ÍTEM III - ESPECIFICACIONES TÉCNICAS DE LAS PKI - CA

3.1 GET TRUST – SOLUCIÓN DE PKI

En nuestra búsqueda de una solución de infraestructura de clave pública (PKI) sólida y segura, hemos implementado "GET Trust", que es compatible con los estándares de la ICAO (OACI). Este sistema PKI de vanguardia ha sido meticulosamente diseñado y ejecutado por nuestro equipo de PID (Departamento Comercial de Pasaportes e Identificación) para cumplir con los más altos estándares de seguridad y garantizar la integridad y autenticidad de las transacciones digitales.

3.1.1 ARQUITECTURA DEL SOFTWARE

GET Trust establece una estructura clara y jerárquica para nuestros certificados digitales. Incluye una Autoridad de Certificación de Firma de País (CSCA) de primer nivel para seguridad a nivel nacional, así como Autoridades de Certificación Técnica (CA Técnicas) para manejar certificados SSL y otros certificados técnicos.

Sus módulos se componen de varios submódulos propietarios de PKI de la OACI que se pueden utilizar para firmar información de forma segura en documentos electrónicos y proteger datos confidenciales como identidades digitales.

- **Extensible**

GET Trust es altamente extensible. Ofrece soporte para múltiples API criptográficas y se integra perfectamente con una variedad de dispositivos de módulo de seguridad de hardware (HSM), lo que garantiza adaptabilidad y compatibilidad en diversos entornos operativos.

- **Escalable**

GET Trust ha sido ingeniosamente diseñado como una arquitectura de microservicios, lo que garantiza flexibilidad y escalabilidad. Este sistema puede escalarse horizontalmente fácilmente agregando sin esfuerzo firmantes de datos adicionales cuando surja la necesidad.

- **Registro**

GET Trust, con su arquitectura de microservicios, también prioriza capacidades de registro sólidas. Proporciona funciones de registro amplias y configurables, lo que permite un seguimiento y análisis exhaustivos de las actividades del sistema para mejorar la seguridad y la resolución de problemas.

- **Gestión de usuarios**

La gestión de usuarios es un aspecto fundamental del conjunto de funciones de GET Trust. El sistema incluye sólidas funcionalidades de administración de usuarios, lo que permite a los administradores crear, administrar y controlar de manera eficiente el acceso, los permisos y los procesos de autenticación de los usuarios para operaciones seguras y sin inconvenientes.

- **Mecanismo de confianza en la máquina (Machine Trust)**

GET Trust incorpora un sofisticado mecanismo Machine Trust que aprovecha las autoridades de certificación técnicas (Technical CA) para emitir certificados SSL. Las claves generadas dentro de este mecanismo se almacenan de forma segura en Módulos de plataforma segura (TPM) y están diseñadas para no ser

exportables. Esta estricta medida de seguridad garantiza la máxima protección de los materiales criptográficos confidenciales, mejorando la postura de seguridad general del sistema.

3.2 GET AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA – CSCA

La Autoridad de Certificación de Firma de País (CSCA) de GFT Trust permitirá las siguientes funcionalidades:

- Confidencialidad: garantía con certificados de cifrado
- Integridad: garantía con certificados de firma.
- Autenticación: garantía con certificados de autenticación
- No repudio: garantía con certificados de firma y autenticación
- Control de acceso: garantía con certificados de autenticación

El software ID-CA actúa en la solución propuesta como CSCA, como fabricante de certificados gestionando su ciclo de vida.

El objetivo del componente ID-CA es permitir una gestión centralizada y segura del ciclo de vida de los certificados gracias a las siguientes funcionalidades:

- Creación de autoridades de certificación.
- Creación de certificados de usuario (entidad final) por parte de las autoridades de certificación.
- Revocación de certificados por parte de las autoridades certificadoras.
- Creación automática de CRL (listas de revocación de certificados) para cada autoridad certificadora.
- Publicación de certificados de usuario (entidad final) y CRL en un directorio LDAP.

Una característica interesante de ID-CA es la multi entidad, que permite crear instancias de un número ilimitado de particiones (dominios), capaces de alojar una jerarquía PKI completa con CA raíz e intermedia. Estas particiones actúan como dominios separados y, por lo tanto, es posible implementar entornos de confianza de clientes completamente independientes dentro de la misma instancia de software.

Centrándose en la capacidad de abordar todo tipo de segmentos del mercado de identidad digital, ID-CA también ha sido diseñado para satisfacer todos los requisitos de las necesidades de Seguridad Corporativa y, en particular:

- Proporcionar una variedad de conectores de interfaz, permitiendo la integración en el sistema de TI de la empresa.
- Implementar una configuración altamente empaquetada y, por lo tanto, eliminar la complejidad de las implementaciones de PKI.
- Instalación y configuración del sistema fáciles de usar.

Como enfoque general, su desarrollo tuvo mucho cuidado en facilitar al máximo el uso de PKI. Por lo tanto, se han revisado todos los aspectos, desde los procedimientos de instalación hasta las tareas administrativas diarias, donde se guía y apoya al administrador durante la configuración y ejecución de la aplicación.

