eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1 Declaración de Seguridad

delivering value

AENOR ER Seguridad Información SI-0013/06

ISO 9001 BUREAU VERITAS Certification Nº ESPMDD005916

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) 91 307 79 80

www.siainternational.com

ÍNDICE

1. INTRODUCCIÓN

1.1 Identificación

1.1.1 Identificación Declaración de Seguridad

Título	eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1 - Declaración de Seguridad
Versión	1.6
Autor	SIA – Software Factory
Fecha	04 de junio de 2010

1.1.2 Identificación del TOE

TOE	eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1
Versión	6.2.1
Autor	SIA – Software Factory
Identificación CC	*Common Criteria for Information Technology Security Evaluation* v3.1 R3 de Julio de 2009
EAL	EAL1+ALC_FLR.1

1.2 Descripción general

El TOE referenciado en esta declaración de seguridad es un subconjunto de elementos que forman parte del producto **eAS/Trusted Signature Platform v6.2.1**, también conocido como SIAVAL. El producto completo es una Plataforma de Firma y Custodia que permite tanto la generación como la validación de firma electrónica, utilizando diferentes formatos como XMLDSig, XAdES 1.2.2, CAdES 1.7.3, PKCS#7 y PDF, así como la Custodia de Documentos (firmados o no), custodia de firmas y almacenamiento simple.

A continuación se describe de manera general el objeto de evaluación de la presente declaración de seguridad.

Los componentes que proporcionan los servicios del TOE son:

- **Módulo Crypto**: Proporciona todos los servicios de firma electrónica, cifrado/descifrado de información y validación de certificados. Estos servicios se ofrecen a través de servicios web WSS o mediante servicios web mediante protocolo binario hessian.

- **API de Integración Crypto**: Este API realiza las llamadas a los servicios que proporciona el módulo Crypto de manera transparente al usuario abstrayendo la complejidad de la construcción de los WSDL o llamadas binarias Hessian, de manera que el usuario realiza las llamadas a través de un API Java.

Las principales características de sus servicios son:

- Soporte para múltiples formatos de firma: XMLDSig, XAdES, PKCS#7, CAdES, S/MIME y PDF.

- Soporte para cifrado y descifrado de datos: XML Encryption y PKCS#7.

- Validación del estado de revocación de los certificados basado en CRL (vía LDAP, HTTP, file, etc) y en OCSP.

- Extracción de información y validación de certificados.

- Verificación de firmas en cualquiera de los formatos que genera el producto.

- Generación de sellados de tiempo internos (fechados) o utilizando servicios externos ofrecidos por TSA (TimeStamp Authority) a través de TSP (TimeStamp Protocol) para los estándares XAdES, CAdES, PKCS#7 y PDF.

- Soporte para múltiples autoridades de certificación, especialmente las reconocidas por la Agencia Tributaria (AEAT).

- Diferentes niveles de validación en base a la política que se aplique a la hora de realizar la validación de un documento firmado. Los niveles posibles que se pueden establecer desde la administración son:

    - Solo integridad

- Integridad y confianza
- Integridad y caducidad
- Integridad, caducidad y confianza
- Validación completa

- Los servicios soportan, en base a la política de validación establecida en la administración, varios mecanismos de recuperación de la información de revocación de un certificado, de tal forma que pueden utilizar cualquiera de ellos (en un orden preestablecido) para recuperar los datos necesarios. Así, por ejemplo, si para un certificado están definidos la descarga de CRLs vía HTTP y vía LDAP y el primero de ellos no está disponible por cualquier causa, los servicios emplearán entonces el segundo para descargar toda la información.

- Soporte para múltiples algoritmos de firma y cifrado.
  - Capacidad de funcionamiento con caché de CRL y OCSP, diferenciada para certificados de usuario y de CAs, TSAs, etc para mejorar el rendimiento en la obtención de información de revocación de certificados.
  - Múltiples soportes para el almacenamiento de claves: HSM, PKCS#11 y PKCS#12.

Teniendo en cuenta sus características y como módulo orientado a servicios web, éstas son las operaciones que se pueden llevar a cabo:

- Generación de firmas en formato PKCS#7 attached y detached.
- Añadido de firmas sobre un documento PKCS#7.
- Generación de Firmas CAdES-BES.
- Añadido de firmas sobre un documento CAdES-BES.
- Generación de firmas en formato PDF, con o sin fechado.
- Añadido de sellados de tiempo a firmas con formato PKCS#7.

- Añadido de sellados de tiempo a firmas con formato CAdES.
- Añadido de sellados de tiempo a firmas con formato XML (XAdES-BES).
- Generación de firmas en paralelo en formato XML.
- Generación de firmas en serie en formato XML.
- Verificación de firmas en formato PKCS#7.
- Extracción de contenido firmado en documentos PKCS#7 Attached.
- Validación de firmas CAdES.
- Extracción de contenido firmado en documentos CAdES Attached.
- Verificación de firmas en formato PDF.
- Verificación de firmas en formato XML.
- Verificación de firmas en formato SMIME.
- Generación de sellados de tiempo para un documento o resumen
- Verificación de sellados de tiempo.
- Cifrado de documentos en formato PKCS#7.
- Cifrado de documentos en formato XML.
- Generación de clave simétrica
- Descifrado de documentos en formato PKCS#7.
- Descifrado de documentos en formato XML.
- Sellado de contexto documentos de XML firmados.
- Sellado de contexto documentos de CAdES firmados.
- Archivado de documentos XML firmados.
- Archivado de documentos CAdES firmados.

- Validación y extracción de información de certificados.
- Adición de firmas a un documento en formato PKCS#7.
- Firma de documentos XML SOAP
- Cifrado de documentos XML SOAP
- Cifrado y firma de documentos XML SOAP
- Descifrado de documentos XML SOAP
- Gestión abierta que facilita la centralización de operaciones de gestión de elementos criptográficos.

El TOE ofrece por lo tanto servicios para firma electrónica y verificación en diferentes estándares, validación de certificados y cifrado/descifrado de datos. Todos estos servicios se ofrecen a través de servicios web seguros mediante WSDL o mediante protocolo binario Hessian y la manera que las aplicaciones clientes tienen de realizar las operaciones ofrecidas por los servicios es a través del API de Integración que abstrae la dificultad de construir las llamadas a los WebServices mediante WSS o mediante protocolo binario Hessian.

El TOE proporciona las funciones de seguridad necesarias para establecer un sistema confiable en el que poder ofrecer los servicios funcionales anteriormente descritos. Las funciones de seguridad del TOE para garantizar la seguridad del servicio son:

- **Control de acceso**: El TOE dispone de un control de acceso donde los usuarios deben autenticarse y autorizarse para poder hacer uso de los servicios del TOE. La autenticación de los usuarios podrá realizarse mediante usuario y contraseña o mediante certificado electrónico.

- **Integridad de la configuración del TOE mediante operaciones criptográficas**: El TOE mantiene en todo momento la integridad de sus ficheros de configuración mediante el uso de operaciones criptográficas internas independientes de las utilizadas para la funcionalidad de los servicios. A diferencia de las claves utilizadas por los servicios funcionales del TOE que pueden residir en elementos externos como un HSM, estas claves internas residen físicamente en la misma máquina que el TOE y quedan bajo su protección.

- **Confidencialidad de los datos de acceso a las claves:** Tanto para las operaciones criptográficas de protección de los ficheros de configuración del TOE, como para las operaciones criptográficas funcionales del TOE, todas las contraseñas utilizadas para el acceso a las claves criptográficas se guardan cifradas para proteger su confidencialidad.

- **Verificación de respuestas de entidades externas**: El TOE verifica las respuestas de peticiones de servicios externos al TOE como OCSPs o TSAs para asegurar su origen.

- **Generación de ficheros de auditoría**: El TOE genera ficheros de auditoría tanto de actividad como de operaciones para determinar el correcto uso del mismo.

