Sistemas Informáticos Abiertos, S.A.
Avenida de Europa, 2
Alcor Plaza Edificio B
Parque Oeste, Alcorcón 28922
Alcorcón - Madrid (España)
Telf: (34) 902 480 580 Fax: (34) 91 641 95 13

www.sia.es

SIAVAL SafeCert Manager

Declaración de Seguridad

Fecha: 28/11/2017

INDICE

RELACION DE TABLAS

RELACION DE ILUSTRACIONES

1. INTRODUCCIÓN

1.1 Identificación

Esta Declaración de Seguridad describe los objetivos de seguridad y requisitos de seguridad para el SIAVAL SafeCert Manager v2.4.02 20150611-1657. Las especificaciones son consistentes con Common Criteria for Information Technology Security Evaluation v3.1 R4.

1.1.1 Identificación de la Declaración de Seguridad

Título	SIAVAL SafeCert Manager – Declaración de Seguridad
Versión	1.5
Autor	Sistemas Informáticos Abiertos S.A. (SIA)
Fecha	28 de Noviembre de 2017

Tabla 1: Identificación de la Declaración de Seguridad

1.1.2 Identificación del TOE

Título	SIAVAL SafeCert Manager
Versión	2.4.02 20150611-1657
Autor	Sistemas Informáticos Abiertos S.A. (SIA)
Identificación CC	Common Criteria for Information Technology Security Evaluation v3.1 R4
EAL	EAL4 + ALC_FLR.1 + AVA_VAN.5

Tabla 2: Identificación del TOE

1.2 Referencias normativas

[1] Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que la que se establece un marco comunitario para la firma electrónica (también referenciada en el documento como “Directiva”).

[2] Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (también referenciado en el documento como "eIDAS" - Electronic Identification and Signature (Electronic Trust Services)).

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev. 4, September 2012.

- Part 1: Introduction and general model.
- Part 2: Security functional components.
- Part 3: Security assurance components.

[4] Common Methodology for Information Technology Security Evaluation CEM, Version 3.1, Rev. 4, September 2012.

[5] CEN/TS 419 241:2014 Security Requirements for Trustworthy Systems Supporting Server Signing.

[6] CEN/TS 419 211 Protection Profiles for Secure Signature Creation Devices.

[7] CEN/TS 419 221 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures.

[8] ISO/IEC 15408 (Common Criteria) Information technology -- Security techniques -- Evaluation criteria for IT security.

[9] ISO/IEC 19790 Information technology — Security techniques — Security requirements for cryptographic modules.

[10] FIPS PUB 140-2 Security Requirements for Cryptographic Modules.

[11] ETSI/TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

1.3 Acrónimos y terminología

AdES: Firma Electrónica Avanzada (Advanced Electronic Signature).

AES: Estándar de Encriptación Avanzada (Advanced Encryption Standard).

API: Interface de programación de aplicaciones (Application Programming Interface).

BBDD: Base de datos.

CAPI: API Criptográfico de Windows (Cryptographic Application Programming Interface or CryptoAPI). Interface de programación de aplicaciones que facilita funciones criptográficas para aplicaciones basadas en Windows.

CC: Common Criteria.

CGA: Aplicación de generación de certificados (Certificate Generation Application).

CSP: Proveedor de servicios criptográficos (Cryptographic Service Provider). Dispone de implementaciones de estándares y algoritmos criptográficos.

CSR: Solicitud de firma de certificado (Certificate Signing Request).

DTBS: Datos a ser firmados (Data To Be Signed).

DTBSR: Representación de los datos a ser firmados (Data To Be Signed Representation).

DTBS/R: Datos a ser firmados o su representación única (Data To Be Signed or its Representation). Datos recibidos por un dispositivo seguro de creación de firma como entrada en una operación de creación de firma. Podría ser el hash de los datos a ser firmados (DTBS) o el hash de una primera parte de los DTBS complementado con la parte restante de los DTBS o los propios DTBS.

EAL: Nivel de garantía de evaluación (Evaluation Assurance Level).

eIDAS: Reglamento (UE) nº 910/2014 del Parlamento Europeo (Electronic Identification and Signature (Electronic Trust Services)).

HMAC: Código de autenticación de mensaje (MAC) construido con una función hash en combinación con una clave privada (Keyed-Hash Message Authentication Code).

HSM: Módulo de Seguridad Hardware (Hardware Security Module).

HTTP: Protocolo de transferencia de hipertexto (Hypertext Transfer Protocol). Es el protocolo usado en cada transacción de la World Wide Web.

IT: Tecnología de la información (Information Technology).

MAC: Código de autenticación de mensaje (Message Authentication Code).

OTP: Contraseña de un único uso (One Time Password).

PIN: Número de identificación personal (Personal Identification Number).

PKI: Infraestructura de clave pública (Public Key Infrastructure).

PKCS: Estándares de criptografía de clave pública (Public-Key Cryptography Standards).

PKCS#1: Estándar criptográfico RSA. Define el formato del cifrado RSA.

PKCS#10: Estándar de solicitud de certificación. Formato de los mensajes enviados a una Autoridad de certificación para solicitar la certificación de una clave pública.

PKCS#11: Interfaz de dispositivo criptográfico. Define un API genérico de acceso a dispositivos criptográficos.

PKCS#12: Estándar de sintaxis de intercambio de información personal. Define un formato de fichero usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

PP: Perfil de protección (Protection Profile).

QES: Firma electrónica cualificada o reconocida (Qualified Electronic Signature).

QSCD: Dispositivo cualificado de creación de firma (Qualified Signature Creation Device).

RA: Autoridad de Registro (Registry Authority).

RSA: "Rivest, Shamir y Adleman". Se trata de un sistema criptográfico de clave pública RSA.

SCA: Aplicación de creación de firma (Signature Creation application).

SCD: Datos de creación de firma (Signature Creation Data). Clave privada utilizada para realizar una operación de firma digital.

SCDev: Dispositivo de creación de firma (Signature Creation Device).

SDO: Objeto de datos firmado (Signed Data Object).

SF: Funciones de seguridad (Security Function).

SFDA: Segundo factor de autenticación.

SFP: Políticas de funciones de seguridad (Security Function Policy).

SFR: Requisitos funcionales de seguridad (Security Functional Requirements).

SMS: Servicio de mensajes cortos (Short Message Service).

SSCD: Dispositivo seguro de creación de firma (Secure Signature Creation Device).

SSL: Capa de conexión segura (Secure Sockets Layer).

ST: Objetivo de seguridad (Security Target).

SVD: Datos de validación de firma (Signature Verification Data). Clave pública vinculada a la SCD y utilizada para realizar la verificación de la firma digital.

TLS: Seguridad en la capa de transporte (Transport Layer Security).

TOE: Objeto de Evaluación (Target of Evaluation).

TSF: Funciones de seguridad del TOE (TOE Security Functions).

TSP: Proveedor de Servicios de Confianza (Trusted Service Provider).

TW4S: Sistemas confiables soportando firma en servidor (Trustworthy Systems Supporting Server Signing).

USB: Bus Universal en Serie (Universal Serial Bus).

VDI: Infraestructura de escritorio virtual (Virtual Desktop Infrastructure).

1.4 Descripción del producto completo *SIAVAL SafeCert*

El TOE identificado como ***SIAVAL SafeCert Manager v2.4.02 20150611-1657*** es parte de una solución global denominada ***SIAVAL SafeCert***, de esta manera, se determina que en esta sección donde se establece el funcionamiento de la solución global de firma en servidor, se reflejan componentes y funcionalidades que no forman parte de la presente evaluación, quedando restringido el ámbito de certificación al TOE definido en el apartado Descripción del TOE.

1.4.1 Características generales de *SIAVAL SafeCert*

SIAVAL SafeCert es una solución de firma centralizada de la familia SIAVAL orientada a facilitar la gestión y el uso de las claves privadas y públicas de los usuarios finales, también identificados como titulares o firmantes.

Funcionando en un entorno operacional seguro, con los componentes con un nivel de seguridad adecuado y siendo gestionado por un prestador cualificado, el producto SIAVAL SafeCert está diseñado para funcionar como un dispositivo cualificado de creación de firma (QSCD), según los requisitos especificados en el Reglamento (UE) nº 910/2014 del Parlamento Europeo (eIDAS: Anexo II), haciendo posible la generación de firmas electrónicas avanzadas (AdES) y de firmas electrónicas cualificas o reconocidas (QES) en un servidor remoto, constituyéndose como un sistema confiable de firma en servidor, Trustworthy Systems Supporting Server Signing (TW4S), según se define en la norma CEN/TS 419 241 que rige este tipo de sistemas.

Tiene las siguientes características generales:

- El producto se centra en la firma del hash o hashes que representa el documento o documentos a firmar, quedando fuera de su alcance la composición de los formatos de los diferentes estándares de firma que pudieran ser construidos por la aplicación de creación de firma que utilizase este producto.

- Permite a los usuarios finales la realización de firmas electrónicas de manera sencilla, sin que éstos deban preocuparse de la gestión y mantenimiento de sus claves.
- Las claves se mantienen seguras y controladas mediante el uso de hardware criptográfico (HSM).
- Facilita la gestión del ciclo de vida de los certificados, puesto que las claves están centralizadas.
- Evita la dispersión o descontrol de las claves de los usuarios al no ser distribuidas y permanecer siempre bajo el control del HSM.
- Controla y audita el acceso a las claves mediante varios niveles de seguridad (PIN, Segundo Factor de Autenticación, etc).
- Dispone de Cliente CSP para Windows, que ofrece a las aplicaciones Windows ya existentes, que utilicen CAPI, la posibilidad de utilizar los certificados del usuario almacenados en SafeCert.
- Permite a los usuarios finales, titulares o firmantes importar certificados (con su clave privada) ya existentes de manera directa, a través del Cliente CSP para Windows.
- Facilita la integración desacoplada con terceros para delegar la generación, gestión y validación del segundo factor de autenticación (SFDA) que puede proteger el acceso a las claves.
- De manera integrada, puede utilizar el producto Identity Guard para la gestión del segundo factor de autenticación, bien mediante el uso de OTPs (One Time Password) enviados por SMS, bien mediante claves de un solo uso generadas en Token físico o software o, también, utilizando Tarjetas de Coordenadas, entre otros.
- Dispone de un componente interno de generación de OTPs (One Time Password) para ser utilizadas como segundo factor de autenticación del firmante.
- Dispone de una Consola web para la administración y gestión centralizada del producto, con distintos niveles de acceso mediante perfilado configurable. Mediante la consola puede realizarse la configuración de repositorios HSMs, conectores de segundo factor de autenticación, sistemas de segundo factor de autenticación, gestión de titulares, asignación y configuración de segundos factores de autenticación para el uso de las claves de cada titular, etc.
- Facilita un conjunto de Servicios web de gestión que permiten que se puedan confeccionar consolas específicas para determinados grupos de administradores con permisos controlados.

- Escalabilidad y Alta Disponibilidad: el diseño de Siaval Safecert y su distribución en formato hardware/appliance permite su adaptación a múltiples entornos de forma sencilla. Por diseño, Safecert permite escalar horizontalmente la infraestructura de firma, de forma que pueda absorber las necesidades de cualquier organización, desde entornos con decenas de firmantes hasta millones de ellos. SIAVAL Safecert ofrece flexibilidad para su instalación en clústeres de Alta Disponibilidad y Tolerancia a Fallos, convirtiéndose en una infraestructura de Firma centralizada totalmente confiable por las organizaciones.

1.4.2 Componentes de SIAVAL SafeCert

La solución completa de SIAVAL SafeCert está formada por diferentes módulos y componentes relacionados de forma lógica tal como se representa en la figura.

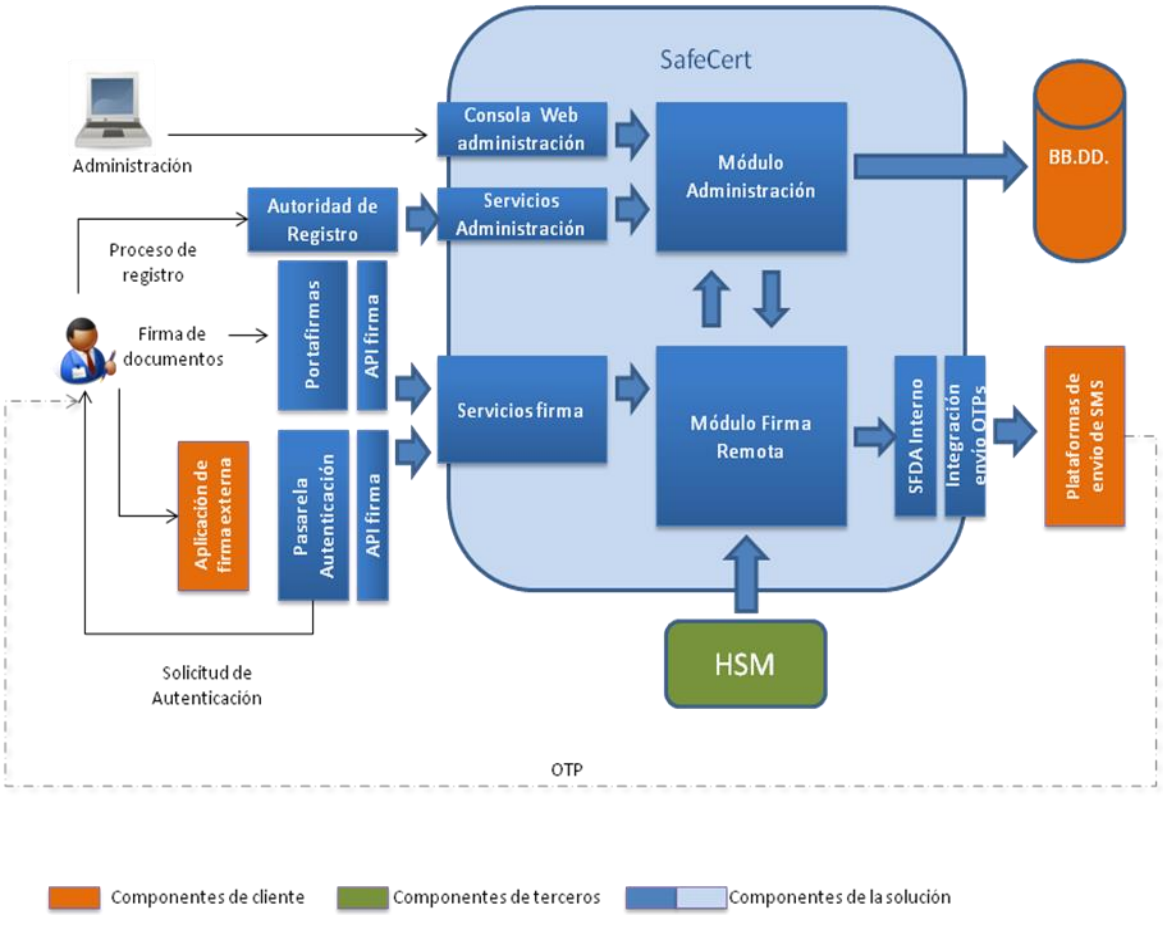


Ilustración 1: Arquitectura lógica completa de SIAVAL SafeCert

Los componentes de la solución son:

- Módulo de firma: Software servidor que proporciona los servicios de firma, importación de claves mediante PKCS#12 y cambio de PIN de claves a través de Servicios Web convencionales y mediante el uso del API de Integración Java.

- Módulo de administración o módulo gestión de repositorio: Componente servidor que permite la gestión de la infraestructura, conectores y sistemas de segundo factor de autenticación, alta/baja de claves/titulares, activación/desactivación temporal de claves de titular, asignación de segundo factor de autenticación a las claves, etc.

- Servicios web de administración que actúan sobre el módulo de administración.

- Consola web de administración que actúa sobre el módulo de administración.

- Repositorio de claves HSM: Hardware criptográfico encargado de la protección segura de las claves, que realiza las operaciones criptográficas de bajo nivel.

- BBDD para el almacenamiento de la configuración de funcionamiento del sistema, datos de trabajo de titulares, trazas de auditoría/operaciones, etc.

- API Java de firma para la explotación de los servicios de firma; dichos servicios de firma también están disponibles como Servicios Web convencionales accesibles de manera directa.

- Componentes de interacción con los firmantes:

    - **SIAVAL Safecert Cliente CSP**: Mediante la utilización de la capa nativa Microsoft CAPI, implementando un Cryptografic Provider propio (CSP). Este mecanismo permite la integración en los entornos Windows, integrándose en el sistema operativo mediante un componente firmado, que permite la ejecución de forma nativa de los servicios criptográficos.

      Este componente permite al usuario de Windows acceder a los certificados que se encuentran dentro del servidor SafeCert mediante el mecanismo estándar, de la misma forma que accede a los certificados que tiene en tarjeta, USB o navegador, y con soporte tanto a escritorios tradicionales como para sistemas VDI o virtualización de aplicaciones con Citrix XenApp, entre otros.

    - **SIAVAL Safecert Pasarela**: Para la integración completamente transparente con aplicaciones, SIAVAL Safecert permite la ejecución en modo “sandbox”, es decir, dentro un entorno totalmente aislado y completamente independiente del de las aplicaciones de negocio. SIAVAL Safecert Pasarela no comparte físicamente ninguna infraestructura con el resto de aplicaciones y a la vez, se evita que en las aplicaciones del cliente se tengan que introducir credenciales o contraseñas. SIAVAL Safecert Pasarela funciona de forma similar a las pasarelas de pago (bancos, PayPal) donde las aplicaciones ceden el control a los entornos especializados, en este caso de firma, que realizan todas las operaciones, incluyendo la interrelación con el cliente.

- **SIAVAL Portafirmas o un SCA de confianza:** Solución de Portafirmas Electrónico que permite la automatización de los flujos de firma, convirtiéndose en un punto de encuentro único entre aplicaciones y usuario. La solución SIAVAL Portafirmas, totalmente integrada con SIAVAL Safecert y con soporte a cualquier certificado electrónico disponible en cualquier dispositivo, facilita la gestión y el despliegue de la firma electrónica de forma sencilla, al permitir controlar los flujos de firma en un entorno independiente, proporcionando firma electrónica a aquellas transacciones que la necesitan, sin tener que modificar la lógica de las aplicaciones.

- **Autoridad de Registro (RA):** Permite gestionar los certificados de los firmantes (titulares), dándolos de alta en el sistema y asegurándose de que cada titular o firmante es el único que conoce los datos de activación de la firma, por ejemplo, requiriendo la presencia de dicho titular durante el proceso de registro para que sea él personalmente el que elija e introduzca dichos datos de activación de la firma.

- Módulo de gestión de Segundo Factor de Autenticación (interno).
- Componentes de integración con Plataformas de envío de OTPs a los titulares.
- Componentes de integración con Plataformas de Segundo Factor de Autenticación.

1.4.3 Características orientadas a la seguridad de SIAVAL Safecert

SIAVAL Safecert, solución de firma centralizada en red, es una plataforma segura, orientada a dar una gran usabilidad de la firma digital, pero siempre manteniendo unos estrictos niveles de control de las claves y trazabilidad en el uso de las mismas.

Los aspectos fundamentales relacionados con la seguridad son:

- Generación de claves basada en HSM FIPS 140-2 Nivel 3.
- Control, protección centralizada de las claves y generación de firmas basados en HSM FIPS 140-2 Nivel 3, evitando la dispersión o descontrol de las claves de los usuarios al no ser distribuidas y permanecer siempre bajo el control del HSM.
- Control de acceso, registro y auditoria de acceso a las claves mediante varios niveles de seguridad (PIN, OTP, etc).
- Segundos factores de autenticación como incremento del nivel de seguridad (OTPs, tokens físicos o móviles, tarjetas de coordenadas,…).

- Registro de actividad de todas las operaciones sensibles realizadas en el sistema (activaciones, firmas, altas, bajas, modificaciones). De esta forma se tiene un control de auditoría de qué ha hecho cada usuario y cuándo lo ha realizado.

- Generación de informes: Listados e informes de la información relativa a usuarios, perfiles, actividad, etc.

Emisión y gestión de certificados: La solución SIAVAL Safecert cuenta además con una solución para la implementación del servicio de registro y emisión telemática de certificados, para cubrir las funciones de una "Autoridad de Registro (RA)", integrada con diferentes Prestadores de Servicios de Certificación. Este componente permite, además de las operaciones propias de emisión y recuperación de claves por parte de los usuarios finales, dotar de una solución completa a los administradores para la gestión del ciclo de vida de los certificados.

1.4.4 Normativas

SIAVAL SafeCert establece su funcionamiento en relación a los requisitos que se establecen en la Directiva 1999/93/CE en su Anexo III así como en el Reglamento Nº 910/2014 (eIDAS) en su Anexo II, ambos del Parlamento Europeo.

En estos requisitos se establece que *"esté garantizada la confidencialidad de los datos de creación de firma"* (Directiva: Anexo III Art. 1.a) (eIDAS: Anexo II Art. 1.a), para ello SIAVAL SafeCert establece los mecanismos de protección adecuados sobre la clave de firma de los firmantes de manera que, en todo momento, quede asegurada su confidencialidad y ésta no pueda ser divulgada.

Igualmente, se determina que *"los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica"* (Directiva: Anexo III Art. 1.a) (eIDAS: Anexo II Art. 1.b), así SIAVAL SafeCert utiliza un dispositivo criptográfico con cumplimiento FIPS 140-2 Nivel 3 que realiza todas aquellas operaciones criptográficas sobre generación de claves que aseguran su unicidad, que *"los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción"***,** y realiza operaciones de firma electrónica que aseguran que *"la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento"* (Directiva: Anexo III Art. 1.b) (eIDAS: Anexo II Art. 1.c)**.**

Además, se determina que *"los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros"* (Directiva: Anexo III Art. 1.c) (eIDAS: Anexo II Art. 1.d)**,** de esta manera SIAVAL SafeCert protege las claves mediante un mecanismo que asegura el control exclusivo de las claves por su legítimos propietarios, esta protección consta de una contraseña cuya posesión es exclusiva del usuario, y un segundo factor de autenticación que se le requerirá al usuario en el momento del uso de su clave de firma.

De la misma forma, se establece que los dispositivos *"no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar"* (Directiva: Anexo III Art. 2) (eIDAS: Anexo II Art. 2), cómo así hace la solución.

La utilización de SIAVAL SafeCert en un entorno donde opere un generador de certificados confiable, una aplicación de creación de firma y sea gestionado por un prestador cualificado de servicios de confianza, establecerá un sistema confiable de generación de firma en servidor, ajustándose a los requisitos, tanto de los dispositivos seguros de creación de firma electrónica (Directiva: Anexo III), como de los dispositivos cualificados de creación de firma electrónica (eIDAS: Anexo II).

1.5 Descripción general del TOE

1.5.1 Tipo del TOE

SIAVAL SafeCert Manager v2.4.02 20150611-1657 es un software de firma electrónica en servidor, que asegura el control exclusivo de las claves de firma por parte del firmante.

1.5.2 Uso del TOE

El conjunto de componentes que conforman el TOE ***SIAVAL SafeCert Manager v2.4.02 20150611-1657*** posibilita la generación de firmas en servidor, de manera que una organización pueda fácilmente establecer un sistema de firma seguro, centralizando los procesos de firma de documentos de sus usuarios. Facilita la gestión del ciclo de vida de las claves, su asociación entre los usuarios, así como el cumplimiento del propósito de uso de dichas claves.

Se establece en todo momento el control exclusivo por parte de los usuarios de sus claves de firma, asegurando el vínculo entre usuario y claves, protegiendo la clave privada de firma de forma tal que únicamente pueda ser utilizada dentro del entorno operativo y por su propietario legítimo.

La forma de interactuar con el TOE es mediante dos interfaces vía webservices, una de uso administrativo y otra de firma, a través de las cuales las aplicaciones invocarán a las operaciones del TOE. Estas interfaces aseguran el control de acceso mediante la autenticación, en todo momento, de los usuarios que acceden a dichos servicios y realizando la autorización en función de perfiles que determinarán el ámbito y uso de las operaciones.

La interfaz WebService vía SOAP de uso administrativo, se utilizará para el aprovisionamiento y activación de las cuentas de los usuarios firmantes en el sistema. De manera que, a través de esta interfaz, la organización establecerá y gestionará a los usuarios firmantes, así como sus claves activas en el sistema.

A la interfaz de firma WebService vía SOAP y mediante mensajes binarios Hessian, se accederá desde aquellas aplicaciones de creación de firma de la organización que se integren con el sistema para posibilitar la firma de documentos. El acceso a estos servicios se accederá autenticando a las aplicaciones solicitantes de la firma, de manera que se establezca un canal seguro entre la aplicación de firma y el TOE. A través de este canal seguro, el usuario, en el momento de la firma, establecerá las credenciales de autenticación a su clave de firma a través de un sistema multicanal, proporcionando una clave secreta que únicamente él conoce, y una contraseña dinámica de un solo uso que se le enviará a su teléfono móvil vía SMS.

Los usuarios firmantes podrán tener asociadas varias claves, de manera que podrán utilizar en cada aplicación de creación de firma la clave requerida en cada momento.

