niveles de profundidad para la subordinación de autoridades.
- Proporciona escalabilidad en la infraestructura en cuanto a la capacidad de atención de múltiples transacciones simultáneas.
- Soporta su configuración en ambientes distribuidos como; clústeres y granjas, garantizando balanceo de cargas.
- Soporta ambientes en alta disponibilidad.
- Permite definir extensiones para los certificados digitales, tales como:

Netscape Certificate Type	TLS Web Client Authentication
SSL Client Authentication	Code Signing
SSL Server Authentication	Secure e-mail
S/MIME (Client)	Time Stamping
Object Signing	OCSP Signing
SSL CA	Microsoft Strong Encryption
S/MIME CA	Encrypting File System
Object Signing CA	Microsoft Smart Card Logon
Key Usage	Netscape Strong Encryption
Digital Signatura	Subject Alternative Names
Non repudiation	Issuer Alternative Names
Key Encipherment	Certificate Policies
Data Encipherment	URL
Key Agreement	Text
Cert Signing	CRL Distribution Point (CDP)
CRL Signing	URL
Encipher Only	Authority Info Access (AIA)
Decipher Only	URL
Enhanced Key Usage	LDAP / http Certificate address

- Soporta su implementación en ambientes virtualizados.
- Puede genera certificados cumpliendo con el RFC5280.
- Soporta la generación de llaves criptográficas RSA de 2048 bits recomendadas para usuarios o servicios.
- Soporta la generación de llaves criptográficas RSA de 4096 bits recomendadas para Autoridades Certificadoras
- Soporta la generación de llaves criptográficas ECC para emplearse con ECDSA, usando las curvas estándar P-224, P-256, P-384 y P-521, recomendadas por NIST.

- Permite emitir extensiones en certificados X.509 para hacer posible la conversión a certificados EDIFACT. Los certificados EDIFACT cumplen con las Guías de implantación mexicanas para seguridad EDIFACT normada por AMECE en los documentos:
  - Servicio de Autenticación de Origen, Integridad y No Repudiación de Origen.
  - Llave de Seguridad y Manejo de Certificado (KEYMAN).
  - Documentos basados en el ISO 9735-5 e ISO 9735-9 respectivamente
- Cuenta con un módulo de conversión de archivos PKCS#12.
- Registra y mantiene bitácoras que permiten el monitoreo de los servicios.
- Soporta en sus diferentes operaciones al menos los siguientes estándares o algoritmos criptográficos:

X.509 V1 y V3 - IETF RFC 3280	PKCS#5
FIPS 140 V2 N3.	PKCS#10
PKCS	PKCS#11
PKCS#1(RSA)	PKCS#12
LDAP	PKCS#5
CRL (RFC 3280, X.509)	SHA256
OCSP (RFC 2560)	SHA512

- Integra y ofrece la funcionalidad para verificar el estado de revocación de un certificado digital, ofreciendo:
- Módulo servidor OCSP para la verificación en línea del estado de revocación de un certificado digital.
- Módulo para la generación automática periódica de la Lista de Certificados Revocados (CRL).
- Garantiza una disponibilidad del 99% en el servicio de consulta del estatus de los certificados digitales a través de OCSP o CRL en condiciones normales.
- Considera un tiempo de indisponibilidad máximo de 4 horas en caso de desastre para los servicios de revocación y un tiempo máximo de 2 horas para los servicios de consulta de estatus (CRL u OCSP).

B. MÓDULO DE LLAMADAS EXTERNAS

- La solución cuenta con un módulo que permite agregar funcionalidad mediante llamadas a una librería dinámica que exporte funciones de acuerdo a una interfaz específica.
- El uso de la librería específica se puede configurar en la interfaz de configuración de la Autoridad Certificadora.
- Las llamadas podrán realizarse al momento de emitir, revocar un certificado digital o en ambos casos.

C. MÓDULO DE HARWARE CRIPTOGRÁFICO

- Compatibilidad para interactuar con dispositivos de hardware criptográficos que cuenten con la certificación FIPS-140-2 Nivel 3 en modalidad de conexión USB, PCI o red.
- Considerando las características de los módulos de hardware criptográfico para el resguardo de las llaves de la Autoridad Certificadora, especificadas en la sección de requerimientos mínimos y funcionales del Anexo Técnico al cual atiende esta propuesta técnica.
- La comunicación a los dispositivos criptográficos es a través del protocolo PKCS#11.
- Cuenta con los mecanismos necesarios para soportar un esquema de custodios para el acceso al dispositivo.

D. MÓDULO DE ADMINISTRACIÓN

- Cuenta con una consola de administración que ofrece la siguiente funcionalidad:
  - Administración de Autoridades Certificadoras subordinadas
  - Administración de Autoridades Registradoras
  - Autorización de emisión de Certificados Digitales.
  - Solicitud de revocación de Certificados Digitales.
  - Solicitud de CRL's.
  - Búsqueda de Certificados Digitales.
  - Soporta diferentes modelos de autenticación (login) del usuario soportando autenticación por software y a través de dispositivos criptográficos.
  - Al momento de aprobar la emisión de un Certificado Digital permite especificar las fechas (día) de inicio y expiración usando un calendario.

E. MÓDULO DE AUTORIDAD REGISTRADORA

- Soporta su instalación en un equipo con sistema operativo Microsoft Windows 10, Microsoft Windows Server 2016 64 bits o superior.
- Cuenta con una consola a través de la cual se pueden ejecutar las siguientes operaciones:
  - Autorización de emisión de Certificados Digitales.
  - Solicitud de revocación de Certificados Digitales.
  - Solicitud de CRL's.
  - Búsqueda de Certificados Digitales.
  - Búsqueda de Requerimientos de Certificación (Generación Web).

- Soporta la autenticación al módulo mediante certificados digitales.
- Al momento de aprobar la emisión de un Certificado Digital permite especificar las fechas (día) de inicio y expiración usando un calendario.

F. INTEFAZ WEB

- Cuenta con una aplicación de tipo Web donde se ofrecen servicios a los usuarios, estos servicios son:
  - Generación de llaves y Requerimiento de Certificación con soporte de múltiples CSP (Cryptographic Service Provider), para resguardar la llave en dispositivos criptográficos vía Web, además de su envío a la Autoridad Certificadora.
  - La generación de llaves no depende de tecnologías propietarias, ejemplo, ActiveX o Applets, es decir, es independiente del navegador web, soporta al menos equipos Windows 7, 8, 10 y Mac (Yosemite, Catalina).
  - Soporta clientes con sistemas operativos Microsoft Windows XP, Microsoft Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 10 Microsoft Windows Server 64 bits o superior.
  - Envío a la Autoridad Certificadora del Requerimiento de Certificación a partir de archivo en formato PKCS#10.
  - Instalación de Certificados Digitales.
  - Consulta de Certificados Digitales y opción a descarga de los mismos.
  - Solicitud y descarga de una CRL.
  - Solicitud y descarga del Certificado Digital de Autoridad Certificadora.
  - Revocación de Certificados Digitales a partir de una clave de revocación.
  - Revocación de Certificados Digitales a partir de su autenticación al servidor Web utilizando SSL con autenticación de usuarios.
  - La aplicación Web permite la modificación de la interface gráfica de acuerdo a la imagen de la institución.
  - La aplicación de generación de llaves e instalación de certificados digitales soporta el uso de tarjetas inteligentes o dispositivos criptográficos.
  - La aplicación Web soporta su implementación en sistemas operativos tanto Windows como UNIX.
  - Funcionamiento del portal bajo protocolo seguro de comunicación HTTPS.

G. INTERFAZ DE DESARROLLO

- Cuenta con herramientas y servicios que permiten su integración a aplicaciones propietarias o de terceros, que soportan los sistemas operativos:
  - Microsoft Windows 10, Microsoft Windows Server 2016 64 bits of superior.
  - UNIX (Solaris, Red Hat, AIX)
- Cuenta con API's con base en lenguajes de programación "C" y "Java", que provean las siguientes funcionalidades:
  - Emisión de Certificados Digitales.
  - Consulta de Certificados Digitales.
  - Revocación de Certificados Digitales.
  - Consulta de CRL's.