Los requerimientos hardware y software del TOE son los siguientes:

Hardware:

- **Máquina Servidor:** No existe requerimiento específico hardware en cuanto al servidor a utilizar.
- **Máquina Cliente:** No existe requerimiento específico hardware en cuanto al cliente a utilizar.
- **Módulo Criptográfico: Cualquier módulo criptográfico con acceso mediante PKCS#11. En el caso concreto de Luna SA de SafeNet también mediante el API propio de SafeNet.**

Software:

- **Sistema Operativo en servidor:** No existe requerimiento específico de sistema operativo a utilizar.

- **Sistema Operativo en cliente:** No existe requerimiento específico de sistema operativo a utilizar.
- **Servidor de Aplicaciones para el módulo Crypto v6.2.1:** Los servidores de aplicaciones soportados son, Apache Tomcat 5.0.x, JBoss 4.0.x, Sun JSAS 8.x, Websphere 6.1.0 y Oracle Application Server 10.
- **Java Runtime Enviroment en servidor:** JDK 1.4.x ó JDK 1.5.x con JCE Unlimited Strength
- **Java Runtime Enviroment en cliente:** JDK 1.5.x con JCE Unlimited Strength
- **Módulo de Administración eAS/TSP Admin v.6.2.1:** El módulo de administración de la plataforma se encarga de generar y enviar el fichero con la configuración del TOE. Este módulo de administración no entra dentro de la evaluación, puesto que este módulo no pertenece al TOE, pero sí el fichero que envía a través del servicio de configuración del TOE.

1.3 Descripción del TOE

El TOE referido en esta descripción de seguridad es parte del producto **eAS/Trusted Signature Platform v6.2.1.** El TOE está compuesto por el módulo Crypto, que ofrece las operaciones funcionales de firma electrónica, cifrado/descifrado de datos, y validación de certificados, el API de integración que facilita las llamadas a los servicios web que ofrece el módulo Crypto y los ficheros de configuración que previamente deberán haber sido establecidos por un módulo de administración externo al TOE.

1.3.1 Configuración del TOE

La configuración del TOE es llevada a cabo mediante un herramienta 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.

Este módulo de configuración podrá residir en la misma máquina o en una máquina remota, la configuración en cualquier caso será enviada al TOE desde la administración a través de los servicios del TOE destinados a tal fin.

En la configuración generada por el módulo de administración se incluyen todos los datos necesarios para realizar el control de acceso a los servicios. Estos datos se establecen por dominios, que es la entidad lógica en la que operan los usuarios. Por cada dominio, se dispondrá de una lista de usuarios con sus datos de autenticación nombre de usuario, contraseña y certificado, y a cada usuario se le asignará un rol que determina los permisos que dispone para realizar las operaciones funcionales a nivel de cifrado/descifrado, firma y validación de documentos.
No existen roles predefinidos en el sistema para el TOE, todos los usuarios del TOE son usuarios peticionarios de sus servicios que tendrán asignado el rol que se establezca desde el módulo de administración, y podrán en función de ese rol realizar las operaciones designadas.

Los ficheros de configuración establecidos por el módulo de Administración determinan la configuración del TOE y se protegen mediante operaciones criptográficas internas del TOE.

Existen dos grupos de claves criptográficas utilizadas por el TOE.

- **Claves Criptográficas internas del TOE**: Claves utilizadas exclusivamente para asegurar los ficheros de configuración y se almacenan en keystores PKCS#12 protegidos mediante contraseña, estas claves no podrán residir en elementos externos a los propios ficheros de configuración y quedan al margen de las claves utilizadas por los usuarios para realizar sus operaciones funcionales ofrecidas por el TOE.

  Estas claves utilizadas para la protección de los ficheros de configuración son generadas en el momento de creación de la configuración y en el momento de la activación del módulo Crypto. Este proceso de creación de la configuración y activación del módulo Crypto se realiza desde el módulo de administración y es un proceso necesario para el correcto funcionamiento del TOE.

- **Claves de Usuarios del TOE:** Para realizar las operaciones funcionales del TOE los usuarios tienen asociadas las claves criptográficas necesarias para llevar a cabo dichas operaciones, estas claves propias de los usuarios podrán estar guardadas en almacenes de tipo PKCS#12 que residirán en la misma máquina que el TOE, o en módulos criptográficos HSM a los que el TOE accederá vía PKCS#11 o en el caso exclusivo del módulo HSM LunaSA, mediante el API ofrecido por el fabricante SafeNet.

    - En el caso de que las claves de usuarios residan en almacenes PKCS#12 estos almacenes deberán residir en la misma máquina que el TOE y en la configuración estará especificado como acceder a ellos. El TOE en ningún caso genera estas claves operativas de los usuarios, de manera que estos almacenes deben proporcionarse en el momento de la configuración desde el módulo de administración.

    - En el caso de que las claves de usuarios residan en un módulo criptográfico externo, será el propio HSM quien gestione las operaciones de creación, almacenamiento y protección de dichas claves. En este caso, el TOE se encargará de proteger los datos asociados a dichas claves manteniendo cifradas las contraseñas de acceso al almacén del HSM en sus ficheros de configuración.

1.3.2 Control de acceso

Para asegurar el acceso a los servicios, el TOE dispone de un control de acceso a través del cual se solicitará el nivel de autenticación y autorización adecuado para poder invocar a los servicios publicados por el TOE. Este control de acceso está determinado por la configuración establecida por el módulo de administración.

El control de acceso determina en primer lugar el nivel de autenticación, verificando que el usuario existe y se identifica correctamente mediante usuario y contraseña o mediante certificado, y un nivel de autorización, que vendrá determinado por el rol asociado al usuario en la configuración. Este rol establecerá si posee los permisos necesarios para realizar una operación determinada.

El proceso de autenticación que realiza el control de acceso se establece dentro de los ficheros de configuración, concretamente en los ficheros de políticas de control de acceso que determinan los procesos a ejecutar para realizar la autenticación y la autorización de la petición.

1.3.3 Verificación de respuestas de entidades externas

Para las operaciones de validación, el TOE tiene diferentes niveles en base a la política que se aplique a la hora de realizar la validación de un documento firmado. Los niveles posibles que se pueden establecer desde la administración son:

- Solo integridad
- Integridad y confianza
- Integridad y caducidad
- Integridad, caducidad y confianza
- Validación completa

Se soportan, en base a la política de validación establecida, varios mecanismos de recuperación de la información de revocación de un certificado, de tal forma que pueden utilizar cualquiera de ellos (en un orden preestablecido) para recuperar los datos necesarios. Así, por ejemplo, si para un certificado están definidos la descarga de CRLs vía HTTP y vía LDAP y el primero de ellos no está disponible por cualquier causa, los servicios emplearán entonces el segundo para descargar toda la información, igualmente se soporta validación de certificados vía OCSP realizando la petición a un servidor externo recuperando la respuesta y verificando que dicha respuesta no ha sido alterada validando su firma y comprobando que el certificado firmante pertenece a una entidad de certificación confiable por el TOE.

1.3.4 Auditoría

El TOE genera ficheros de auditoría tanto a nivel de actividad para determinar el correcto funcionamiento del mismo, como ficheros de operaciones donde comprobar las operaciones que realizan los usuarios contra el TOE. De esta manera se podrá comprobar el correcto funcionamiento del TOE y las operaciones invocadas a través de sus servicios.

1.3.5 Entorno del TOE

A continuación se describen los componentes necesarios que integran el TOE así como su arquitectura.

1.3.5.1 Componentes del TOE

Para ofrecer todos los servicios del TOE se deben disponer de los siguientes componentes.