Considerando los esquemas de evaluación de seguridad de terceros como garantía de calidad, seguridad y robustez, ID-CA se somete a un proceso de certificación Common Criteria, dirigido al nivel EAL4+. Este enfoque es una apuesta clara por mantener continuamente el nivel de seguridad del software, como lo demuestran las certificaciones EAL3+ y EAL4+ obtenidas por productos anteriores.

GESTIÓN DEL ALMACÉN DE CLAVES

Un KeyStore es la configuración para acceder al contenedor de claves criptográficas de hardware o software.

Permite generar pares de claves criptográficas basadas en servicios criptográficos proporcionados por bibliotecas de software, tokens de tarjetas inteligentes (a través del middleware PKCS11) o mediante un Crypto Server (capa de abstracción de hardware), conectado a un HSM.

El tipo de algoritmos, parámetros y longitudes de clave dependen únicamente del recurso elegido. Por lo tanto, con el software o hardware adecuado, ID-CA admite RSA hasta 4096 bits y ECDSA hasta 512 (curvas NIST, Brain Pool y otros parámetros).

Los HSM compatibles son de la familia EVIDEN Trustway Proteccio, Safenet y Thales (nCipher). Cualquier otro HSM estándar basado en PKCS#11 puede ser compatible después de la calificación.

La gestión del KeyStore consiste en Creación, Edición, Actualización y Eliminación.

GESTIÓN DE DEPOSITOS EN GARANTIA

ID-CA integra la gestión de depósitos en garantía (Escrow Management) como función principal.

El depósito de claves es un acuerdo en el que las claves necesarias para descifrar datos cifrados se mantienen en depósitos de garantía y, en determinadas circunstancias, el propietario o un tercero autorizado puede obtener acceso a esas claves. El depósito en garantía se utiliza a menudo con la generación de claves centralizada (es decir, emisión de pares de claves en el lado de PKI), para limitar el riesgo de filtración de la clave.

La clave maestra para escrow, la clave simétrica y la clave de usuario final se generan en un recurso criptográfico de hardware, cada vez que existe una solicitud de generación de clave centralizada.

De forma predeterminada, la clave maestra es una clave RSA de 3072 bits y la CLAVE simétrica es una clave AES de 256.

Están disponibles las siguientes funciones:

- **Creación de configuración de generación de claves:** cree una configuración de generación de claves para la partición actual.
- **Habilitar la generación centralizada de pares de claves en el perfil de certificado:** habilite la generación de pares de claves mediante PKI (generación centralizada de pares de claves) para un perfil de certificado en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.

- **Habilitar depósito en garantía en perfil de certificado:** habilite el depósito en garantía para un perfil de certificado en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- **Clave de depósito en garantía:** deposita en custodia una clave para un certificado en una partición de destino.
- **Recuperar clave en custodia:** recupere una clave que ha sido en custodia para un certificado en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.

AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA

ID-CA permite una gestión de autoridades de certificación muy sofisticada y eficaz.

Una Autoridad de Certificación (CA) es la parte esencial de un sistema PKI. Su función principal es emitir certificados y gestionar su ciclo de vida. Una CA puede tener varios certificados, que deben tener el mismo DN (Domain Name).

Con ID-CA están disponibles las siguientes funciones de gestión de CA disponibles en el mercado:

- **Generación de pares de claves de CA:** genere un par de claves para un certificado de CA
- **Creación de certificado de CA firmado localmente/renovación de certificado con nueva clave:** crear un certificado de CA para una configuración de CA
- **Creación de certificado de CA firmado externamente/renovación de certificado con nueva clave:** cree una CSR para firmarlo externamente e importar el certificado resultante.
- **Importar certificado de CA/renovación de certificado:** importar un certificado de CA a una CA

ID-CA implementa una característica particular, el concepto *CA Group*, que permite una gestión de CA altamente flexible y segura.

CA Groups permite a los administradores gestionar varias CA en una sola entidad. En general, los *CA Groups* están formados por una sola CA y, por lo tanto, el concepto de grupo se oculta en aras de la simplicidad. Los *CA Groups* permiten:

- Garantizar que el servicio de firmas permanezca disponible incluso cuando el tráfico de firmas esté en su nivel más alto: una CA definida en un *CA Group* puede tener una cuota de firmas. Cuando una CA alcanza la cuota de firmas, el servicio de firma cambia a la siguiente *CA Group* que aún no ha alcanzado la cuota de firmas.
- Administrar las CRL (listas de revocación de certificados) para todas las CA dentro del *CA Group*.
- Predefina las CA antes de crear certificados de CA: los *CA Groups* se pueden crear y configurar antes de que se hayan creado los certificados de CA; luego los certificados de CA se pueden cargar cuando estén disponibles.

La función *CA Groups* es de particular interés para proyectos de identidad a gran escala donde se necesita producir una gran cantidad de certificados de ciudadanos (usuarios). De hecho, *CA Groups* evita ataques criptoanalíticos a una única clave privada de CA. *CA Group* se administra fácilmente mediante configuración y mecanismos GUI.