H. MÓDULO OCSP RESPONDER

- Trabaja bajo el protocolo OCSP (RFC 2560).
- Soporta su instalación en un equipo con sistema operativo Microsoft Windows Server 2012 o superior.
- Permite configurar los tres esquemas de validación definidos por el RFC 2560:
  - AC que emitió el certificado en cuestión (Issuer CA).
  - Un respondedor confiable para el solicitante (Trusted Responder).
  - Un respondedor autorizado por la AC (Authorized Responder)
- Responde a paquetes con múltiples certificados (emitidos por la misma autoridad).
- Cuenta con API's que permiten generar las peticiones hacia el servicio para la validación de estatus.
- Cuenta con un cliente gráfico que permita realizar consultas por certificados específicos.
- Permite su operación y configuración en sistemas distribuidos como clústeres o granjas para garantizar balanceo de cargas o alta disponibilidad.
- Soporta su implementación en ambientes virtualizados.
- Cuenta con una consola de configuración donde se establecen:
  - Autoridades Certificadoras de Confianza y su configuración.
  - Par de llaves para operación del servicio.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

- Permite establecer el puerto TCP de operación del servicio para comunicación de aplicaciones de acuerdo a las definiciones del cliente
- Permite la administración del servicio, el poder iniciarlo y detenerlo.
- Permite registrar servicios OCSP de cualquier Autoridad Certificadora.
- Permite su configuración como OCSP intermediario que sirve como punto único de contacto para facilitar la integración de los componentes de PKI en arquitecturas de más de una Autoridad Certificadora.
-

I. CONSIDERACIONES GENERALES

- Los componentes de la autoridad certificadora son modulares y permiten crear entornos distribuidos para cualquier tipo de configuración.
- Las características de sus componentes permiten configurar entornos de balanceo de carga en modalidad activo-activo.
- La modularidad de la aplicación permite establecer políticas restrictivas entre servidores.
- La fecha y hora de emisión d ellos certificados son obtenidos directamente de los equipos en donde se ejecutan las consolas de agente o administrador.
- Tiene la capacidad de crear diversas Autoridades Certificadoras cada una con parámetros de operación independientes.
- Tiene la capacidad de crear una o más Entidades Registradoras por Autoridad Certificadora.
- Tiene la definición paramétrica de perfiles para la ejecución de funciones de administración, agentes registradores y agentes certificadores.
- Tiene la capacidad para definir de forma paramétrica la asignación de extensiones a ser aplicados a certificados digitales.
- Puede generar correos electrónicos paramétricos para notificación a solicitantes de certificados digitales.
- Puede generar correos electrónicos paramétricos para notificación a administradores de la Autoridad Certificadora y Registradora.
- Tiene definición paramétrica de reglas para publicación de certificados digitales.
- Da cumplimiento a lineamientos establecidos por entidades reguladoras, tales como: SAT, SE, Banxico.

J. LA GENERACIÓN DE CERTIFCADOS DIGITALES X.509

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

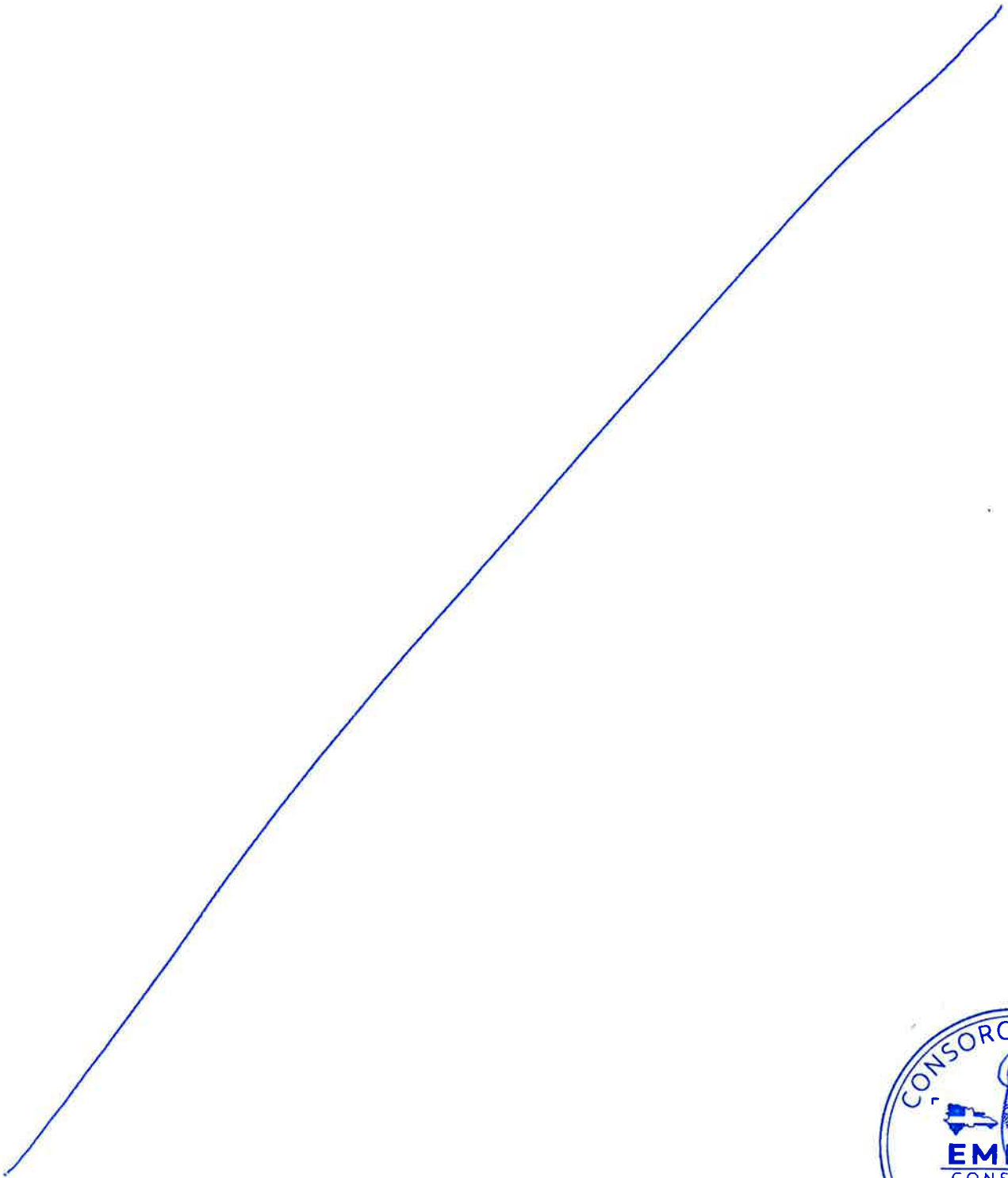
- Soporta los siguientes estándares o algoritmos criptográficos en su operación:
  - X.509 – (RFC 3280)
  - En las siguientes versiones del certificado X.509 V1, V2 y V3.

1. Versión	V3
2. Serial Number	Número secuencial del Certificado Digital emitido por la AC.
3. Signature Algorithm	SHA256withRSAEncryption SHA1withRSAEncryption
4. Issuer Distinguished Name	CN=AC DNIE XXX OU=SEGOB O= DGRNPIP C=MX S=DF
5. Validity	Not Before: Jul 1 16:04:02 2008 GMT Not After: Dec 31 16:04:02 2010 GMT
6. Subject	CN=APELLIDO1 APELLIDO2, NOMBRE(S) G=NOMBRE SN= FECHA DE NACIMIENTO C= MX
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 1024 bits

- Anexo V2

1. issuerUniqueIdentifier	RFC
2. subjectUniqueIdentifier	CURP

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD



CONSORCIO EMDOC
EMDOC CONSORCIO
Santo Domingo, R.D.