El TOE, mediante configuración, podrá establecer diferentes políticas sobre diferentes aspectos de seguridad:

- Bloqueo/suspensión de las claves tras n fallos de intentos de autenticación en el momento de la firma o cambio de contraseña por parte del usuario firmante.

- Activación del uso de las claves durante periodos de tiempo.

1.5.2.1 Características principales de seguridad del TOE

Las características de seguridad fundamentales del TOE se resumen en:

- **Control de Acceso**: Se establece control de acceso para todas las operaciones realizadas en el TOE de manera que solamente los usuarios autorizados puedan realizar las operaciones para las que tienen permisos.

- **Protección de las claves de firma**: Se asegura en todo momento la protección de las claves de firma de los firmantes, de manera que solamente puedan ser utilizadas dentro del entorno operativo del TOE y no puedan ser divulgadas para su uso ilegítimo.

- **Control Exclusivo de la clave de firma**: La clave de firma se asocia al firmante de manera que éste tenga el control exclusivo para su activación en el momento de la firma.

- **Firma segura**: Se asegura todo el ciclo del proceso de firma, desde el momento en que desde la aplicación de creación de firma se solicita al TOE una firma, tanto en la transmisión de los datos a firmar al TOE, como en la generación de la firma, así como en la devolución de la firma a la aplicación. Así mismo, la firma generada tiene la fortaleza necesaria para que pueda verificarse su integridad.

- **Comprobación de la configuración**: Se asegurará, en todo momento, el acceso a la configuración que se encuentra en la base de datos, verificando que de los datos configurados hayan sido generados por el TOE.

- **Autenticación multicanal**: Se efectúa una autenticación multicanal con secreto estático y contraseña dinámica (OTP) mediante envío de SMS al usuario en la operación de firma, asegurando en todo momento la identidad del firmante.

- **Datos de auditoría:** Se registran datos de auditoría de todas las operaciones realizadas por los usuarios firmantes en el uso de sus claves de firma.

1.5.2.2 Elementos hardware/software/firmware que no forman parte del TOE pero que son necesarios para su correcto funcionamiento.

Los siguientes componentes software y hardware se consideran externos al TOE, aunque son necesarios para su correcto funcionamiento:

- Máquina con el sistema operativo, servidor de aplicaciones y otras utilidades de gestión pre-instaladas, en la que se instala y entrega el software del TOE en modo appliance.
    - El TOE se sirve en una máquina *Dell PowerEdge R320 4 CPU's Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz*.
    - Sistema operativo: CentOS release 6.3 de 64 bits.
    - Servidor de aplicaciones: Apache Tomcat 7.0.82.
    - Cliente HSM: Luna PCI 5.2.1.
    - Java Runtime Enviroment: JDK 1.8.0.152 con JCE Unlimited Strength.
- Consola web de administración de SIAVAL SafeCert que actúa sobre el módulo de administración y establece los parámetros generales de configuración en el TOE.
    - Consola web de administración: SIAVAL/SafeCert Console v2.4.02 20150611-1657.
- Módulo criptográfico (HSM): Hardware criptográfico encargado de las operaciones criptográficas llevadas a cabo por el TOE. Se encarga de realizar las operaciones criptográficas necesarias para la protección de las claves y la operación de firma.
    - **HSM**: Luna PCI (PED) Key Export With Cloning Mode K6Model.
- BBDD para el almacenamiento de la configuración de funcionamiento del sistema, datos de trabajo de titulares, trazas de auditoría/operaciones, etc.
    - PostgreSQL 9.3.
- Componentes de interacción con los firmantes y de integración con el TOE:
    - **Autoridad de Registro (RA):** Permite gestionar los certificados de los firmantes (titulares), dándolos de alta en el sistema y asegurándose de que cada titular o firmante es el único que conoce los datos de activación de la firma, por ejemplo, requiriendo la presencia de dicho titular durante el proceso de registro para que sea él personalmente el que elija e introduzca dichos datos de activación de la firma.

- **Pasarela de envío de SMS:** Se encargará de enviar los SMS a los móviles de los usuarios firmantes que incluyen las contraseñas dinámicas generadas por el TOE para la verificación de la identidad del titular.

- **Aplicación de creación de firma (SCA):** Aplicación que se encargará de enviar la solicitud de firma al TOE y que sirve de intermediario con el usuario firmante para mostrarle los datos a firmar (DTBS/R) y solicitarle los datos de autenticación/activación (SAD) que posteriormente enviará al TOE en el momento de la firma.

- **Aplicación de creación de certificados (CGA):** Aplicación que se encargará de generar el certificado asociado a la clave de firma obtenida a partir de la SVD generada por el TOE.

1.6 Descripción del TOE

1.6.1 Descripción de alto nivel del TOE

El TOE *SIAVAL SafeCert Manager* v*2.4.02 20150611-1657* se compone de los siguientes módulos:

- Módulo de firma, que ofrece las operaciones funcionales de firma electrónica y autenticación a través de servicios,
- Módulo de gestión ofrecido a través de servicios web.
- Módulo de Segundo Factor de Autenticación interno, que gestiona las OTPs utilizadas en los procesos de firma/autenticación.
- Módulo de integración con la Plataforma de envío de OTPs vía SMS.
- Módulo criptográfico que se encargará de invocar las operaciones criptográficas en el HSM.

1.6.2 Definición del TOE

1.6.2.1 Alcance físico del TOE

El TOE es un software donde todos los componentes que lo conforman están incluidos y se suministran en un único fichero de tipo .war, de nombre **"rss-webapp.war"** ***en su versión 2.4.02 20150611-1657*** que vendrá especificado en su fichero MANIFEST interno.

El software se le entrega al consumidor final instalado en una máquina hardware, a modo de appliance, con el sistema operativo, servidor de aplicaciones y resto de utilidades e interfaces necesarios previamente instalados.

En la máquina en modo appliance ya se incluye además del software instalado, los fichero de configuración necesarios para la correcta inicialización del sistema, entre esta configuración inicial se encuentran, los ficheros y claves relativos a la generación HMAC que proporcionarán la autoría por parte del TOE de sus datos en la base de datos. No obstante, una vez configurada la conexión con la base de datos, y ejecutado el script inicial de creación de datos de configuración, será necesario lanzar un proceso que se encargará de calcular los valores HMAC para estos datos iniciales de configuración.

Junto con el software del TOE se facilita un conjunto de manuales, en formato .pdf, en los que se describe la forma de instalar, configurar y operar cada uno de los componentes que lo constituyen, los ficheros .wsdl y el interface Hessian en los que se incluye la documentación de los servicios web facilitados por el software del TOE junto con los esquemas de xml para el envío de datos a través de los servicios.

Listado de manuales del TOE:

- SIAVAL_SafeCert v2.4.02-Manual_de_Instalación v3.1
- SIAVAL_SafeCert v2.4.02-Manual_de_Integración v3.0
- SIAVAL SafeCert v2.4.02-Manual de operaciones v1.1
- SIAVAL SafeCert v2.4.02-Manual de configuración segura v1.2
- Soporte Técnico - Procedimiento Resolución de Incidencias v1.2

Definición de los servicios de firma y gestión

Servicios Web vía SOAP para los servicios de firma y gestión:

- AdminRSS_Services.wsdl.
- RemoteRSS_Services.wsdl.

Servicios Web Binarios Hessian para los servicios de firma:

- Services-Hessian-Firma-1.0.jar

Definición de los esquemas de datos para los servicios de firma y gestión

- Services_2.xsd, XMLExtra_1.xsd, MonitorRSS_1.xsd, MonitorRSS_Result_1.xsd, Commons_Types_2.xsd, Operation_Error_1.xsd, Operation_Result_1.xsd.

En caso de tener que instalar alguna actualización del producto en una máquina de la que ya disponga el consumidor final, a éste se le facilita, por correo electrónico o accesible mediante acceso FTP, un proceso de actualización, en formato **".tgz"**, que incluye el pre-proceso, el proceso y el post-proceso de la actualización del producto, que el consumidor final puede ejecutar sobre la máquina appliance utilizando la herramienta de gestión disponible para tal fin.

1.6.2.2 Alcance lógico del TOE

El TOE es un subconjunto de los componentes que conforman la solución global aportada por el producto.

Los componentes lógicos incluidos en el TOE son:

- ***Módulo de firma:*** Software que proporciona los servicios de firma, importación de claves mediante PKCS#12 y cambio de PIN de activación de la clave privada a través de Servicios Web convencionales y mediante el uso del API de Integración Java.

- ***Módulo criptográfico:*** Que invoca al HSM para realizar las operaciones criptográficas de protección de las claves y firma electrónica.

- ***Servicios web de administración:*** Que actúan sobre el módulo de administración.

- ***Módulo de gestión de Segundo Factor de Autenticación*** (interno).

- ***Componentes de integración con Plataformas de envío de OTPs*** a los titulares.

- ***Componentes de integración con Plataformas de Segundo Factor de Autenticación.***

- ***Ficheros de configuración y claves para la generación y comprobación de la autoría de los datos.***

En la siguiente ilustración se representa la arquitectura lógica de los componentes que constituyen la solución completa, distinguiendo entre los que pertenecen al TOE y aquellos componentes que no forman parte del TOE y son externos a él pero que son necesarios para su correcto funcionamiento:

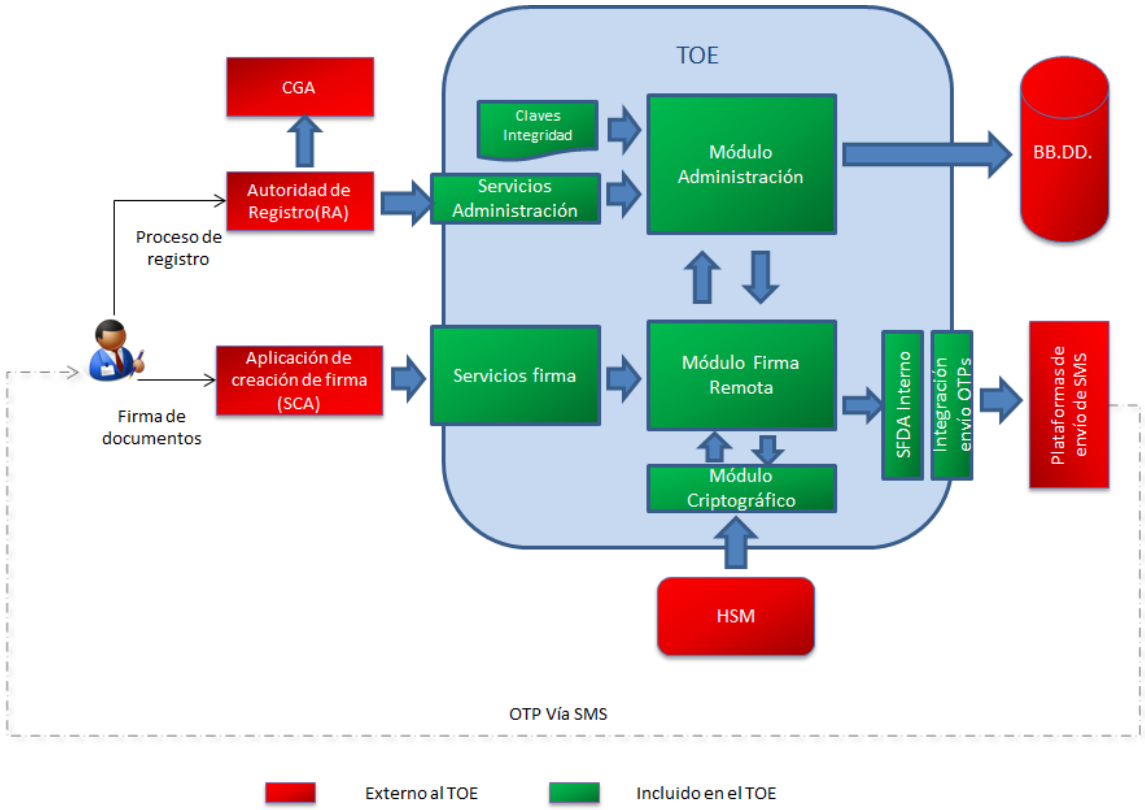


Ilustración 2: Arquitectura lógica del TOE

1.6.2.3 Características de seguridad

1.6.2.3.1 Control de acceso

El acceso a las funcionalidades ofrecidas a través de los servicios tanto de administración como de firma se realiza bajo el control de acceso que establece el requerimiento de autenticación mediante certificados. De esta manera, se establece un canal seguro entre los clientes que utilizan los servicios y el TOE protegiendo en todo momento la comunicación y autenticando de forma unívoca las aplicaciones solicitantes de los servicios del TOE.

Cada aplicación/usuario tendrá asociado un perfil con las funcionalidades que determinarán las operaciones que podrá invocar para llevar a cabo las acciones de administración, registro o firma y autenticación de usuarios firmantes.

1.6.2.3.2 Servicios de administración y gestión

El sistema utiliza servicios de administración y de gestión diferenciados del servicio de firma, a través de estos servicios las aplicaciones de registro pueden llevar a cabo las operaciones de:

- Gestión de cuentas de usuarios firmantes.
- Gestión de claves de firma

- Creación de par de claves de firma
- Creación de claves y su certificado autofirmado
- Asociación de certificados emitidos por un TSP a las claves de firma generadas por el TOE
- Borrado/Bloqueo de las claves de los titulares
- Importación de claves mediante almacenes tipo PKCS#12
- Cambio de contraseñas de activación de la clave privada de firma

- Asociación de segundos factores de autenticación
- Consulta de los datos de auditoría

1.6.2.3.3 SERVICIOS DE FIRMA

El sistema proporciona servicios de firma/autenticación a través de los cuales las aplicaciones de creación de firma puedan invocar las operaciones necesarias para proporcionar a los usuarios de firma la posibilidad de autenticarse o realizar firmas digitales.

Estos servicios proporcionan las operaciones de:

- Consulta de certificados de un usuario firmante
- Operación de firma digital en formato raw utilizando la clave privada asociada al usuario firmante
- Operación de autenticación utilizando la clave privada asociada al usuario firmante
- Operación de cambio de contraseñas de activación de sus claves privadas
- Importación de claves mediante almacenes tipo PKCS#12

1.6.2.3.4 PROTECCIÓN DE LAS CLAVES DE FIRMA

El sistema protege en todo momento las claves de firma. Se utiliza un HSM FIPS 140-2 Nivel 3 para realizar las operaciones criptográficas necesarias tanto para la creación de las claves en él, como para proteger la clave de firma (SCD), de manera que esta protección establece el control exclusivo por parte del usuario.

Las claves privadas de los usuarios se almacenan en la base de datos protegidas. En el momento de la utilización de las claves, serán importadas al HSM para su activación ya que únicamente pueden ser activadas dentro ya del dispositivo criptográfico.

1.6.2.3.5 CONTROL EXCLUSIVO DEL USUARIO DE SUS CLAVES DE FIRMA

El TOE protege las claves de firma con un sistema tal que su uso únicamente puede realizarse por el propietario de la clave que conoce la contraseña que estableció en el momento del registro de la clave en el sistema. Esta contraseña y una clave maestra que se encuentra en el HSM son utilizadas conjuntamente para realizar la protección criptográfica de manera que la clave de firma del usuario únicamente puede activarse proporcionando la contraseña de activación y realizar la operación criptográfica desde el HSM que contiene la clave maestra.

En el sistema se disponen de políticas de contraseñas que son aplicadas a las contraseñas de activación de las claves privadas establecidas por los usuarios firmantes. De esta manera, el usuario deberá proporcionar una clave de activación lo suficientemente robusta para evitar que esta pueda ser descubierta por atacantes que pretendan utilizar sus claves de firma.

1.6.2.3.6 AUTENTICACIÓN MULTICANAL PARA EL CONTROL EXCLUSIVO

Adicionalmente a la protección criptográfica de las claves de firma que imposibilita la utilización de las claves sin la contraseña de activación y fuera del HSM, el uso de dichas claves a través de los servicios de firma del TOE requerirá de un segundo factor de autenticación para garantizar que la clave está siendo utilizada por el propietario legítimo; este segundo factor de autenticación para los usuarios firmantes constará de una contraseña de un solo uso (One Time Password) que será enviada vía SMS al dispositivo registrado en la cuenta del usuario, de manera que para el uso de la clave de firma, el usuario firmante deberá proporcionar la contraseña de activación que únicamente conoce él y la contraseña de un solo uso que se le proporcionará a través de su dispositivo móvil en el momento de la firma.

Mediante este sistema de autenticación con segundo factor, el sistema se protege contra ataques de repetición al establecer las contraseñas de un solo uso, no sirviendo para posteriores operaciones de firma.

1.6.2.3.7 AUTORÍA Y CONFIDENCIALIDAD DE LOS DATOS DEL SISTEMA

El sistema establece un control de establecimiento de la autoría por parte del TOE sobre los datos de configuración, de usuario y auditoría, de manera tal que cualquier lectura de datos no generados por el TOE que se pueda producir desde la base de datos, es detectada y abortado su uso, alertando de tal circunstancia para que los administradores del sistema puedan tomar las medidas oportunas.

Así mismo, todos los datos sensibles que maneja el sistema son cifrados para evitar su divulgación y únicamente puedan ser manejados por los usuarios administradores del sistema a través de las funciones de gestión del TOE.

1.6.2.3.8 AUDITORÍA DEL SISTEMA

El sistema proporciona un sistema de auditoría tanto de las operaciones que se realizan desde los interfaces de administración como para las operaciones que realizan los usuarios firmantes, de esta manera se podrán auditar todas aquellas firmas, cambios de contraseñas de activación, autenticaciones, etc que realizan los usuarios firmantes. Estos datos de auditoría disponen del mismo sistema de autoría que los demás datos del sistema, estableciendo de esta manera la fuente desde donde han sido generados.

Se dispone de un sistema de alerta, el cual avisará a los administradores cuando las tablas que contienen los datos de auditoría sobrepasen el límite establecido de registros para preservar el desbordamiento de espacio establecido en la base de datos. Hay que tener en cuenta el gran volumen de datos que pueden almacenarse en el sistema al realizar un uso intensivo del mismo.

1.6.3 Configuración del TOE

La configuración del TOE consta de dos fases, una primera donde se realiza la generación de los ficheros y claves que posteriormente utilizará el TOE para proteger diferentes aspectos de seguridad y una segunda fase de configuración funcional.

La configuración inicial ya se proporciona con el TOE instalado en modo appliance y consta de:

- Almacén de claves PKCS#12 donde se almacenará la clave de firma y generación de HMAC.
- Fichero de configuración de generación HMAC, este fichero determina que el TOE debe generar valores HMAC para establecer la autoría por parte del TOE de sus datos en la base de datos.
- Fichero con la contraseña cifrada de acceso al almacén de claves PKCS#12 anteriormente descrito.
- Almacén de claves para asegurar la transmisión de datos entre el TOE y la pasarela de envío de SMS.

Una vez establecida esta configuración inicial y tras la instalación del appliance en el entorno operativo, se pasaría a una segunda fase de configuración más funcional.

Esta configuración del TOE es llevada a cabo mediante la consola web de administración, que para la presente evaluación queda fuera del ámbito del TOE. Este proceso de configuración es requisito imprescindible para el correcto funcionamiento del TOE. Una vez establecida la configuración, el TOE funcionará de manera autónoma según el entorno que más adelante se describe. Esta configuración deja preparada la infraestructura, usuarios de aplicación permitidos, perfiles, configuraciones de uso de servicios externos (como la Plataforma de envío de OTPs), etc.

Una vez establecida esta configuración inicial, se podrán utilizar los servicios proporcionados por el módulo de administración para realizar operaciones como el registro de titulares, generación de pares de claves, asociación de certificados, configuración de Segundo Factor de Autenticación para los titulares, etc. Estos servicios son los utilizados habitualmente por la Autoridad de Registro.

La configuración del TOE, que debe ser utilizada para cumplir los requisitos de seguridad definidos en la presente declaración de seguridad para la evaluación Common Criteria, consiste en que se use:

- Comunicaciones seguras entre el TOE y los componentes externos al TOE, en todos los casos, utilizando SSL/TLS.
- Configuración de las claves para la utilización de HMAC en la BBDD, para asegurar la autoría por parte del TOE de la información contenida en ella.
- En el proceso inicial de configuración, deberá generarse la clave maestra del sistema en el HSM y las claves maestras que protegen la configuración de seguridad del sistema.
- Se recomienda el uso de una fuente de tiempo de confianza para asegurar la exactitud del tiempo.
- Configuración del sistema de envío de OTPs para utilizar en la autenticación multicanal.
- Configuración de la conexión con la plataforma de envío de SMS de manera que pueda verificarse la integridad y la confianza de las respuestas de dicha plataforma.
- Configuración de las diversas políticas de seguridad del sistema, como por ejemplo, política de contraseñas de activación de las claves privadas de firma, política de bloqueo de claves, etc. Una vez especificada esta configuración en el TOE, se hará uso de la misma para establecer los criterios de acceso y control de seguridad en función de los parámetros de seguridad establecidos.

Entre los documentos incluidos en el TOE se facilitan los manuales, en formato .pdf, en el que se describen la forma de configurar y operar el producto en su configuración Common Criteria:

- SIAVAL SafeCert v2.4.02- Manual de operaciones v1.1
- SIAVAL SafeCert v2.4.02- Manual de configuración segura v1.2

Aunque el TOE soporta otras plataformas, las pruebas para llevar a cabo la evaluación del TOE se realizan sobre una plataforma concreta que tiene las siguientes características significativas:

- **Hardware**:
    - **Máquina servidor donde reside el TOE**: Dell PowerEdge R320 4 CPU's Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz.

- **HSM**: Luna PCI (PED) Key Export With Cloning Mode K6Model.
- **Máquina servicios externos al TOE**: PC genérico con procesador Intel 64 bits.

- **Software**:
  - **Sistema operativo en el servidor del TOE**: CentOS release 6.3 de 64 bits.
  - **Sistema operativo en el servidor de los servicios externos al TOE**: CentOS release 6.3 de 64 bits.
  - **Servidor de aplicaciones**: Apache Tomcat 7.0.82.
  - **Base de Datos**: PostgreSQL 9.3.
  - **Cliente HSM**: Luna PCI 5.2.1.
  - **Java Runtime Enviroment en servidor del TOE**: JDK 1.8.0.152 con JCE Unlimited Strength .
  - **Consola web de administración**: SIAVAL/SafeCert Console v2.4.02 20150611-1657.
  - Aplicación de creación de firma que invoca a los servicios de firma del TOE (SCA).
  - Aplicación de registro (RA).
  - Aplicación de creación de certificados (CGA).
  - Plataforma de envío de SMS simulada para el envío de OTPs

2. DECLARACIÓN DE CONFORMIDAD

Se declara la conformidad del TOE con las Partes 2 y 3 de Common Criteria for Information Technology Security Evaluation, v3.1 Revisión 4.

- Requisitos Funcionales de seguridad Parte 2 de Common Criteria v3.1 R4 extendida.
- Requisitos de Garantía de Seguridad Parte 3 de Common Criteria v3.1 R4 para el Nivel de Certificación **EAL4+ALC_FLR.1+AVA_VAN.5**.

La metodología de evaluación es Common Methodology for Information Technology Security Evaluation CEM v3.1 R4.

La Declaración de Seguridad de *SIAVAL SafeCert Manager v2.4.02 20150611-1657* no es conforme a ningún PP.

3. DEFINICIÓN DEL PROBLEMA DE SEGURIDAD

En este apartado se identifican los elementos que permiten definir el problema de seguridad del TOE.

3.1 Activos y objetos

Se identifican los siguientes activos y objetos relacionados con el TOE:

1. **D.SCD:** Datos de creación de firma (SCD): Clave privada utilizada para realizar una operación de firma digital.

2. **D.SIGNATURE_REQUEST:** Petición de firma: Conjunto de datos que representan la petición de firma del firmante, incluyendo entre otros:

   - Datos a ser firmados (DTBS) o la representación de esos datos a ser firmados (DTBSR)
   - Contraseña estática de activación de la clave privada
   - Contraseña dinámica (OTP) de autenticación

3. **D.SIGNATURE_DATA:** Firma generada: Dato que representa la firma generada del DTBS utilizando el SCD.

4. **D.AUTHENTICATION_DATA:** Datos de autenticación de las aplicaciones/usuarios que realizarán peticiones al sistema, entre otros:

   - Certificados de usuarios/aplicaciones
   - Certificados de administradores
   - OTPs (One Time Passwords) generadas
   - Datos de acceso a servicios externos

5. **D.SERVICES_TOE:** Servicios del TOE: Servicios a través de los cuales se invocan a los diferentes operaciones del TOE tanto de firma/autenticación como de administración.

6. **D.CONFIGURATION:** Configuración del sistema e información interna del TOE. Los parámetros del sistema y datos del TOE sólo pueden ser modificados por el administrador del sistema. Algunos de los parámetros del sistema y datos que se utilizan en el TOE son, por ejemplo:

   - Atributos de la política de contraseñas estáticas de activación de las claves privadas.
   - Configuración de comunicación con el sistema de entrega de OTPs.