En detalle, están disponibles las siguientes funciones de *CA Group*:

- Creación de *CA Group* mediante la importación de un certificado: Cree un *CA Group* en la Partición actual o cualquier Partición en un nivel inferior de la rama del árbol, con dentro, una CA y un certificado importado.
- Creación de *CA Group* con certificado firmado localmente: cree un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol, con una CA interna y su certificado firmado por una CA local.
- Creación de *CA Group* con certificado firmado externamente: cree un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol, con dentro, una CA y su certificado firmado por una CA externa.
- Edición de *CA Group*: edite el *CA Group* en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- Importación de *CA Group*: cree un *CA Group* en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol, desde un archivo XML.
- Exportación de *CA Group*: exportación XML de un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- Eliminación de *CA Group*: elimine un *CA Group* que no tenga un certificado de CA en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.

ADMINISTRACIÓN DE PERFILES DE CERTIFICADOS

La principal tarea de una Autoridad de Certificación es, por definición, producir certificados digitales.

ID-CA realiza esta tarea con un enfoque particular en el rendimiento y la facilidad de uso, para permitir una rápida definición del perfil de certificado y la producción de certificados en gran volumen.

En lo que a tareas de administración se refiere, se puede:

- Crear/Editar perfiles de certificados
- Importar/exportar perfiles de certificados

La estructura de un certificado se puede crear de una manera muy sencilla mediante soporte GUI, en un proceso guiado que permite al usuario ingresar solo valores que no están predefinidos.

Además, y para poder combinarlo con productos anteriores de CA, es posible importar perfiles de certificados también en formato XML.

Para configurar rápidamente varios entornos, como ensayo, preproducción y producción, también se pueden exportar perfiles de certificados, así como otros datos de configuración, en formato XML.

Un perfil de certificado está asociado con una CA o un grupo de CA. Determina las propiedades del certificado, como el tamaño de la clave pública, el período de validez, el DN y los usos de clave para todos los certificados emitidos por la CA o el grupo de CA asociado con el perfil del certificado.

A través de la GUI, se puede definir, editar y modificar casi todos los elementos dentro de un perfil de certificado. La gestión del perfil del Certificado IDnomic ID-CA permite, en particular, definir libremente:

- El formato del certificado
- El algoritmo utilizado para el certificado.
- La firma del Grupo CA
- La información del certificado y cómo obtener esta información.

ADMINISTRACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS

Periódicamente se genera y publica una lista de revocación de certificados (CRL), a menudo en un intervalo definido.

ID-CA implementa todas las funciones de gestión de CRL necesarias para producir y distribuir información de revocación a todas las aplicaciones relevantes. Además de la publicación (automática), también se puede recuperar la CRL manualmente a través de la GUI.

Una CRL también se puede publicar inmediatamente después de que se haya revocado un certificado. La CRL siempre la emite la CA que emite los certificados correspondientes. Todas las CRL tienen una vida útil durante la cual son válidas. Durante el período de validez de una CRL, una aplicación habilitada para PKI puede consultarla para verificar un certificado antes de su uso.

También es posible generar una CRL Delta, que es la lista de cambios desde la última CRL.

Las funciones de Gestión de CRL de ID-CA consisten en:

- **Configuración de generación de CRL en grupo CA:** configure la información de CRL de un grupo CA para producir CRL (y opcionalmente Delta CRL).
- **Producción automática de CRL:** produzca periódicamente una CRL completa (y opcionalmente una CRL Delta) para todas las CA válidas de un grupo de CA.
- **Producción automática de Delta CRL:** produzca una Delta CRL periódicamente para todas las CA válidas en un grupo de CA.
- **Producción manual de CRL:** produzca periódicamente una CRL completa (y opcionalmente una CRL Delta) para todas las CA válidas de un grupo de CA.
- **Descarga de CRL mediante GUI:** descarga mediante GUI, la última CRL completa o Delta CRL de una CA en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- **Descarga de CRL vía HTTP:** Descarga vía HTTP, última CRL completa o Delta CRL de CA.

ADMINISTRACIÓN DE PUBLICACIÓN

La publicación de la información producida (certificados y CRL) es una tarea clave en los sistemas PKI para hacer que los datos públicos estén disponibles para verificar la identidad digital y su validez. La publicación en ID-CA está disponible tanto para Certificados como para CRL al ser datos públicos de una CA.

ID-CA tiene una gestión de publicaciones muy fácil de usar, que consiste en un proceso de configuración basado en GUI combinado con elementos de configuración. La publicación se puede realizar de forma automática o manual.

En particular, las características de ID-CA Publication Management consisten en todas las funciones del ciclo de vida, como creación, edición y eliminación para terminales, estrategia de publicación y política de publicación.

Además, ID-CA admite de forma nativa la política de publicación de enlaces para la publicación de certificados y CRL, así como la publicación automática.

Para configurar una publicación se necesitan varias configuraciones (Endpoint, Estrategia de publicación, Política de publicación).

ADMINISTRACIÓN DE CA DE CONFIANZA (TRUSTED CA)

El paradigma de seguridad de ID-CA se basa en el más alto nivel de confianza. Por lo tanto, una CA interna sólo se puede utilizar si es de confianza. Las CA confiables se utilizan para la autenticación de usuarios y la verificación de firmas de solicitudes de servicios web.

El concepto Trusted CA se implementa en toda la aplicación para permitir y controlar la comunicación segura y el acceso a las funciones del producto.