1.21.2 Descripción técnica de Autoridad Emisora de Estampas de Tiempo (TSA - SeguriNotary)

Software encargado de emitir acuses de recibo permitiendo demostrar la existencia de la información en un tiempo determinado.

A. MÓDULO DE ADMINITRACIÓN DE ESTAMPILLAS ELECTRÓNICAS

- Plataforma sistema operativo Microsoft Windows Server 2016 64 bits o superior.
- Módulo de consola gráfica de configuración para facilitar al administrador su operación y configuración.
- Operación y comunicación del servicio basada en TCP.
- Operación con base de datos:
  - Microsoft SQL Server 2016 o superior
  - Oracle
  - IBM DB2
- Soporta múltiples servicios de Autoridad de Estampillas de Tiempo independientes en el mismo equipo.
- Infraestructura escalable soportando múltiples transacciones simultáneas.
- Garantiza la integridad de los sellos de tiempo, es decir, tiene mecanismos criptográficos que permiten validar que el sello no ha sido alterado.
- Garantiza que la información que resguarda los sellos de tiempo, incluidas los mecanismos criptográficos de validación, pueda ser auditada para determinar su integridad, es decir, verifica que no se produzca alguna modificación en la información, de tal manera que puede reportarse en una auditoría todos aquellos registros que han sufrido alteración.
- Genera Estampillas de Tiempo de Acuerdo al protocolo TSP (RFC 3161).
- Cuando se cuenta con un PKCS#7, elservicio puede entregar como resultado un CAdES-A que tiene insertado un sello de tiempo de archivado (ATSv3) según el estándar ETSI TS 101 733 v2.2.1 sobre documentos CAdES-BES/EPES/T/XLong/XL T1/XL T2/A.
- El cliente mencionado en el numeral anterior también permite procesar un documento XML-Sig como entrada y la salida en este caso es un sello de archivado para XAdES según el estándar ETSI TS 103 171 v2.1.1, para ser embebidas en archivos XAdES-LT.
- Módulo de auditoría automático para operaciones de Autoridad de Estampillas de Tiempo, garantizando la integridad de los recibos emitidos mediante el cifrado electrónico de los registros de base de datos.
- Soporta su implementación en ambientes virtualizados.
- Soporta operación en alta disponibilidad en arquitectura tipo Clúster.

- Servicios web tipo REST con soporte mandatorio a TLSv1.2.
- Comunicación de servicios web bajo protocolo seguro de comunicación HTTPS.
- El sello digital de tiempo está compuesto por los siguientes elementos básicos:
    - Datos sobre la identidad de la autoridad emisora (identidad jurídica, clave pública a utilizar en la verificación del sello, numero de bits de la clave, el algoritmo de cifrado digital y la función hash utilizada).
    - Tipo de solicitud cursada (si es un valor hash o un documento).
    - Parámetros del secuenciador (valor hash de la transacción consecutiva).
    - Fechas utilizadas en formato Internet date / time UTC (AAMMDDhhmmss).
    - Evidencias criptográficas de todo lo anterior con la clave pública y esquema de cifrado digital.
- Estándares o algoritmos criptográficos soportados:

RSA	SHA256
PKCS	SHA384
X.509 - IETF RFC 3280	SHA512
PKCS#5	MD5
SHA1	TSP – IETF RFC 3161
SHA224	

B. MÓDULO DE ADMINISTRACIÓN

- Plataforma con sistema operativo Microsoft Windows Server 2016 o superior. Operaciones soportadas para las pistas de auditoría sobre transacciones registradas:
    - Consulta.
    - Extracción de información.
    - Generación de reportes.

C. INTERFAZ DE DESARROLLO

- Plataforma con sistema operativo:
    - Microsoft Windows Server 2019 64 bits ó superior
    - UNIX (Solaris, Red Hat, AIX, Suse)
- Herramientas y servicios para desarrolladores para integración de funcionalidad en aplicaciones propietarias o de terceros.
- API's basados en lenguajes de programación "C", y "Java", proporcionando funciones de:

CONSORCIO EMDOC Santo Domingo, RD

- Solicitud de generación de estampillas de tiempo
- Autenticación de estampillas de tiempo.

1.21.3 Descripción técnica de Motor de Firma Electrónica (SeguriSign)

Software de firma o de criptografía asimétrica SeguriSign que provee múltiples servicios que permiten a una aplicación de terceros realizar el registro, autentificación y generación de evidencias criptográficas para conformar documentos cifrados electrónicamente, auto auditables y con resguardo de evidencias criptográficas que incluyan sellos digitales de tiempo.

A. MÓDULO DE ADMINISTRACIÓN Y AUTENTICACIÓN DE EVIDENCIAS CRIPTOGRÁFICAS

- Soporta su instalación en equipos con sistema operativo Microsoft Windows Server 2019 64 bits o superior.
- Esta bajo la categoría software como servicio (SaaS, del inglés Software as Service).
- Proporciona escalabilidad en la infraestructura en cuanto a la capacidad de atención de múltiples transacciones simultáneas.
- Soporta su instalación y operación en sistemas distribuidos como Clústeres y Granjas para garantizar el balanceo de cargas.
- Soporta su implementación en ambientes de alta disponibilidad.
- Soporta su implementación en ambientes virtualizados.
- Soporta el uso de varios servicios de autenticación de evidencias criptográficas en el mismo equipo, cada servicio deberá administrarse de manera independiente.
- Cuenta con una consola gráfica de configuración para facilitar al administrador su operación.
- Permite establecer el puerto TCP de operación del servicio, para comunicación de aplicaciones de acuerdo a las definiciones del cliente.
- Soporta los siguientes servidores de Base de Datos para almacenamiento y administración de la información.
  - Microsoft SQL Server 2016 o superior
  - Oracle
- Permite la verificación del estado de revocación de un Certificado Digital, conectándose a un Servidor OCSP y a través de una lista CRL.
- Permite la integración a una Autoridad de Estampillas de Tiempo para la generación de las mismas (bajo el estándar RFC 3161).
- Permite la operación con al menos 2 Autoridades Certificadoras de Confianza.

- Permite la interoperabilidad con los módulos para la solicitud de cadenas de certificados y validación del estatus de revocación.
- Permite la solicitud y almacenamiento de constancias de la NOM151 para la conservación de mensajes de datos.
- Soporta al menos los siguientes estándares o algoritmos criptográficos para su operación:

X.509 – (RFC 3280)	ECDSA/P-256
PKCS # 1 (RFC8017).	ECDSA/P-384
PKCS#5 (RFC2898)	ECDSA/P-521
CMS (RFC 5652)	OCSP (RFC 2560)
PKCS#12 (RFC7992)	CRL (RFC 3280)
PKCS#15	TSP (RFC 3161)
RSA/SHA1	PDF Signature ISO 32000-1.
RSA/SHA256	LDAP
RSA/SHA512	
ECDSA/P-224	

- Puede almacenar las evidencias criptográficas con contenido y sin contenido de los documentos y transacciones.
- El archivo cifrado electrónicamente es independiente del equipo de cómputo dónde se realiza la transacción de cifrado o del sistema operativo del cual se intercambia el documento.
- Soporta el formato CAdES, así como el formato PAdES.
- Soporta la comprobación de las evidencias criptográficas a través de cualquier visor PDF con soporte para el estándar ISO 32000-1.
- Soporta el uso de llaves criptográficas en formato PKCS#12, al igual que en formato .cer y .key.
- Ofrece los componentes tipo API y Servicios Web que permiten consumir en aplicaciones de terceros la funcionalidad para validar los certificados y generar estampillas de tiempo con la finalidad de conformar documentos encriptados electrónicamente bajo el estándar PDF Signature.
- La plataforma puede integrarse a cualquier sistema que pueda utilizar o consumir Servicios Web.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

- Los servicios para PDF Signature, pueden ejecutarse lo mismo desde una computadora de escritorio, así como desde un teléfono inteligente o tableta con sistema operativo iOS o Android en sus versiones más recientes.
- Cuenta con un Portal Web disponible para generar múltiples flujos que permita obtener las evidencias criptográficas de los firmantes de un documento electrónico en particular (firmantes, destinatarios, fecha de expiración de proceso de firma e incluir notas).
- El Portal Web cuenta con la capacidad para poder utilizar distintos dispositivos criptográficos que resguarden la llave privada del usuario.
- El Portal Web cuenta con un control de acceso a través de autenticación de certificado digital.
- Funcionamiento del portal bajo protocolo seguro de comunicación HTTPS.
- El Portal web de gestión del ciclo de vida de los certificados digitales (emisión y revocación) que se emitirán a la ciudadania y que se podrán almacenar en las cédulas de identidad, como una solución web con granuralidad en los permisos o dicho de otro modo, control de acceso. Asi como poder realizar consultas o reportes de los certificados. 1
- El portal web de la gestión del ciclo de vida de los certificados, se brinda para el personal de la JCE.
- Para ingresar al portal web cada usuario debe tener un certificado de autenticación.