- Fichero de configuración y claves para la generación HMAC

  Las claves y certificados internos del TOE son utilizados exclusivamente para las operaciones criptográficas de aseguramiento del fichero de configuración de HMAC del TOE y para la propia operación del cálculo HMAC, quedando claramente diferenciadas de las claves de operaciones funcionales del TOE. Estas claves internas residen en un almacén criptográfico PKCS#12 y se aloja en la misma máquina del TOE junto con el fichero de configuración.

  Existen dos claves internas del TOE:

  - Clave asimétrica de cifrado/descifrado y firma del fichero de configuración HMAC.

    Estas claves son utilizadas por el TOE para descifrar y verificar el fichero de configuración HMAC asegurando la integridad y confidencialidad del fichero.

  - Clave para el cálculo de resúmenes HMAC.

- Datos de acceso y uso del HSM.

7. **D.USER_DATA:** Datos de trabajo de los usuarios generados por el TOE. Por ejemplo:

   - Identificador y datos propios del usuario.
   - Vínculo entre firmante y sus datos de creación de firma (SCD) y su a clave pública (SVD)
   - Vínculo entre el SCD y la configuración del Sistema de Segundo Factor de Autenticación para esa clave (por ejemplo, el número de teléfono móvil).

8. **D.EXTERNAL_SERVER**: Comunicación entre el TOE y los agentes externos al mismo necesarios para su funcionamiento, entre ellos:

   - Servidor de envío de SMS
   - HSM
   - Base de datos

9. **D.AUDIT_DATA**: Datos de auditoría generados por el TOE.

3.2 Usuarios

3.2.1 Administradores/Operadores del entorno operativo

Todos los administradores/Operadores del entorno tendrán credenciales de acceso, al menos a alguna parte de los componentes que conforman el TOE. De manera que dependiendo del tipo de administrador tendrán credenciales de acceso para desempeñar su función. De esta manera, se pueden clasificar a los administradores y operadores del entorno en las siguientes categorías.

Operadores del sistema: son responsables de operar sobre el sistema de manera habitual y están autorizados para realizar la copia de seguridad y recuperación del sistema.

Administradores del sistema: están autorizados para instalar, configurar y mantener el sistema pero con control de acceso a la información relacionada con la seguridad.

Auditores del sistema: está autorizado para ver los archivos y registros de auditoría del sistema a los efectos de la auditoría de las operaciones del sistema de acuerdo con la política de seguridad.

Los administradores de sistemas son usuarios del sistema con privilegios.

Los auditores de sistemas tienen funciones privilegiadas, pero no son capaces de administrar o configurar el sistema.

3.2.1.1 SuperAdministrador

El TOE dispone de una cuenta especial de usuario administrador, que está asociada al perfil de SuperAdministrador con la que el administrador podrá empezar a realizar las labores de configuración inicial del producto.

Esta cuenta siempre tiene acceso a todas las opciones de gestión y configuración.

3.2.2 Usuarios/Aplicaciones que utilizan el TOE

3.2.2.1 Titulares o firmantes

Se trata de los usuarios que utilizan el TOE, a través de un SCA externo al TOE, con el propósito de realizar operaciones de firma digital. El firmante utiliza la información de la que dispone el TOE y de los datos de activación de firma que conoce y que le facilita el sistema mediante un mecanismo de autenticación multi-canal, para realizar las firmas apoyado en el control exclusivo de las claves que le facilita el sistema.

3.2.2.2 Autoridad de registro

Una Autoridad de Registro (RA) establece, verifica y garantiza la identidad de un titular o firmante a un proveedor de servicios de confianza (TSP - Trusted Service Provider).

El TSP confiará en la RA para ejecutar los procesos relacionados con la fase de inscripción y registro del firmante de forma que se pueda realizar la asignación posterior de certificados por parte del TSP.

Cada RA deberá verificar la identidad del firmante de acuerdo con algún determinado procedimiento. Para diferenciar un firmante de otro, a cada uno de ellos se le asignará un identificador único, lo que le permitirá ser reconocido más adelante en el contexto de aplicación.

La RA será responsable de solicitar al sistema la creación del SCD para un titular y solicitar al TSP la generación de un certificado que vincule el SCD a la identidad del titular. También se encargará de suministrar al sistema el certificado generado para cada titular.

La RA externa al TOE, se autenticará al sistema utilizando un usuario definido para poder invocar los servicios de administración. El usuario de la aplicación de la RA tendrá asignado un perfil con las funcionalidades que permitan solamente hacer uso de los servicios necesarios para realizar dichas operaciones.

3.2.2.3 Aplicación de Creación de Firma (SCA)

La aplicación de firma, externa al TOE, se autenticará al sistema utilizando un usuario definido para poder invocar los servicios que permitan generar firmas a los titulares propietarios de las claves. El usuario de la aplicación de creación de firma tendrá asignado un perfil con las funcionalidades que permitan solamente hacer uso de los servicios necesarios para realizar dichas operaciones.

3.3 Amenazas

3.3.1 Agentes

- **Agente externo**

Ser humano o proceso que no dispone de credenciales de acceso a ningún componente del entorno operativo del TOE. y que su objetivo principal es acceder a los datos de creación de firma (SCD) o falsificar la firma digital a través de los servicios web del TOE. Por ejemplo:

- Intentando utilizar los servicios web del TOE

- Intentando acceder a la red lógica donde opera el TOE para observar el tráfico de red.

- **Agente interno**

Ser humano con un alto potencial de ataque dentro de los usuarios declarados como Administradores/**Operadores del Entorno** Operativo que pueden tener acceso a parte de la información interna del sistema en el entorno operacional del TOE, y que podrían tratar de aprovecharla para realizar una operación de firma en nombre de un titular o firmante del sistema.

A continuación se identifican los agentes internos potencialmente atacantes:

-

- Usuarios del TOE con permisos restringidos (Auditores, Usuarios de servicios del TOE) que quisieran elevar sus privilegios en el sistema.

- Usuarios de la consola de administración de SafeCert que disponen de privilegios restringidos que quisieran elevar sus privilegios en el sistema.

- Usuarios de la consola de administración webmin que disponen de privilegios restringidos en la máquina del TOE que quisieran elevar sus privilegios en el sistema.

3.3.2 Amenazas

Lista de amenazas identificadas:

T.ACCESS_CONTROL: Acceso no autorizado a los servicios del TOE:

Un agente externo puede acceder a los servicios administrativos del TOE y realizar operaciones para las cuales no tiene permiso.

Activos comprometidos: D.SERVICES_TOE.

T. SIGNATURE-SUPPLANT_USER: Uso ilegítimo de los datos de creación de firma (SCD):

Un agente externo consigue utilizar los datos de creación de firma (SCD) a través de los servicios de firma para generar firmas en nombre del usuario propietario.

Activos comprometidos: D.SCD.

T.DTBS-FORGERY: Falsificación de los datos a firmar (DTBS o DTBSR):

Un agente externo modifica los datos a ser firmados (DTBS o DTBSR) enviados por la aplicación de creación de firma (SCA). De esta forma, los datos a ser firmados (DTBS o DTBSR) utilizados por el TOE para realizar la firma no coinciden con los DTBS que el firmante tiene intención de firmar.

Activos comprometidos: D.SIGNATURE_REQUEST.

T.SIGNATURE-FORGERY: Falsificación de la firma digital:

Sin utilizar los datos de creación de firma (SCD), un agente externo falsifica los datos con la firma digital asociada, de forma que la verificación de la firma digital realizada por los datos de validación de firma (SVD) no detecta la falsificación.

Activos comprometidos: D.SIGNATURE_DATA.

T.SIGNER_AUTHENTICATION-DIVULG: Acceso a los datos de autenticación:

Un agente externo accede a la información de autenticación de los firmantes y obtiene las contraseñas estáticas de activación y/o dinámicas.

Activos comprometidos: D.AUTHENTICATION_DATA.

T.HACK_MANINTHEMIDDLE: Ataques de tipo "man in the middle":

Un agente externo consigue información del sistema o de los firmantes, interceptando las comunicaciones realizadas entre el TOE y el resto de componentes con los que dicho TOE interactúa.

Activos comprometidos: D.SERVICES_TOE, D.EXTERNAL_SERVER

T.SCD-DIVULG: Divulgación de los datos de creación de firma (SCD):

Un agente interno extrae los datos de creación de firma (SCD) fuera del entorno operativo del TOE. Puede obtener los datos de creación de firma (SCD) durante su generación, almacenamiento y uso para la creación de firma.

Activos comprometidos: D.SCD.

T.MODIFY_USER_DATA: Modificación no autorizada de los datos de trabajo de los usuarios:

Un agente externo o interno sin permisos para realizar operaciones administrativas, altera los datos de trabajo de los usuarios, por ejemplo para:

- Alterar la relación que vincula el SCD de la persona atacada y se lo asigna a otra persona.
- Alterar la configuración del sistema de segundo factor (por ejemplo el número de móvil) para que la contraseña de un solo uso llegue al atacante en lugar de al usuario legítimo.

Activos comprometidos: D.USER_DATA

T.MODIFY_CONFIGURATION_DATA: Modificación no autorizada de los datos de configuración del TOE:

Un agente externo o interno altera los datos de configuración del TOE, por ejemplo para:

- Modificar los certificados de acceso a los servicios.
- Configuración de la comunicación con agentes externos al TOE.

Activos comprometidos: D.CONFIGURATION

T.OTP-STOLEN: El atacante obtiene una OTP durante la generación, almacenamiento o transferencia a un titular:

Un agente externo intercepta la contraseña de un solo uso cuando ésta se genera, almacena o se envía al titular.

Activos comprometidos: D.EXTERNAL_SERVER.

T.MODIFY_AUDIT_DATA: Modificación de los datos de auditoría:

Un agente externo o interno altera los datos de auditoría modificando, por ejemplo, la autoría de una operación de firma realizada.

Activos comprometidos: D.AUDIT_DATA

T.DATA_NOT_GENERATED_BY_TOE: Datos no generados por el TOE:

Un agente interno o externo establece en la base de datos vinculada al entorno operativo del TOE, datos no generados por el propio TOE. Aun cuando los administradores del entorno operativo son considerados confiables se podrían producir fallos humanos, como por ejemplo:

- Configuración del acceso de la base de datos erróneamente en el TOE. Podría configurarse por error en un entorno productivo, una base de datos de un entorno diferente haciendo funcionar al TOE con una configuración no adecuada con datos generados por otro TOE de un entorno diferente.

- Se podría recuperar un backup de base de datos de un entorno diferente al pretendido recuperar, estableciendo datos que hayan sido generados por otro TOE en otro entorno operativo distinto.

Activos comprometidos: D.AUDIT_DATA, D.CONFIGURATION, D.USER_DATA

3.4 Políticas de seguridad organizacionales

P.Q-CERTIFICATE: Certificado cualificado:

El propietario del TOE utilizará una CGA confiable para generar un certificado cualificado o no cualificado (Directiva: Art.2: 9, Art.2: 10, Anexo I) (eIDAS: Art.3: 14, Art.3: 15, Anexo I) para los SVD generados por el SSCD de acuerdo a la política establecida en el procedimiento de emisión de certificados. Por ejemplo, los certificados contendrán al menos el nombre del firmante y serán generados a partir de la SVD proporcionada por el SSCD que proporciona el TOE.

P.Q-SIGNATURE: Firmas electrónicas:

El sistema crea la firma digital con unos SCD que el firmante mantiene bajo su control exclusivo y que están vinculados a los DTBS o DTBSR de tal manera que cualquier cambio posterior de los mismos sea detectable.

P.REGISTRY_PROCESS: Proceso de registro:

El proceso de registro del titular se realizará utilizando un procedimiento de comprobación de la identidad seguros.

P.ACCESS_CONTROL_SCA: Control de acceso de las aplicaciones de creación de firma:

Los datos de los usuarios y certificados para acceder a los servicios del TOE por parte de las aplicaciones de creación de firmas (SCA), se mantendrán con los niveles de seguridad adecuados para proteger su confidencialidad, así como los datos de autenticación a su clave de firma en el momento de la firma.

P.CONFIGURATION_TOE: Configuración del TOE.

La configuración del TOE se realizará de acuerdo a la documentación proporcionada con el producto.

P.VALIDATION-HMAC: Validación periódica de los HMAC generados en base de datos:

Existirá un usuario que se encargará de recibir y revisar las alertas de HMAC que se pudieran dar en el sistema cuando se detecten datos no generados por el TOE en los datos almacenados en la base de datos.

P.SECURE-HSM: Alto nivel de seguridad del HSM

El dispositivo de creación de firma utilizado por el TOE cumplirá con los requerimientos necesarios para que las operaciones criptográficas sean los suficientemente robustas.

P.ROL_ACCESS_EXCLUSIVE: Perfiles de acceso excluyentes

Los usuarios que tengan acceso tanto a los activos del TOE como al entorno operativo tendrán asociados los perfiles adecuados y estos serán excluyentes, de manera que un usuario no pueda realizar todas las operaciones sobre el TOE y sobre el entorno operacional.

P.ARCHIVE-DATA-AUDIT: Archivado de datos de auditoría

Se establecerá el archivado periódico de los datos de auditoría. Los datos de auditoría que se generan en la base de datos se trasladarán periódicamente a un fichero convenientemente protegido salvaguardando su integridad mediante firma electrónica.

P.BACKUP/RECOVERY-DATA-SYSTEM: Backup/Recovery de los datos del sistema

Se establecerá un backup periódico de todos los datos del sistema que sean necesarios para que tras un posible fallo del sistema, este pueda recuperarse y seguir operando correctamente.

P.SECURE-ALGORITHMS-SIGN: Algoritmos seguros para la firma

Se establecerá en el sistema la utilización de los algoritmos que recomienda la especificación técnica ETSI/TS 119 312, de manera que el hash enviado al TOE para su firma desde la aplicación de creación de firma cumpla con las recomendaciones establecidas así como el algoritmo RSA y sus tamaños de claves utilizados en el HSM solicitados por la RA.

3.5 Hipótesis

A.TRUSTED_TSP: Trusted Service Provider confiable (TSP):

El TSP protege la autenticidad del nombre del firmante y la clave de verificación de firma generando y firmando certificados por una firma electrónica del TSP. Se supone que la autoridad de certificación que expide el certificado para el servicio de autenticación implementa prácticas que se ajustan a una política de certificación autorizada.

A.TRUSTED_SCA: Aplicación de creación de firma de confianza (SCA):

El firmante utiliza únicamente una SCA de confianza. El SCA genera y envía los DTBS o DTBSR con los datos que el firmante desea firmar en una forma adecuada para que sean firmados por el TOE.

A.SECURE_ENVIRONMENT: Entorno seguro:

El entorno operativo ofrecerá medidas suficientes para proteger el TOE y se gestionará y configurará de forma segura desde el entorno operativo de la organización.

A.MGMT_SEND-OTP: Gestión de sistemas para envío de OTPs:

Los sistemas que realizan el envío de OTPs se gestionarán y configurarán de forma segura desde el entorno operativo de la organización.

A.MGMT_BBDD: Gestión de BBDD de configuración:

Los sistemas de BBDD utilizados para almacenar la configuración y datos de los titulares se gestionan y configuran de forma segura desde el entorno de la organización.

A.MGMT_HSM: Gestión de HSM de la organización:

Se supone que los sistemas HSM utilizados por el TOE se gestionan y configuran de forma segura desde el entorno de producción de la organización.

A.CONTROL_TLF_MOVILE: Control del teléfono móvil del firmante:

El firmante mantendrá su teléfono móvil, mediante el que recibe las OTPs, bajo su control y que informará a la organización en el caso de que el teléfono móvil deje de estar en su poder, con el fin de que la cuenta del firmante sea actualizada y no se envíen OTPs a personas incorrectas.

A.TRUSTED_USERS: Usuarios capacitados y de confianza:

Todos los usuarios del entorno operativo del TOE estarán suficientemente capacitados para operar el TOE de forma segura, que salvaguardarán y protegerán los datos utilizados para realizar la autenticación en el sistema, entre ellos se incluyen los usuarios administradores y operadores de la base de datos vinculada al TOE en el entorno operativo.

Los administradores del entorno operativo del TOE estarán suficientemente entrenados para instalar, configurar el TOE y el entorno del TOE de forma segura.

Así mismo, todos aquellos administradores y operadores que tengan algún privilegio de acceso al entorno operativo, serán considerados de confianza y que preservarán la integridad y el buen uso del mismo.

4. OBJETIVOS DE SEGURIDAD

Esta sección identifica y define los objetivos de seguridad para el TOE y para el entorno operativo. Los objetivos de seguridad reflejan la intención de contrarrestar las amenazas identificadas, así como de cumplir con las políticas y consideraciones de seguridad de la organización.

4.1 Objetivos de Seguridad del TOE

O.AUTHENTICATION_USER: Autenticación de usuarios:

Se solicitará autenticación antes de realizar cualquier operación sobre los activos del TOE. El TOE no realizará ninguna operación sin la solicitud de una autenticación previa.

O.ACCESS_CONTROL: Control de acceso:

Se controlará el acceso a los servicios del TOE para determinar los permisos necesarios para realizar operaciones sobre dichos servicios. El TOE a través de sus servicios de operaciones verificará que se tengan los permisos necesarios para realizar la operación solicitada.

O.CONFIDENTIAL_PRIVATE_KEY: Confidencialidad de las claves privadas de los usuarios:

Se mantendrá en todo momento la confidencialidad de las claves privadas de los usuarios, de manera tal que no puedan ser obtenidas para su uso por parte de usuarios ilícitos. El secreto de los SCD (utilizados para la generación de firma) está asegurado mediante protección combinada mediante un secreto solo conocido por el propietario que nunca es almacenada en el TOE y una clave maestra almacenada en el HSM que no puede exportarse hacia el exterior.

O.SIGNER-SOLECONTROL: Control exclusivo de las claves privadas de firma por parte de los usuarios:

Se mantendrá el control exclusivo por parte de los usuarios de sus claves privadas, de forma tal que solamente los legítimos dueños de las claves tendrán la posibilidad de la activación de las claves en el mismo momento de la firma. Esto se conseguirá ya que solamente se podrá activar el SCD en el momento de la firma suministrando el secreto que únicamente conoce el propietario de la clave y un segundo factor de autenticación a través de un dispositivo bajo el control del usuario, junto con además la clave maestra no exportable almacenada en el interior del dispositivo HSM.

De esta manera se protegerá el uso de la clave de firma para protegerla tanto dentro del entorno del TOE como fuera del mismo, ya que si un atacante externo o interno al sistema, obtuviera de la base de datos la clave protegida, no podría utilizarla puesto que esta se encuentra asegurada por la combinación de la contraseña secreta del usuario más la clave maestra que reside en el HSM.

O.SCD_SVD-CORRESPONDENCE: Correspondencia entre SVD y SCD:

El TOE garantizará la correspondencia entre la SVD y el SCD generados por el TOE. Esto incluye la referencia inequívoca de un par SVD/SCD creado para la exportación de los SVD y la creación de una firma digital con el SCD. El TOE verificará en el momento de la asociación entre el SCD y su SVD que efectivamente el par de claves se corresponden mutuamente.

O.SIGNATURE-SECURE: Seguridad criptográfica de la firma digital:

El TOE utilizando el HSM generará firmas digitales que no se pueden realizar sin conocer el SCD a través de técnicas de encriptación robustas. El SCD no podrá ser reconstruido usando firmas digitales o cualquier otro dato exportado desde el TOE. Así mismo, se garantizará la integridad de los datos generados que representan la firma, utilizando algoritmos de criptografía robustos que garanticen su integridad y posterior verificación para demostrar su validez.

O.SCD-ANTIREPLAY: Protección contra ataques de repetición:

La activación de los SCD para su uso desde el TOE estarán protegidos contra ataques de repetición puesto que la activación de la clave de firma requerirá de una contraseña de segundo factor de autenticación enviada al dispositivo móvil del firmante en cada firma.

O.CONFIGURATION-INTEGRITY: Mantener autoría de la configuración:

Se garantizará que los datos de configuración solo puede ser modificados por los usuarios que tengan privilegios suficientes tras su autenticación. Estos datos de configuración incluyen entre otros, los certificados de acceso al sistema, la configuración de envío de la contraseña dinámica de un solo uso (OTP) que se envía para la autenticación de doble factor, etc. Esto se conseguirá mediante el control de acceso de modo que se establezcan los perfiles de acceso a los diferentes usuarios para gestionar correctamente la configuración.

Se verificará que los datos de configuración leídos desde la base de datos han sido generados por el propio TOE y no por otro mediante la generación de un valor HMAC, que permita la verificación de que no han sido generados por otro TOE diferente.

O.USER-DATA-INTEGRITY: Mantener autoría de los datos de trabajo de los usuarios:

Se garantizará que los datos de trabajo solo pueden ser modificados por los usuarios que tengan privilegios suficientes tras su autenticación a través de los servicios del TOE. Estos datos de trabajo incluye, los vínculos entre SCD y SVD con el usuario propietario, datos de usuarios, etc. Esto se conseguirá mediante el control de acceso, de modo que se establezcan los perfiles de acceso a los diferentes usuarios para gestionar correctamente la configuración.

Se verificará que los datos de trabajo de los usuarios leídos desde la base de datos, han sido generados por el propio TOE y no por otro mediante la generación de un valor HMAC, que permita la verificación de que no han sido generados por otro TOE diferente.

O.AUDIT-INTEGRITY: Generación de datos de auditoría

Se generarán datos de auditoría para todas las operaciones realizadas por el TOE, de manera que queden reflejadas las operaciones funcionales del TOE y las operaciones específicas realizadas por los usuarios firmantes a través de los servicios de firma.

Se verificará que los datos de auditoría leídos desde la base de datos han sido generados por el propio TOE y no por otro mediante la generación de un valor HMAC, que permita la verificación de que no han sido generados por otro TOE diferente.

O.VERIFICATION-SERVER-SMS: Verificación de las respuestas del servidor de envío de SMS

El TOE establecerá una comunicación segura entre él y la plataforma de envío de SMS de forma que deberá verificar la autenticidad e integridad de las respuestas de la plataforma de envío de SMS.

O.PROTECT-HMAC-KEY: Protección de la clave de generación HMAC

El TOE salvaguardará la clave con la que se genera el valor HMAC con la que establece la autoría de los datos almacenados en la base de datos. La clave se mantendrá en todo momento en un almacén PKCS#12 protegido por contraseña.

O.CIPHER-PASS: Cifrado de contraseñas de almacenes de claves o configuración de accesos

El TOE salvaguardará las contraseñas de acceso al almacén de claves de generación HMAC, así como la configuración de envío de contraseñas de segundo factor de autenticación, cifrando dichas contraseñas utilizando algoritmos de clave simétrica.

O.DETECT-FUNCTION-SECURITY-SYSTEM: Detección de eventos de seguridad en el sistema

El TOE enviará alertas a los usuarios administradores que se definan, cuando se detecten datos no generados por el propio TOE en la base de datos y cuando el nivel de registros establecidos paras las tablas de auditoría llegue al nivel establecido, de esta manera se podrá programar el archivado de los datos de auditoría.

4.2 Objetivos de Seguridad del Entorno Operacional

OE.RESTRICTED_ACCESS: Acceso restringido

El TOE estará instalado en un servidor físico y en un servidor de aplicaciones ubicados en un entorno seguro y controlado por administradores de confianza los cuales serán los encargados de gestionar el acceso físico al TOE, tanto a sus ficheros de configuración como a los ficheros ejecutables del TOE.

Así mismo, la base de datos utilizada por el TOE para almacenar los datos de configuración, datos de trabajo de usuario y datos de auditoría, deberá tener el control de acceso suficiente para evitar el acceso de agentes externos que pudieran realizar modificaciones que alteren el correcto funcionamiento del TOE.

OE.SECURE_COMMUNICATIONS: Comunicaciones seguras

Las comunicaciones que se establecen a los servicios del TOE serán siempre establecidos a través de mecanismos seguros. La conexión desde los clientes al TOE se realizará a través de una conexión http sobre SSL/TLS; de esta manera las aplicaciones clientes se aseguran que se conectan a un servidor seguro, puesto que deberán confiar en el certificado correspondiente del servidor.

Así mismo las comunicaciones que se realicen desde el TOE a los diferentes componentes necesarios para su funcionamiento, como son, BBDD, Pasarela de envío de SMS, se realizarán también bajo una comunicación segura mediante protocolo SSL. La comunicación al HSM se realizará sin que se produzca comunicación exterior al ser este un módulo PCI instalado en la misma máquina que el TOE y acceder a él mediante los mecanismos PKCS#11 sin producirse comunicación por red.

OE.SVD-VALIDATION: Autenticidad de la SVD

El TSP (Trusted Service Provider) comprobará la validez de la SVD utilizando la prueba de posesión exportada desde el TOE (CSR o firma de la clave pública) antes de suministrar un certificado apropiado para esa SVD.

OE.SCD-SVD-UNICITY: Unicidad de los datos de creación de firma

El HSM garantizará la calidad criptográfica de un par SCD/SVD que se crea como adecuado para la firma electrónica. El SCD utilizado para la creación de firma prácticamente puede darse sólo una vez y no puede ser reconstruido a partir de la SVD. En ese contexto, lo de que 'prácticamente puede darse sólo una vez' significa que la probabilidad de que haya SCDs iguales es insignificante.