- Módulo Crypto:
  - Ofrece el interfaz en formato de Servicios Web a través de los cuales los usuarios o aplicaciones solicitan las operaciones funcionales del TOE.
  - Realiza el oportuno control de acceso a las solicitudes de operaciones a través de los servicios web aplicando las políticas de control de acceso establecidas y en base a los roles definidos en la configuración.
  - Realiza la validación de integridad de los ficheros de configuración y políticas de control de acceso. Esta validación consta de la validación de integridad del fichero de configuración y de la validación de integridad y confidencialidad de los ficheros de control de acceso.

    Para realizar todas las operaciones de validación de integridad y confidencialidad el TOE realizará las operaciones criptográficas accediendo a claves almacenadas en keystores y certificados que son parte de los ficheros de configuración establecidos sin necesidad de realizar operaciones criptográficas a módulos criptográficos externos al TOE.

- API de Integración de Crypto
  - Este componente se localiza en la parte cliente desde la cual los usuarios o aplicaciones solicitan los servicios al módulo Crypto. Este API proporciona un interfaz programático para facilitar las llamadas a los servicios web que proporciona el módulo Crypto en la parte servidora.

- Configuración establecida previamente desde un módulo de administración externa al TOE

- Los ficheros de configuración son requisito imprescindible para el funcionamiento del Módulo Crypto y debe ser establecido por el Módulo de Administración que como se ha mencionado anteriormente queda fuera del TOE.

1.3.5.2 Arquitectura de evaluación del TOE

1.3.5.2.1 Arquitectura Física

En la arquitectura seleccionada para la evaluación se han incluido como elementos externos al TOE un módulo criptográfico Luna SA de SafeNet que se utiliza para realizar las operaciones criptográficas relacionadas con los servicios funcionales del módulo Crypto y un servidor donde se encuentra un emisor de sellos de tiempo TSA y un OCSP para la validación de certificados, así como el módulo de administración necesario para proporcionar la configuración al TOE. Concretamente para el entorno de evaluación, el módulo de administración residirá en una máquina distinta a la del TOE.

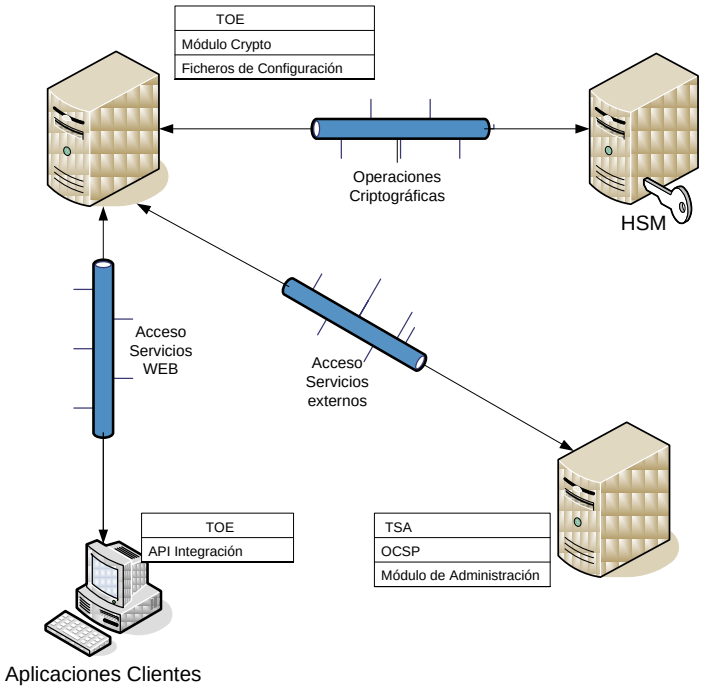

Ilustración 1: Arquitectura física de evaluación

Todos los componentes de software externos al TOE se instalarán conforme a las especificaciones de sus fabricantes, estos son: JDK, Servidor de Aplicaciones y cliente del HSM y configurados según se indica en los manuales del TOE.

Concretamente el entorno seleccionado para la evaluación del TOE es el siguiente:

Hardware:

- **Máquina Servidor del TOE:** Máquina PC genérica con procesador Intel 32 bits
- **Máquina Cliente del TOE:** Máquina PC genérica con procesador Intel 32 bits
- **Máquina Servicios Externos:** Máquina PC genérica con procesador Intel 32 bits
- **Módulo Criptográfico:** Luna SA v4.4 de SafeNet mediante acceso de API cliente propio de SafeNet.

Software:

- **Sistema Operativo en servidor del TOE:** Microsoft Windows 2003 Server
- **Sistema Operativo en servidor de servicios externos:** Microsoft Windows 2003 Server
- **Sistema Operativo en cliente:** Microsoft Windows XP SP3
- **Servidor de Aplicaciones:** JBOSS 4.0.4 GA
- **Java Runtime Enviroment en servidor:** JDK 1.5.0.15 con JCE Unlimited Strength
- **Java Runtime Enviroment en cliente:** JDK 1.5.0.15 con JCE Unlimited Strength
- **Módulo de administración:** Módulo que establece la configuración al TOE eAS/TSP tspAdmin v6.2.1
- **TSA:** Módulo para el sellado de tiempo eAS/TSP TSA v6.2.1 que cumple con la RFC3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"
- **OCSP:** OCSP que cumple con la RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"

1.3.5.2.2 ARQUITECTURA LÓGICA

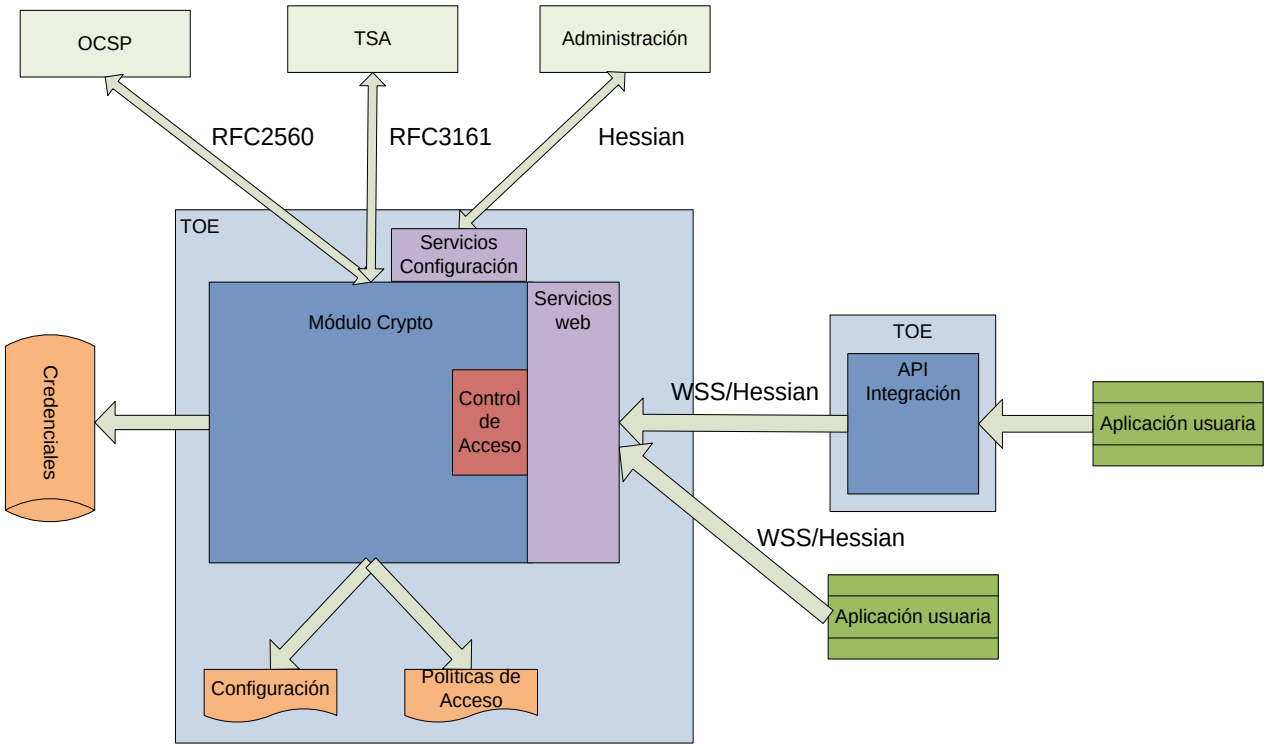

Ilustración 2: Arquitectura Lógica

El TOE está compuesto por los siguientes elementos:

- Módulo Crypto: Formado por los servicios web que ofrecen la funcionalidad del módulo, y el control de acceso que establece que usuarios tienen permisos para solicitar los servicios web.
- Ficheros de configuración: Estos ficheros de configuración son establecidos por un módulo de administración que queda fuera del TOE a través de los servicios de configuración del módulo Crypto.
- API de integración: Este API que será utilizado por el usuario desde la parte cliente se encarga de componer las llamadas a los servicios web del módulo Crypto, este API puede utilizar llamadas WSS o protocolo binario Hessian. Las aplicaciones podrán llamar directamente a los webservices WSS, para ello se dispone de la definición mediante el WSDL correspondiente a utilizar.