B. VALIDACIONES DE EVIDENCIAS CRIPTOGRÁFICAS BAJO EL ESTÁNDA PDF SIGNATURE

- Al abrir un archivo con evidencias criptográficas a través de un visor PDF soporta el estándar ISO 32000-1, se puede comprobar lo siguiente:
  - Que se cumpla con la integridad de la información cifrada.
  - La validez de los certificados implicados.
  - Que el certificado de firma ha sido emitido por la Autoridad Certificadora aceptada como de confianza.
  - Verificar de forma automática la integridad y autenticidad del documento sin necesidad de abrirlo con un visor PDF.
- Un documento firmado bajo el estándar PDF Signature, contiene las siguientes evidencias criptográficas:
  - Respuesta OCSP del certificado del firmante.
  - Sello digital de tiempo.
  - Certificado del firmante.
  - Certificado de la Autoridad Certificadora emisora del firmante.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

- Certificado de la Autoridad Emisora de Estampillas de Tiempo que emite el sello digital de tiempo.
- CMS (del inglés Cryptographic Message Syntax) embebido en el PDF Signature

- Soporte a Long Term Validation (LTV) acorde a las condiciones de operación.

C. COMPONENTES CLIENTE

- Componente de firma en cliente para navegadores web.
  - No depende de tecnologías propietarias como Applet o ActiveX.
  - No requiere instalarse nada en el equipo cliente.
  - Soporta su operación con Sistema Operativo Windows XP o superior.
  - Soporta su operación con Navegadores Web 32 o 64 bits:
    - Microsoft Internet Explorer 11 o superior.
    - Mozilla Firefox 37 o superior.
    - Google Chrome Versión 37 o superior.
    - Safari versión 7.1 o superior.
- Brinda servicios criptográficos mediante alguna de las siguientes tecnologías.
  - WCAPI
  - Apple Key Chain
- Librerías propietarias de encripción y servicios criptográficos.

D. MÓDULO DE ADMINISTRACIÓN

- Cuenta con un módulo a través del cual se haga la administración de las transacciones.
- Permite la consulta y extracción de información.
- Permite la generación de reportes de acuerdo a las transacciones procesadas.
- Registra y mantiene bitácoras que permiten el monitoreo de los servicios.

E. INTERFAZ DE DESARROLLO

- Cuenta con herramientas y servicios que permiten su integración a aplicaciones propietarias o de terceros, soporta su operación en sistemas operativos tanto Microsoft Windows como UNIX.
- Soporte mandatorio a enlace seguro vía TLSv1.2.
- Cuenta con API's basados en lenguajes de programación "C", "Java" y "C#", así como, Servicios Web ofreciendo la siguiente funcionalidad:
  - Autenticación de una operación criptográfica ante el motor de firma.
  - Recuperación del documento original relacionado a partir de un número de secuencia.

CONSORCIO EMDOC CONSORCIO Santo Domingo, R.D

- Retorno de evidencia criptográfica especificada, a partir de un número de secuencia.
- Solicitud de inicio de un proceso de firma multilateral.
- Autenticación de un mensaje criptográfico perteneciente a un proceso de firma multilateral.
- Estatus de un proceso de firma multilateral.
- Solicitud de digestión a firmar para un proceso de firma PDF.
- Solicitud de digestión a firmar para un proceso de firma PDF incluyendo una imagen de la firma digital del usuario.
- Solicitud de digestión a firmar para un proceso de firma PDF e incluyendo una imagen y la biometría asociada al trazo de la firma
- Finalización y obtención de constancia NOM-151 de un proceso de firma multilateral.
- Verificación de la información parametrizada corresponde al proceso de firma indicado por un identificador.
- Validación y registro de paquetes CMS firmado y con contenido.

1.21.4 Descripción técnica de Módulo CryptoServer CP5 SE 500 de Utimaco

El Utimaco CryptoServer CP5 brinda soporte a los Trusted SErvice Providers (TSPs) en el cumplimiento de los requisitos de política y seguridad definidos en varios estándares técnicos de ETSI (ETSI EN 319 401, EN 319 411, EN 319 421). Gracias a sus funcionalidades avanzadas de autorización de claves, es ideal para la creación de firmas cualificadas conforme a eIDAS y para la firma remota. Otras aplicaciones incluyen la emisión de certificados (cualificados), OCSP (Online Certificate Status Protocol) y sellado de tiempo.

El CryptoServer CP5 se basa en la plataforma de hardware CryptoServer Se Gen2 y cuenta con certificación Common Criteria de acuerdo con el Perfil de Protección (PP) eIDAS EN 419 221-5 para módulos criptográficos en servicios de confianza.

Dentro de sus principales características se encuentran:

- Ideal para aplicaciones con requerimientos de alto o bajo performance
- Administración remota extensa
- Gestión eficiente de claves y actualizaciones de firmware a través de acceso remoto.
- Automatización del diagnóstico remoto mediante SNMP (Simple Network Management Protocol).
- Simulador de software dedicado para evaluación y pruebas de integración

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

Especificaciones técnicas

Algoritmos criptográficos soportados (incluida la implementación completa de NIST Suite B)
• RSA, ECDSA with NIST and Brainpool curves • ECDH with NIST and Brainpool curves • AES • CMAC, HMAC • SHA2-Family, SHA3 • Hash-based deterministic random number generator (DRG.4 acc. AIS 31) • True random number generator (PTG.2 acc. AIS 31) • Up to 3,000 RSA or 2,500 ECDSA signing operations in bulk processing mode
Plataformas soportadas
• Los sistemas operativos Windows y Linux incluyen la distribución de RedHat, SUSE y los principales proveedores de servicios de la nube que funcionan como máquinas virtuales o en contenedores
Interfaces de programación de aplicaciones (API)
• PKCS#11 • Cryptography Next Generation (CNG) • Cryptographic eXtended services Interface (CXI) – La interface de alto rendimiento de Utimacoasegura una integración fácil de las funcionalidades criptográficas con las aplicaciones del cliente
Conectividad de servidor
• Puertos duales Gigabit Ethernet (dos segmentos de red)
Cumplimiento con la seguridad
• IEC/EN 60950-1, IEC/EN 62368-1, UL, • CB Certificate, CE, FCC Class B • Security: FIPS 140-2 Level 3
Conformidad de los estándares de seguridad y medioambientales
• RoHS III, WEEE

Alta disponibilidad
• Almacenamiento sólido • Bandeja de campo, fuentes de administración intercambiables dobles
Administración supervisión
• Configuración remota • Registro de auditoría seguro. • Soporte de diagnóstico Syslog • Agente de supervisión SNMP.
Características físicas
• Dimensiones de bastidor estándar 1U 19 pulgadas: 44 x 446 x 533.4 mm • Peso: 10 kg • Voltaje de entrada: 100-240 V AC cambio automático 50-60 Hz • Consumo de potencia: 45W / 66 VA max 50W / 70 VA • Disipación del calor: 171 BTU/hora (carga completa)

Rendimiento disponible

Modelo CryptoServer CP5	**SE 500**
Rendimiento de firma RSA para longitudes de clave recomendadas por NIST	
2048 bits	800 transacciones por segundo
4096 bits	100 transacciones por segundo
Rendimiento de firma ECDSA principal para las longitudes de clave recomendadas NIST	
secp256r1	1,600 transacciones por segundo
brainpoolP256r1	1,100 transacciones por segundo
Licencias para cliente	
Incluido	2 clientes

En caso de requerir conectar más servidores se deben contratar licencias clientes adicionales

1.21.5 Descripción técnica de Módulo CryptoServer CP5 SE 12 de Utimaco

El Utimaco CryptoServer CP5 brinda soporte a los Trusted SErvice Providers (TSPs) en el cumplimiento de los requisitos de política y seguridad definidos en varios estándares técnicos de ETSI (ETSI EN 319 401, EN 319 411, EN 319 421). Gracias a sus funcionalidades avanzadas de autorización de claves, es ideal para la creación de firmas cualificadas conforme a eIDAS y para la firma remota. Otras aplicaciones incluyen la emisión de certificados (cualificados), OCSP (Online Certificate Status Protocol) y sellado de tiempo.