OE.CERTIFICATE-GENERATION: Generación de certificados

La Autoridad de Registro solicitará al TSP, que genere unos certificados de acuerdo a lo que se indica en Directiva: Art.2: 9, Art.2: 10, Anexo I y eIDAS: Art.3: 14, Art.3: 15, Anexo I y que incluyan, entre ellos:

- el nombre del firmante,
- la SVD que coincida con el SCD generada a través del TOE y controlado por el firmante,
- la firma del TSP.

OE.AUTHENTICATION_DATA-PROTECTION: Protección de los datos de autenticación introducidos por el usuario

El sistema que solicita los datos al usuario asegurará la confidencialidad e integridad de los mismos hasta que sean enviados al TOE.

Por ejemplo: la contraseña estática de activación del usuario titular, así como la OTP se mantendrán confidenciales y no se revelarán a terceros.

OE.DTBS-CORRECT: La SCA envía al sistema los DTBS correctos

El firmante utilizará un Sistema de Creación de Firma confiable que:

- genera el DTBS/R de los datos que ha sido presentado como DTBS y que el firmante tiene la intención de firmar en una forma que sea apropiada para el TOE.
- envía el DTBS/R al TOE utilizando un canal que asegura la confidencialidad y la integridad DTBS/R.
- se aplica la firma producida por el TOE a los datos, obteniendo la firma final del usuario.

OE.TOE-CONFIGURATION: Configuración TOE de acuerdo a las recomendaciones suministradas

Se proporcionarán todos los manuales suficientes para que el sistema se configure de manera completa y segura.

OE.SEND_OTP-MGMT: Administración y configuración segura del sistema de envío de OTPs

La gestión y configuración del sistema de envío de OTPs se realizará de manera segura y solamente por las personas autorizadas.

OE.SIGNER-ACTIVATION_ACCOUNT: Activación de la cuenta por el firmante

La Autoridad de Registro comprobará la identidad del firmante de manera segura y solicitará la activación de la cuenta del usuario en el sistema. La RA se encargará de solicitar al firmante de manera segura que establezca la contraseña estática que protegerá su SCD. La RA asegurará la integridad y confidencialidad de dicha contraseña hasta su envío al TOE.

OE.SECURE-BACKUPS/RECOVERY-DATA-SYSTEM: Backup y Recovery de los datos del sistema

Se gestionarán y mantendrán los backups de los sistemas externos al TOE de manera segura, asegurando la confidencialidad e integridad de los mismos.

Se determinará periódicamente la ejecución de un backup de todos los datos y elementos del Sistema que se necesiten respaldar para que tras un fallo del sistema, pueda restaurarse a un estado operativo igual al que existía previo al fallo.

Mediante la guía operativa del producto se determinará cuáles de todos los datos son necesarios realizar respaldo, por ejemplo:

- Base de datos
- Claves de entorno: claves y ficheros de configuración operativas
- Configuración de entorno: configuración de conexión a base de datos

- Configuración de acceso al HSM y clave maestra que reside en el HSM

Igualmente se determinará el procedimiento para realizar un recovery del sistema a partir del backup realizado.

Este backup se ciñe al Reglamento (UE) Nº 910/2014 (eIDAS) Anexo II Art. 4 que establece que se podrán duplicar los datos de creación de firma para el propósito de realizar una copia de seguridad con el mismo nivel de protección que el original.

OE.SECURE-HSM: Alto nivel de seguridad del HSM utilizado:

El HSM utilizado por el sistema proporcionará un alto nivel de seguridad, por ejemplo:

- Cumpla los requisitos del CEN/TS EN 419 211;
- O cumpla los requisitos identificados en CEN/TS 419 221-2, CEN/TS 419 221-3 o CEN/TS 419 221-4;
- O sea un sistema confiable que sea evaluado como EAL 4 o superior en cumplimiento con la ISO/IEC 15408, o con un criterio de seguridad equivalente o superior;
- O cumpla los requisitos identificados en ISO/IEC 19790:2006, nivel 3 o superior.
- O cumpla FIPS PUB 140-2, nivel 3.

OE.VALIDATION-HMAC: Validación periódica de los HMAC generados en base de datos:

Se establecerá una validación periódica de la tarea de validación de HMAC para detectar posibles datos no generados por el TOE en los datos de trabajo del usuario, auditoría y/o configuración del TOE.

OE.DOCUMENTATION-SIGNER: Documentación para la formación de usuarios firmantes

Se dispondrá de manuales y procedimientos de uso para que los usuarios firmantes utilicen el entorno operativo de manera segura, sepan proceder ante situaciones como pérdida/cambio del móvil a través del cual recibirán las contraseñas dinámicas y mantengan su contraseña estática de manera que no pueda ser conocida por terceros.

OE.ROL_ACCESS_EXCLUSIVE: Perfiles de acceso excluyentes

Se determinará que para el correcto uso del control de acceso y que los usuarios no puedan realizar todas las operaciones sobre el TOE y sobre el entorno operacional, se determina que:

- Los usuarios con el perfil "*Security Officer"* no podrán tener al mismo tiempo el perfil "*System Auditor"*
- Los usuarios con el perfil "*System Administrator"* y/o *"System Operator"* no podrán tener al mismo tiempo el perfil de "*System Auditor*" y/o "*Security Officer*".

OE.ARCHIVE_AUDIT_DATA: Archivado periódico de los datos de auditoría

Se determinará periódicamente la ejecución del proceso de archivado que proporciona el TOE que genera el archivado de los datos de auditoría desde la base de datos a un fichero que se almacenará de forma segura.

OE.SECURE-ALGORITHMS-SIGN: Utilización de algoritmos seguros

Se especificarán los algoritmos que cada uno de los elementos del sistema puedan utilizar para cumplir las recomendaciones de la especificación técnica ETSI/TS 119 312.

Las aplicaciones de creación de firma utilizarán algoritmos de hashing de SHA-256 o superior.

La aplicación de registro solicitará generación de claves asimétricas de firma con algoritmo de firma RSA con un tamaño de clave no inferior a 2048 bits.

4.3 Justificación de necesidad y suficiencia de los objetivos de seguridad para resolver el problema de seguridad

4.3.1 Mitigación de Amenazas con los Objetivos de Seguridad

AMENAZAS / OBJETIVOS DE SEGURIDAD	T.ACCESS_CONTROL	T. SIGNATURE-SUPPLANT_USER	T.DTBS-FORGERY	T.SIGNATURE-FORGERY	T.SIGNER_AUTHENTICATION-DIVULG	T.SCD-DIVULG	T.HACK_MANINTHEMIDDLE	T.MODIFY_USER_DATA	T.MODIFY_CONFIGURATION_DATA	T.OTP-STOLEN	T.MODIFY_AUDIT_DATA	T.DATA_NOT_GENERATED_BY_TOE
O.AUTHENTICATION_USER	X											
O.ACCESS_CONTROL	X							X	X		X	
O.CONFIDENTIAL_PRIVATE_KEY						X						
O.SIGNER-SOLECONTROL		X				X						
O.SCD_SVD-CORRESPONDENCE		X										
O.SIGNATURE-SECURE				X								
O.SCD-ANTIREPLAY		X										
O.CONFIGURATION-INTEGRITY					X		X					X
O.USER-DATA-INTEGRITY					X					X		X
O.AUDIT-INTEGRITY												X
O.VERIFICATION-SERVER-SMS					X		X			X		
O.PROTECT-HMAC-KEY												X
O.CIPHER-PASS										X		X
O.DETECT-FUNCTION-SECURITY-SYSTEM												X
OE.RESTRICTED_ACCESS								X	X		X	
OE.SECURE_COMMUNICATIONS			X	X	X		X	X	X	X	X	

Tabla 3: Mitigación de Amenazas con los Objetivos de Seguridad

AMENAZAS / OBJETIVOS DE SEGURIDAD	T.ACCESS_CONTROL	T. SIGNATURE-SUPPLANT_USER	T.DTBS-FORGERY	T.SIGNATURE-FORGERY	T.SIGNER_AUTHENTICATION-DIVULG	T.SCD-DIVULG	T.HACK_MANINTHEMIDDLE	T.MODIFY_USER_DATA	T.MODIFY_CONFIGURATION_DATA	T.OTP-STOLEN	T.MODIFY_AUDIT_DATA	T.DATA_NOT_GENERATED_BY_TOE
OE.SVD-VALIDATION				X								
OE.SCD-SVD-UNICITY				X								
OE.AUTHENTICATION_DATA-PROTECTION		X								X		
OE.DTBS-CORRECT			X									
OE.TOE-CONFIGURATION					X		X			X		
OE.SEND_OTP-MGMT					X					X		
OE.SIGNER-ACTIVATION_ACCOUNT		X										
OE.SECURE-BACKUPS/RECOVERY-DATA-SYSTEM												
OE.SECURE-HSM				X								
OE.VALIDATION-HMAC												X
OE.CERTIFICATE-GENERATION												
OE.DOCUMENTATION-SIGNER					X					X		
OE.ARCHIVE_AUDIT_DATA												
OE.ROL_ACCESS_EXCLUSIVE	X											
OE.SECURE-ALGORITHMS-SIGN				X								

Tabla 4: Mitigación de Amenazas con los Objetivos de Seguridad

T.ACCESS_CONTROL: Acceso no autorizado a los servicios del TOE

El acceso no autorizado a los servicios del TOE se mitiga mediante los objetivos de seguridad **O.AUTHENTICATION_USER** y **O.ACCESS_CONTROL,** de manera que cualquier acceso a los servicios del TOE para realizar cualquier operación se requiere una autenticación y una autorización.

Adicionalmente se establece el objetivo del entorno por el cual los usuarios del sistema no puedan realizar todas las operaciones sobre el TOE y sobre el entorno operacional, cumpliendo **OE.ROL_ACCESS_EXCLUSIVE**.

T. SIGNATURE-SUPPLANT_USER: Uso ilegítimo de los datos de creación de firma (SCD)

El uso ilegítimo de los datos de creación de firma será mitigado completamente mediante la combinación de los objetivos de seguridad **O.SIGNER-SOLECONTROL, O.SCD_SVD-CORRESPONDENCE y O.SCD-ANTIREPLAY y mediante los objetivos de seguridad del entorno OE.AUTHENTICATION_DATA-PROTECTION y OE.SIGNER-ACTIVATION_ACCOUNT.**

La utilización de los datos de creación de firma podrían ser utilizados de forma ilegítima tanto desde los servicios propios del TOE como desde fuera de este si se obtuviera el SCD fuera del entorno.

Para mitigar la utilización ilegítima fuera del entorno operacional del TOE, el SCD se protege mediante el cumplimiento del objetivo **O.SIGNER-SOLECONTROL,** de esta manera no será posible acceder al SCD ya que se encuentra protegida en todo momento y solamente puede ser activado en el entorno operacional del TOE.

Para evitar el uso ilegítimo del SCD desde los servicios del TOE por parte de atacantes, se consigue a través de los objetivos operacionales que establecen que el proceso de alta en el sistema de las claves y la vinculación del SCD con el SVD se realice de forma segura, de manera que sea el propietario legítimo quien establezca la contraseña de protección del SCD y el TOE se asegura que en el momento del alta en el sistema la correspondencia del SCD y SVD es la correcta, **OE.SIGNER-ACTIVATION_ACCOUNT, O.SCD_SVD-CORRESPONDENCE**. Igualmente se asegurarán los datos de autenticación en la aplicación de creación de firma, **OE.AUTHENTICATION_DATA-PROTECTION** y se establecen sistemas de protección contra repetición de envío de peticiones al TOE mediante **O.SCD-ANTIREPLAY.**

T.DTBS-FORGERY: Falsificación de los datos a firmar (DTBS o DTBSR)

La falsificación de los datos a firmar se mitiga mediante el objetivo **OE.SECURE_COMMUNICATIONS y OE.DTBS-CORRECT** de manera que la transmisión de los datos a firmar se realice mediante comunicaciones seguras de manera que no puedan ser modificados en el transcurso de la transmisión y asegurando de que la aplicación de creación de firma no altera los datos a firmar enviados al TOE.

T.SIGNATURE-FORGERY: Falsificación de la firma digital

La falsificación de la firma generada se mitiga mediante los objetivos **O.SIGNATURE-SECURE,** firmas seguras mediante algoritmos y claves suficientemente robustos para asegurar la integridad de la misma **OE.SECURE-ALGORITHMS-SIGN** y **OE.SECURE_COMMUNICATIONS** que establece la transmisión de los datos de la firma de forma segura, **OE.SVD-VALIDATION y OE.SCD-SVD-UNICITY** que determina que la firma pueda verificarse con su SVD correspondiente ya que se garantiza su correspondencia, finalmente se asegura la robustez durante el proceso de la firma en el HSM mediante **OE.SECURE-HSM.**

T.SIGNER_AUTHENTICATION-DIVULG: Acceso a los datos de autenticación

El acceso a los datos de autenticación, contraseña estática de protección del SCD y la contraseña dinámica generada en el momento de la firma y enviada al dispositivo físico en propiedad del usuario, se efectuará mediante la protección de los datos en la transmisión de los mismos con **OE.SECURE_COMMUNICATIONS,** la protección del envío mediante SMS de la contraseña dinámica mediante **OE.SEND_OTP-MGMT, O.VERIFICATION-SERVER-SMS,** y la comprobación de que los datos leídos fueron generados por el TOE mediante **O.CONFIGURATION-INTEGRITY y O.USER-DATA-INTEGRITY,** de esta manera se comprueba que la pasarela de envío de SMS es confiable, por lo tanto se asegura la comunicación segura del segundo factor de autenticación. Así mismo, de determina la correcta configuración de la pasarela de envío de SMS mediante **OE.TOE-CONFIGURATION**, y que se proporcionará la documentación necesaria a los usuarios firmantes para que sepan gestionar sus credenciales de autenticación de forma segura, **OE.DOCUMENTATION-SIGNER.**

T.SCD-DIVULG: Divulgación de los datos de creación de firma (SCD)

La divulgación de los datos de creación de firma se mitigan mediante **O.CONFIDENTIAL_PRIVATE_KEY y O.SIGNER-SOLECONTROL,** de esta manera el SCD se mantiene en todo momento protegido mediante clave secreta conocida únicamente por el propietario legítimo de la clave y la clave maestra establecida en el HSM.

T.HACK_MANINTHEMIDDLE: Ataques de tipo "man in the middle"

Los ataques del tipo man in the middle para interceptar y/o modificador los datos transmitidos entre la SCA y los servicios del TOE o desde el TOE a la pasarela de envío de SMSs se mitigan mediante el aseguramiento de las comunicaciones entre las partes mediante **OE.SECURE_COMMUNICATIONS** y comprobando en cada lectura de datos la de la configuración del TOE en cuanto a las comunicaciones seguras y la configuración del servidor de envío de SMS que fueron generados por el TOE mediante **O.CONFIGURATION-INTEGRITY** y se configuraron correctamente mediante **OE.TOE-CONFIGURATION**. Así mismo, se comprobará la respuesta de la pasarela de envío de SMS verificando la firma de su respuesta, **O.VERIFICATION-SERVER-SMS**, de esta manera queda asegurada la confiabilidad de la comunicación entre el TOE y la pasarela de envío de SMS.

T.MODIFY_USER_DATA: Modificación no autorizada de los datos de trabajo de los usuarios

La modificación no autorizada por parte de un usuario que no tenga los privilegios necesarios para acceder a los datos de trabajo de usuario, se evitará mediante el control de acceso establecido en los servicios del TOE a través de **O.ACCESS_CONTROL,** y mediante el objetivo de entorno **OE.RESTRICTED_ACCESS** que establece el acceso restringido a todos los elementos del entorno operativo del TOE, entre ellos la base de datos. De esta manera, se protege la modificación de los datos a través de los servicios del TOE para usuarios sin autorización y la modificación de los datos a través del acceso no autorizado a la base de datos.

Además se establece **OE.SECURE_COMMUNICATIONS** para preservar los datos durante su envío desde el TOE hasta la base de datos.

T.MODIFY_CONFIGURATION_DATA: Modificación no autorizada de los datos de configuración del TOE

La modificación no autorizada por parte de un usuario que no tenga los privilegios necesarios para la modificación de la configuración del TOE, se evitará mediante el control de acceso establecido en los servicios del TOE mediante **O.ACCESS_CONTROL,** y mediante el objetivo de entorno **OE.RESTRICTED_ACCESS** que establece el acceso restringido a todos los elementos del entorno operativo del TOE, entre ellos la base de datos. De esta manera, se protege la modificación de los datos a través de los servicios del TOE para usuarios sin autorización y la modificación de los datos a través del acceso no autorizado a la base de datos.

Además se establece **OE.SECURE_COMMUNICATIONS** para preservar los datos durante su envío desde el TOE hasta la base de datos.

T.OTP-STOLEN: El atacante obtiene una OTP durante la generación, almacenamiento o transferencia a un titular

La obtención de una contraseña dinámica de un solo uso por parte de un atacante en las diferentes fases de generación, almacenamiento y transmisión de la misma hasta el usuario se mitiga mediante el cifrado seguro de la contraseña **O.CIPHER-PASS** almacenándola de forma segura en la base de datos manteniendo su integridad **O.USER-DATA-INTEGRITY**. Posteriormente para el envío seguro de la contraseña a través de la pasarela de envío de SMS se establecen, comunicaciones seguras **OE.SECURE_COMMUNICATIONS,** configuración en el TOE de la plataforma de envío de SMS y su correspondiente certificado de verificación de su respuesta, **O.VERIFICATION-SERVER-SMS, OE.TOE-CONFIGURATION y OE.SEND_OTP-MGMT.**

Una vez transmitido el certificado al usuario, se establece el envío seguro del mismo a los servicios del TOE para su autenticación mediante **OE.SECURE_COMMUNICATIONS y OE.AUTHENTICATION_DATA-PROTECTION.**

El usuario mantendrá el móvil en su poder a través del cual recibirá la contraseña dinámica y sabrá proceder notificando cualquier pérdida o cambio de teléfono móvil al haber recibido la formación necesaria, **OE.DOCUMENTATION-SIGNER.**

T.MODIFY_AUDIT_DATA: Modificación de los datos de auditoría

La generación no autorizada por parte de un usuario que no tenga los privilegios necesarios para el acceso a los interfaces del TOE, se evitará mediante el control de acceso establecido en los servicios del TOE mediante **O.ACCESS_CONTROL,** y mediante el objetivo de entorno **OE.RESTRICTED_ACCESS** que establece el acceso restringido a todos los elementos del entorno operativo del TOE, entre ellos la base de datos donde se almacenan los datos de auditoría. De esta manera, se protege la generación de los datos a través de los servicios del TOE para usuarios sin autorización y la modificación de los datos a través del acceso no autorizado a la base de datos.

Además se establece **OE.SECURE_COMMUNICATIONS** para preservar los datos durante su envío desde el TOE hasta la base de datos.

T.DATA_NOT_GENERATED_BY_TOE: Datos no generados por el TOE

El establecimiento de datos no generados por el TOE en la base de datos, se mitiga mediante la comprobación de la autoría de los datos por parte del TOE a través de **O.CONFIGURATION-INTEGRITY, O.USER_DATA_INTEGRITY y O.AUDIT_INTEGRITY** de terminan la comprobación por parte del TOE de cada lectura de datos que se realiza, de la comprobación del valor HMAC correspondiente en cada registro de base de datos, este valor determina la autoría de los datos por parte del TOE a través de su clave única de cálculo de HMAC. A través de **O.PROTECT-HMAC-KEY** y **O.CIPHER-PASS** se protege el acceso a la clave de cálculo HMAC y mediante **O.DETECT-FUNCTION-SECURITY-SYSTEM** y **OE.VALIDATION-HMAC** se establece la configuración de la tarea de alertas que se generarán para notificar posibles datos no generados por el TOE en la base de datos.

4.3.2 Cumplimiento de Políticas/Hipótesis con los Objetivos de Seguridad

POLÍTICAS / HIPÓTESIS OBJETIVOS DE SEGURIDAD	P.Q-CERTIFICATE	P.Q-SIGNATURE	P.REGISTRY_PROCESS	P.ACCESS_CONTROL_SCA	P.CONFIGURATION_TOE	P.VALIDATION-HMAC	P.SECURE-HSM	P.ROL_ACCESS_EXCLUSIVE	P.ARCHIVE-DATA-AUDIT	P.BACKUP/RECOVERY-DATA-SYSTEM	P.SECURE-ALGORITHMS-SIGN		A.TRUSTED_TSP	A.TRUSTED_SCA	A.SECURE_ENVIRONMENT	A.MGMT_SEND-OTP	A.MGMT_BBDD	A.MGMT_HSM	A.CONTROL_TLF_MOVILE	A.TRUSTED_USERS
O.AUTHENTICATION_USER				X	X															
O.ACCESS_CONTROL				X	X															
O.CONFIDENTIAL_PRIVATE_KEY		X																		
O.SIGNER-SOLECONTROL		X																		
O.SCD_SVD-CORRESPONDENCE		X	X																	
O.SIGNATURE-SECURE		X																		
O.SCD-ANTIREPLAY		X																		
O.CONFIGURATION-INTEGRITY					X	X														
O.USER-DATA-INTEGRITY						X														
O.AUDIT-INTEGRITY						X														
O.VERIFICATION-SERVER-SMS		X																		
O.PROTECT-HMAC-KEY						X														
O.CIPHER-PASS						X														
O.DETECT-FUNCTION-SECURITY-SYSTEM						X			X											

Tabla 5: Cumplimiento de Políticas/Hipótesis con los Objetivos de Seguridad

POLÍTICAS / HIPÓTESIS OBJETIVOS DE SEGURIDAD	P.Q-CERTIFICATE	P.Q-SIGNATURE	P.REGISTRY_PROCESS	P.ACCESS_CONTROL_SCA	P.CONFIGURATION_TOE	P.VALIDATION-HMAC	P.SECURE-HSM	P.ROL_ACCESS_EXCLUSIVE	P.ARCHIVE-DATA-AUDIT	P.BACKUP/RECOVERY-DATA-SYSTEM	P.SECURE-ALGORITHMS-SIGN		A.TRUSTED_TSP	A.TRUSTED_SCA	A.SECURE_ENVIRONMENT	A.MGMT_SEND-OTP	A.MGMT_BBDD	A.MGMT_HSM	A.CONTROL_TLF_MOVILE	A.TRUSTED_USERS
OE.RESTRICTED_ACCESS					X										X	X	X	X		X
OE.SECURE_COMMUNICATIONS				X	X										X					
OE.SVD-VALIDATION	X	X											X							
OE.SCD-SVD-UNICITY	X	X																		
OE.AUTHENTICATION_DATA-PROTECTION			X	X										X						
OE.DTBS-CORRECT		X												X						
OE.TOE-CONFIGURATION				X	X										X	X	X	X		X
OE.SEND_OTP-MGMT																X				
OE.SIGNER-ACTIVATION_ACCOUNT		X	X																	
OE.SECURE-BACKUPS/RECOVERY-DATA-SYSTEM										X							X	X		
OE.SECURE-HSM		X					X											X		
OE.VALIDATION-HMAC						X														
OE.CERTIFICATE-GENERATION	X	X											X							
OE.DOCUMENTATION-SIGNER			X																X	
OE.ROL_ACCESS_EXCLUSIVE								X												
OE.ARCHIVE_AUDIT_DATA									X											
OE.SECURE-ALGORITHMS-SIGN											X									

Tabla 6: Cumplimiento de Políticas/Hipótesis con los Objetivos de Seguridad

4.3.2.1 Justificación de Políticas con los Objetivos de Seguridad

P.Q-CERTIFICATE: Certificado cualificado

Desde la CGA se generarán los certificados conforme a **OE.CERTIFICATE-GENERATION** y mediante **OE.SVD-VALIDATION y OE.SCD-SVD-UNICITY,** de esta manera se asegurará que el certificado se emitirá a partir del correspondiente SVD proporcionado por el TOE y la correcta correspondencia con su SCD.

P.Q-SIGNATURE: Firmas electrónicas

El firmante utiliza un sistema de creación de firma para firmar datos con firma electrónica avanzada, que es una firma electrónica cualificada si está basada en un certificado cualificado válido.

Mediante **O.SCD_SVD-CORRESPONDENCE, OE.SVD-VALIDATION, OE.CERTIFICATE-GENERATION, OE.SECURE-HSM y OE.SCD-SVD-UNICITY** se asegura la generación segura y única del par de claves SCD y su correspondiente SVD.

Durante el proceso de firma se asegura la generación de los datos de firma mediante la confidencialidad en todo momento de la clave de firma, **O.CONFIDENTIAL_PRIVATE_KEY** y el aseguramiento que dicha clave queda bajo el control único del usuario mediante **O.SIGNER-SOLECONTROL,** así como la robustez de la firma mediante **O.SIGNATURE-SECURE** y la integridad de los datos a firmar con **OE.DTBS-CORRECT.**

Se evidencia que el usuario ha sido quien ha realizado la firma mediante **O.SCD-ANTIREPLAY,** no se pueden realizar envíos de solicitud de firmas repetidas**.** Que los datos de trabajo del usuario están asegurados así como el momento de la activación de la cuenta del mismo mediante **OE.SIGNER-ACTIVATION_ACCOUNT.** Por último, se asegura el envío de la contraseña dinámica mediante **O.VERIFICATION-SERVER-SMS**.