Los certificados de autenticación de usuario que permiten conexiones a la aplicación ID-CA deben haber sido emitidos por una autoridad de certificación (CA) en la que la aplicación ID-CA confíe para la autenticación de actores. ID-CA también debe poder verificar la cadena de confianza del certificado hasta un ancla de confianza.

Para la firma de solicitudes de certificados, las CA que emiten certificados que firman solicitudes de certificados deben ser confiables para la firma de solicitudes y la CA de ID debe poder verificar la cadena de confianza del certificado hasta un ancla de confianza.

Cuando se confía en una CA en una partición, también se confía en todas las particiones debajo de esta partición.

Trusted CA Management consiste en:

- **Creación de CA de confianza externa:** cree una CA de confianza en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- **Edición de CA de confianza externa:** edite la CA de confianza en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- **Edición de CA de confianza interna:** edite la CA de confianza interna en la partición actual o inferior

ADMINISTRACIÓN DE NOTIFICACIONES

En modo operativo, esta función de notificación es esencial para garantizar un alto nivel de disponibilidad de la aplicación PKI.

ID-CA ha integrado de forma nativa la gestión de notificaciones dirigidas a sus administradores.

El módulo de Notificación se utiliza para advertir a una persona sobre los diferentes eventos que ocurren en la plataforma o sobre entidades administradas por una CA. Las funcionalidades de Notificación ID-CA consisten en:

- **Notificación de caducidad:** notifica a un usuario acerca de un certificado que caducará pronto en la partición de destino.
- **Configuración de notificación:** configure la notificación para la partición actual y cualquier partición en un nivel inferior de la rama del árbol.

ADMINISTRACIÓN DE ACTORES

Los actores son Personas, Máquinas o Dispositivos que pueden acceder al sistema, normalmente identificados y autenticados mediante un certificado. Disponible para la asignación de doble factor de autenticación mediante OTP.

Están autorizados a realizar Acciones dependiendo del Rol que se les asigne en una Partición específica y sus hijos.

- Los **roles** (roles) son una colección de derechos. Los roles se definen para casos de uso específicos identificados de la aplicación y para garantizar la separación de funciones.
- Los **permisos** (rights) son una colección coherente de posibles acciones en el sistema para una característica específica. Actualmente, no es posible editar derechos ni crear roles (los roles y derechos son estáticos).

En resumen, el **triplete** de Rol, Partición y Actor es necesario para determinar si una acción está autorizada o no en el sistema, en una partición específica.

Rol	Descripción
Super Administrator	Posee todos los roles
Rights Administrator	Puede ver certificados y usuarios.
Connector Enroll	Puede crear y editar usuarios.
Connector Revoke	Puede realizar la inscripción de certificados a través del servicio web (SOAP)
Connector Recovery	Puede realizar la revocación de certificados a través del servicio web (SOAP)
Configuration Administrator	Puede realizar recuperación de claves a través del servicio web (SOAP)
Certificate Administrator	Puede realizar todas las tareas de configuración, así como ver certificados
Revocation Administrator	Puede realizar búsquedas, inscripciones y revocaciones de certificados a través de GUI
Recovery Administrator	Puede ver todos los ajustes de configuración, excepto los clústeres criptográficos. Puede ver, suspender, revocar y reactivar/reanudar certificados. Puede suspender, revocar y reactivar/reanudar certificados mediante servicios web
Key Administrator	Puede realizar la recuperación de claves a través de GUI
Audit Administrator	Puede gestionar funciones de generación de claves.

Tabla 1. Roles y Permisos.

ADMINISTRACIÓN DE AUDITORIA, REPORTES Y SUPERVISIÓN

ID-CA registra todos los eventos funcionales y técnicos. Los registros de auditoría se utilizan para monitorear la plataforma tanto a nivel de proceso comercial como a nivel técnico.

Se pueden diferenciar dos tipos de trazas:

- **Seguimientos técnicos:** Estos seguimientos son generados por los componentes internos (servidor web Apache, base de datos PostgreSQL, directorio LDAP, etc.) implicados en el funcionamiento de ID-CA. Accesibles como un archivo de texto a través del sistema de archivos, estos seguimientos proporcionan indicadores sobre el estado de ejecución de cada uno de estos componentes. Estos rastros son generados por los propios componentes según su propia lógica de aplicación.
- **Seguimientos de aplicaciones:** Para garantizar la trazabilidad y la rendición de cuentas, ID-CA genera seguimientos completos de las aplicaciones para cada una de las acciones realizadas. Cada rastro tiene un número único que permite seguir los eventos que originaron la emisión de este rastro y seguir las acciones realizadas posteriormente. Por ejemplo, a partir de un seguimiento generado durante la validación de una solicitud de tarjeta, será posible:

- Volver a la solicitud inicial.
- Seguimiento del futuro de la solicitud.

En general, cada rastro se compone de datos que especifican "quién" hizo "qué", "cuándo", "dónde" y "el resultado". Un seguimiento suele ir acompañado de los datos correspondientes (solicitudes, certificados, etc.).

Los seguimientos de aplicaciones de ID-CA se pueden interconectar con la herramienta Syslog.