El CryptoServer CP5 se basa en la plataforma de hardware CryptoServer Se Gen2 y cuenta con certificación Common Criteria de acuerdo con el Perfil de Protección (PP) eIDAS EN 419 221-5 para módulos criptográficos en servicios de confianza.

Dentro de sus principales características se encuentran:

- Ideal para aplicaciones con requerimientos de alto o bajo performance
- Administración remota extensa
- Gestión eficiente de claves y actualizaciones de firmware a través de acceso remoto.
- Automatización del diagnóstico remoto mediante SNMP (Simple Network Management Protocol).
- Simulador de software dedicado para evaluación y pruebas de integración

Compatible con la generación de claves fuera de línea y los entornos de desarrollo, a la vez que ofrece soporte completo a los algoritmos y las API.

Especificaciones técnicas

Algoritmos criptográficos soportados (incluida la implementación completa de NIST Suite B)
• RSA, ECDSA with NIST and Brainpool curves • ECDH with NIST and Brainpool curves • AES • CMAC, HMAC • SHA2-Family, SHA3 • Hash-based deterministic random number generator (DRG.4 acc. AIS 31)

• True random number generator (PTG.2 acc. AIS 31) • Up to 3,000 RSA or 2,500 ECDSA signing operations in bulk processing mode
Plataformas soportadas
• Los sistemas operativos Windows y Linux incluyen la distribución de RedHat, SUSE y los principales proveedores de servicios de la nube que funcionan como máquinas virtuales o en contenedores
Interfaces de programación de aplicaciones (API)
• PKCS#11 • Cryptography Next Generation (CNG) • Cryptographic eXtended services Interface (CXI) – La interface de alto rendimiento de Utimacoasegura una integración fácil de las funcionalidades criptográficas con las aplicaciones del cliente
Conectividad de servidor
• Puertos duales Gigabit Ethernet (dos segmentos de red)
Cumplimiento con la seguridad
• IEC/EN 60950-1, IEC/EN 62368-1, UL, • CB Certificate, CE, FCC Class B • Security: FIPS 140-2 Level 3
Conformidad de los estándares de seguridad y medioambientales
• RoHS III, WEEE
Alta disponibilidad
• Almacenamiento sólido • Bandeja de campo, fuentes de administración intercambiables dobles
Administración supervisión
• Configuración remota • Registro de auditoría seguro. • Soporte de diagnóstico Syslog • Agente de supervisión SNMP.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

Características físicas
• Dimensiones de bastidor estándar 1U 19 pulgadas: 44 x 446 x 533.4 mm • Peso: 10 kg • Voltaje de entrada: 100-240 V AC cambio automático 50-60 Hz • Consumo de potencia: 45W / 66 VA max 50W / 70 VA • Disipación del calor: 171 BTU/hora (carga completa)

Rendimiento disponible

Modelo CryptoServer CP5	**SE 12**
Rendimiento de firma RSA para longitudes de clave recomendadas por NIST	
2048 bits	16 transacciones por segundo
4096 bits	2 transacciones por segundo
Rendimiento de firma ECDSA principal para las longitudes de clave recomendadas NIST	
secp256r1	120 transacciones por segundo
brainpoolP256r1	110 transacciones por segundo

En caso de requerir conectar más servidores se deben contratar licencias clientes adicionales

CONSORCIO EMDOC Santo Domingo, R.D

2. Especificaciones de la (PKI) para la emisión de la identidad física y digital (CI/CIE)

Nuestra propuesta incluye la implantación de una infraestructura de llave pública (PKI), conforme a las especificaciones de la OACI establecidas en el Doc 9303 vigente, para emitir y revocar certificados digitales que se utilizarán para firmar electrónicamente las tarjetas electrónicas (CSCA) y para verificar tarjetas electrónicas (CVCA). La infraestructura de llave publica que describimos en esta sección será utilizada para la emitir los certificados y firmar digitalmente las identidades digitales, y poder asegurar el ciclo de vida de los certificados y las verificaciones de identidad que menciona el estándar ISO 18013-5, en cumplimiento al estándar ISO ISO 15408 (Nivel de Garantía de Evaluación de Criterios Comunes (EAL) 4+ o superior).

2.1 Especificaciones de la (PKI) para la emisión de la identidad física y digital (CI/CIE)

En esta sección procedemos a describir los componentes de la PKI necesarios para los sistemas de documentos de identidad electrónico y de la tarjeta de identificación digital:

- Tarjeta eID
  - Autenticación pasiva (PA) PKI
  - Control de acceso ampliado (EAC) PKI
  - PKI para digital
- Identificación móvil
  - ISO 18013-5 PKI