P.REGISTRY_PROCESS: Proceso de registro

El proceso de registro del usuario firmante se realizará mediante la aplicación de registro (RA), de forma que se verifique la identidad del usuario firmante antes de crear las claves asociadas al usuario protegidas con el SAD mediante un sistema multicanal con el cumplimiento de **OE.SIGNER-ACTIVATION_ACCOUNT y OE.AUTHENTICATION_DATA-PROTECTION.** Así mismo se encargará de solicitar el certificado a la aplicación de generación de certificados (CGA) y enviándolo al TOE para asociar el certificado con la clave privada, cumpliendo **O.SCD_SVD-CORRESPONDENCE** se mantiene el vínculo SCD-SVD.

Los usuarios firmantes deberán mantener en todo momento el secreto y no difundir su clave estática de autenticación a su clave de firma, a los usuarios se les suministrará documentación para que puedan seguir los procedimientos adecuados para el correcto uso del sistema, **OE.DOCUMENTATION-SIGNER.**

P.ACCESS_CONTROL_SCA: Control de acceso de las aplicaciones de creación de firma:

Los certificados para acceder a los servicios del TOE por parte de las aplicaciones de creación de firmas (SCA), se mantendrán con los niveles de seguridad adecuados para proteger su confidencialidad. Las aplicaciones de creación de firma accederán a los servicios del TOE mediante autenticación con certificado y un nivel de control de acceso adecuado a las operaciones de firma cumpliendo **O.AUTHENTICATION_USER y O.ACCESS_CONTROL.** La transmisión de los datos se realizará siempre de manera que se envíen bajo un canal seguro, **OE.SECURE_COMMUNICATIONS** y salvaguardarán la difusión de sus credenciales de acceso al TOE y los datos de autenticación de los usuarios firmantes cumpliendo **OE.AUTHENTICATION_DATA-PROTECTION.** Por último, la configuración entre la aplicación de firma y el TOE se realizará de acuerdo a la documentación proporcionada por el TOE, **OE.TOE-CONFIGURATION.**

P.CONFIGURATION_TOE: Configuración del TOE

La configuración del TOE se realizará de forma correcta y segura mediante el cumplimiento de **OE.TOE-CONFIGURATION** que establece la entrega de la documentación necesaria para la correcta configuración del TOE, así mismo se establece la autenticación y el control de acceso para la configuración mediante **OE.RESTRICTED_ACCESS, OE.SECURE_COMMUNICATIONS, O.AUTHENTICATION_USER** y **O.ACCESS_CONTROL** y la comprobación de la autoría de dicha configuración mediante **O.CONFIGURATION-INTEGRITY.**

P.VALIDATION-HMAC: Validación periódica de los HMAC generados en base de datos

Se podrá comprobar la autoría por parte del TOE de los datos de configuración, datos de trabajo de usuario y datos de auditoría mediante el cumplimiento de **OE.VALIDATION-HMAC** a partir de las alertas generadas al detectar cualquier dato no generado por el TOE en los datos almacenados en la base de datos mediante **O.DETECT-FUNCTION-SECURITY-SYSTEM**, **O.CONFIGURATION-INTEGRITY, O.USER-DATA-INTEGRITY, O.AUDIT-INTEGRITY.** El aseguramiento del valor HMAC se realiza mediante el cumplimiento de **O.PROTECT-HMAC-KEY y O.CIPHER-PASS.**

P.SECURE-HSM: Alto nivel de seguridad del HSM

El dispositivo de creación de firma utilizado por el TOE cumplirá con los requerimientos necesarios para que las operaciones criptográficas sean los suficientemente robustas. A través de **OE.SECURE-HSM** se establece el nivel de cumplimiento del HSM.

P.ROL_ACCESS_EXCLUSIVE: Perfiles de acceso excluyentes

Se establecerán los perfiles de cada grupo de usuarios de manera que un mismo usuario no pueda realizar todas las operaciones sobre el TOE, cumpliendo **OE.ROL_ACCESS_EXCLUSIVE** se determinarán qué perfiles podrá tener un mismo usuario y por lo tanto el nivel de control de acceso a los objetos del TOE.

P.ARCHIVE-DATA-AUDIT: Archivado de datos de auditoría

Se establecerá el archivado periódico de los datos de auditoría en función de las alertas recibidas mediante **O.DETECT-FUNCTION-SECURITY-SYSTEM** que determinan que el nivel de datos de auditoría ha llegado al nivel de archivado.

El administrador entonces determinará el archivado de los datos de auditoría mediante **OE.ARCHIVE_AUDIT_DATA** que establece el archivado de los datos periódicamente.

P.BACKUP/RECOVERY-DATA-SYSTEM: Backup/Recovery de los datos del sistema

Se realizarán backups de los datos del sistema necesarios para la recuperación del entorno en caso de fallo crítico del sistema, se establecerán mediante **OE.SECURE-BACKUPS/RECOVERY-DATA-SYSTEM,** que determina la periodicidad y los procedimientos para realizar el backup de todos los datos necesarios para el sistema, así como los procedimientos para realizar la restauración del sistema a partir de un backup realizado.

P.SECURE-ALGORITHMS-SIGN: Utilización de algoritmos seguros para la firma

Se utilizarán únicamente algoritmos seguros dentro del proceso de firma según determina **OE.SECURE-ALGORITHMS-SIGN,** que determina la utilización de los algoritmos y parámetros de seguridad que recomienda la especificación técnica ETSI/TS 119 312.

4.3.2.2 Justificación de Hipótesis con los Objetivos de Seguridad

A.TRUSTED_TSP: Trusted Service Provider (TSP)

El TSP protegerá la autenticidad del nombre del firmante y la clave de verificación de firma generando y firmando certificados por una firma electrónica del TSP. El TSP validará la SVD generada desde el TOE **OE.SVD-VALIDATION** y generará el certificado de acuerdo a **OE.CERTIFICATE-GENERATION.** De esta manera, se asegura la generación de certificados a partir del SVD generado por el TOE confiables y válidos para la creación de firmas cualificadas.

A.TRUSTED_SCA: Aplicación de creación de firma de confianza (SCA)

El firmante utiliza SCAs de confianza. El SCA genera y envía los DTBS o DTBSR con los datos que el firmante desea firmar en una forma adecuada para que sean firmados por el TOE. La aplicación se autenticará al TOE mediante **OE.AUTHENTICATION_DATA-PROTECTION** de manera que solamente SCA confiables podrán hacer uso de los servicios del TOE. La aplicación enviará los datos a firmar a través de los canales seguros al TOE obteniendo los datos binarios representativos de la firma generada, **OE.DTBS-CORRECT.**

A.SECURE_ENVIRONMENT: Entorno seguro

Al entorno operativo solamente se puede acceder con los permisos y controles de acceso necesarios establecidos por **OE.RESTRICTED_ACCESS,** de esta manera solamente podrán acceder a configurar el TOE los usuarios administradores con los permisos necesarios. Los usuarios administradores configurarán el TOE mediante las especificaciones de la documentación del TOE **OE.TOE-CONFIGURATION** y asegurando las comunicaciones con terceros mediante las especificaciones de seguridad **OE.SECURE_COMMUNICATIONS.**

A.MGMT_SEND-OTP: Gestión de sistemas para envío de OTPs

La gestión de la plataforma de OTPs se configurará de forma segura estableciendo los niveles de control de acceso necesarios para que solamente los usuarios con permisos puedan acceder a su configuración, **OE.RESTRICTED_ACCESS.** Así mismo, la configuración de la plataforma de envío de OTPs se configurará en el TOE tal y como indica la documentación del producto, **OE.TOE-CONFIGURATION.**

De igual forma, se establece la configuración de forma segura entre el TOE y de la plataforma de envío de SMS mediante **OE.SEND_OTP-MGMT.** De esta manera, se asegura la confidencialidad de la contraseña dinámica en su envío entre el TOE y el usuario de firma.

A.MGMT_BBDD: Gestión de BBDD de configuración

La base de datos tendrá las restricciones de accesos necesarias para que solamente los usuarios autorizados puedan acceder tanto a su configuración como a los datos almacenados, **OE.RESTRICTED_ACCESS.** Así mismo, se efectuarán los backups periódicos necesarios para asegurar la recuperación del sistema en caso de fallo o detección de ataque mediante **OE.SECURE-BACKUPS/RECOVERY-DATA-SYSTEM.** La configuración de la conexión a la base de datos dentro del TOE se realizará de acuerdo a la documentación establecida por el producto, **OE.TOE-CONFIGURATION.**

A.MGMT_HSM: Gestión de HSM de la organización

El HSM tendrá las restricciones de accesos necesarias para que solamente los usuarios autorizados puedan acceder tanto a su configuración como a los datos almacenados en él, **OE.RESTRICTED_ACCESS.** Así mismo, se efectuarán los backups periódicos necesarios para asegurar la recuperación del sistema en caso de fallo o detección de ataque mediante **OE.SECURE-BACKUPS/RECOVERY-DATA-SYSTEM.** La configuración del acceso al HSM dentro del TOE se realizará de acuerdo a la documentación establecida por el producto, **OE.TOE-CONFIGURATION** y cumpliendo con los niveles de seguridad establecidos en **OE.SECURE-HSM**.

A.CONTROL_TLF_MOVILE: Control del teléfono móvil del firmante

El teléfono móvil del usuario firmante deberá mantenerse bajo su control de acuerdo a recibir en él las contraseñas dinámicas necesarias para activar la firma, para ello se informará al usuario mediante la entrega de la documentación de uso de la plataforma de firma, así como los procedimientos que deberá seguir en caso de pérdida del control de su teléfono móvil para desactivar o modificar sus datos en el sistema, **OE.DOCUMENTATION-SIGNER.**

A.TRUSTED_USERS: Usuarios capacitados y de confianza

Todos los usuarios de TOE estarán suficientemente capacitados para operar el TOE de forma segura, tendrán establecido los diferentes accesos de acuerdo con el perfil de cada uno de ellos, **OE.RESTRICTED_ACCESS,** y podrán desempeñar su trabajo convenientemente al disponer de la documentación necesaria y suficiente para configurar y gestionar el TOE, **OE.TOE-CONFIGURATION**.

4.3.3 Conclusión

Como se evidencia en los apartados anteriores, todas las amenazas se mitigan con uno o varios objetivos de seguridad al igual que cada política e hipótesis planteadas, tienen sus correspondientes objetivos para su cumplimiento, y que todos los objetivos establecidos son necesarios para dar solución al problema de seguridad.

5. DEFINICIÓN DE COMPONENTES EXTENDIDOS

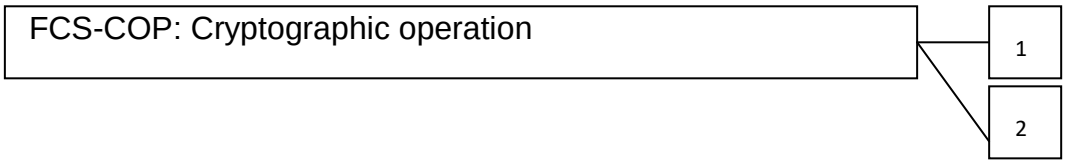
A continuación se definen aquellos componentes extendidos necesarios para cubrir los requisitos de seguridad del TOE que no son cubiertos por componentes Common Criteria v3.1 R4.

5.1 Operaciones criptográficas

A continuación se extiende la clase **CLASS FCS: CRYPTOGRAPHIC SUPPORT** definida en Part 2: Security functional components de Common Criteria v3.1 R4 para adaptar de manera adecuada los requisitos funcionales de seguridad del TOE en lo referente a las operaciones criptográficas utilizadas por el TOE.

Se justifica la extensión de la clase **FCS: Cryptographic Support** ya que no existe componente que establezca las operaciones criptográficas que son invocadas por el TSF y que son realizadas en su implementación por un dispositivo externo. De esta manera, se amplía la familia **Cryptographic operation (FCS_COP)** definiendo un nuevo nivel **FCS_COP.2** que establece la delegación de las operaciones criptográficas en un dispositivo que cumpla un nivel evaluado de FIPS 140-2 SL3.

Component levelling



FCS_COP.2 Delegated Cryptographic operation, requires a cryptographic operation to be performed into an external device **validated to FIPS 140-2 SL3**.

Management: FCS_COP.2

There are no management activities foreseen.

Audit: FCS_COP.2

There are no auditable events foreseen

FCS_COP.2 **Delegated cryptographic operation**

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.2.1 **The TSF shall invoke an external entity validated to FIPS 140-2 SL3 to perform [assignment:** *cryptographic operations**]***

5.2 Confidencialidad de los datos de usuario almacenados

A continuación se extiende la clase **CLASS FDP: USER DATA PROTECTION** definida en Part 2: Security functional components de Common Criteria v3.1 R4 para adaptar de manera adecuada los requisitos funcionales de seguridad del TOE en lo referente a la protección de los datos de usuario almacenados.

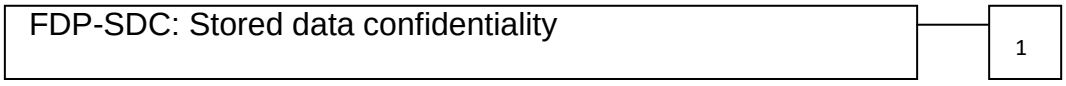
Se justifica la extensión de la clase **FDP: User Data Protection** ya que no existe componente que establezca la protección para asegurar la confidencialidad de los datos almacenados. De esta manera, se crea la familia **Stored data confidentiality** (**FDP_SDC**) que asegura la confidencialidad de los datos de usuario almacenados a través del TSF.

Stored data confidentiality (FDP_SDC)

Family Behaviour

This family provides requirements that address protection for confidentiality of user data while it is stored within containers controlled by the TSF. Confidentiality may affect user data stored in memory, or in a storage device.

Component levelling



This family consists of only one component, FDP_SDC.1 Basic confidentiality of user data, addresses the protection from disclosure of user data stored.

Management: FDP_SDC.1

There are no management activities foreseen.

Audit: FDP_SDC.1

There are no auditable events foreseen.

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_SDC.1.1 The TSF shall provide confidentialiy on the [assignment: user data stored**].**

5.3 Correspondencia entre SVD y el SCD

A continuación se extiende la clase **CLASS FDP: USER DATA PROTECTION** definida en Part 2: Security functional components de Common Criteria v3.1 R4 para adaptar de manera adecuada los requisitos funcionales de seguridad del TOE en lo referente a la asociación y correspondencia entre los datos del usuario.

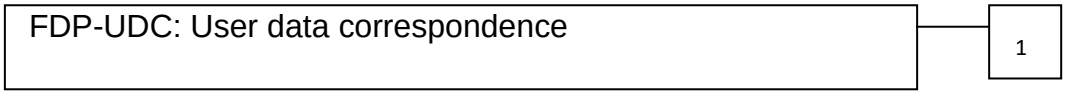
Se justifica la extensión de la clase **FDP: User Data Protection** ya que no existe componente que establezca el aseguramiento del vínculo entre datos de usuario para proporcionar la integridad de asociación entre dos datos. De esta manera, se crea la familia **User data correspondence** (**FDP_UDC**) que asegura la correspondencia entre datos del usuario, por ejemplo los datos de creación de firma SCD(clave privada de firma) y los datos de verificación de firma SVD(clave pública).

User data correspondence (FDP_UDC)

Family Behaviour

This family provides requirements that address correspondence of user data controlled by the TSF.

Component levelling



This family consists of only one component, FDP_UDC.1 Addresses the correspondence of user data.

Management: FDP_UDC.1

There are no management activities foreseen.

Audit: FDP_UDC.1

There are no auditable events foreseen.

FDP_UDC.1 User data correspondence

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_UDC.1.1 The TSF shall guarantee the correspondence between the SVD exported and the SCD generated by the TOE

FDP_UDC.1.2 The TSF shall guarantee the correspondence between the Certificate imported and the SCD generated by the TOE

6. REQUISITOS DE SEGURIDAD

6.1 Requisitos funcionales de seguridad

6.1.1 Requisitos relativos a auditoría de eventos

6.1.1.1 FAU_GEN.1 Audit data generation – operaciones del TOE

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***selection: minimum***] level of audit; and
c) [***assignment: listados en la Tabla 7: Eventos auditables de las operaciones del TOE***].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***assignment: Fecha, Tipo Operación, descripción de la operación, nombre entidad, usuario***]

NOTA: La lista de los eventos auditables son los siguientes.

Eventos auditables de operaciones del TOE	Código_operación	Descripción
Creación de la cuenta de un usuario de firma	1001	Refleja una operación de creación de una cuenta de usuario de firma
Modificación de una cuenta de un usuario de firma	1002	Refleja una operación de modificación de una cuenta de usuario de firma
Borrado de una cuenta de un usuario de firma	1003	Refleja una operación de borrado de una cuenta de usuario de firma
Borrado de certificado/clave	2003	Refleja una operación de borrado de un certificado y su clave de firma de un usuario firmante
Activación de certificado	4001	Refleja una operación de activación de un certificado
Desactivación de certificado	4002	Refleja una operación de desactivación de un certificado
Asignación de claves y certificado	5001	Refleja una operación de asignación de clave de firma y certificado a un usuario de firma.
Asociación de certificado	5006	Refleja una operación de asociación de certificado a una clave de firma ya generada de un usuario firmante
Creación de una OTP	6001	Refleja la operación de creación de una OTP
Actualización de una OTP	6002	Refleja la operación de actualización de una OTP
Firma	7001	Refleja una operación de firma
Listado de certificados de un usuario de firma	7002	Refleja una operación de listado de certificados activos de un usuario de firma

Preparación OTP	7003	Refleja una operación de generación y envío de una OTP
Cambio de Contraseña(PIN)	7004	Refleja una operación de cambio de contraseña estática
Generación de claves	7006	Refleja una operación de generación de un par de claves para un usuario firmante
Autenticación	7007	Refleja una operación de autenticación de un usuario firmante
Consulta lista certificados	7008	Refleja una operación de consulta de todos los certificados de un usuario firmante
Asociación de certificado	9012	Refleja una operación de asociación de certificado a una clave de firma ya generada de un usuario firmante
Vinculación SFDA a Certificado	8007	Refleja una operación de asociación de un sistema de segundo factor de autenticación y un certificado
Desvinculación SFDA a Certificado	8009	Refleja una operación de borrado de la asociación de un sistema de segundo factor de autenticación y un certificado
Bloqueo de un certificado	13003	Refleja el evento sucedido cuando un certificado es bloqueado por un administrador
Desbloqueo de un certificado	13004	Refleja el evento sucedido cuando un certificado es desbloqueado por un administrador
Requerimiento de contraseña para firma	13006	Refleja la operación de establecimiento del requerimiento de contraseña para el uso de un certificado
No requerimiento de contraseña para firma	13007	Refleja la operación de establecimiento del no requerimiento de contraseña para el uso de un certificado

Tabla 7: Eventos auditables de las operaciones del TOE

6.1.1.2 FAU_GEN.1 Audit data generation - operaciones de los usuarios firmantes

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***selection: minimum***] level of audit; and
c) [***assignment: eventos listados en la Tabla 8: Eventos auditables de las operaciones de usuarios firmantes***]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***assignment: fecha, codigo_operacion, nombre_operacion, titular, unidad_titular, usuario, dn_certificado, num_serie_certificado, huella_certificado***].

NOTA: La lista de los eventos auditables son los siguientes.

Eventos auditables de operaciones de los usuarios fimantes	Código_operación	Descripción
Firma	OW-01-0001	Refleja una operación de firma

Multifirma	OW-01-0002	Refleja una operación de firma de múltiples documentos
Cambio de Contraseña(PIN)	OW-01-0004	Refleja una operación de cambio de contraseña estática
Preparación OTP	OW-01-0005	Refleja una operación de generación y envío de una OTP
Autenticación con contraseña	OW-01-0006	Refleja una operación de autenticación solo con contraseña
Autenticación con SFDA	OW-01-0007	Refleja una operación de autenticación solo con SFDA
Autenticación con contraseña y SFDA	OW-01-0008	Refleja una operación de autenticación con contraseña y SFDA
Listado de certificados de un usuario de firma	OW-01-0009	Refleja una operación de listado de certificados activos de un usuario de firma
Creación de la cuenta de un usuario de firma	OW-02-0001	Refleja una operación de creación de una cuenta de usuario de firma
Borrado de una cuenta de un usuario de firma	OW-02-0002	Refleja una operación de borrado de una cuenta de usuario de firma
Modificación de una cuenta de un usuario de firma	OW-02-0003	Refleja una operación de modificación de una cuenta de usuario de firma
Asignación de claves y certificado	OW-02-0004	Refleja una operación de asignación de clave de firma y certificado a un usuario de firma.
Asociación de certificado	OW-02-0005	Refleja una operación de asociación de certificado a una clave de firma ya generada de un usuario firmante
Borrado de certificado/clave	OW-02-0006	Refleja una operación de borrado de un certificado y su clave de firma de un usuario firmante
Generación de claves	OW-02-0007	Refleja una operación de generación de un par de claves para un usuario firmante
Activación de certificado	OW-02-0008	Refleja una operación de activación temporal de un certificado..
Asociación SFDA	OW-02-0010	Refleja una operación de asociación de un SFDA con un certificado de un usuario firmante
Borrado de asociación de SFDA	OW-02-0011	Refleja una operación de borrado de un SFDA de un certificado de un usuario firmante
Desbloqueo certificado	OW-02-0014	Refleja una operación de desbloqueo de un certificado bloqueado por un administrador
Consulta lista certificados	OW-02-0015	Refleja una operación de consulta de todos los certificados de un usuario firmante
Desactivación de certificado	OW-02-0016	Refleja una operación de desactivación de un certificado
Consulta de un certificado	OW-02-0018	Refleja una operación de consulta de un certificado
Bloqueo de un certificado por superar el número máximo de intentos fallidos	OW-02-0019	Refleja el evento sucedido cuando un certificado es bloqueado si el usuario supera el número máximo de intentos fallidos de autenticación.
Desbloqueo de un certificado	OW-02-0020	Refleja la operación de desbloqueo de un certificado cuando este se encontraba bloqueado por superar el número máximo de intentos de autenticación.
Requerimiento de contraseña para firma	OW-02-0021	Refleja la operación de establecimiento del requerimiento de contraseña para el uso de un certificado
No requerimiento de contraseña para firma	OW-02-0022	Refleja la operación de establecimiento del no requerimiento de contraseña para el uso de un certificado
Generación de claves y certificado autofirmado	OW-02-0023	Refleja la operación de generación de un par de claves y un certificado autofirmado para un usuario firmante
Información de la cuenta de un usuario firmante	OW-06-0001	Refleja la operación de consulta de la cuenta de un usuario firmante
Listado de certificados de un usuario de firma	OW-06-0003	Refleja una operación de listado de certificados de un usuario de firma desde el servicio web

Tabla 8: Eventos auditables de las operaciones de usuarios firmantes

6.1.1.3 FAU_GEN.2 User identity association - Identificación del usuario de la operación

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.4 FAU_SAR.1 Audit review – revisión de los datos de auditoría de operaciones del TOE

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [***assignment: usuarios con un perfil que tenga asignada la funcionalidad ADMIN_LIST_AUDIT_OPERATIONS_SERVICE***] with the capability to read [***assignment: operaciones del TOE***] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.5 FAU_SAR.1 Audit review – revisión de los datos de auditoría de operaciones del usuario firmante

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [***assignment: usuarios con un perfil que tenga asignado la funcionalidad ADMIN_LIST_OPERATIONS_SERVICE o LIST_OWNER_OPERATIONS_SERVICE***] with the capability to read [***assignment: operaciones de los usuarios firmantes***] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.6 FAU_SAR.2 Restricted audit review – acceso restringido a los datos de auditoría del TOE

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

NOTA: El acceso restringido a los datos de auditoría aplica tanto a los datos de auditoría de las operaciones del TOE como a las operaciones generadas por los usuarios firmantes.

6.1.1.7 FAU_SEL.1 Selective audit – selección de los datos de auditoría de operaciones del TOE

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [***selection: event type***]
b) [***assignment: Fecha, descripción de la operación, nombre entidad, usuario***]

6.1.1.8 FAU_SEL.1 Selective audit – selección de los datos de auditoría de operaciones de los usuarios firmantes

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [***selection: event type***]
b) [***assignment: codigo_operacion, nombre_operacion, titular, unidad_titular, usuario, unidad_usuario, dn_certificado, num_serie_certificado, huella_certificado, sfda, fecha_ini_operacion, operacion_correcta, resultado_operacion, descripcion_error***]

6.1.1.9 FAU_STG.3 Action in case of possible audit data loss – archivado de datos de auditoría del TOE

Hierarchical to:	No other components.
Dependencies:	FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall [***assignment: alertar del límite configurado para el registro de datos de auditoría de operaciones del TOE y operaciones de los usuarios firmantes***] if the audit trail exceeds [***assignment: número de registros configurados***].

6.1.2 Requisitos relativos a No repudio

6.1.2.1 FCO_NRO.1 Selective proof of origin – CSR Generación del certificado

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [***assignment: CSR(PKCS#10)***] at the request of the [***selection: recipient***].