La arquitectura lógica del TOE a evaluar está compuesta de un único servidor donde se encontrará ubicado el módulo Crypto junto con la configuración establecida por el módulo de administración a través del servicio de configuración. Esta configuración consta de un conjunto de ficheros de configuración firmados por el módulo de administración, en estos ficheros se establecen todos los datos para el correcto funcionamiento de los servicios del módulo Crypto, usuarios, dominios, roles, incluyendo los datos necesarios para el acceso a las claves de operaciones funcionales que estarán almacenadas en el módulo criptográfico HSM y en keystores PKCS#12. Todas las contraseñas que se almacenan en la configuración son cifradas por el módulo de Administración mediante un algoritmo simétrico. Estas contraseñas se descifrarán por el TOE con la misma clave que es generada por la administración a través del mismo proceso de generación de la clave simétrica por parte del módulo de administración y del TOE, de manera que los dos módulos generan la misma clave simétrica para el cifrado y descifrado respectivamente.

La configuración también consta de las claves y certificados internos con las que se realizarán todas las operaciones criptográficas para asegurar la integridad y confidencialidad de la configuración del TOE. Las claves se almacenarán en keystores PKCS#12 que estarán físicamente junto con el módulo Crypto no pudiendo estas residir dentro de un módulo externo al TOE a diferencia de las claves de los usuarios para sus operaciones funcionales.

Por último, la configuración establecida determinará el control de acceso a los servicios del TOE mediante los ficheros de políticas de control de acceso, estos ficheros estarán firmados y cifrados por el TOE para proteger su integridad y confidencialidad.

El acceso de los usuarios al módulo Crypto se realizará desde una máquina cliente diferente al servidor a través de peticiones a los servicios web publicados, el acceso a los servicios se realizará a través del API de Integración, ya sea mediante WebServices o protocolo binario Hessian. Las llamadas a los webservices WSS podrán realizarse directamente sin utilizar el API de integración utilizando para ello la definición WSDL disponible públicamente. Las llamadas a los servicios mediante protocolo binario Hessian se deberán realizar a través del API de integración o directamente si se implementa el interfaz Hessian disponible.

De esta manera cuando los usuarios acceden a los servicios publicados por el módulo Crypto, este realiza las operaciones solicitadas de acuerdo a la configuración establecida. En el caso concreto del entorno de evaluación la configuración necesaria para los procesos de verificación o TimeStamp residirán tanto en la misma máquina como en un módulo externo TSA para emisión de sellos de tiempo y llamadas externas a un servidor OCSP de validación de certificados.

2. CONFORMIDAD

Se declara la conformidad del TOE con las Partes 2 y 3 de *Common Criteria for Information Technology Security Evaluation*, v3.1 (Revisión 3), Julio de 2009.

- Requisitos Funcionales de seguridad Parte 2 de Common Criteria v3.1 R3 extendida.
- Requisitos de Garantía de Seguridad Parte 3 de Common Criteria v3.1 R3 para el Nivel de Certificación **EAL 1+ALC_FLR.1**.

La metodología de evaluación es Common Methodology for Information Technology Security Evaluation CEM v3.1 R3.

3. OBJETIVOS DE SEGURIDAD

A continuación se describen los objetivos de seguridad.

3.1 Objetivos de seguridad para el entorno

Se establecen, a continuación, los objetivos de seguridad específicos para el entorno donde el TOE debe operar.

3.1.1 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.

3.1.2 Comunicaciones seguras

Las comunicaciones que se establecen a los servicios del TOE deben siempre realizarse a través de mecanismos seguros. La conexión desde los clientes al TOE deberá realizarse a través de una conexión http sobre SSL; 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.

3.1.3 Datos de autenticación

El entorno debe asegurar los distintos datos de autenticación de los usuarios y, en el caso de autenticación mediante certificados, éstos deberán ser emitidos por una fuente fiable y disponer de los procesos pertinentes para la renovación y verificación de los mismos.

4. DEFINICIÓN DE COMPONENTES EXTENDIDOS

A continuación se extiende la clase **Class FPT: Protection of the TSF** definida en Part 2: Security functional components de Common Criteria v3.1 R3 para adaptar de manera adecuada los requisitos funcionales de seguridad del TOE en lo referente a la protección de los datos necesarios para su correcto funcionamiento (ficheros de configuración).

Se justifica la extensión de la clase **FPT: Protection of the TSF**, ya que no existe componente que establezca la protección de los datos en cuanto a la importación de los mismos al TSF. De esta manera, se crea la familia **Confidentiality and integrity of imported TSF data (FPT_CII)** para la importación segura de los datos del TSF preservando su confidencialidad e integridad.

Se crea el componente **FPT_CII.1 Basic confidentiality and integrity of imported data** perteneciente a la familia FPT_CII que establece la protección necesaria de los datos durante el proceso de importación de los datos del TSF.

Confidentiality and integrity of imported TSF data (FPT_CII)

Family Behaviour

This family defines the rules for the protection from unauthorised disclosure and modification of TSF data imported. This data could, for example, be TSF critical data such as passwords, keys, audit data, or TSF executable code.

Component levelling

This family consists of only one component, FPT_CII.1 Basic confidentiality and integrity of imported data, addresses the protection from disclosure and the detection of modifications of the TSF data imported.

Management: FPT_CII.1

There are no management activities foreseen.

Audit: FPT_CII.1

There are no auditable events foreseen.

FPT_CII.1 Basic confidentiality and integrity of imported data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_CII.1.1 The TSF shall protect [*assignment: list of TSF data***] transmitted to the TSF from another trusted IT product from unauthorised disclosure.**

FPT_CII.1.2 The TSF shall provide the capability to detect modification of [*assignment: list of TSF data***] transmitted to the TSF from another trusted IT product within the following metric: [***assignment: a defined modification metric***].**

FPT_CII.1.3 The TSF shall provide the capability to verify the integrity of [*assignment: list of TSF data***] transmitted to the TSF from another trusted IT product and perform [***assignment: action to be taken***] if modifications are detected.**

User application notes

Operations

Assignment:

- In **FPT_CII.1.1, 2 & 3**, the PP/ST author shall specify the TSF data to be protected.
- In **FPT_CII.1.2**, the PP/ST should specify the modification metric that the detection mechanism must satisfy. For example, checking a hash code allocated to the TSF data.
- In **FPT_CII.1.3**, the PP/ST should specify the actions to be taken if a modification of TSF data has been detected.

5. REQUISITOS DE SEGURIDAD

5.1 Requisitos funcionales de seguridad

5.1.1 Objetos

Los requisitos funcionales de seguridad estarán enfocados en los siguientes objetos del TOE:

- **Ficheros de configuración**

  La configuración del TOE reside en varios ficheros donde se almacena la configuración. En ellos se almacenan los usuarios del sistema, roles, configuración de validaciones, contraseñas cifradas para el acceso a los almacenes criptográficos PKCS#12 o HSM, etc.