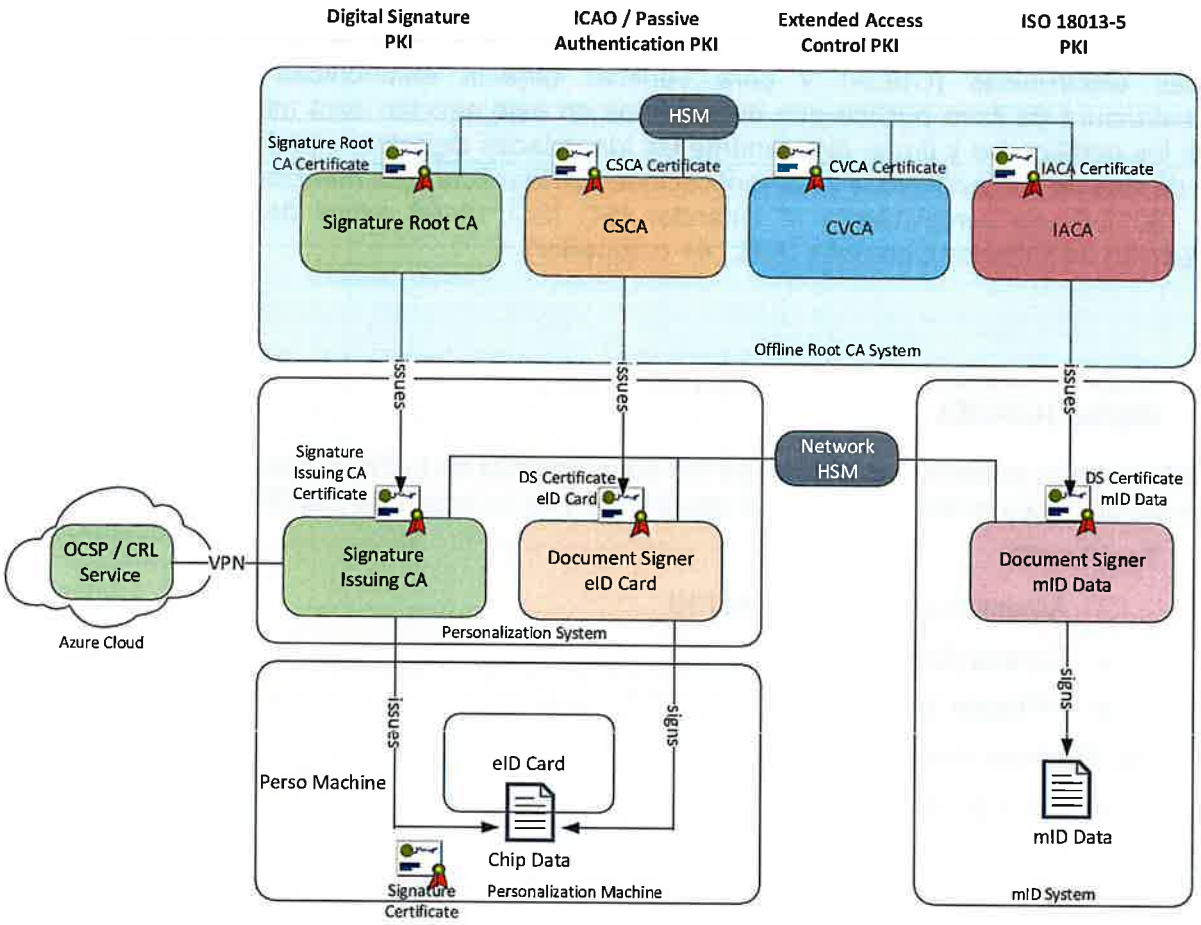


Figura1 : Visión general de la infraestructura PKI

2.2 Requisitos del sistema

El sistema propuesto soportará la personalización de documentos de identidad electrónicos y datos de identificación móviles aplicando los siguientes métodos de seguridad relacionados con la PKI:

1. Autenticación pasiva (PA)
2. Control de acceso ampliado (CAE)
3. Certificados para firmas digitales
4. ISO 18013-5 PKI

La autenticación pasiva (PA) garantiza la autenticidad e integridad de los datos almacenados en el chip del documento de identidad electrónico. Garantiza que los datos del chip proceden de la autoridad emisora legítima y que los datos no han sido manipulados. La PKI para la autenticación pasiva (PA) cumple con las especificaciones de la OACI, descritas en el documento 9303-12 y también se conoce como PKI de la OACI. Los objetos de la PKI de PA (certificados, CRL, listas maestras) deben intercambiarse con otros Estados y cargarse en sus puestos de control fronterizo. Todos los certificados emitidos y gestionados de este sistema cumplen la norma X.509 v3.

El control de acceso ampliado (EAC) garantiza la autenticidad y confidencialidad de los datos biométricos almacenados en el chip. Garantiza que los datos biométricos sólo puedan ser leídos por un lector autorizado y que el chip sea auténtico. La PKI para el control de acceso ampliado debe cumplir la directriz técnica TR-03110 de la BSI. Ambos sistemas deben proporcionar interfaces normalizadas para interactuar con el sistema de personalización de tarjetas de identidad electrónica y otros sistemas.

Los certificados de **firma** digital permiten crear firmas digitales de confianza con la tarjeta eID. El material clave para el certificado de firma se generará durante la personalización de la tarjeta y se solicitará a la PKI central un certificado conforme a la norma X.509v3 que se escribirá en la tarjeta.

El **ISO 18013-5 PKI** garantiza la autenticidad y la integridad de las identidades móviles y de los datos de los permisos de conducir móviles (mDL). Garantiza que los datos proceden de la autoridad emisora legítima y que no han sido manipulados. La PKI debe cumplir la norma ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application.

2.3 Integración del sistema

2.3.1 Autenticación pasiva PKI

La autenticación pasiva se utiliza para garantizar la autenticidad de los datos del chip, que están estructurados en una estructura lógica de datos (LDS). Para la autenticación pasiva se necesita una autoridad de certificación de firma de país (CSCA) y un firmante de documentos (DS). La siguiente imagen muestra la vista lógica de los componentes necesarios.

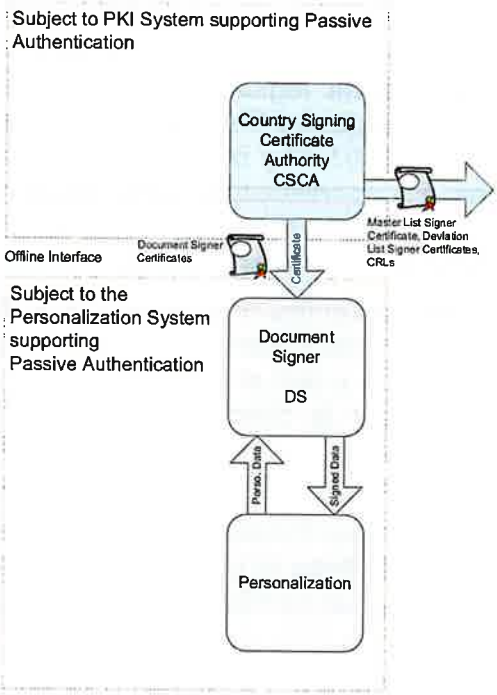


Figura2 : Infraestructura PKI para autenticación pasiva

2.3.2 Sistema PKI de control de acceso ampliado

El control de acceso ampliado (EAC) protege los datos biométricos almacenados en el chip frente a accesos no autorizados.

Las huellas dactilares se protegen mediante el protocolo EAC, tal como se especifica en BSI TR-03110 v1.11. EAC es un mecanismo de autenticación mutua basado en PKI asimétrica. Se utilizan certificados especiales verificables mediante tarjeta para definir los derechos de los terminales utilizados para la verificación de documentos.

Este sistema PKI comprende únicamente la CVCA. Al crear las claves y el certificado CVCA y escribir este anclaje de confianza en el chip, el sistema de tarjeta de identidad electrónica está preparado para su posterior ampliación mediante datos biométricos de huellas dactilares.

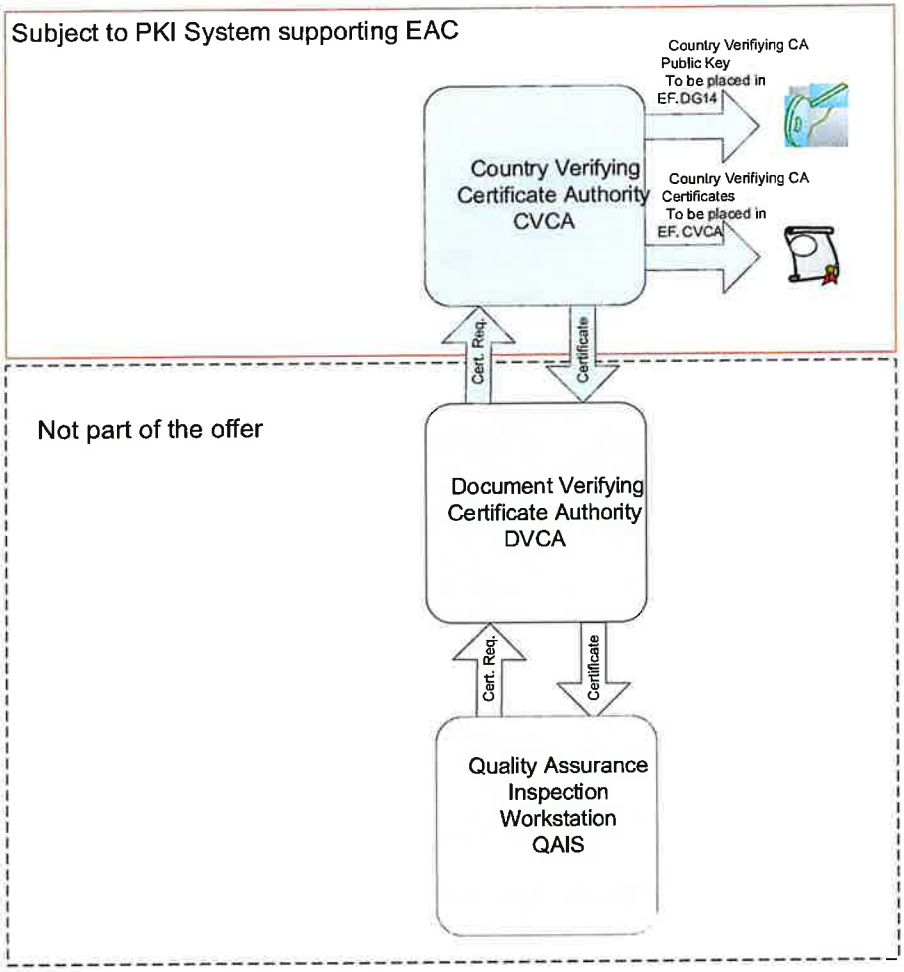


Figura3 : Infraestructura EAC para sistemas de personalización

2.3.3 Firma digital PKI

La PKI de firma digital se encarga de emitir certificados de firma para cada tarjeta eID personalizada. Los certificados están personalizados para el titular de la tarjeta. Éste puede utilizar el certificado y la clave de firma para crear firmas digitales fiables localmente en el ordenador personal o en otros dispositivos que admitan la integración del documento de identidad electrónico. La PKI consta de dos niveles: la CA raíz, que funciona fuera de línea, y la CA emisora, con conexión en línea al sistema de personalización del documento de identidad electrónico