FCO_NRO.1.2 The TSF shall be able to relate the [***assignment: SCD***] of the originator of the information, and the [***assignment: CSR(PKCS#10)***] of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [***selection: recipient***] given [***assignment: la firma electronica con la SCD***].

6.1.3 Requisitos relativos a la Gestión de claves criptográficas

6.1.3.1 FCS_COP.1 Cryptographic operation - descifrado/cifrado simétrico de datos

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [***assignment: descifrado/cifrado simétrico de datos***] in accordance with a specified cryptographic algorithm [***assignment: 3DES***] and cryptographic key sizes [***assignment: 192bits***] that meet the following: [***assignment: ninguno***].

6.1.3.2 FCS_CKM.1 Cryptographic key generation - descifrado/cifrado simétrico de datos

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***assignment: mediante la función propietaria rareGetBytes***] and specified cryptographic key sizes [***assignment: 192 bits***] that meet the following: [***assignment: ninguno***].

NOTA: La función *rareGetBytes* es una función propietaria del TOE que genera una clave en memoria que cumple con los requisitos para ser utilizada con un algoritmo 3DES.

6.1.3.3 FCS_CKM.3 Cryptographic key access – clave protección fichero de configuración HMAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.3.1 The TSF shall perform [***assignment: acceso a claves criptográficas utilizadas para la protección de los ficheros de configuración HMAC***] in accordance with a specified cryptographic key access method [***assignment: PKCS#12***] that meets the following: [***assignment: PKCS#12***].

NOTA: Estas claves son utilizadas por el TOE para asegurar la integridad y la confidencialidad del fichero de configuración que controla la generación del HMAC, estas claves se encuentran almacenadas en el keystore proporcionado en el momento de establecer la configuración del TOE**.**

6.1.3.4 FCS_COP.1 Cryptographic operation - descifrado fichero configuración HMAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [***assignment: descifrado del fichero de configuración HMAC***] in accordance with a specified cryptographic algorithm [***assignment: RSA***] and cryptographic key sizes [***assignment: 1024bits***] that meet the following: [***assignment: XML Encryption***].

6.1.3.5 FCS_COP.1 Cryptographic operation - verificación fichero configuración HMAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [***assignment: verificación electrónica del fichero de configuración HMAC***] in accordance with a specified cryptographic algorithm [***assignment: RSA signature with SHA-1 hashing***] and cryptographic key sizes [***assignment: RSA 1024, SHA-1***] that meet the following: [***assignment: PKCS #1 - RSA Encryption Standard (RSA)***].

6.1.3.6 FCS_COP.1 Cryptographic operation – cálculo/verificación HMAC

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [***assignment: cálculo/verificación electrónica del valor HMAC***] in accordance with a specified cryptographic algorithm [***assignment: MAC with SHA-256 hashing***] and cryptographic key sizes [***assignment: SHA-256***] that meet the following: [***assignment: HMAC-SHA-256***].

NOTA: Esta clave es utilizada por el TOE para la generación del valor HMAC que asegura la autoría de los datos almacenados en BBDD, esta clave se encuentra almacenada en el keystore proporcionado en el momento de establecer la configuración inicial del TOE**.**

6.1.3.7 FCS_CKM.3 Cryptographic key access – almacén clave de firma/verificación plataforma de envío de SMS

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.3.1 The TSF shall perform [***assignment: acceso al almacén de claves criptográficas utilizadas para la firma y verificación de las peticiones enviadas y recibidas con la plataforma de envío de SMS***] in accordance with a specified cryptographic key access method [***assignment: PKCS#12, JKS***] that meets the following: [***assignment: PKCS#12, JKS***].

6.1.3.8 FCS_COP.1 Cryptographic operation – firma petición envío plataforma SMS

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [***assignment: firma electrónica de la petición de envío de la OTP a través de la pasarela SMS***] in accordance with a specified cryptographic algorithm [***assignment: RSA signature with SHA-256 hashing***] and cryptographic key sizes [***assignment: RSA 1024, SHA-256***] that meet the following: [***assignment: PKCS #1 - RSA Encryption Standard (RSA)***].

NOTA: El almacén de claves que contiene la clave de firma será parte de la configuración establecida en el entorno operacional del TOE.

6.1.3.9 FCS_COP.1 Cryptographic operation - verificación firma de respuesta plataforma SMS

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [***assignment: verificación electrónica de la respuesta recibida tras el envío de una OTP a la plataforma de envío de SMS***] in accordance with a specified cryptographic algorithm [***assignment: RSA signature with SHA-256 hashing***] and cryptographic key sizes [***assignment: RSA 1024, SHA-256***] that meet the following: [***assignment: PKCS #1 - RSA Encryption Standard (RSA)***].

NOTA: El almacén de claves que contiene la clave de firma será parte de la configuración establecida en el entorno operacional del TOE.

6.1.3.10 FCS_COP.2 Delegated Cryptographic operation – generación de SCD/SVD

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.2.1 The TSF shall invoke an external entity validated to FIPS 140-2 SL3 to perform [***assignment: generateKeyPair , deriveKey, wrapKey, destroyObject***]

NOTA: Estas operaciones son delegadas al HSM en el ámbito de la operación de creación del par de claves SCD/SVD, el TOE invoca la generación del par de claves mediante la función generateKeyPair y protege el SCD invocando las operaciones deriveKey y wrapKey, finalmente se elimina de la sesión los objetos mediante destroyObject.

6.1.3.11 FCS_COP.2 Delegated Cryptographic operation – activación del SCD en firma/autenticación

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.2.1 The TSF shall invoke an external entity validated to FIPS 140-2 SL3 to perform [***assignment: deriveKey, unwrapKey, sign, destroyObject***]

NOTA: Estas operaciones son delegadas al HSM en el ámbito de la operación de una firma, el TOE activa el SCD que fue generado mediante la operación FCS_COP.2 Delegated Cryptographic operation – generación de SCD/SVD, invocando

las operaciones deriveKey y unwrapKey, posteriormente si la activación se ha producido con éxito, se invoca a la firma mediante la función sign y finalmente se elimina la clave mediante destroyObject.

6.1.3.12 FCS_COP.2 Delegated Cryptographic operation – cambio de contraseña

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.2.1 The TSF shall invoke an external entity validated to FIPS 140-2 SL3 to perform [***assignment: deriveKey, unwrapKey, wrapKey, destroyObject***]

NOTA: Estas operaciones son delegadas al HSM en el ámbito de la operación de un cambio de contraseña, el TOE activa el SCD del titular invocando las operaciones deriveKey y unwrapKey, posteriormente si la activación se ha producido con éxito, se invoca a las funciones, deriveKey y wrapKey para proteger la clave con la nueva contraseña, finalmente de eliminan los objetos de la sesión del HSM mediante destroyObject**.**

6.1.4 Requisitos relativos a la Identificación y Autenticación

6.1.4.1 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user**.**

6.1.4.2 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3 FIA_UAU.5 Multiple authentication mechanisms – para los usuarios firmantes en las operaciones de firma y cambio de contraseña

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_UAU.5.1 The TSF shall provide [***assignment: Contraseña estática, más una contraseña dinámica (OTP)***] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [***assignment: la autenticación del usuario firmante en las operaciones de firma/cambio de contraseña se realiza mediante la regla:***

- ***Validación de la OTP enviada previamente a la operación y si es superada esta primera fase, validación de la contraseña estática de activación del SCD que protege su clave***]

6.1.4.4 FIA_AFL.1 Authentication failure handling – usuarios firmantes en la operación de firma/cambio de contraseña

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [***selection: un valor entero positivo configurable por un administrador entre [assignment: 1-n]***] unsuccessful authentication attempts occur related to [***assignment: fallos consecutivos de autenticación para la activación del SCD***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***selection: alcanzado***], the TSF shall [***assignment: bloqueo del certificado asociado al firmante***].

6.1.5 Requisitos relativos a la Protección de los datos de usuario

6.1.5.1 FDP_ACC.2 Complete access control – Acceso a los servicios web SFP

Hierarchical to: FDP_ACC.1 Subset access control.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the **[*assignment*: *Acceso a los servicios web SFP*]** on **[*assignment: Subject = Usuario servicios web del TOE, Object = Cuentas de los usuarios de los servicios web, Cuentas de los usuarios firmantes, claves y certificados de los usuarios firmantes, datos de auditoría, Contraseñas dinámicas OTPs*]** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP**.**

6.1.5.2 FDP_ACC.1 Subset access control – Operaciones de los usuarios firmantes SFP

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [***assignment: Operaciones de los usuarios firmantes SFP***] on [***assignment: Subject = Usuario firmante, Object = Cuenta de usuario firmante, claves de los usuarios firmantes SCD/SVD, Contraseñas estáticas de activación de las claves, Política de contraseñas, Contraseñas dinámicas OTPs Operations = creación del par de claves SCD/SVD, firma digital/autenticación, cambio de contraseña***].

6.1.5.3 FDP_ACF.1 Security attribute based access control - Acceso a los servicios web SFP

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [***assignment: Acceso a los servicios* web SFP**] to objects based on the following:

[***assignment:***

- ***Lista de objetos:***
  - ***Cuentas de los usuarios firmantes***

- ***Claves de los usuarios firmantes (SCD/SVD)***

- ***Lista de sujetos:***
  - ***Usuarios de los servicios web del TOE***

Atributos para invocación al servicio web del TOE:

• La identidad del usuario formada por el certificado de autenticación.

• Funcionalidades contenidas en el Perfil asignado al usuario de los servicios web del TOE

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment:***

- ***Caso del acceso de los sujetos <usuarios de los servicios web del TOE>***
  - ***Que el certificado de autenticación enviado en la petición exista dado de alta en la configuración y esté asociado a un usuario del sistema.***
  - ***Que tras superar el proceso de autenticación del usuario, este tenga asociado un perfil donde se establezcan permisos suficientes de ejecución para las operaciones solicitadas mediante las funcionalidades disponibles en los servicios del TOE.***

].

FDP_ACF.1.3/Acceso a los servicios web SFP The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***assignment: ninguno***].

FDP_ACF.1.4/ Acceso a los servicios web SFP The TSF shall explicitly deny access of subjects to objects based on the [***assignment: ninguno***].

6.1.5.4 FDP_ACF.1 Security attribute based access control - Operaciones de los usuarios firmantes SFP

Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [***assignment: Operaciones de los usuarios firmantes SFP***] to objects based on the following: [***assignment:***

- ***Lista de objetos:***
  - ***Claves privadas de los usuarios firmantes***

Atributos de Objetos:

- ***Contraseña estática para la activación de la clave privada (SCD)***
- ***Contraseña dinámica OTP como segundo factor de autenticación***
- ***Certificado de la clave a utilizar***

- ***Lista de sujetos:***
  - ***Usuarios firmantes***

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment:***

- ***Caso del acceso de los sujetos <usuarios firmantes> a la operación de Creación de Claves***
  - ***Que se supere la política de control de acceso a los servicios web tal y como describe FDP_ACF.1 Security attribute based access control - Acceso a los servicios web SFP***
  - ***Una vez superada la fase de autorización del usuario de acceso para la operación, se determinará que la contraseña estática de activación de la clave privada establecida por el usuario firmante cumple con la política de contraseñas definida en el sistema, en caso contrario se denegará la generación de las claves.***
  - ***Si se cumplen todas las reglas, se generarán las claves y como respuesta se exportará un CSR que contendrá el SVD firmado por el SCD para la generación del certificado.***

- ***Caso del acceso de los sujetos <usuarios firmantes> a la operación de Firma Digital/Autenticación***
  - ***Que se supere la política de control de acceso a los servicios web tal y como describe FDP_ACF.1 Security attribute based access control - Acceso a los servicios web SFP***
  - ***Una vez superada la fase de autorización del usuario para la operación, se determinará la autenticación del firmante propietario de las claves dependiendo de:***
    - ***Operación de firma: Se comprueban los dos factores de autenticación enviados en la solicitud de la firma:***
      - ***Se comprueba la OTP solicitada para la activación del SCD***
      - ***Solamente si se supera la fase de comprobación de la OTP, se pasará a activar la clave privada (SCD), comprobando, que el estado de la clave se encuentre ACTIVO y no BLOQUEADO, entonces se pasará a activar la SCD con la contraseña estática y la clave maestra almacenada en el HSM, si esta fase es superada correctamente, entonces se tendrá acceso a la clave privada.***
      - ***Tras cualquier activación de la clave para la fase de firma, tras su utilización para la firma solicitada se volverá a desactivar requiriendo una nueva activación para su uso tanto para firma como para autenticación.***
    - ***Operación de autenticación:***
      - ***Se comprobará que la clave se encuentra en estado ACTIVO y no BLOQUEADO y entonces la operación de autenticación se podrá realizar mediante estos tres tipos de autenticación:***
        - ***Con solamente contraseña: Se activará la SCD con la contraseña estática enviada en la solicitud, si la activación resulta positiva, entonces se responderá con una autenticación positiva.***

- ***Con contraseña estática más OTP: Se realizará el mismo proceso que en la firma, se comprobará en primer lugar la validación de la OTP y posteriormente la correcta activación de la SCD.***
- ***Solamente con OTP: En este caso especial, no se tendrá acceso a la clave privada SCD, verificando únicamente la OTP enviada.***

- ***Tras cualquier activación de la clave para la fase de autenticación, se volverá a desactivar requiriendo una nueva activación para su uso tanto para firma como para autenticación.***

- ***Caso del acceso de los sujetos <usuarios firmantes> a la operación cambio de contraseña***
  - ***Que se supere la política de control de acceso a los servicios web tal y como describe FDP_ACF.1 Security attribute based access control - Acceso a los servicios web SFP***
  - ***Una vez superada la fase de autorización del usuario para la operación***
    - ***Cambio de contraseña individual por cada clave privada del usuario***
      - ***Se comprueba la OTP solicitada para la activación del SCD***
      - ***Se comprueba si la nueva contraseña cumple con la política de contraseñas definida en el sistema.***
      - ***Solamente si se supera la fase de comprobación de la OTP y la política de contraseñas, se pasará a activar el SCD con la contraseña estática y la clave maestra almacenada en el HSM, si esta fase es superada correctamente entonces se tendrá acceso a la clave de firma.***
      - ***Una vez activada la clave, se protegerá con la nueva clave estática y se procederá a desactivar, de manera que a partir de este momento, se solicitarán los nuevos datos de activación tanto para una operación de firma como una de autenticación.***
    - ***Cambio de contraseña para todas las claves privadas del usuario***
      - ***Se comprueba que la nueva contraseña cumple con la política de contraseñas establecida en el sistema y si es así, se procede a ir activando cada una de las claves del usuario y protegiéndolas con la nueva contraseña y la clave maestra almacenada en el HSM. En este caso todas las claves privadas del usuario poseerán la misma clave de activación.***

].

FDP_ACF.1.3/Operaciones de los usuarios firmantes SFP The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***assignment: ninguno***].

FDP_ACF.1.4/Operaciones de los usuarios firmantes SFP The TSF shall explicitly deny access of subjects to objects based on the [***assignment: incumplimiento de la política de contraseñas para las operaciones de creación de claves y cambio de contraseña***].

NOTA: La definición de la política de contraseñas del sistema consta de una serie de requerimientos en cuanto a tamaño y caracteres utilizados así como un histórico de contraseñas en la que no debe estar incluida la nueva contraseña**.**

6.1.5.5 FDP_ETC.2 Export of user data with security attributes - Exportación CSR

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1 The TSF shall enforce the [***assignment: Operaciones de los usuarios firmantes SFP***] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [***assignment: ninguno***].

NOTA: El requisito se ejercerá como respuesta de la operación de generación de claves SCD/SVD donde se devuelve el SVD para la emisión del correspondiente certificado y su posterior asociación en el sistema.

6.1.5.6 FDP_ITC.1 Import of user data without security attributes – Histórico de contraseñas

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1 The TSF shall enforce the [***assignment: Operaciones de los usuarios firmantes SFP***] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***assignment: comprobación de la política y el histórico de contraseñas***].

NOTA: El requisito se ejercerá al importar la contraseña desde la operación de creación de claves y cambio de contraseña almacenando su hash en el histórico de contraseñas para su posterior comprobación**.**

6.1.5.7 FDP_ITC.1 Import of user data without security attributes - Asociación de Certificado

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1 The TSF shall enforce the [***assignment: Acceso a los servicios* web SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***assignment: comprobación de la clave pública del certificado con su correspondiente SVD generada por el TOE***].

6.1.5.8 FDP_SDI.1 Stored data integrity monitoring

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_SDI.1.1 The TSF shall monitor user data stored in containers controlled by the TSF for [***assignment: autoría de los datos almacenados en la base de datos***] on all objects, based on the following attributes: [***assignment: todos los registros almacenados en la base de datos***].

6.1.5.9 FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_SDC.1.1 The TSF shall provide confidentialiy on the [***assignment:***

- ***SCD clave privada de firma,***
- ***Contraseña de acceso a la partición del HSM,***
- ***contraseñas dinámicas OTP***].

6.1.5.10 FDP_UDC.1 User data correspondence

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_UDC.1.1 The TSF shall guarantee the correspondence between the SVD and the SCD generated by the TOE

FDP_UDC.1.2 The TSF shall guarantee the correspondence between the Certificate imported and the SCD generated by the TOE

6.1.6 Requisitos relativos a la Generación de alertas

6.1.6.1 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [***assignment: comprobación de los valores HMAC de los registros de base de datos de los datos de auditoría***] known to indicate a potential security violation;
b) [***assignment: ninguna***].

6.1.6.2 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [***assignment: envío de alertas al administrador cuando se detecte violación de los datos verificados en FAU_SAA***] upon detection of a potential security violation.

6.1.7 Requisitos relativos a la protección de los datos de la TSF

6.1.7.1 FPT_RPL.1 Replay detection

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [***assignment: operaciones de firma y autenticación mediante SFDA***].

FPT_RPL.1.2 The TSF shall perform [***assignment: rechazo de la operación***] when replay is detected.

6.1.8 Requisitos relativos a la gestión de la seguridad

6.1.8.1 FMT_MSA.1 Management of security attributes – ADMIN-OWNER

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [***assignment: Acceso a los servicios web SFP***] to restrict the ability to [***selection: crear, modificar, borrar***] the security attributes [***assignment: cuentas de los usuarios firmantes***] to [***assignment: usuarios de los servicios web del TOE***].

6.1.8.2 FMT_MSA.1 Management of security attributes - CREATE_KEY

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [***assignment: Acceso a los servicios web SFP***] to restrict the ability to [***selection: crear claves para un usuario firmante***] the security attributes [***assignment: SCD/SVD***] to [***assignment: usuarios de los servicios web del TOE***].

6.1.8.3 FMT_MSA.1 Management of security attributes - CHANGE_PASSWORD_SERVICE

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [***assignment: Operaciones de los usuarios firmantes SFP y Acceso a los servicios web SFP***] to restrict the ability to [***selection: modificar la contraseña de activación de la clave privada (SCD)***] the security attributes [***assignment: SCD***] to [***assignment: usuarios firmantes y usuarios de los servicios web del TOE***].

NOTA: El cambio de la contraseña de activación implica la modificación del atributo de seguridad de la clave privada (SCD), no almacenando ni modificando directamente la contraseña de activación, sino la propia clave privada al ser protegida con la nueva contraseña de activación**.**

6.1.8.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***assignment:***

- ***Gestión de cuentas de usuarios firmantes (creación, modificación y borrado)***
- ***Generación de par de claves SCD/SVD***
- ***Asociación de Certificados***
- ***Cambio de Contraseña de activación de la clave privada***
- ***Borrado de certificado y su clave privada asociada***

].

6.1.8.5 FMT_MTD.1 Management of TSF data – Consulta datos de auditoría

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [***selection: consultar***] the [***assignment: datos de auditoria de las operaciones del TOE, datos de auditoria de las operaciones de los usuarios firmantes]*** to ***[assignment: usuarios de los servicios web del TOE con la funcionalidad ADMIN_LIST_OPERATIONS_SERVICE, ADMIN_LIST_AUDIT_OPERATIONS_SERVICE y LIST_OWNER_OPERATIONS_SERVICE asignadas***].

6.1.9 Requisitos relativos a Comunicaciones seguras

6.1.9.1 FTP_ITC.1 Inter-TSF trusted channel - Aplicación de Registro

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***selection: another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [***assignment: ninguna***].

6.1.9.2 FTP_ITC.1 Inter-TSF trusted channel - Aplicación de Creación de Firma

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***selection: another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [***assignment: ninguna***].

6.1.9.3 FTP_ITC.1 Inter-TSF trusted channel – Base de datos

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***selection: the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [***assignment: todos los accesos a la base de datos***].

6.1.9.4 FTP_ITC.1 Inter-TSF trusted channel – Plataforma envío SMS

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***selection: the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [***assignment: envío de OTPs vía SMS***].

6.2 Razonamiento de dependencias

A continuación se enumeran las dependencias de los requisitos funcionales de seguridad y la justificación de aquellas que no se cumplen.

REQUISITOS FUNCIONALES de SEGURIDAD	Dependencias	Justificación
FAU_GEN.1 operaciones del TOE		**FPT_STM.1**
FAU_GEN.1 operaciones de los usuarios firmantes		**FPT_STM.1**
FAU_GEN.2 Identificación del usuario de la operación	**FAU_GEN.1 Audit data generation** **FIA_UID.2 User identification before any action**	
FAU_SAR.1 revisión de los datos de auditoría de operaciones del TOE	**FAU_GEN.1 operaciones del TOE**	
FAU_SAR.1 revisión de los datos de auditoría de operaciones del usuario firmante	**FAU_GEN.1 operaciones de los usuarios firmantes**	
FAU_SAR.2 acceso restringido a los datos de auditoría del TOE	**FAU_SAR.1 revisión de los datos de auditoría de operaciones del TOE** **FAU_SAR.1 revisión de los datos de auditoría de operaciones del usuario firmante**	
FAU_SEL.1 selección de los datos de auditoría de operaciones del TOE	**FAU_GEN.1 operaciones del TOE** **FMT_MTD.1 Consulta datos de auditoría**	
FAU_SEL.1 selección de los datos de auditoría de operaciones de los usuarios firmantes	**FAU_GEN.1 operaciones de los usuarios firmantes** **FMT_MTD.1 Consulta datos de auditoría**	
FAU_STG.3 archivado de datos de auditoría del TOE		**FAU_STG.1**
FCO_NRO.1 CSR Generación del certificado	**FIA_UID.2 User identification before any action**	
FCS_COP.1 descifrado/cifrado simétrico de datos	**FCS_CKM.1 descifrado/cifrado simétrico de datos**	**FCS_CKM.4**
FCS_CKM.1 descifrado/cifrado simétrico de datos	**FCS_COP.1 descifrado/cifrado simétrico de datos**	**FCS_CKM.4**
FCS_CKM.3 clave protección fichero de configuración HMAC		**FCS_CKM.1** **FCS_CKM.4**

Tabla 9: Razonamiento de dependencias

REQUISITOS FUNCIONALES de SEGURIDAD	Dependencias	Justificación
FCS_COP.1 descifrado fichero configuración HMAC		**FCS_CKM.1 FCS_CKM.4**
FCS_COP.1 verificación fichero configuración HMAC		**FCS_CKM.1 FCS_CKM.4**
FCS_COP.1 cálculo/verificación HMAC		**FCS_CKM.1 FCS_CKM.4**
FCS_CKM.3 almacén clave de firma/verificación plataforma de envío de SMS		**FCS_CKM.1 FCS_CKM.4**
FCS_COP.1 firma petición envío plataforma SMS		**FCS_CKM.1 FCS_CKM.4**
FCS_COP.1 verificación firma de respuesta plataforma SMS		**FCS_CKM.1 FCS_CKM.4**
FCS_COP.2 activación del SCD en firma/autenticación		**FCS_CKM.1 FCS_CKM.4**
FCS_COP.2 cambio de contraseña		**FCS_CKM.1 FCS_CKM.4**
FCS_COP.2 generación de SCD/SVD		**FCS_CKM.1 FCS_CKM.4**
FIA_UID.2 User identification before any action	-	
FIA_UAU.2 User authentication before any action	**FIA_UID.2 User identification before any action**	
FIA_UAU.5 para los usuarios firmantes en las operaciones de firma y cambio de contraseña	-	
FIA_AFL.1 usuarios firmantes en la operación de firma/cambio de contraseña	**FIA_UAU.2 User authentication before any action**	
FDP_ACC.2 Acceso a los servicios web SFP	**FDP_ACF.1 Acceso a los servicios web SFP**	
FDP_ACC.1 Operaciones de los usuarios firmantes SFP	**FDP_ACF.1 Generación SCD/SVD SFP**	
FDP_ACF.1 Acceso a los servicios web SFP	**FDP_ACC.2 Acceso a los servicios web SFP**	**FMT_MSA.3**
FDP_ACF.1 Operaciones de los usuarios firmantes SFP	**FDP_ACC.1 Operaciones de los usuarios firmantes SFP**	**FMT_MSA.3**
FDP_ETC.2 Exportación CSR	**FDP_ACC.1 Operaciones de los usuarios firmantes SFP**	

Tabla 10: Razonamiento de dependencias

REQUISITOS FUNCIONALES de SEGURIDAD	Dependencias	Justificación
FDP_ITC.1 Histórico de contraseñas	**FDP_ACC.1 Operaciones de los usuarios firmantes SFP**	**FMT_MSA.3**
FDP_ITC.1 Asociación de Certificado	**FDP_ACC.2 Acceso a los servicios web SFP**	**FMT_MSA.3**
FDP_SDI.1 Stored data integrity monitoring	-	
FDP_SDC.1 Stored data confidentiality	-	
FDP_UDC.1 User data correspondence	-	
FAU_SAA.1 Potential violation analysis	**FAU_GEN.1 operaciones del TOE** **FAU_GEN.1 operaciones de los usuarios firmantes**	
FAU_ARP.1 Security alarms	**FAU_SAA.1 Potential violation analysis**	
FPT_RPL.1 Replay detection	-	
FMT_MSA.1 ADMIN-OWNER	**FDP_ACC.1 Acceso a los servicios web SFP** **FMT_SMF.1 Specification of Management Functions**	**FMT_SMR.1**
FMT_MSA.1 CREATE_KEY	**FDP_ACC.1 Operaciones de los usuarios firmantes SFP** **FMT_SMF.1 Specification of Management Functions**	**FMT_SMR.1**
FMT_MSA.1 CHANGE_PASSWORD_SERVICE	**FDP_ACC.1 Operaciones de los usuarios firmantes SFP** **FMT_SMF.1 Specification of Management Functions**	**FMT_SMR.1**
FMT_SMF.1 Specification of Management Functions	-	
FMT_MTD.1 Consulta datos de auditoría	**FMT_SMF.1 Specification of Management Functions**	**FMT_SMR.1**
FTP_ITC.1 Aplicación de Registro	-	
FTP_ITC.1 Aplicación de Creación de Firma	-	
FTP_ITC.1 Base de datos	-	
FTP_ITC.1 Plataforma envío SMS	-	

Tabla 11: Razonamiento de dependencias

6.2.1 Justificación de las dependencias no cubiertas

- En los requisitos **FAU_GEN.1 operaciones del TOE y FAU_GEN.1 operaciones de los usuarios firmantes** no se cumple con la dependencia **FPT_STM.1 Reliable time stamps,** ya que no es una funcionalidad de seguridad del TOE asegurar la fecha y hora reflejada en los ficheros de auditoría. El TOE recoge la fecha y hora del sistema que puede configurarse para que pueda estar sincronizada con servidores de tiempo mediante protocolo ntp.