La Gestión de Auditoría consiste en:

- Normalización de auditoría: normalice periódicamente los eventos de auditoría en la base de datos para realizar consultas en la base de datos.
- Vista de auditoría: vea información de auditoría en la partición actual o debajo
- Búsqueda de auditoría: busque registros de auditoría disponibles en la partición actual o debajo
- Exportación de auditoría: exporta registros de auditoría en la partición actual o debajo

En términos de funciones de informes, ID PKI puede manejar la siguiente información:

1. Para una fecha determinada, una tabla muestra el número total de certificados (emitidos antes de esta fecha) por partición o perfil y por estado:
- válido (no revocado en un período de validez)
- revocado (en un período de validez)
- aún no válido y no revocado
- aún no válido y revocado
- caducado y no revocado
- caducado y revocado

2. Por rango de tiempo, una lista de eventos relacionados con certificados por perfil o partición
- Inscribirse
- Revocación
- Vencimiento

A nivel global, cada administrador de sistemas necesita verificar el estado de las aplicaciones en ejecución.

ID-CA proporciona información básica sobre el estado de las aplicaciones y expone varios indicadores basados en los procesos de Monitoreo del sistema y Monitoreo de aplicaciones.

Los elementos de monitoreo del sistema son:

- CPU, RAM, uso del disco, tiempo de actividad del servidor,
- Estado de salud del repositorio LDAP, la base de datos y el agente JMS.

Los elementos de monitoreo de aplicaciones PKI son:

- Tiempo de actividad y estado del servidor
- Estado de salud de HSS (capa de abstracción de hardware criptográfico)
- Caducidad de CA
- Información de gestión de CRL
- Producción de CRL
- Publicación CRL
- Alerta de publicación de CRL

ADMINISTRACIÓN DE PARTICIONES

El sistema de partición permite implementar fácilmente el arrendamiento múltiple dentro de ID PKI. Permite configurar varios entornos CA completamente independientes dentro de una única instancia del software.

Las particiones se definen en una estructura de árbol, siendo cada nodo una partición en la que se pueden adjuntar recursos (por ejemplo, configuraciones, certificados, etc.). Según las necesidades del cliente podemos aislar o compartir recursos comunes.

Debido a la asociación de los roles y acciones del actor a una partición y sus hijos, es posible dedicar una partición completa a un cliente. Puede actuar como un entorno PKI individual.

El principio de partición lógica se describe a continuación:

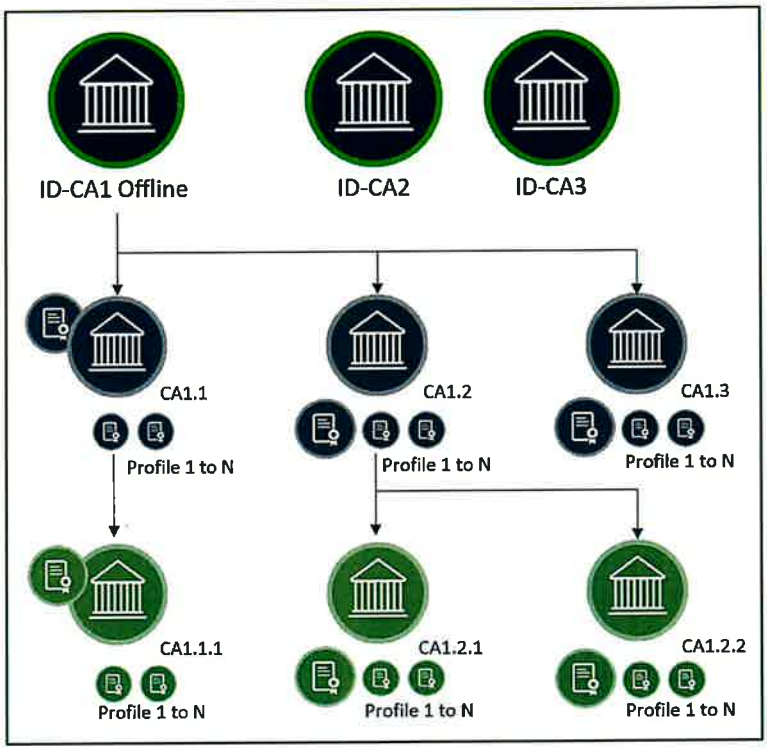


Ilustración 1. Principios de partición de datos.

La gestión de particiones consiste en:

- **Creación de partición:** creación de una nueva partición (son posibles estructuras anidadas)
- **Edición de partición:** edición de la partición actual o cualquier partición en un nivel inferior de la rama.

Es posible **compartir** (colocar recursos más arriba en el árbol) y **aislar** (crear ramas en el árbol de partición).

La gestión de particiones se realiza de una manera extremadamente fácil de usar, a través de una sencilla GUI mediante mecanismos de hacer clic, arrastrar y soltar. Para una mayor visibilidad, se puede asociar un logotipo a cada partición para resaltar mejor unas de otras.

SELLADO DE TIEMPO

El producto Time Stamping nos permite proporcionar tokens de tiempo certificados y fiables.

En combinación con una fuente de tiempo y un medio de firma digital, esto permitirá a los clientes garantizar, por ejemplo, la existencia de un documento en un momento preciso en el tiempo.