- **Ficheros de políticas de control de acceso**

  Los ficheros de políticas de control de acceso forman parte de los ficheros de configuración y establecen el proceso que se ejecutará a la hora de autenticar al usuario. Estos ficheros están basados en XACML donde se establece el control de acceso pertinente para determinar si la petición tiene la autorización necesaria.

- **Claves y certificados internos del TOE**

  Las claves y certificados internos del TOE son utilizados exclusivamente para las operaciones criptográficas de aseguramiento de la configuración del TOE, quedando claramente diferenciadas de las claves de operaciones funcionales del TOE. Estas claves internas residen en almacenes criptográfico PKCS#12 y se alojan en la misma máquina del TOE junto con los ficheros de configuración.

  Existen tres claves internas del TOE:

  - Certificado de la administración. Este certificado se utiliza para verificar que los ficheros de configuración están firmados por un módulo de administración confiable.
  - Clave asimétrica de cifrado/descifrado para la contraseña de autenticación.

Los usuarios/aplicaciones cuando realizan la autenticación mediante usuario y contraseña pueden enviar la contraseña cifrada. Cuando esto sucede, se debe utilizar por parte del cliente la clave pública para cifrar la contraseña y el TOE utilizará la clave privada para descifrar la contraseña y así poder verificar la autenticación.

- Clave asimétrica de cifrado/descifrado y firma de los ficheros de políticas de control de acceso.

  Estas claves son utilizadas por el TOE para firmar y cifrar los ficheros de políticas de control de acceso y así preservar la confidencialidad y privacidad de estos ficheros.

- **Servicios del TOE**

  Servicios a través de los cuales el TOE ofrece su funcionalidad de cifrado/descifrado, firma y validación de documentos.

5.1.2 Sujetos

Los sujetos relativos al TOE serán los usuarios/aplicaciones peticionarios de los servicios del TOE.

Los usuarios/aplicaciones utilizadores accederán a los servicios del TOE mediante peticiones a los servicios web publicados.

Los atributos de seguridad dependerán de si la petición se realiza mediante usuario y contraseña o mediante certificado:

- **Mediante usuario y contraseña:**

  Los atributos de seguridad son:

  El identificador del usuario y dominio al que pertenece el mismo. Si se omite el dominio en la petición, se asume que el usuario pertenece al dominio por defecto.

  Si se supera el nivel de autenticación entonces se identifica el rol asignado del usuario y con él se determina si posee la autorización necesaria para realizar la operación solicitada.

- **Mediante certificado:**

  Los atributos de seguridad son:

La firma utilizada en la petición y el dominio al que pertenece el usuario. Si se omite en la petición el dominio se asume que el usuario pertenece al dominio por defecto.

Si se supera el nivel de autenticación entonces se identifica el rol asignado del usuario y con él se determina si posee la autorización necesaria para realizar la operación solicitada.

5.1.3 Requisitos criptográficos

5.1.3.1 FCS_COP.1 Cryptographic operation descifrado simétrico de contraseñas

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1 Cryptographic key generation

FCS_COP.1.1 The TSF shall perform [assignment: descifrado de contraseñas almacenadas en el fichero de configuración] in accordance with a specified cryptographic key generation algorithm [assignment: 3DES] and specified cryptographic key sizes [assignment: 192 bits] that meet the following: [assignment: ninguno].

5.1.3.2 FCS_CKM.1 Cryptographic key generation descifrado simétrico de contraseñas

Hierarchical to: No other components.

Dependencies: 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: propietaria mediante la función rareGetBytes] and specified cryptographic key sizes [assignment: 192 bits] that meet the following: [assignment: ninguno].

5.1.3.3 FCS_COP.1 Cryptographic operation cifrado/descifrado políticas de control de acceso

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1 Cryptographic key generation

FCS_COP.1.1 The TSF shall perform [assignment: cifrado y descifrado de los ficheros de políticas de control de acceso] in accordance with a specified cryptographic algorithm [assignment: RSA] and cryptographic key sizes [assignment: 1024bits] that meet the following: [assignment: XML Encryption].

5.1.3.4 FCS_COP.1 Cryptographic operation firma/verificación políticas control de acceso

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1 Cryptographic key generation

FCS_COP.1.1 The TSF shall perform [assignment: firma y verificación electrónica del fichero de políticas de control de acceso] 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)].

5.1.3.5 FCS_CKM.1 Cryptographic key generation políticas control de acceso

Hierarchical to: No other components.

Dependencies: 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: RSA] and specified cryptographic key sizes [assignment: RSA 1024] that meet the following: [assignment: PKCS #1 - RSA Encryption Standard (RSA)].

5.1.3.6 FCS_COP.1 Cryptographic operation cifrado/descifrado datos de autenticación

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1 Cryptographic key generation

FCS_COP.1.1 The TSF shall perform [assignment: cifrado y descifrado de la contraseña de autenticación al servicio web] in accordance with a specified cryptographic algorithm [assignment: RSA] and cryptographic key sizes [assignment: 1024bits] that meet the following: [assignment: PKCS #1 - RSA Encryption Standard (RSA)].

NOTA: El requisito será ejercitado siempre dentro de la especificación de uso seguro del TOE que establece la obligación de cifrar la contraseña cuando se utilice el método de autenticación de usuario y contraseña.

5.1.3.7 FCS_COP.1 Cryptographic operation verificación firma respuestas servidores externas

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1 Cryptographic key generation

FCS_COP.1.1 The TSF shall perform [assignment: verificación de firma electrónica de las respuestas de servidores externos] in accordance with a specified cryptographic algorithm [assignment: RSA signature with SHA-1 y SHA-256 hashing] and cryptographic key sizes [assignment: RSA 512, 1024, 2048, SHA-1 y SHA-256] that meet the following: [assignment: PKCS #1 - RSA Encryption Standard (RSA)].

5.1.3.8 FCS_COP.1 Cryptographic operation verificación firma ficheros de configuración

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1 Cryptographic key generation

FCS_COP.1.1 The TSF shall perform [assignment: verificación de firma electrónica de los ficheros de configuración] 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)].

5.1.3.9 FCS_CKM.3 Cryptographic key access claves de configuración

Dependencies: 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] in accordance with a specified cryptographic key access method [assignment: PKCS#12] that meets the following: [assignment: PKCS#12].

NOTA: Estas claves son las utilizadas por el TOE para asegurar la integridad y la confidencialidad de los ficheros de configuración que se encuentran almacenadas en los keystores proporcionados en el momento de establecer la configuración del TOE.

5.1.4 Requisitos de control de acceso

5.1.4.1 FDP_ACC.2 Complete access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [assignment:CONTROL_ACCESO] on [assignment:

- Lista de objetos:
  - Servicios del TOE

- Lista de sujetos:
  - Usuarios de los servicios web

] 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.

5.1.4.2 FDP_ACF.1 Security attribute based access control

Dependencies: FDP_ACC.2 Complete access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [assignment:CONTROL_ACCESO] to objects based on the following: [assignment:

- Lista de objetos:
    - Servicios del TOE
- Atributos de Objetos:
    - El identificador de la operación del servicio. Este identificador se utilizará para una vez verificada la autenticación determinar si el usuario tiene los permisos para invocar a esta operación del servicio.

- Lista de sujetos:
    - Usuarios de los servicios web

      Atributos para invocación a un servicio web:

        • La identidad del usuario formada por nombre de usuario más dominio y la contraseña o el certificado con el que realizó la firma de la petición. En caso de no enviar dominio en la identificación, por defecto se asumirá que el dominio a utilizar es el marcado como dominio por defecto en la configuración.

        • Rol asignado al usuario/aplicación

].