- En el requisito, **FAU_STG.3 archivado de datos de auditoría del TOE** no se cumple con la dependencia **FAU_STG.1 Protected audit trail storage.** La custodia de los ficheros con los datos de auditoría generados por el TOE una vez creados, quedan en manos del entorno operativo para ser custodiados en lugar seguro para que no puedan ser destruidos.

- En los requisitos, **FCS_COP.1 descifrado/cifrado simétrico de datos y FCS_CKM.1 descifrado/cifrado simétrico de datos** no se cumple con la dependencia **FCS_CKM.4 Cryptographic key destruction.** La clave no es eliminada explícitamente por el TOE ya que la clave siempre que se genera, se mantiene en memoria y es destruida una vez que el proceso se descarga de memoria.

- En los requisitos, **FCS_CKM.3 clave protección fichero de configuración HMAC, FCS_COP.1 descifrado fichero configuración HMAC, FCS_COP.1 verificación fichero configuración HMAC y FCS_COP.1 cálculo/verificación HMAC** no se cumple con las dependencias:

    - **FCS_CKM.1 Cryptographic key generation:** Las claves no son generadas por el TOE. Estas claves son parte de los ficheros de configuración que se establecen en el TOE como parte del proceso de instalación y configuración inicial.

    - **FCS_CKM.4 Cryptographic key destruction:** Las claves no son eliminadas por el TOE. Estas claves son parte de los ficheros de configuración que se establecen en el TOE como parte del proceso de instalación y configuración inicial y que serán destruidas manualmente una vez que el TOE sea desinstalado.

- En los requisitos, **FCS_CKM.3 almacén clave de firma/verificación plataforma de envío de SMS, FCS_COP.1 firma petición envío plataforma SMS y FCS_COP.1 verificación firma de respuesta plataforma SMS** no se cumple con las dependencias:

    - **FCS_CKM.1 Cryptographic key generation:** Las claves no son generadas por el TOE. Estas claves son parte de los ficheros de configuración que se establecen en el TOE como parte del proceso de instalación y configuración inicial.

    - **FCS_CKM.4 Cryptographic key destruction:** Las claves no son eliminadas por el TOE. Estas claves son parte de los ficheros de configuración que se establecen en el TOE como parte del proceso de instalación y configuración inicial y que serán destruidas manualmente una vez que el TOE sea desinstalado.

- En los requisitos, **FCS_COP.2 activación del SCD en firma/autenticación , FCS_COP.2 cambio de contraseña** y **FCS_COP.2 generación de SCD/SVD** no se cumple con las dependencias:

- **FCS_CKM.1 Cryptographic key generation:** Las claves no son generadas por el TOE. Estas claves son generadas como parte de las operaciones invocadas en el propio dispositivo externo HSM a través de la operación *generateKeyPair* e importadas en el dispositivo a través de la operación *unwrapKey.* La clave que se genera en cada operación mediante la operación *deriveKey* se genera en cada sesión dentro del dispositivo y no por el TOE.

- **FCS_CKM.4 Cryptographic key destruction:** Las claves no son eliminadas por el TOE. Las claves utilizadas en cada operación, son destruidas dentro del dispositivo HSM mediante la operación *destroyObject* que invoca el TOE al finalizar cada operación.

- En los requisitos, **FDP_ACF.1 Acceso a los servicios web SFP y FDP_ACF.1 Operaciones de los usuarios firmantes SFP,** no se cumple con la dependencia **FMT_MSA.3 Static attribute initialisation.** La gestión de perfiles/funcionalidades que establecen el control de acceso e inicialización de los valores por defecto del sistema, quedan fuera del ámbito del TOE puesto que para la presente evaluación del TOE no se encentra incluida la consola web de administración. Los perfiles y valores de configuración se han establecido en el proceso de instalación y configuración inicial del TOE proporcionando de esta manera los perfiles y valores de las diferentes políticas de acceso pertinentes para el correcto funcionamiento del TOE.

- En los requisitos, **FDP_ITC.1 Histórico de contraseñas y FDP_ITC.1 Asociación de Certificado,** no se cumple con la dependencia **FMT_MSA.3 Static attribute initialisation.** La gestión de perfiles/funcionalidades que establecen el control de acceso e inicialización de los valores por defecto del sistema, quedan fuera del ámbito del TOE puesto que para la presente evaluación del TOE no se encuentra incluida la consola web de administración. Los perfiles y valores de configuración se han establecido en el proceso de instalación y configuración inicial del TOE proporcionando de esta manera los perfiles y valores de las diferentes políticas de acceso pertinentes para el correcto funcionamiento del TOE.

- En los requisitos, **FMT_MSA.1 ADMIN-OWNER, FMT_MSA.1 CREATE_KEY, FMT_MSA.1 CHANGE_PASSWORD_SERVICE,** no se cumple con la dependencia **FMT_SMR.1 Security roles.** La gestión de roles o perfiles/funcionalidades que establecen el control de acceso, quedan fuera del ámbito del TOE puesto que para la presente evaluación del TOE no se encuentra incluida la consola web de administración. Los perfiles y valores de configuración se han establecido en el proceso de instalación y configuración inicial del TOE proporcionando de esta manera los perfiles y valores de las diferentes políticas de acceso pertinentes para el correcto funcionamiento del TOE.

- En el requisito, **FMT_MTD.1 Consulta datos de auditoría** no se cumple con la dependencia **FMT_SMR.1 Security roles.** La gestión de roles o perfiles/funcionalidades que establecen el control de acceso, quedan fuera del ámbito del TOE puesto que para la presente evaluación del TOE no se encuentra incluida la consola web de administración. Los perfiles y valores de configuración se han establecido en el proceso de instalación y configuración inicial del TOE proporcionando de esta manera los perfiles y valores de las diferentes políticas de acceso pertinentes para el correcto funcionamiento del TOE.

6.3 Razonamiento de los requisitos funcionales de seguridad

OBJETIVOS DE SEGURIDAD DEL TOE / REQUISITOS FUNCIONALES de SEGURIDAD	O.AUTHENTICATION_USER	O.ACCESS_CONTROL	O.CONFIDENTIAL_PRIVATE_KEY	O.SIGNER-SOLECONTROL	O.SCD_SVD-CORRESPONDENCE	O.SIGNATURE-SECURE	O.SCD-ANTIREPLAY	O.CONFIGURATION-INTEGRITY	O.USER-DATA-INTEGRITY	O.AUDIT-INTEGRITY	O.VERIFICATION-SERVER-SMS	O.PROTECT-HMAC-KEY	O.CIPHER-PASS	O.DETECT-FUNCTION-SECURITY-SYSTEM
FAU_GEN.1 operaciones del TOE										X				
FAU_GEN.1 operaciones de los usuarios firmantes										X				
FAU_GEN.2 Identificación del usuario de la operación										X				
FAU_SAR.1 revisión de los datos de auditoría de operaciones del TOE										X				
FAU_SAR.1 revisión de los datos de auditoría de operaciones del usuario firmante										X				
FAU_SAR.2 acceso restringido a los datos de auditoría del TOE										X				
FAU_SEL.1 selección de los datos de auditoría de operaciones del TOE										X				
FAU_SEL.1 selección de los datos de auditoría de operaciones de los usuarios firmantes										X				
FAU_STG.3 archivado de datos de auditoría del TOE														X
FCO_NRO.1 CSR Generación del certificado					X									
FCS_COP.1 descifrado/cifrado simétrico de datos								X	X	X		X	X	
FCS_CKM.1 descifrado/cifrado simétrico de datos								X	X	X		X	X	
FCS_CKM.3 clave protección fichero de configuración HMAC								X	X	X		X		

Tabla 12 : Razonamiento RFS/OT

OBJETIVOS DE SEGURIDAD DEL TOE / REQUISITOS FUNCIONALES de SEGURIDAD	O.AUTHENTICATION_USER	O.ACCESS_CONTROL	O.CONFIDENTIAL_PRIVATE_KEY	O.SIGNER-SOLECONTROL	O.SCD_SVD-CORRESPONDENCE	O.SIGNATURE-SECURE	O.SCD-ANTIREPLAY	O.CONFIGURATION-INTEGRITY	O.USER-DATA-INTEGRITY	O.AUDIT-INTEGRITY	O.VERIFICATION-SERVER-SMS	O.PROTECT-HMAC-KEY	O.CIPHER-PASS	O.DETECT-FUNCTION-SECURITY-SYSTEM
FCS_COP.1 descifrado fichero configuración HMAC								X	X	X		X	X	
FCS_COP.1 verificación fichero configuración HMAC								X	X	X		X		
FCS_COP.1 cálculo/verificación HMAC					X			X	X	X				X
FCS_CKM.3 almacén clave de firma/verificación plataforma de envío de SMS											X			
FCS_COP.1 firma petición envío plataforma SMS											X			
FCS_COP.1 verificación firma de respuesta plataforma SMS											X			
FCS_COP.2 activación del SCD en firma/autenticación			X	X		X								
FCS_COP.2 cambio de contraseña			X	X										
FCS_COP.2 generación de SCD/SVD			X	X	X	X								
FIA_UID.2 User identification before any action	X													
FIA_UAU.2 User authentication before any action	X													
FIA_UAU.5 para los usuarios firmantes en las operaciones de firma y cambio de contraseña	X			X			X							
FIA_AFL.1 usuarios firmantes en la operación de firma/cambio de contraseña	X													
FDP_ACC.2 Acceso a los servicios web SFP		X												
FDP_ACC.1 Operaciones de los usuarios firmantes SFP		X					X							
FDP_ACF.1 Acceso a los servicios web SFP		X												
FDP_ACF.1 Operaciones de los usuarios firmantes SFP		X					X							

Tabla 13: Razonamiento RFS/OT

OBJETIVOS DE SEGURIDAD DEL TOE / REQUISITOS FUNCIONALES de SEGURIDAD	O.AUTHENTICATION_USER	O.ACCESS_CONTROL	O.CONFIDENTIAL_PRIVATE_KEY	O.SIGNER-SOLECONTROL	O.SCD_SVD-CORRESPONDENCE	O.SIGNATURE-SECURE	O.SCD-ANTIREPLAY	O.CONFIGURATION-INTEGRITY	O.USER-DATA-INTEGRITY	O.AUDIT-INTEGRITY	O.VERIFICATION-SERVER-SMS	O.PROTECT-HMAC-KEY	O.CIPHER-PASS	O.DETECT-FUNCTION-SECURITY-SYSTEM
FDP_ETC.2 Exportación CSR					X									
FDP_ITC.1 Histórico de contraseñas			X											
FDP_ITC.1 Asociación de Certificado					X									
FDP_SDI.1 Stored data integrity monitoring								X	X	X				
FDP_SDC.1 Stored data confidentiality			X										X	
FDP_UDC.1 User data correspondence					X									
FAU_SAA.1 Potential violation analysis								X	X	X				X
FAU_ARP.1 Security alarms								X	X	X				X
FPT_RPL.1 Replay detection							X							
FMT_MSA.1 ADMIN-OWNER		X												
FMT_MSA.1 CREATE_KEY		X												
FMT_MSA.1 CHANGE_PASSWORD_SERVICE		X												
FMT_SMF.1 Specification of Management Functions				X	X									
FMT_MTD.1 Consulta datos de auditoría		X												X
FTP_ITC.1 Aplicación de Registro					X									
FTP_ITC.1 Aplicación de Creación de Firma						X								
FTP_ITC.1 Base de datos								X	X	X				
FTP_ITC.1 Plataforma envío SMS											X			

Tabla 14: Razonamiento SRF/OT

6.3.1 Justificación de los requisitos funcionales de seguridad

En este apartado se demostrará la suficiencia de los requisitos funcionales de seguridad establecidos para cubrir todos los objetivos de seguridad del TOE.

O.AUTHENTICATION_USER: Autenticación de usuarios

Este objetivo se cubre mediante la identificación y la autenticación de los usuarios que acceden a los servicios del TOE con**, FIA_UID.2** *User identification before any action* y **FIA_UAU.2** *User authentication before any action***.**

Los usuarios firmantes además deben autenticarse en el momento de realizar la firma/autenticación y cambio de contraseña mediante un sistema de doble factor según **FIA_UAU.5** *para los usuarios firmantes en las operaciones de firma y cambio de contraseña***,** igualmente se determina un número máximo de intentos de autenticación con **FIA_AFL.1** *usuarios firmantes en la operación de firma/cambio de contraseña*.

O.ACCESS_CONTROL: Control de acceso

Este objetivo se cubre mediante la definición de las políticas de control de acceso y los requisitos de seguridad establecidos en las operaciones que acceden a los activos de seguridad del TOE mediante **FDP_ACC.2** *Acceso a los servicios web SFP*, **FDP_ACC.1** *Operaciones de los usuarios firmantes SFP*, **FDP_ACF.1** *Acceso a los servicios web SFP* y **FDP_ACF.1** *Operaciones de los usuarios firmantes SFP*.

De esta manera se define que cualquier usuario que accede a los servicios del TOE debe tener autorización para acceder a los activos del TOE.

Para el control de acceso de las operaciones de gestión del TOE se establecen los requisitos **FMT_MSA.1** *ADMIN-OWNER***, FMT_MSA.1** *CREATE_KEY* y **FMT_MSA.1** *CHANGE_PASSWORD_SERVICE* donde se definen los atributos de seguridad gestionados en cada operación.

Igualmente se define el acceso para la consulta de datos de auditoría mediante **FMT_MTD.1** *Consulta datos de auditoría*, para delimitar los usuarios que pueden acceder a estos datos.

O.CONFIDENTIAL_PRIVATE_KEY: Confidencialidad de las claves privadas de los usuarios

Este objetivo se cubre mediante la protección de la clave privada de firma(SCD), desde el momento en que es generada en el HSM mediante **FCS_COP.*2*** *generación de SCD/SVD*, se extrae del dispositivo para ser almacenada en la base de datos mediante **FDP_SDC.1** *Stored data confidentiality*, hasta el momento que debe ser activada nuevamente en el HSM para su uso mediante **FDP_ITC.1** *Histórico de contraseñas* donde se efectúa la importación de la contraseña de activación para generar el histórico de contraseñas, **FCS_COP.2** *cambio de contraseña para el cambio de la contraseña* y su utilización en una firma o autenticación mediante **FCS_COP.2** *activación del SCD en firma/autenticación.*

O.SIGNER-SOLECONTROL: Control exclusivo de las claves privadas de firma por parte de los usuarios

Este objetivo se cubre mediante la protección de la clave de firma a partir de una contraseña estática conocida únicamente por el usuario y una clave maestra almacenada en el HSM mediante las operaciones **FCS_COP.2** *activación del SCD en firma/autenticación*, **FCS_COP.2** *cambio de contraseña*, **FCS_COP.2** *generación de SCD/SVD* y la necesidad de una autenticación multicanal mediante **FIA_UAU.5** *para los usuarios firmantes en las operaciones de firma y cambio de contraseña*.

La generación de las claves se encuentra dentro de las funciones de gestión definidas en **FMT_SMF.1** Specification of Management Functions.

O.SCD_SVD-CORRESPONDENCE: Correspondencia entre SVD y SCD

Este objetivo se cubre con la generación segura de un par de claves mediante **FCS_COP.2** *generación de SCD/SVD*, estableciendo las medidas necesarias para la generación del certificado de acuerdo a las claves generadas mediante la exportación del fichero CSR con el que solicitar el certificado mediante **FDP_ETC.2** *Exportación CSR*, **FCO_NRO.1** *CSR Generación del certificado*, creando el enlace con el certificado emitido con las claves mediante **FDP_ITC.1** *Asociación de Certificado*, **FDP_UDC.1** *User data correspondence*, **FTP_ITC.1** *Aplicación de Registro*. La autoría del vínculo creado entre la clave pública (SVD) y la clave privada(SCD) en la configuración, se mantendrá mediante **FCS_COP.1** *cálculo/verificación HMAC*.

La asociación del certificado mediante su correspondencia entre la clave pública y privada se encuentra dentro de las funciones de gestión definidas en **FMT_SMF.1** Specification of Management Functions

O.SIGNATURE-SECURE: Seguridad criptográfica de la firma digital

Este objetivo se cubre mediante la generación de claves criptográficas robustas a través de **FCS_COP.2** *generación de SCD/SVD* y la utilización de algoritmos de firma segura mediante **FCS_COP.2** *activación del SCD en firma/autenticación* a través de canales seguros entre la aplicación de firma y el TOE seguros mediante **FTP_ITC.1** *Aplicación de Creación de Firma*.

O.SCD-ANTIREPLAY: Protección contra ataques de repetición

Este objetivo se cubre mediante el establecimiento en cada petición de firma/autenticación de un segundo factor de autenticación de un solo uso OTP a través de **FIA_UAU.5** *para los usuarios firmantes en las operaciones de firma y cambio de contraseña*, **FDP_ACC.1** Operaciones de los usuarios firmantes SFP, **FDP_ACF.1** Operaciones de los usuarios firmantes SFP, de manera que se denegará aquella petición repetida por no cumplir con la autenticación **FPT_RPL.1** *Replay detection*.

O.CONFIGURATION-INTEGRITY: Mantener autoría de la configuración

Este objetivo se cubre mediante la generación de valores HMAC para cada registro de base de datos a través de **FCS_COP.1** *descifrado/cifrado simétrico de datos*, **FCS_CKM.1** *descifrado/cifrado simétrico de datos*, **FCS_CKM.3** *clave protección fichero de configuración HMAC*, **FCS_COP.1** *descifrado fichero configuración HMAC*, **FCS_COP.1** *verificación fichero configuración HMAC*, **FCS_COP.1** *cálculo/verificación HMAC*. El TOE dispondrá de procesos de verificación de la autoría de los datos almacenados tanto online como offline alertando de posibles datos no generados por el TOE mediante **FDP_SDI.1** *Stored data integrity monitoring*, **FAU_SAA.1** *Potential violation analysis*, y **FAU_ARP.1** *Security alarms*.

La comunicación con la base de datos se efectuará a través del canal seguro establecido mediante **FTP_ITC.1** Base de datos, de esta manera se aseguran los datos durante el envío.

O.USER-DATA-INTEGRITY: Mantener autoría de los datos de trabajo de los usuarios

Este objetivo se cubre mediante la generación de valores HMAC para cada registro de base de datos a través de **FCS_COP.1** *descifrado/cifrado simétrico de datos*, **FCS_CKM.1** *descifrado/cifrado simétrico de datos*, **FCS_CKM.3** *clave protección fichero de configuración HMAC*, **FCS_COP.1** *descifrado fichero configuración HMAC*, **FCS_COP.1** *verificación fichero configuración HMAC*, **FCS_COP.1** *cálculo/verificación HMAC***.** El TOE dispondrá de procesos de verificación de la autoría de los datos, tanto online como offline alertando de posibles inconsistencias mediante **FDP_SDI.1** *Stored data integrity monitoring*, **FAU_SAA.1** *Potential violation analysis*, y **FAU_ARP.1** *Security alarms***.**

La comunicación con la base de datos se efectuará a través del canal seguro establecido mediante **FTP_ITC.1** Base de datos, de esta manera se aseguran los datos durante el envío.

O.AUDIT-INTEGRITY: Generación de datos de auditoría

Este objetivo se cubre mediante la generación de datos de auditoría a través de **FAU_GEN.1** *operaciones del TOE*, **FAU_GEN.1** *operaciones de los usuarios firmantes*, **FAU_GEN.2** *Identificación del usuario de la operación*, su accesibilidad para consultar total o parcialmente los datos generados mediante **FAU_SAR.1** *revisión de los datos de auditoría de operaciones del TOE*, **FAU_SAR.1** *revisión de los datos de auditoría de operaciones del usuario firmante*, **FAU_SEL.1** *selección de los datos de auditoría de operaciones del TOE*, **FAU_SEL.1** *selección de los datos de auditoría de operaciones de los usuarios firmantes*, y determinando el control de acceso mediante **FAU_SAR.2** *acceso restringido a los datos de auditoría del TOE*.

Así mismo se cubrirá la autoría de los datos de auditoría mediante el sistema de generación HMAC a través de **FCS_COP.1** *descifrado/cifrado simétrico de datos*, **FCS_CKM.1** *descifrado/cifrado simétrico de datos*, **FCS_CKM.3** *clave protección fichero de configuración HMAC*, **FCS_COP.1** *descifrado fichero configuración HMAC*, **FCS_COP.1** *verificación fichero configuración HMAC*, **FCS_COP.1** *cálculo/verificación HMAC*, **FDP_SDI.1** *Stored data integrity monitoring*, **FAU_SAA.1** *Potential violation analysis* y **FAU_ARP.1** *Security alarms*.

La comunicación con la base de datos se efectuará a través del canal seguro establecido mediante **FTP_ITC.1** Base de datos, de esta manera se aseguran los datos durante el envío.

O.VERIFICATION-SERVER-SMS: Verificación de las respuestas del servidor de envío de SMS

Este objetivo se cubre mediante el aseguramiento de las comunicaciones entre la pasarela de SMS y el TOE con **FTP_ITC.1** *Plataforma envío SMS* y firmando las peticiones que el TOE envía a la plataforma de envío de SMS mediante **FCS_CKM.3** *almacén clave de firma/verificación plataforma de envío de SMS*, **FCS_COP.1** *firma petición envío plataforma SMS*, así mismo el TOE verifica la respuesta de la pasarela mediante **FCS_COP.1** *verificación firma de respuesta plataforma SMS*.

O.PROTECT-HMAC-KEY: Protección de la clave de generación HMAC

Este objetivo se cubre mediante la protección de los ficheros que constituyen la configuración y claves necesarias para el cálculo de los valores HMAC que posibilitan la integridad de los datos de auditoría, configuración y de usuario.

De esta manera mediante **FCS_COP.1** *descifrado/cifrado simétrico de datos* y **FCS_CKM.1** *descifrado/cifrado simétrico de datos*, se protege la contraseña del almacén de claves HMAC y mediante **FCS_CKM.3** *clave protección fichero de configuración HMAC*, **FCS_COP.1** *descifrado fichero configuración HMAC* y **FCS_COP.*1*** *verificación fichero configuración HMAC***,** se accede a la configuración que establece la generación de los datos HMAC para la autoría de los datos por parte del TOE.

O.CIPHER-PASS: Cifrado de contraseñas de almacenes de claves o configuración de accesos

El objetivo de proteger aquellos datos almacenados en el entorno operativo mediante cifrado simétrico se consigue mediante **FCS_COP.1** *descifrado/cifrado simétrico de datos*, **FCS_CKM.1** *descifrado/cifrado simétrico de datos,* **FCS_COP.1** *descifrado fichero configuración HMAC* y **FDP_SDC.1** *Stored data confidentiality*, de esta manera, todos los datos sensibles se cifran para preservar su confidencialidad.