En términos de implementación, un cliente transmite solicitudes de sellado de tiempo a la plataforma, que determina con gran precisión la hora y la fecha, firma y envía esta información de vuelta al cliente.

El protocolo de comunicación subyacente para este procedimiento está definido en RFC 3161, al que el producto Time Stamping cumple plenamente.

La firma de los tokens de tiempo se basa en dispositivos criptográficos (módulos de seguridad de hardware) que admiten la interfaz PKCS#11.

El producto consta de dos servidores:

- Un servidor de administración, encargado de proporcionar servicios de gestión basados en GUI para operadores acreditados.
- Un servidor de firma, encargado de producir técnicamente los tokens (de tiempo) firmados.

Se admiten las siguientes funciones:

- Administración basada en GUI del servicio de sellado de tiempo
- Gestión de los espacios de trabajo del cliente, incluido el manejo de pares de claves criptográficas asociadas
- Gestión de entidades de sellado de tiempo, sus políticas y extensiones aceptadas
- Gestión de actores
- Auditoría y estadísticas

El acceso a los servidores solo se concede mediante autorización basada en autenticación mutua (HTTPS SSL/TLS).

Además, el sellado de tiempo ofrece las siguientes ventajas:

- Tokens producidos totalmente compatibles con IETF RFC 3161 e IETF RFC 5816
- Gestión flexible de particiones de clientes (cada una dedicada a un espacio de trabajo de sellado de tiempo)
- Máximo rendimiento
- Cumplimiento de la normativa Eidas

3.3 FIRMADO DE DOCUMENTOS GET TRUST (DOCUMENT SIGNER)

ADMINISTRACIÓN BASADA EN WEB

La interfaz de administración basada en web ofrece las siguientes funcionalidades:

- Gestión de espacios de trabajo (dominio del cliente)
- Gestión de entidades firmantes (comúnmente denominadas "Firmantes de documentos" o DS)
- Gestión de claves de firma (claves de firma de respuestas y sus certificados asociados)
- Gestión de los usuarios del servicio
- Auditoría de operaciones de administración
- Consulta de estadísticas de producción.

Solo se puede acceder al sitio de administración mediante un certificado de usuario final (UE), que se puede almacenar en una tarjeta inteligente. El servidor web frontal autentica a la UE que se conecta. Para que la UE esté autorizada a acceder al sitio, la CA que emitió su certificado debe estar definida como una CA confiable del servidor web frontal.

Una vez que el Usuario Final haya sido autenticado por el servidor Web frontal, se abrirá la página de inicio de la plataforma DS. Dependiendo del perfil de Usuario final utilizado para conectarse al sitio, tendrá acceso a ciertas funcionalidades, pero no a todas.

Están disponibles los siguientes perfiles:

- Perfil **"Gestión del espacio de trabajo":** Otorga acceso al menú "Gestión del espacio de trabajo". Un Usuario Final con este perfil puede crear, seleccionar, ver o modificar un espacio de trabajo.
- Perfil **"Gestión de claves":** Otorga acceso al menú "Gestión de claves". Un Usuario Final con este perfil puede generar un par de claves en el equipo criptográfico y recuperar la solicitud de certificado emitido (CSR en formato PKCS#10).
- Perfil **"Administración DS":** Otorga acceso al menú "Administración DS". Un Usuario Final con este perfil puede registrar, ver, activar, desactivar y bloquear certificados DS.
- Perfil **"Gestión de usuarios":** Otorga acceso al menú "Gestión de usuarios". Un Usuario Final con este perfil puede registrar, activar, desactivar o bloquear usuarios y gestionar los derechos de los usuarios registrados.
- Perfil **"Gestión de Auditoría":** Otorga acceso al menú "Auditoría". Un usuario final con este perfil puede ver información relacionada con la auditoría, así como estadísticas de producción.

INTERFACE CON LA PLATAFORMA DE DS

La interfaz de la plataforma DS se basa en el enfoque de servicios web (XML sobre HTTP(S)) y permite, por lo tanto, una interfaz sencilla e independiente del contexto.

IDnomic proporciona al Cliente:

- Una documentación para la interfaz de especificación
- Apoyo a la integración

ESPECIFICACIONES DE LA PLATAFORMA DE DS

Software	Especificaciones
ICAO - DOCUMENT SIGNER®	La plataforma DS se suministra y puede configurarse. Normalmente se instala en el sitio de producción en interfaz directa con la cadena de personalización. **Funciones principales:** • Verificación de certificados DS. • Enrutamiento de una solicitud de firma a una clave disponible con control de cuota (número máximo de firmas por clave). • Generación de un lote de claves y DS CSR. • Realiza codificación ASN.1 y firma de SOD. Interfaz DS: servicio web (XML) sobre protocolo HTTP(S)

ALGORITMOS

- RSA 2048 y 4096
- SHA-1, SHA-256 y SHA-512
- ECDSA 256

3.4 PKI CIUDADANA – PKI SUBORDINADA X509

CA SUBORDINADA DE LA CA ROOT

Una CA subordinada es una CA que obtiene su certificado de una CA raíz (también conocida como CA principal). La CA subordinada podrá emitir certificados a otras entidades (ciudadanos), pero su certificado es verificado por la CA raíz.