El estado de cada certificado emitido es gestionado por el sistema CA y replicado al Certificate Status Server. A intervalos regulares se crean CRL que contienen los números de serie de todos los certificados revocados. También estas CRL se replican a este servidor. El servidor de estado de certificados publica la información a través del protocolo OCSP (Online Certificate Status Protocol) y mediante la descarga de CRL. El

Servidor de Estado de Certificados está alojado en un sistema en la nube proporcionado por el Cliente.

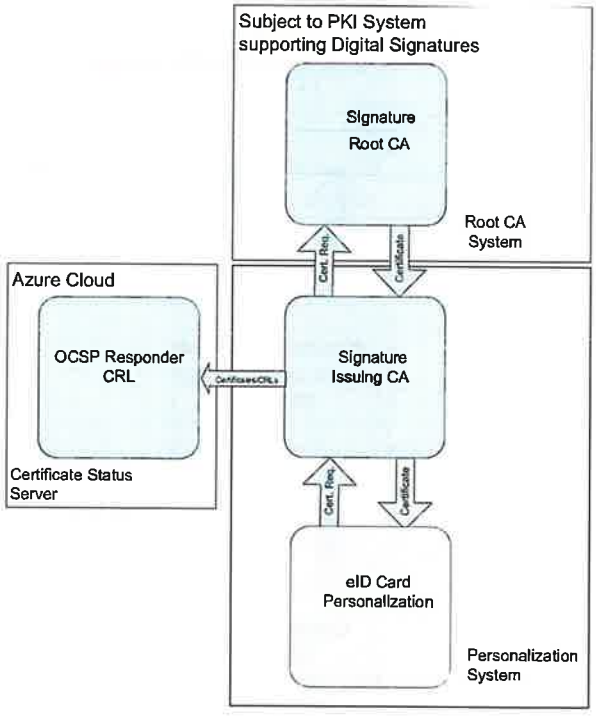


Figura4 : PKI de firma para sistemas de personalización

2.3.4 ISO 18013-5 PKI

La PKI ISO es muy similar a la PKI de autenticación pasiva. Se utiliza para garantizar la autenticidad de los datos de identidad móviles. Consta de una Autoridad Emisora Autoridad de Certificación (IACA) y un Firmante de Documentos (DS). La siguiente imagen muestra la vista lógica de los componentes necesarios.

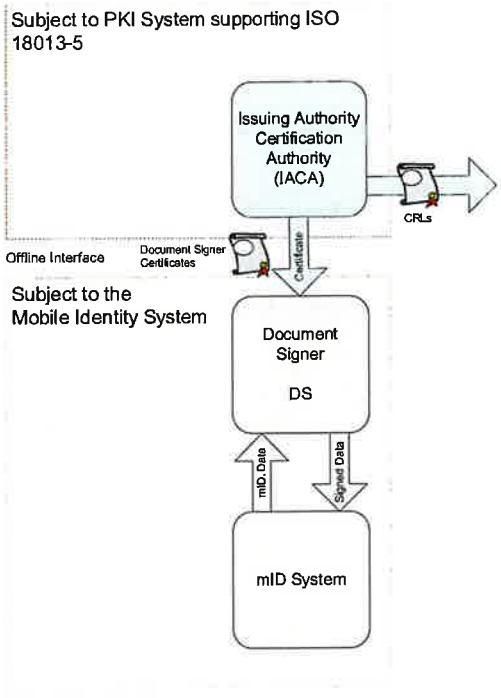


Figura5 : Infraestructura PKI para ISO PKI

2.4 Interfaces del sistema

2.4.1 Autoridad de certificación con firma de país (CSCA)

El CSCA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

1. Archivos de solicitud de certificado en formato PKCS#10
2. Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
3. Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

2.4.2 Autoridad de certificación verificadora de países (CVCA)

El CSCA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

1. Archivos de solicitud de certificado en formato PKCS#10
2. Ficheros de certificados según la norma ISO 7816 - 8 (Certificados verificables mediante tarjeta)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

2.4.3 Firma digital PKI

Firma CA raíz

La CA Raíz de Firma funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

1. Archivos de solicitud de certificado en formato PKCS#10
2. Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
3. Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

Firma CA emisora

La CA emisora de firmas funciona en línea. Las interfaces con otros sistemas se basan en la web (REST API):

- Solicitud de certificados
- Ficheros de certificados
- Lista de revocación de certificados (CRL) según X509v3
- Información sobre el estado del certificado

Servidor de estado de certificados

El servidor de estado de certificados funciona en un servicio en la nube. Proporciona una interfaz de importación a la CA emisora para obtener información de estado y CRL y publica la información en Internet:

1. Importación de información sobre el estado de los certificados
2. Respuestas OCSP a través de http
3. Descarga de CRL a través de http

2.4.4 Autoridad emisora Autoridad de certificación (IACA)

La IACA funciona sin conexión. Todas las interfaces con otros sistemas se basan en archivos:

1. Archivos de solicitud de certificado en formato PKCS#10
2. Archivos de certificado según X509v3 en formato binario DER o ASCII PEM
3. Archivos de listas de revocación de certificados (CRL) según X509v3 en formato DER binario

2.5 Funcionalidad

2.5.1 Autoridad de certificación con firma de país (CSCA)

De acuerdo con el Informe Técnico de la OACI Doc9303 Parte 12 "Infraestructura de Clave Pública para MRTDs", esta PKI consiste en una Autoridad de Certificación de Firma de País (CSCA) como CA Raíz. La principal tarea de la CSCA es la emisión de los certificados de firmante de documentos.

El CSCA utiliza un módulo de seguridad de hardware (HSM) para la generación segura de claves, la protección de claves de hardware y la gestión del ciclo de vida de las claves, y es capaz de realizar operaciones criptográficas asimétricas con longitudes y tipos de clave conformes con la OACI.

El CSCA ofrece las siguientes funciones:

1. Generación y renovación de una clave de firma de país.
2. Generación, emisión y renovación de certificados CSCA y CSCA link autofirmados
3. Generación y emisión de certificados de firmante de documentos (X.509v3) solicitados mediante PKCS#10.
4. Generación y emisión de certificados de firmante de lista maestra (X.509v3) solicitados mediante PKCS#10.
5. Generación y emisión de certificados de firmante de lista de desviación (X.509v3) y solicitados mediante PKCS#10.
6. Generación y exportación de listas de revocación de certificados
7. Protección de claves por hardware.
8. Destrucción de las claves generadas de forma segura (tras su caducidad)

2.5.2 Autoridad de certificación de verificación de país (CVCA) .

La Autoridad de Certificación verificadora del país es el nivel raíz de la PKI de la ICAO.