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>
    - Llamada a un servicio web:

      Las reglas de acceso a través de los servicios web proporcionados por el TOE serán:

        - Que el identificador formado por nombre de usuario y dominio enviado en la petición exista dado de alta en la configuración o en caso de que la petición sea mediante certificado que un usuario del dominio especificado tenga asociado el mismo certificado utilizado en la firma de la petición. En caso de que no se envíe dominio se adoptará como dominio de la petición el dominio por defecto establecido en la configuración.

- Que el usuario tenga asociado un rol.
- Que el rol establezca permisos de ejecución para la operación solicitada.

A partir del rol recuperado se verificará si dispone del permiso necesario para realizar el servicio invocado especificado por el identificador de operación del servicio.

].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: ninguna adicional].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: ninguna adicional].

5.1.4.3 FIA_UID.2 User identification before any action

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.

5.1.4.4 FIA_UAU.2 User authentication before any action

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.

5.1.4.5 FIA_UAU.5 Multiple authentication mechanisms

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [assignment: Autenticación a los servicios web por nombre de usuario y contraseña o Autenticación por certificado] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment:

Los usuarios/aplicaciones que invocan a los servicios web del TOE pueden autenticarse tanto con usuario y contraseña como firmando la petición al servicio mediante un certificado. La utilización de los dos mecanismos vendrá dada únicamente por la decisión de los usuarios de utilizar uno u otro en función de sus preferencias. El único requisito es, que si se decide acceder a los servicios mediante certificado, en la configuración se deberá haber establecido al usuario el certificado con el cual se realizará la autenticación.

- Mediante nombre de usuario, domino y contraseña: el cliente envía, en la petición al servicio web, el nombre de usuario, el dominio al que pertenece y su contraseña asociada. Se comprueba que el nombre de usuario existe en el fichero de configuración en el dominio especificado y la contraseña coincide con la guardada en la configuración; en el caso de que se envíe la contraseña cifrada, previamente se realiza la operación de descifrado para poder comprobar la contraseña. En caso positivo, se recupera el rol asociado al usuario para verificar que posee los permisos necesarios para realizar la operación solicitada.

- Mediante certificado: para autenticarse mediante certificado al servicio web, el usuario en el dominio especificado debe tener asociado en la configuración el certificado con el cuál verificar la firma realizada. El proceso consiste en que: la petición al servicio web es firmada con la clave privada; una vez recibida la petición se verifica la firma y se recupera el certificado con el que se realizó la firma y se busca qué usuario tiene asignado dicho certificado en el dominio especificado, en caso de no enviar dominio en la petición se utilizará el dominio por defecto; en caso de encontrar un usuario con ese certificado, se autoriza el acceso, estableciendo el rol asociado al usuario y verificando que posee los permisos necesarios para realizar la operación solicitada].

5.1.5 Requisitos relativos a auditoría de eventos

5.1.5.1 FAU_GEN.1 Audit data generation actividad del TOE

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:

- Start-up and shutdown of the audit functions;
- All auditable events for the [not specified] level of audit; and [assignment: Actividad del TOE según la siguiente tabla:

DEBUG	Información en máximo detalle de la actividad del TOE. Se detalla toda la actividad del TOE además de los mensajes de Error.
INFO	Informa de aquellos mensajes que tengan cierto nivel de información de actividad además de los mensajes de Error.
WARN	Informa de aquellos mensajes que tengan un nivel de peligro en la actividad del TOE sin llegar a considerarse error, además de aquellos considerados como errores de actividad.
ERROR	Informa de aquellos mensajes del TOE considerados como error de actividad.
FATAL	Solamente se informará de aquellos mensajes de error críticos para la actividad del TOE.

  ].

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

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
  - For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: Descripción de la actividad del TOE].

5.1.5.2 FAU_GEN.1 Audit data generation operaciones de los servicios del TOE

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:

- Start-up and shutdown of the audit functions;
- All auditable events for the [not specified] level of audit; and [assignment: Operaciones de los servicios del TOE].

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

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
    - For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: Fecha, IP, usuario, operación, descripción del resultado de la operación].

5.1.6 Requisitos relativos a la protección del TOE

5.1.6.1 FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_CII.1.1 The TSF shall protect [assignment: Fichero en formato zip que contiene la configuración del TOE] transmitted to the TSF from another trusted IT product from unauthorised disclosure.

FPT_CII.1.2 The TSF shall provide the capability to detect modification of [assignment: Fichero en formato zip que contiene la configuración del TOE] transmitted to the TSF from another trusted IT product within the following metric: [assignment: RSA signature with SHA-1 hashing].

FPT_CII.1.3 The TSF shall provide the capability to verify the integrity of [assignment: Fichero en formato zip que contiene la configuración del TOE] transmitted to the TSF from another trusted IT product and perform [assignment: El TOE rechaza los datos enviados y permanence con los ficheros de configuración previos] if modifications are detected.

5.1.7 Razonamiento de dependencias

A continuación se enumeran aquellas dependencias de requisitos que no se cumplen y su razonamiento.

- En el requisito ***FCS_COP.1 Cryptographic operation descifrado simétrico de contraseñas*** no se cumple con la dependencia de destrucción de clave ***FCS_FKM.4.*** 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 el requisito ***FCS_COP.1 Cryptographic operation cifrado/descifrado políticas de control de acceso*** no se cumple la dependencia de destrucción de clave FCS_CKM.4. Estas claves no son destruidas explícitamente por el TOE si no a través de un proceso manual por el cual, cuando ya no son necesarias se eliminan físicamente todos los ficheros de configuración del TOE, incluidos los keystores que almacenan las claves.

- En el requisito ***FCS_COP.1 Cryptographic operation firma/verificación políticas control de acceso*** no se cumple la dependencia de destrucción de clave FCS_CKM.4. Estas claves no son destruidas explícitamente por el TOE si no a través de un proceso manual por el cual, cuando ya no son necesarias se eliminan físicamente todos los ficheros de configuración del TOE, incluidos los keystores que almacenan las claves.

- En el requisito ***FCS_COP.1 Cryptographic operation cifrado/descifrado datos de autenticación*** no se cumplen con la dependencias de generación, ni de destrucción de claves FMT_CKM.1 y FCS_CKM.4 ya que las claves no son generadas por el TOE. Estas claves son parte de los ficheros de configuración que se establecen en el TOE a través del requisito *FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración.* Las claves son eliminadas con un proceso manual mediante un borrado físico de todos los ficheros de configuración del TOE, incluidos los keystores que almacenan las claves.

- En el requisito ***FCS_COP.1 Cryptographic operation verificación firma respuestas servidores externas*** no se cumplen con las dependencias de generación, ni de destrucción de claves FMT_CKM.1 y FCS_CKM.4 ya que las claves no son generadas por el TOE. Estas claves son parte de los ficheros de configuración que se establecen en el TOE a través del requisito *FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración.* Las claves son eliminadas con un proceso manual mediante un borrado físico de todos los ficheros de configuración del TOE, incluidos los keystores que almacenan las claves.

- En el requisito ***FCS_COP.1 Cryptographic operation verificación firma ficheros de configuración*** no se cumplen con las dependencias de generación, ni de destrucción de claves FMT_CKM.1 y FCS_CKM.4 ya que las claves no son generadas por el TOE. Estas claves son parte de los ficheros de configuración que se establecen en el TOE a través del requisito *FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración.* Las claves son eliminadas con un proceso manual mediante un borrado físico de todos los ficheros de configuración del TOE, incluidos los keystores que almacenan las claves.

- En el requisito ***FCS_CKM.1 Cryptographic key generation descifrado simétrico de contraseñas*** no se cumple la dependencia de destrucción de claves FCS_CKM.4. 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 el requisito ***FCS_CKM.1 Cryptographic key generation políticas control de acceso*** no se cumple la dependencia de destrucción de claves FCS_CKM.4. Estas claves no son destruidas explícitamente por el TOE si no a través de un proceso manual por el cual, cuando ya no son necesarias se eliminan físicamente todos los ficheros de configuración del TOE, incluidos los keystores que almacenan las claves.