PROCESO DE EMISIÓN DE CERTIFICADOS

El proceso de emisión de certificados en la PKI Ciudadana con una CA subordinada es el siguiente:

1. Solicitud de certificado: Una entidad (Ciudadano) solicita un certificado a la CA subordinada.
2. Verificación de identidad: La CA subordinada verifica la identidad de la entidad (Ciudadano) que solicita el certificado. (Tarea delegada al sistema de verificación de identidad de la JCE)
3. Generación de clave pública: La entidad genera un par de claves (pública y privada).
4. Solicitud de certificado a la CA raíz: La CA subordinada solicita un certificado a la CA raíz para la entidad.
5. Emisión de certificado x509: La CA raíz emite un certificado para la CA subordinada, que a su vez emite un certificado para la entidad.
6. Firma del certificado: El certificado es firmado digitalmente por la CA subordinada y la CA raíz.

ESTRUCTURA DEL CERTIFICADO X.509

Un certificado X.509 tiene la siguiente estructura:

- **Número de versión:** Indica la versión del certificado.
- **Número de serie:** Un número único que identifica el certificado.
- **Algoritmo de firma:** El algoritmo utilizado para firmar el certificado.
- **Emisor:** La entidad que emitió el certificado (CA subordinada).
- **Sujeto:** La entidad a la que se emitió el certificado.
- **Clave pública:** La clave pública de la entidad.
- **Validez**: La fecha de inicio y fin de validez del certificado.
- **Extensiones**: Información adicional sobre el certificado.

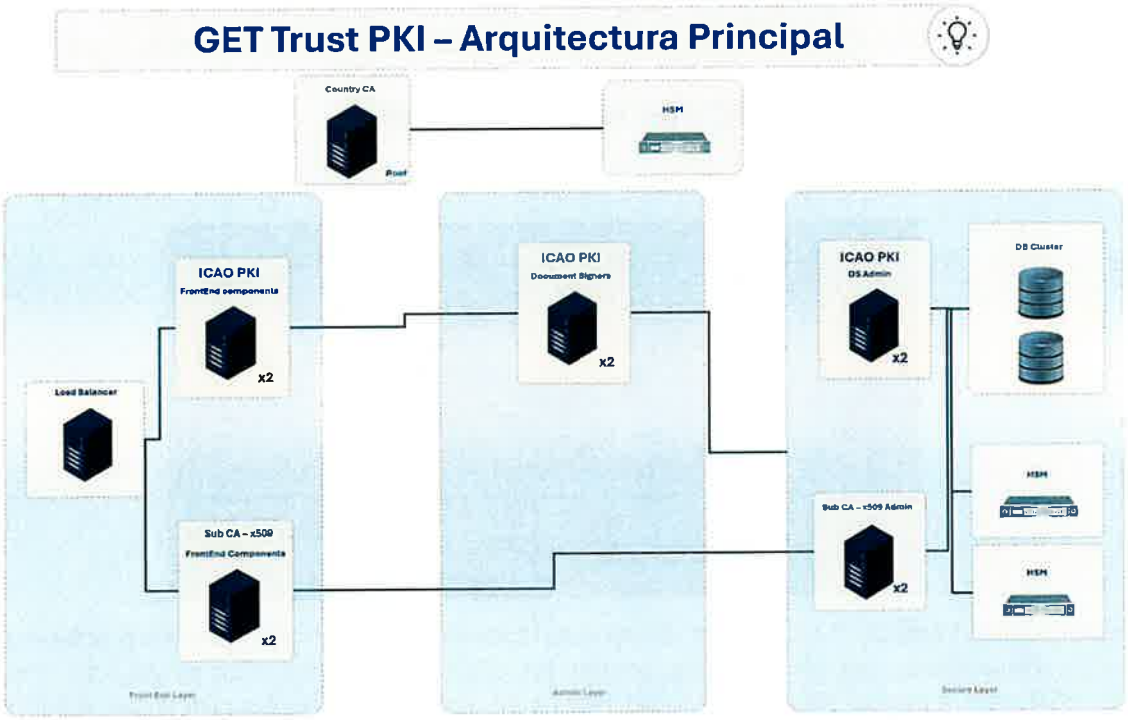
VENTAJAS DE LA PKI CON CA SUBORDINADA

La PKI con CA subordinada ofrece varias ventajas, como:

- **Mayor flexibilidad:** La CA subordinada puede emitir certificados para entidades específicas.
- **Mejora la seguridad**: La CA raíz puede revocar el certificado de la CA subordinada si es necesario.
- **Reducir costos:** La CA subordinada puede reducir los costos de emisión de certificados.

3.5 INFRAESTRUCTURA GET TRUST

La infraestructura de GET Trust está diseñada para permitir la comunicación digital segura, la autenticación y la protección de datos durante todo el proceso de personalización. La infraestructura que se describe a continuación comprende componentes esenciales del sistema y la intercomunicación entre ellos. Abarca la Autoridad de Certificación de Firma de País (CSCA), la Autoridad de Certificación Técnica (CA Técnica) responsable de los certificados SSL, los firmantes de datos y los sitios de emisión.