La CVCA ofrece las siguientes funciones:

1. Generación y renovación de una clave de verificación de país.
2. Generación, emisión y renovación de certificados CVCA autofirmados y certificados CVCA de enlace
3. Firma de certificados de verificador de documentos para un verificador de documentos
4. Exportación de los certificados
5. Protección de claves de hardware
6. Destrucción de las claves generadas de forma segura (tras su caducidad)

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D

2.5.3 Firma digital PKI

Firma CA raíz

La CA Raíz de Firma es el nivel raíz de la PKI de Firma Digital. Sirve como ancla de confianza para esta PKI.

La CA Raíz de Firma proporciona la siguiente funcionalidad:

1. Generación y renovación de una clave de CA raíz
2. Generación y emisión de certificados de CA emisora
3. Generación y emisión de CRL
4. Protección de claves por hardware.
5. Destrucción de las claves generadas de forma segura (tras su caducidad).

Firma CA emisora

La CA emisora de firmas proporciona la siguiente funcionalidad:

1. Generación y renovación de una clave de CA emisora
2. Generación y emisión de solicitudes de certificados de CA emisora
3. Importación de certificados de CA emisoras
4. Generación y emisión de CRL
5. Publicación de información sobre el estado de los certificados
6. Verificación de la identidad y autorización de los solicitantes de certificados
7. Generación de certificados de firma solicitados por el sistema de personalización
8. Protección de claves por hardware.
9. Destrucción de las claves generadas de forma segura (tras su caducidad)

Servidor de estado de certificados

El servidor de estado de certificados ofrece las siguientes funciones:

1. Importación y almacenamiento de información sobre el estado de los certificados y CRL
2. Respuesta a las solicitudes de la OSCP
3. Respuesta a las solicitudes de descarga de CRL

La CA Emisora de Firma es responsable de la producción de certificados de firma durante la personalización de las tarjetas eID. Está alojada en una máquina virtual (VM) dedicada en el hipervisor de la red interna. Para la gestión y protección de las claves privadas de la CA emisora se utilizan HSM de red. Estos HSM se compartirán con el sistema de

personalización mID, pero las claves de las CA emisoras se gestionarán en una sección (ranura) dedicada de los HSM.

Según se requiera, la CA raíz y la CA emisora utilizarán la especificación de clave RSA con un tamaño de clave de 4096 bits, los certificados de usuario (ciudadano) se emitirán con un tamaño de clave de 2048 bits. Todos los certificados se basan en las normas X.509v3 y RFC 5280. A petición también se pueden utilizar curvas elípticas según las especificaciones NIST y Brainpool.

2.5.4 Autoridad emisora Autoridad de certificación (IACA)

De conformidad con la norma ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application, esta PKI consta de una Autoridad de Certificación Emisora (IACA) como CA Raíz. La tarea principal de la IACA es la emisión de los certificados Document Signer para las identidades digitales móviles.

La IACA utiliza un módulo de seguridad de hardware (HSM) para la generación segura de claves, la protección de claves de hardware y la gestión del ciclo de vida de las claves, y es capaz de realizar operaciones criptográficas asimétricas con longitudes y tipos de clave conformes a ISO. La principal diferencia con el CSCA según la OACI es el formato de clave utilizado en el certificado raíz.

La IACA ofrece las siguientes funciones:

1. Generación y renovación de una clave de firma de país.
2. Generación, emisión y renovación de certificados autofirmados IACA e IACA link
3. Generación y emisión de certificados de firmante de documentos (X.509v3) solicitados mediante PKCS#10.
4. Generación y exportación de listas de revocación de certificados
5. Protección de claves por hardware.
6. Destrucción de las claves generadas de forma segura (tras su caducidad).

2.6 Requisitos no funcionales

2.6.1 Disponibilidad del sistema

Todos los sistemas Root PKI, la CSCA, la CVCA, la IACA y la CA Raíz de Firma, están alojados en un sistema de servidor con HSM integrado. Después de cada operación se realiza una copia de seguridad del sistema (incluido el material de claves del HSM).

Un dispositivo de servidor redundante con HSM se mantiene en una ubicación separada. En caso de fallo del hardware primario, la copia de seguridad se restaurará en el hardware de reserva. Este sistema de copia de seguridad proporcionará una funcionalidad idéntica a la del sistema primario y garantizará la continuación sin problemas de todas las operaciones.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, RD

2.6.2 Seguridad del sistema

Todos los sistemas de la PKI raíz, la CSCA, la CVCA, la IACA y la CA raíz de firma, están alojados en un sistema de servidor aislado que funciona en un entorno de alta seguridad. Sólo se accede al sistema si es necesario realizar una operación.

El sistema admite la autenticación de dos factores con token y PIN para que los operadores inicien sesión.

Todas las conexiones de red están protegidas por cifrado mediante conexiones TLS autenticadas mutuamente.

La copia de seguridad del material clave está protegida por un conjunto de tarjetas inteligentes con PIN individuales. La restauración del material de claves requiere la presencia de un número mínimo definido de tarjetas inteligentes.

2.6.3 Despliegue del sistema

El Sistema PKI se desplegará en el Centro de Datos de la sede central, excepto el Servidor de Estado de Certificados de la PKI de Firma Digital que se alojará en un servicio en la nube.

Los módulos de seguridad de hardware (HSM) certificados según se utilizan para almacenar y gestionar de forma segura claves criptográficas y ejecutar funciones criptográficas en un entorno reforzado. El HSM de red se despliega en una disposición redundante con un segundo dispositivo conectado a la red. Los dispositivos HSM ofrecidos están certificados conforme a Common Criteria (CC) EAL4+ para sus basados en el perfil de protección eIDAS EN 419 221-5 [4].

Se utiliza un sistema de servidor dedicado con PCI HSM integrado para alojar la CSCA fuera de línea, la CVCA, la IACA y la CA raíz de firma.

Se desplegará un sistema de prueba para los distintos sistemas PKI en un entorno independiente.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

2.7 Hardware y software del sistema PKI

En este capítulo se enumeran todos los componentes relevantes del sistema. Este capítulo resume los componentes de hardware y software necesarios asignados a los bloques de construcción definidos anteriormente. Los siguientes componentes de hardware del sistema PKI se consideran :[1]

No.	Cantidad	Articulo	Comentario
1	2	Sistema de servidor montable en bastidor de 19 pies, ranura PCIe de tamaño completo (para la tarjeta HSM	Requisitos mínimos: 1 CPU, 16 GB RAM, 200GB HD
2	2	Conmutador de red	Vinculación del sistema CA con la estación de trabajo de administración
3	1	Puesto de administración	PC o portátil con Windows
4	10	Fichas criptográficas USB	Para material de claves y certificados de autenticación de clientes
5	1	Disco duro USB	Copiar archivos de copia de seguridad del sistema sin conexión
6	2	Utimaco CryptoServer CP5 Se52 PCIe, CC certificado según EN419221-5	Para el sistema CA raíz
7	2	Utimaco CC eIDAS en CryptoServer HSM de red de uso general SecurityServer Se100 LAN V5	Para sistemas CA emisores

Se consideran los siguientes componentes de software del Sistema PKI:

No.	Cant.	Artículo	Observaciones
1	1	Licencia del software VeriKEY Certificate Manager CSCA/CVCA/IACA	Licencia de Veridos para el manejo de aplicaciones sw CSCA, CVCA e IACA

[1] Bastidores, SAI y otros componentes de infraestructura no enumerados aquí

2	1	Licencia del software Starfish PKI	Licencia para el manejo de CA raíz de firma y CA emisora
3	1	Middleware AET SafeSign	Para la integración de tokens Crypto USB en el puesto de trabajo de administrador.

Referencias:

[1] Doc. 9303 de la OACI, Documentos de viaje legibles por máquina, octava edición 202, Parte 12: Infraestructura de clave pública para MRTD.

[2] BSI TR-03110, Mecanismos avanzados de seguridad para documentos de viaje legibles por máquina

[3] ISO/IEC 18013-5:2021(en) - Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application (Identificación personal - Permiso de conducción conforme a ISO - Parte 5: Aplicación de permiso de conducción móvil)

[4] CSN EN 419221-5, Perfiles de protección para módulos criptográficos TSP - Parte 5: Módulo criptográfico para servicios de confianza.