- En el requisito ***FCS_CKM.3 Cryptographic key access*** no se cumple la dependencia de destrucción de claves FCS_CKM.4. Estas claves no son destruidas explícitamente por el TOE si no a través de un proceso manual por el cual, cuando ya no son necesarias se eliminan físicamente todos los ficheros de configuración del TOE, incluidos los keystores que almacenan las claves.

- En el requisito **FDP_ACF.1 Security attribute based access control** no se cumple la dependencia con FMT_MSA.3, puesto que la gestión de los atributos de seguridad no se encuentran dentro del ámbito del TOE, al quedar fuera de él la consola de administración.

- En los requisitos **FAU_GEN.1** no se cumple la dependencia con FPT_STM.1, ya que no es una funcionalidad de seguridad del TOE asegurar la fecha y hora reflejada en los ficheros de auditoría.

5.2 Requisitos de garantía

5.2.1 Security Target evaluation

5.2.1.1 ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

- **ASE_INT.1.1D** The developer shall provide an ST introduction.

Content and presentation elements:

- **ASE_INT.1.1C** The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
- **ASE_INT.1.2C** The ST reference shall uniquely identify the ST.
- **ASE_INT.1.3C** The TOE reference shall identify the TOE.

- **ASE_INT.1.4C** The TOE overview shall summarize the usage and major security features of the TOE.
- **ASE_INT.1.5C** The TOE overview shall identify the TOE type.
- **ASE_INT.1.6C** The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
- **ASE_INT.1.7C** The TOE description shall describe the physical scope of the TOE.
- **ASE_INT.1.8C** The TOE description shall describe the logical scope of the TOE.

5.2.1.2 ASE_CCL.1 Conformance claims

Dependencies: **ASE_INT.1** ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements:

- **ASE_CCL.1.1D** The developer shall provide a conformance claim.
- **ASE_CCL.1.2D** The developer shall provide a conformance claim rationale.

Content and presentation elements:

- **ASE_CCL.1.1C** The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
- **ASE_CCL.1.2C** The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
- **ASE_CCL.1.3C** The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
- **ASE_CCL.1.4C** The CC conformance claim shall be consistent with the extended components definition.
- **ASE_CCL.1.5C** The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
- **ASE_CCL.1.6C** The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
- **ASE_CCL.1.7C** The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

- **ASE_CCL.1.8C** The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
- **ASE_CCL.1.9C** The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
- **ASE_CCL.1.10C** The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

5.2.1.3 ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

- **ASE_ECD.1.1D** The developer shall provide a statement of security requirements.
- **ASE_ECD.1.2D** The developer shall provide an extended components definition.

Content and presentation elements:

- **ASE_ECD.1.1C** The statement of security requirements shall identify all extended security requirements.
- **ASE_ECD.1.2C** The extended components definition shall define an extended component for each extended security requirement.
- **ASE_ECD.1.3C** The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
- **ASE_ECD.1.4C** The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
- **ASE_ECD.1.5C** The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

5.2.1.4 ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies.

Developer action elements:

- **ASE_OBJ.1.1D** The developer shall provide a statement of security objectives.

Content and presentation elements:

- **ASE_OBJ.1.1C** The statement of security objectives shall describe the security objectives for the operational environment.

5.2.1.5 ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements:

- **ASE_REQ.1.1D** The developer shall provide a statement of security requirements.
- **ASE_REQ.1.2D** The developer shall provide security requirements rationale.

Content and presentation elements:

- **ASE_REQ.1.1C** The statement of security requirements shall describe the SFRs and the SARs.
- **ASE_REQ.1.2C** All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
- **ASE_REQ.1.3C** The statement of security requirements shall identify all operations on the security requirements.
- **ASE_REQ.1.4C** All operations shall be performed correctly.
- **ASE_REQ.1.5C** Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
- **ASE_REQ.1.6C** The statement of security requirements shall be internally consistent.

5.2.1.6 ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements:

- **ASE_TSS.1.1D** The developer shall provide a TOE summary specification.

Content and presentation elements:

- **ASE_TSS.1.1C** The TOE summary specification shall describe how the TOE meets each SFR.

5.2.2 Development

5.2.2.1 ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements:

- **ADV_FSP.1.1D** The developer shall provide a functional specification.
- **ADV_FSP.1.2D** The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

- **ADV_FSP.1.1C** The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
- **ADV_FSP.1.2C** The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
- **ADV_FSP.1.3C** The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.
- **ADV_FSP.1.4C** The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

5.2.3 Guidance documents

5.2.3.1 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

- **AGD_OPE.1.1D** The developer shall provide operational user guidance.

Content and presentation elements:

- **AGD_OPE.1.1C** The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
- **AGD_OPE.1.2C** The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
- **AGD_OPE.1.3C** The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
- **AGD_OPE.1.4C** The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
- **AGD_OPE.1.5C** The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
- **AGD_OPE.1.6C** The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
- **AGD_OPE.1.7C** The operational user guidance shall be clear and reasonable.

5.2.3.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

- **AGD_PRE.1.1D** The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

- **AGD_PRE.1.1C** The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

- **AGD_PRE.1.2C** The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

5.2.4 Life-cycle support

5.2.4.1 ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage Objectives

Developer action elements:

- **ALC_CMC.1.1D** The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

- **ALC_CMC.1.1C** The TOE shall be labelled with its unique reference.

5.2.4.2 ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies. Objectives

Developer action elements:

- **ALC_CMS.1.1D** The developer shall provide a configuration list for the TOE.

Content and presentation elements:

- **ALC_CMS.1.1C** The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
- **ALC_CMS.1.2C** The configuration list shall uniquely identify the configuration items.

5.2.4.3 ALC_FLR.1 Basic flaw remediation

Dependencies: No dependencies.

Developer action elements:

- **ALC_FLR.1.1D** The developer shall document and provide flaw remediation procedures addressed to TOE developers.

Content and presentation elements:

- **ALC_FLR.1.1C** The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
- **ALC_FLR.1.2C** The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
- **ALC_FLR.1.3C** The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
- **ALC_FLR.1.4C** The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements:

- **ALC_FLR.1.1E** The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Test

5.2.5.1 ATE_IND.1 Independent testing - conformance

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures Objectives

Developer action elements:

- **ATE_IND.1.1D** The developer shall provide the TOE for testing.

Content and presentation elements:

- **ATE_IND.1.1C** The TOE shall be suitable for testing.

5.2.6 Vulnerability assessment

5.2.6.1 AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures Objectives

Developer action elements:

- **AVA_VAN.1.1D** The developer shall provide the TOE for testing.

Content and presentation elements:

- **AVA_VAN.1.1C** The TOE shall be suitable for testing.

5.2.7 Razonamiento requisitos de garantía

Los requisitos de garantía son los necesarios para un nivel de evaluación EAL1+ALC_FLR.1.

Para cumplir con este nivel de evaluación, se proporciona la declaración de seguridad y la documentación del producto, junto con el TOE, para su evaluación y testeo.

6. ESPECIFICACIÓN RESUMIDA DEL TOE

A continuación, se detalla como el TOE implementa los requisitos funcionales anteriormente especificados.

6.1 Protección del TOE

6.1.1 FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración

El TOE recibe los ficheros de configuración desde un módulo de administración. Este módulo de administración se encarga de crear los ficheros de configuración y se los transmite al TOE a través del servicio de configuración que el TOE dispone para este fin. El TOE establece los elementos de protección necesarios para recibir los datos de configuración y comprobar que los datos provienen de una fuente confiable y que los datos no han sido modificados.