3.5.1 CARACTERÍSTICAS CLAVES

GET Trust cuenta con la notable capacidad de operar en entornos Windows y Linux y, al mismo tiempo, se adapta a diferentes estándares de API criptográfica, incluidos PKCS11, CNG y CSP. Además, la excepcional flexibilidad de GET Trust se extiende a su compatibilidad con módulos de seguridad de hardware (HSM) y soluciones de software HSM como el 'DB Crypto Engine'. Esta interoperabilidad dinámica garantiza que GET Trust pueda integrarse perfectamente en una amplia gama de infraestructuras de TI, brindando a las organizaciones la libertad de elegir las herramientas y plataformas que mejor se adapten a sus necesidades de seguridad.

- Máxima seguridad probada, Modulo CA certificado en CC EAL4+

- Multi-tenant por diseño: implemente, configure y administre varias PKI de forma independiente con una instancia de software.
- Cumplimiento de normas y estándares:
  - Cumplimiento del formato del certificado: X.509v3, RFC 5280 y RFC 3739
  - Solicitudes de certificados: PKCS#10, CSR, SPKAC
  - Algoritmos de firma RSA (1024 - 4096), (RSA PKCS#1 v1.5, RSA PSS PKCS#1 v2.1), ECDSA (192-521)
  - Algoritmos hash SHA-224, SHA-256, SHA-384, SHA-512, SHA-256 MGF1, SHA-384 MGF1, SHA512 MGF1
  - Contenido del certificado: UTF8, T61, imprimible, correo electrónico,
  - SAN (RFC822, UPN), etc.
- Cumplimiento:
  - Certificado RGS considerando todos los usos de los certificados y para todas sus clasificaciones (1, 2 y 3). LSTI N° 8029-1318-V3.0 / EN319411-1 V1.1.1
  - Cumple con eIDAS: obtención del Certificado LSTI N° 8029-1318-V3.0.

3.6 MÓDULO DE SEGURIDAD POR HARDWARE (HSM)

Nos permitimos ofrecer el modelo Eviden Trustway Crypt2pay, el cual presenta las siguientes características.

Eviden Trustway Crypt2pay ™ es un Módulo de Seguridad Hardware (HSM) que ofrece soluciones de software en un entorno altamente seguro y de alto rendimiento, permitiendo la ejecución de operaciones criptográficas muy sensibles. Este HSM combina medidas sólidas de seguridad física con un núcleo criptográfico que cumple con los estándares de seguridad más estrictos, lo que lo convierte en uno de los módulos criptográficos más certificados del mundo para integrarse en sistemas de información corporativos y servicios en la nube. Su implementación simplificada, diseñada para despliegue independiente, proporciona a los entornos críticos una solución ideal para garantizar la seguridad absoluta de sus datos sensibles, todo a un precio competitivo.

Algunas características clave de Eviden Trustway Crypt2pay incluyen:

- Nivel de seguridad alto: Diseño a prueba de manipulaciones (Anti-tampering) con un alto nivel de certificación.
- -Gestión sencilla: Fácil instalación y administración intuitiva.
- Disponibilidad alta: Mecanismos nativos para alta disponibilidad, conmutación por error y copias de seguridad.

- Protección de datos: Soluciones de protección de datos que le permiten cifrar, gestionar y controlar el acceso a sus datos, independientemente de su ubicación (local, virtual y en la nube).
- Autenticación: Eleva la seguridad de su aplicación mediante el control de acceso a sus datos y la protección de generadores de claves.
- Seguridad en la nube: Proporciona una raíz de confianza para servicios en la nube al asegurar la comunicación entre la nube privada y el sitio local, la encriptación de datos para soluciones locales y basadas en la nube, y servicios criptográficos bajo demanda.

- **APIs:**
  - PKCS#11
  - OpenSSL
  - Java Cryptography Architecture/Extension (JCA/JCE)
  - Microsoft Crypto API (CSP), Cryptography Next Generation (CNG)
- **Diseño Anti-Tampering certificado en:**
  - Common Criteria EAL4+ en cumplimiento con CWA 14167-2-PP
  - NATO SECRET
  - Cumple con eIDAS.
  - Qualification Renforcée (la más alta calificación de la ANSSI)
  - FIPS 140-2 level 3.
- **Algoritmos**
  - DES: Triple DES
  - RSA: Keys up to 4069bits
  - 5 and PSS signature
  - SHA-1, SHA-2, SHA-3
  - HMAC
  - AES: 128, 192 and 256 bit keys
  - ECDSA: ANSI and Brainpool named curves
  - CHACHA & Poly1305
  - EdDS
- **Interfaces y características físicas**
  - Performance: Crypt2pay XT: 100 to 3600 PVV tps
  - Voltage: 85 – 264 Vac
  - Red: 3 x 1Gb
  - 2 Hot Plug PSU
  - Frecuencia: 47 – 63 Hz
  - Humedad: 30% – 70% noncondensing
  - Temperatura de Operación: 10/45°C
  - Dimensiones: Crypt2pay XT: 442x346x76mm
  - Peso: Crypt2pay XT: 14 kg
- **Tipos de Llaves**
  - Payment Industry keys.
  - Smart metering Industry keys.
  - PKCS#11 keys.

- Generic secret keys.
- Import / Export keys feature.