O.DETECT-FUNCTION-SECURITY-SYSTEM: Detección de eventos de seguridad en el sistema

El cumplimiento de este objetivo se consigue mediante la generación de valores HMAC que aseguran la integridad de los datos almacenados en la base de datos y que permiten detectar posibles modificaciones no autorizadas mediante **FCS_COP.1** *cálculo/verificación HMAC***, FAU_SAA.1** *Potential violation analysis***, FAU_ARP.1** *Security alarms***.**

Mediante **FAU_STG.3** *archivado de datos de auditoría de operaciones del TOE* se detectarán los límites establecidos de almacenamiento de base de datos que determinarán cuando se deberá ejecutar el proceso de archivado por parte de los administradores de base de datos**.**

A través de la consulta de los datos de auditoría **FMT_MTD.1 Consulta datos de auditoría,** se podrán consultar las diferentes operaciones realizadas en el sistema y determinar si se pueden estar produciendo operaciones o intentos de acceso al sistema de manera anómala.

6.4 Requisitos de garantía de seguridad

El desarrollo y evaluación del TOE se realizará conforme al nivel de garantía EAL4 + AVA_VAN.5 + ALC_FLR.1.

Los requisitos de garantía para este nivel de garantía, tal y como se especifican en Common Criteria Parte 3 v3.1 R4, se resumen en la siguiente tabla:

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification

	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.1: Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Tabla 15: Requisitos de garantía de seguridad

6.4.1 Justificación de los requisitos de garantía

Esta declaración de seguridad declara conformidad con el paquete de garantía EAL4 aumentado con los componentes AVA_VAN.5 y ALC_FLR.1.

El paquete predefinido EAL4 permite que el usuario final obtenga la máxima confianza en el producto desarrollado en base métodos de ingeniería sistemáticos y buenas prácticas de desarrollo.

La selección del componente AVA_VAN.5 proporciona unas garantías superiores a las del paquete predefinido EAL4, requiriendo un análisis de vulnerabilidades que permite valorar la resistencia a ataques de penetración realizados por un atacante con potencial de ataque alto (“High”).

7. ESPECIFICACIÓN RESUMIDA DEL TOE

7.1 Auditoría (FAU)

El TOE genera dos tipos de datos de auditoría.

7.1.1 Datos de auditoría de operaciones del TOE

Estos datos de auditoría se generan en la base de datos mediante **FAU_GEN.1 operaciones del TOE** y representan las operaciones funcionales de gestión que se realizan en el TOE ya sea mediante llamadas a los servicios de administración del TOE como a través de los servicios de firma. En cada operación reflejada se identifica de forma unívoca el usuario utilizado para realizar la operación en el TOE, **FAU_GEN.2 Identificación del usuario de la operación.**

Estos datos de auditoría pueden ser revisados a través de los servicios de administración. Mediante un usuario con el perfil y permisos adecuados para invocar al servicio se podrán consultar los datos filtrando por los diferentes campos generados en los datos de auditoría. Concretamente en la configuración establecida para la evaluación del TOE, aquellos usuarios que tengan asociado un perfil con la funcionalidad *ADMIN_LIST_AUDIT_OPERATIONS_SERVICE* cumpliendo así **FAU_SAR.2 acceso restringido a los datos de auditoría del TOE.**

A través de este servicio se podrán consultar los datos pudiendo filtrar por diferentes campos para seleccionar aquellos datos de auditoría que se requieran cumpliendo **FAU_SAR.1 revisión de los datos de auditoría de operaciones del TOE, FAU_SEL.1 selección de los datos de auditoría de operaciones del TOE.**

Para garantizar la generación de los datos de auditoría, se establecerá un tamaño suficiente de almacenamiento en la base de datos, y mediante el mecanismo de alertas se avisará de que el tamaño máximo de almacenamiento ha llegado al límite establecido**,** cumpliendo **FAU_STG.3 archivado de datos de auditoría del TOE.**

7.1.2 Datos de auditoría de operaciones de los usuarios firmantes

Estos datos de auditoría se generan en la base de datos mediante **FAU_GEN.1 operaciones de los usuarios firmantes** y representan las operaciones que un usuario firmante realiza en el TOE o aquellas operaciones que realiza un administrador sobre los activos de un determinado usuario firmante. En cada operación reflejada se identifica de forma unívoca el usuario utilizado para realizar la operación en el TOE y el usuario firmante involucrado en la operación, **FAU_GEN.2 Identificación del usuario de la operación.**

Estos datos de auditoría pueden ser revisados a través de los servicios de administración. Mediante un usuario con el perfil y permisos adecuados para invocar al servicio se podrán consultar los datos filtrando por los diferentes campos generados en los datos de auditoría. Concretamente en la configuración establecida para la evaluación del TOE, aquellos usuarios que tengan asociado un perfil con la funcionalidad *ADMIN_LIST_OPERATIONS_SERVICE* o *LIST_OWNER_OPERATIONS_SERVICE* cumpliendo así **FAU_SAR.2 acceso restringido a los datos de auditoría del TOE.**

A través de este servicio se podrán consultar los datos pudiendo filtrar por diferentes campos para seleccionar aquellos datos de auditoría que se requieran cumpliendo **FAU_SAR.1 revisión de los datos de auditoría de operaciones del usuario firmante, FAU_SEL.1 selección de los datos de auditoría de operaciones del usuario firmante.**

Para garantizar la generación de los datos de auditoría, se establecerá un tamaño suficiente de almacenamiento en la base de datos, y mediante el mecanismo de alertas se avisará de que el tamaño máximo de almacenamiento ha llegado al límite establecido, cumpliendo **FAU_STG.3 archivado de datos de auditoría del TOE.**

7.1.3 Autoría de los datos de auditoría

La autoría de los datos de auditoría, tanto para las operaciones del TOE como de las operaciones de los usuarios firmantes, se mantienen mediante el cálculo de un valor HMAC de cada registro escrito en la base de datos, de manera que mediante **FAU_SAA.1 Potential violation analysis,** que establece la comprobación de cada registro leído de la base de datos y **FAU_ARP.1 Security alarms** que establece la generación de alertas cuando una validación HMAC sobre los datos de auditoría no se verifica correctamente, se asegura la detección de cualquier dato que no haya generado el TOE sobre los datos de auditoría almacenados en la base de datos.

7.2 No repudio (FCO)

El TOE asegura el no repudio utilizando criptografía asimétrica basada en RSA, de manera que se asegura el origen del SVD exportado para la generación del certificado vinculado al SCD generando un CSR(Certificate Signing Request) el cual es firmado por el SCD tal y como indica **FCO_NRO.1 CSR Generación del certificado.** De esta manera, se asegurará que el certificado emitido por el prestador de servicios de generación de certificados genera un certificado de acuerdo a una determinada SCD.

7.3 Operaciones criptográficas (FCS)

El TOE realiza diferentes operaciones criptográficas, como cifrado, descifrado, firmas y verificación de firmas, de acuerdo a algoritmos y tamaños de clave especificados a continuación:

7.3.1 Descifrado/cifrado simétrico de datos

Las operaciones criptográficas para el descifrado/cifrado de datos almacenados en los ficheros de configuración y en la base de datos se componen de:

- **FCS_COP.1 descifrado/cifrado simétrico de datos**

  Los datos sensibles que se almacenan en la base de datos, ciertos datos de configuración, OTPs y las contraseñas de acceso a los almacenes de claves, se guardan cifradas utilizando un algoritmo simétrico 3DES (192 bits).

- **FCS_CKM.1 descifrado/cifrado simétrico de datos**

  Las contraseñas almacenadas en los ficheros de configuración y los datos sensibles que se almacenan en la base de datos son cifradas mediante una clave simétrica por el TOE por el módulo de administración o por el proceso de inicialización del TOE. Estos datos se cifran/descifran generando la misma clave a través de la función *rareGetBytes* a partir de una clave común incluida en el código, un identificador único que identifica el dato y el algoritmo común entre el TOE y el módulo de administración que finalmente generan una clave 3DES de 192 bits que es almacenada únicamente en memoria.

7.3.2 Operaciones generación de autoría mediante HMAC

Las operaciones criptográficas necesarias para la generación de valores de autoría de los datos mediante valores HMAC son:

La configuración de generación de valores HMAC para proteger a los datos almacenados en la base de datos se encuentra en los ficheros de configuración que se establecen en la inicialización del TOE, de manera que las claves residen en un almacén PKCS#12 y la configuración en un fichero que está cifrado y firmado.

- **FCS_CKM.3 clave protección fichero de configuración HMAC**

  - Inicialmente se recuperan los datos necesarios para acceder al almacén físico.
  - En segundo lugar se descifra la contraseña guardada en el fichero de configuración para acceder al almacén físico. Esta contraseña se ha cifrado desde el proceso de inicialización del TOE y es descifrada según establece el requisito *FCS_COP.1 descifrado/cifrado simétrico de datos.*
  - La clave privada se encuentra en un almacén criptográfico y su acceso y uso se realiza según establece el estándar PKCS#12.
  - Las claves públicas se encuentran en formato X509 v3

- **FCS_COP.1 descifrado fichero configuración HMAC**

  - El fichero de configuración que es generado en el proceso de inicialización del TOE se cifra para preservar su confidencialidad. El TOE en el arranque del mismo realiza la operación de descifrado para mediante un algoritmo XMLEncryption accediendo a la clave de descifrada mediante *FCS_CKM.3 clave protección fichero de configuración HMAC***.**

- **FCS_COP.1 verificación fichero configuración HMAC**

- El fichero en su proceso de generación además de ser cifrado es firmado para preservar su integridad. Una vez descifrado se procede a verificar su firma accediendo a la clave mediante *FCS_CKM.3 clave protección fichero de configuración HMAC***.**

- **FCS_COP.1 cálculo/verificación HMAC**

  - El TOE una vez accedido a la configuración HMAC después de haber descifrado el fichero y comprobado su integridad, determinará la generación de valores HMAC para cada registro almacenado en la base de datos. En la actual configuración de evaluación se especifica la generación de valores HMAC mediante un algoritmo HMac-SHA256.

- **FCS_COP.1 firma/verificación archivado datos de auditoría**

  El archivado de los datos de auditoría exportará los datos desde la base de datos a un fichero el cual se firmará por el TOE mediante firma electrónica accediendo a la clave de firma del TOE mediante *FCS_CKM.3 clave protección fichero de configuración HMAC***.**

7.3.3 Operaciones comunicación con plataforma envío SMS

El TOE en su comunicación con la plataforma de envío de SMS realizará las operaciones criptográficas necesarias para asegurar el envío de las OTPs a los usuarios.

La configuración de acceso a la plataforma de envío de SMS establecerá el almacén de claves del tipo PKCS#12 o JKS que contiene la clave de firma para las peticiones que el TOE realizará hacia la plataforma de envío de SMS.

- **FCS_CKM.3 almacén clave de firma/verificación plataforma de envío de SMS**

  En este almacén se configurará la clave de firma para las peticiones que el TOE realizará hacia la plataforma de envío de SMS, así como el certificado para verificar las respuestas de la misma. El acceso al mismo se realizará descifrando los datos de configuración establecidos mediante *FCS_COP.1 descifrado/cifrado simétrico de datos* y una vez obtenida la contraseña acceder mediante el estándar PKCS#12 o JKS.

- **FCS_COP.1 firma petición envío plataforma SMS**

  Las peticiones realizadas por el TOE hacia la pasarela de envío de SMS serán firmadas mediante firma electrónica accediendo a la clave de firma mediante *FCS_CKM.3 almacén clave de firma/verificación plataforma de envío de SMS.*

- **FCS_COP.1 verificación firma de respuesta plataforma SMS**

  Las respuestas recibidas por parte de la plataforma de SMS se verificarán mediante la comprobación de la firma electrónica y verificación del certificado utilizado para la firma. El acceso al certificado se realiza mediante *FCS_CKM.3 almacén clave de firma/verificación plataforma de envío de SMS.*

7.3.4 Operaciones delegadas en el HSM

El TOE para las operaciones relacionadas con las claves pública y privada del usuario firmante delega la ejecución de las operaciones criptográficas en el módulo criptográfico HSM.

- **FCS_COP.2 Delegated Cryptographic operation – generación de SCD/SVD**

La operación de generación de un par de claves para un determinado usuario se realiza mediante la invocación al interfaz PKCS#11 realizando la siguiente secuencia de pasos:

  - Se estable una sesión a la partición del HSM configurada en el TOE, para ello se accede con usuario y contraseña de la partición obteniendo estos datos de la configuración del TOE.

  - Una vez establecida la sesión con el HSM, se invoca a la función *generateKeyPair* que se encarga de generar una par de claves RSA.

  - Una vez obtenidas las claves se generará el CSR incluyendo la clave pública y firmando la estructura PKCS#10 para poder posteriormente solicitar la generación del certificado en la correspondiente entidad emisora.

  - Una vez obtenidas el par de claves, se procede a derivar la clave de protección de la clave privada, esto se realiza mediante la llamada a la función *deriveKey* que se encarga de derivar una clave a partir de la contraseña establecida por el usuario propietario de las claves y una clave maestra AES que reside en el HSM.

  - Una vez obtenida la clave derivada, se procede a proteger la clave privada mediante la llamada a la función *wrapKey*. Finalmente se eliminan todos los objetos creados en la sesión mediante la llamada a la función *destroyObject*.

- **FCS_COP.2 Delegated Cryptographic operation – activación del SCD en firma/autenticación**

  La operación de activación de la clave privada del usuario para la operación de firma se realiza mediante la invocación al interfaz PKCS#11 realizando la siguiente secuencia de pasos:

  - Se estable una sesión a la partición del HSM configurada en el TOE, para ello se accede con usuario y contraseña de la partición obteniendo estos datos de la configuración del TOE.

  - Una vez obtenida la sesión, se procede a derivar la clave de protección de la clave privada, esto se realiza mediante la llamada a la función *deriveKey* que se encarga de derivar una clave a partir de la contraseña establecida por el usuario propietario de las claves y una clave maestra AES que reside en el HSM.

- Una vez derivada la clave se procede a activar la clave de firma, esto se realiza mediante la llamada a la función *unwrapKey* a partir de la clave derivada. Si la operación es correcta la clave de firma queda activada y lista para realizar la operación de firma mediante la llamada a la función *sign.* Finalmente se eliminan todos los objetos creados en la sesión mediante la llamada a la función *destroyObject*.

- **FCS_COP.2 Delegated Cryptographic operation – cambio de contraseña**

  La operación de cambio de contraseña de la clave privada del usuario para la operación de firma se realiza mediante la invocación al interfaz PKCS#11 realizando la siguiente secuencia de pasos:

  - Se estable una sesión a la partición del HSM configurada en el TOE, para ello se accede con usuario y contraseña de la partición obteniendo estos datos de la configuración del TOE.

  - Una vez obtenida la sesión, se procede a derivar la clave de protección de la clave privada, esto se realiza mediante la llamada a la función *deriveKey* que se encarga de derivar una clave a partir de la contraseña establecida por el usuario propietario de las claves y una clave maestra AES que reside en el HSM.

  - Una vez derivada la clave se procede a activar la clave de firma, esto se realiza mediante la llamada a la función *unwrapKey* a partir de la clave derivada. Si la operación es correcta la clave de firma queda activada y lista para realizar nuevamente la protección con la nueva clave del usuario.

  - Se vuelve a realizar la función *deriveKey* para generar una nueva clave a partir de la nueva contraseña y posteriormente realizar la protección de la clave mediante la llamada a la función *wrapKey.* Finalmente se destruyen las claves generadas en la sesión mediante destroyObject.

El TOE al realizar las operaciones criptográficas sobre un dispositivo que cumple con el nivel FIPS 140-2 SL3 asegura la generación de los datos de creación de firma de manera que solo puedan aparecer una vez en la práctica. Igualmente se determina la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento.

7.4 Identificación y Autenticación

El TOE no permite realizar ninguna acción a los usuarios que no estén autenticados. Todo usuario del TOE debe identificarse y autenticarse antes de realizar ninguna acción sobre el sistema mediante autenticación con certificados a través de los servicios web.

El TOE no permite realizar ninguna acción a los usuarios que no estén autorizados. Todo usuario del TOE debe identificarse y autenticarse antes de realizar ninguna acción sobre el sistema y su perfil debe autorizarle para realizar la acción que solicita, de esta manera se ejercen los requisitos de seguridad **FIA_UAU.2 User authentication before any action y FIA_UID.2 User identification before any action.**

Además, el TOE exige a los usuarios firmantes la autenticación mediante dos canales y dos factores antes de poder realizar una firma o el cambio de contraseña utilizando su SCD. Deberán proporcionar la contraseña que solo el firmante conoce y que no es almacenada por el TOE y una contraseña de un solo uso que se enviará al dispositivo móvil del firmante, de esta manera se cumple **FIA_UAU.5 Multiple authentication mechanisms - para los usuarios firmantes en las operaciones de firma y cambio de contraseña.**

Los usuarios firmantes al intentar hacer uso de sus claves privadas, podrán bloquearlas tras un número concreto de intentos de acceso incorrecto. Cuando se alcanza el número de intentos fallidos de autenticación, el sistema dejará bloqueado dicha clave. El bloqueo de claves por número de intentos puede configurarse para que sea temporal y el firmante pueda volver a usar su clave privada(SCD) pasado un tiempo determinado sin que deba ser desbloqueado por un administrador. De esta manera se cumple **FIA_AFL.1 Authentication failure handling – usuarios firmantes en la operación de firma/cambio de contraseña.**

7.5 Protección de los datos del usuario

7.5.1 Políticas de control de acceso

- **FDP_ACC.2 Complete access control – Acceso a los servicios web SFP**

El TOE dispone de políticas de control de acceso para acceder a los servicios web del TOE.

El acceso a cada una de las operaciones que se ofrecen a través de los servicios web tiene su correspondiente reflejo en el perfil de acceso mediante su correspondiente 'funcionalidad'. De esta manera, cualquier usuario que acceda a los servicios web solicitando una determinada operación deberá poseer del perfil adecuado que contenga el permiso para ejecutar la operación solicitada.

- **FDP_ACC.1 Subset access control - Operaciones de los usuarios firmantes SFP**

El acceso a aquellas operaciones de los servicios web que requieren de la intervención del usuario propietario de las claves, requiere el mismo control de acceso que cualquier otra operación en cuanto a la autenticación y autorización del usuario, pero se establecen controles adicionales en función de la operación donde se requiere de la autenticación del usuario firmante para hacer uso de la clave privada.

Las políticas de control de acceso se aplicarán en base al identificador único de los usuarios de los servicios web autenticados, en base al perfil que tengan asignado y tras la autenticación correcta de los mismos. Cada perfil contiene las funcionalidades permitidas definiendo claramente la autorización de la que dispone el usuario, de esta manera se establece de manera general que para todos las operaciones del TOE se requiere la autenticación y autorización tal y como indica las reglas de la política **FDP_ACF.1 Security attribute based access control - Acceso a los servicios web SFP.**

Igualmente, para las operaciones que requieren de verificaciones adicionales para cumplir con la funcionalidad de seguridad requerida, se define la política específica **FDP_ACF.1 Security attribute based access control - Operaciones de los usuarios firmantes SFP** donde se definen las reglas de acceso para la realización de cada operación en la que los usuarios firmantes deben interactuar.

7.5.2 Exportación/Importación de datos de usuario

El TOE realiza la exportación de datos con atributos de seguridad cuando en la operación de creación de claves devuelve la clave pública generada firmada por la clave privada en una estructura PKCS#10 (CSR) que servirá para solicitar a la aplicación de generación de certificados el certificado con la clave pública asociada a la clave privada, de esta manera se ejercerá **FDP_ETC.2 Exportación CSR y FDP_ITC.1 Asociación de Certificado** para el momento de la asociación del certificado generado con la clave pública y su vinculación con su clave privada en el TOE.

El TOE además, importa la contraseña de activación de la clave privada en las operaciones de generación de claves y cambio de contraseña, de manera que esta contraseña es *hasheada* y almacenada en un histórico de contraseñas que posteriormente servirá para validar la política de contraseñas establecida en el sistema, ejerciendo así **FDP_ITC.1 Histórico de contraseñas.**

7.5.3 Protección de datos: confidencialidad y autoría

El TOE mediante su configuración, determina la monitorización tanto online, como offline, de los datos almacenados en la base de datos verificando en cada lectura de la base de datos que estos han sido generados por el TOE comprobando que su valor HMAC es correcto, de esta manera se establece un monitorización continua de los valores almacenados en la base de datos, rechazando cualquier operación que no verifique correctamente la autoría de los datos utilizados en la operación. Igualmente, se establece un proceso de generación de alertas sobre posibles datos no generados por el TOE almacenados en la base de datos cumpliendo con **FDP_SDI.1 Stored data integrity monitoring.**

En cuanto a la confidencialidad de los datos, el TOE almacena de manera cifrada toda la información confidencial de los firmantes, como puedan ser sus claves de firma (SCDs). El TOE no almacena de ningún modo la contraseña estática que solo conoce el firmante. Los SCDs del firmante no pueden ser recuperados ni utilizados sin la contraseña de protección que solo conoce el firmante.

Las contraseñas dinámicas (OTPs) generadas para cada operación que requiere realizar el firmante se almacenan cifradas así como los datos relevantes de acceso al HSM y de acceso a la plataforma de envío de SMS, de esta manera se cumple con **FDP_SDC.1 Stored data confidentiality.**

El TOE asegura la relación entre el SVD y el SCD apoyado en la criptografía asimétrica RSA. Los SVD exportados desde el TOE siempre van almacenados en un contenedor (PKCS#10 o PKCS#1) en el que dicha clave pública (SVD) se firma con la clave privada (SCD) asociada. Adicionalmente, mediante HMAC se asegura la autoría de la relación de ambos datos y su relación con el firmante correcto ejerciendo de esta manera con **FDP_UDC.1 User data correspondence.**

En cuanto a la detección de réplica, el TOE exige para cada operación de firma y cambio de contraseña, una contraseña dinámica de un solo uso (OTP), de manera que un reenvío de petición es directamente rechazado puesto que no se validará correctamente una OTP que ya ha sido utilizada, de esta manera se cumple con **FPT_RPL.1 Replay detection,** no aceptando replicación de la petición de firma ni cambio de contraseña.

7.6 Protección de los datos de la TSF

El TOE deberá estar configurado para disponer de una hora fiable e incorporará esa información horaria en cada una de las trazas de auditoría que genere, para ello se deberá configurar el sistema de sincronización mediante protocolo ntp del que dispone el sistema en el que está instalado el TOE. De esta manera, se utilizará la información horaria para controlar la utilización de las claves privadas y para decidir si las OTPs han caducado**.**

7.7 Funciones de gestión de la seguridad

El TOE trabaja internamente mediante perfiles configurables que permiten granular la capacidad de acceso sobre diferentes funcionalidades. De esta manera, se definen perfiles que solamente pueden consultar cierta información, perfiles que solamente pueden gestionar la infraestructura sin consultar datos de los usuarios finales, perfiles que solamente pueden gestionar datos de usuario, etc. De esta manera cada gestión de la seguridad estará asociada a un perfil y una funcionalidad específica, pudiendo determinar funciones para la gestión de las cuentas de los usuarios firmantes mediante **FMT_MSA.1 Management of security attributes – ADMIN-OWNER,** funciones de gestión para la generación de claves de firma con **FMT_MSA.1 Management of security attributes - CREATE_KEY** y cambio de contraseñas **FMT_MSA.1 Management of security attributes - CHANGE_PASSWORD_SERVICE.**

El TOE por lo tanto establece funciones de gestión desde las operaciones establecidas en los servicios de administración, y las operaciones establecidas en los servicios de firma cumpliendo con **FMT_SMF.1 Specification of Management Functions.**

El acceso a los datos de auditoría se realiza sobre los servicios web de administración mediante el perfil que contiene la funcionalidad específica para las operaciones de listado de datos de auditoría, de esta manera se establece un control sobre que usuarios pueden acceder a los datos de auditoría según establece **FMT_MTD.1 Management of TSF data – Consulta datos de auditoría.**

7.8 Comunicaciones seguras

El TOE utiliza canales de comunicación que aseguran el cifrado y la autenticidad de las partes. Todos los accesos a los servicios proporcionados por el TOE deben realizarse a través de canales TLS, quedando claramente autenticado el TOE, y solicitando la información de autenticación del otro punto a través de este canal cifrado. **FTP_ITC.1 Inter-TSF trusted channel - Aplicación de Registro** y **FTP_ITC.1 Inter-TSF trusted channel - Aplicación de Creación de Firma.**

Para aquellas comunicaciones que realiza el TOE a entidades externas como pueden ser la base de datos y la plataforma de envío de SMS, el TOE comprobará el certificado del servidor al establecer la comunicación SSL, y con la pasarela de firma además enviará la petición firmada para que esta pueda comprobar el origen de la petición y el TOE verificará la firma en su respuesta. De esta manera se establece la seguridad en las comunicaciones con **FTP_ITC.1 Inter-TSF trusted channel – Base de datos** y **FTP_ITC.1 Inter-TSF trusted channel – Plataforma envío SMS**.