Todos estos ficheros que conforman la configuración, se establecen a través de los servicios de configuración del TOE. Los servicios de configuración establecen tres operaciones:

- **Activación del TOE**: Una vez instalado el TOE en la máquina física, desde el módulo de administración se debe activar el módulo a través del servicio de configuración. En esta fase se crean las claves criptográficas del TOE que utilizará posteriormente para cifrar y firmar los ficheros de políticas de control de acceso que recibirá cuando se establezcan los ficheros de configuración. En caso de que no se haya establecido manualmente el certificado de confianza del módulo de administración, se asumirá el certificado que se envía en la firma de solicitud de activación. A partir de ese momento, el TOE verificará todas las peticiones que lleguen al servicio de configuración mediante el certificado de confianza establecido. Como respuesta a la activación, el TOE envía la clave pública al módulo de administración para que este a su vez cifre los datos de configuración para el TOE.

- **Establecimiento de la configuración en el TOE**: Una vez activado el TOE, el módulo de administración podrá enviar la configuración al TOE. Los ficheros que conforman la configuración se envían empaquetados en un fichero con formato zip y este es firmado por el módulo de administración y cifrado para el TOE. El TOE al recibir los datos verificará que están firmados por una fuente de administración confiable y los descifrará con su clave privada, ya que el módulo de administración los envía cifrados para el TOE con la clave pública que recuperó en el paso de activación.

- **Desactivación del TOE:** Desde el módulo de administración se puede desactivar el TOE, de manera que cuando se recibe la operación de desactivación y previa verificación de que la solicitud proviene de una fuente de administración confiable, elimina físicamente el certificado de la administración y el módulo de administración elimina la clave pública del TOE. Posteriormente, desde el módulo de administración podrá volverse a activar el módulo si se desea.

Los ficheros que conforman la configuración del TOE que son enviados a través del servicio de configuración del TOE son los siguientes:

- Ficheros que contienen la configuración general del TOE.
    - **Fichero de configuración** firmado por el módulo de administración donde se almacena la lista de dominios del sistema.
    - **Almacén criptográfico** donde se almacena la clave para el descifrado de la contraseña de autenticación de los usuarios/aplicaciones que se autentican a los servicios web cifrando la contraseña.
    - **Ficheros de políticas de control de acceso**. Estos ficheros basados en XACML contienen las reglas que se deben cumplir para que una petición sea autorizada.

- Ficheros que contienen la configuración por cada uno de los dominios definidos. Por cada dominio definido en el sistema se guarda la siguiente información:

- **Fichero de configuración** firmado por el módulo de administración donde se almacenan los usuarios del dominio, sus contraseñas cifradas y referencias a sus certificados de autenticación. Así como, los roles y credenciales asociadas a cada uno de los roles y demás configuración asociada a la funcionalidad del TOE.

  Las credenciales asociadas a un determinado rol contienen los datos necesarios para acceder a las claves de operaciones funcionales que serán utilizadas cuando un usuario invoca una determinada operación a través de un servicio web. En el caso de que la clave se almacene en un fichero PKCS#12, este fichero será enviado por el módulo de administración junto con el resto de ficheros de la configuración, estando por tanto, físicamente en la misma máquina que el TOE. Todas las contraseñas utilizadas para el acceso a los almacenes criptográficos, ya sean PKCS#12 o HSM, están cifradas en el fichero por el módulo de administración.
- Almacén criptográfico donde se almacenan los **certificados de autenticación de los usuarios**. Los certificados (clave pública) con los que los usuarios se podrán autenticar contra los servicios web se almacenan en un keystore PKCS#12.
- **Almacenes PKCS#12 de claves privadas de usuarios**. Como anteriormente se mencionó, las claves privadas utilizadas por los usuarios para realizar las operaciones criptográficas funcionales del TOE en el caso de que estén almacenadas en keystores del tipo PKCS#12, residirán físicamente en la misma máquina que el TOE, por lo tanto estos ficheros serán parte de los ficheros de configuración que serán enviados por el módulo de administración al TOE.

Los ficheros que completan la configuración, junto con los ficheros descritos anteriormente que son enviados desde el módulo de administración son:

- **Almacén criptográfico** donde se almacenan las **claves internas del TOE** que se utilizan para la protección de los ficheros de políticas de control de acceso. Estas claves son generadas por el propio TOE en el momento que desde el módulo de administración se procede a activar el módulo. Hasta el momento de la activación, el TOE no posee ningún fichero de configuración y no es posible operar con él, solamente después de la activación y del envío de la configuración, el TOE quedará en situación de ser operativo.

- **Certificado de la administración** con el que se verificará que los datos que se reciben a través del servicio de configuración provienen de un módulo de administración confiable, y que aquellos ficheros de configuración firmados por el módulo de administración no han sido alterados de forma anómala. Este certificado puede ser establecido manualmente previamente a la activación del TOE, o se recuperará en el momento de la activación del TOE, de manera que si no se ha establecido manualmente ningún certificado de administración confiable se aceptará como certificado confiable el que viene en la firma de solicitud de activación del TOE.

6.2 Control de Acceso

6.2.1 FDP_ACC.2 Complete access control

A través del control de acceso se asegura que solamente aquellos usuarios con los permisos necesarios acceden a los servicios del TOE.

El control de acceso se basa en la configuración del TOE para determinar el proceso de autenticación y de autorización.

El control de acceso determina la autenticación y la autorización basándose en los siguientes ficheros de configuración:

- Ficheros de políticas de control de acceso. Establecen los procesos a ejecutar para realizar la autenticación y la autorización.
- Ficheros de configuración de cada uno de los dominios. Contienen la lista de usuarios, contraseñas y roles de cada uno de los dominios.

6.2.2 FDP_ACF.1 Security attribute based access control

La implementación de las reglas que definen el control de acceso a los sujetos cuando invocan a los servicios del TOE se define de la siguiente manera:

Al recibir una petición a uno de sus servicios web, se comprueba en los ficheros de políticas de control de acceso cual es el proceso que se debe ejecutar para realizar la primera fase que es la autenticación del usuario, este proceso será diferente si la autenticación se realiza mediante usuario y contraseña, o si se realiza mediante certificado.

- **Autenticación mediante usuario y contraseña**: una vez que el control de acceso determina que la autenticación se realiza mediante usuario y contraseña, se comprueba si el identificador de usuario compuesto por nombre de usuario y dominio existe en el fichero de configuración del dominio mencionado, este dominio puede establecerse en la misma petición o se asumirá el dominio por defecto en su omisión.
  En caso de existir el usuario en el dominio especificado, se comprueba que la contraseña enviada coincide con la almacenada en el fichero de configuración. Para realizar esta comprobación, se realiza el descifrado de la contraseña almacenada según el requisito *FCS_COP.1 Cryptographic operation descifrado simétrico de contraseñas,* de esta manera se comprueba si la contraseña del usuario coincide con la enviada.
  Si la comprobación se realiza correctamente, se recupera el rol asociado al usuario; esto querrá decir que se tiene acceso al servicio y ahora se comprueba que se tiene la autorización necesaria para realizar la operación solicitada.
  Para comprobar que se tiene autorización para realizar la operación solicitada se comprueba que la política de acceso del rol recuperado posee permisos para la operación solicitada.

- **Autenticación mediante certificado**: una vez que el control de acceso determina que la autenticación se realiza mediante certificado, se verifica que la firma enviada es correcta y se comprueba si existe un usuario en el dominio especificado que tenga configurado el mismo certificado utilizado para realizar la firma de la solicitud, el dominio puede enviarse en la petición o en su omisión se asumirá el dominio por defecto.

Si existe un usuario con el mismo certificado, se recupera el rol asociado al usuario; esto querrá decir que se tiene acceso al servicio y ahora se comprueba que se tiene la autorización necesaria para realizar la operación solicitada.

Para comprobar que se tiene autorización para realizar la operación solicitada se comprueba que la política de acceso del rol recuperado posee permisos para la operación solicitada.

6.2.3 FIA_UID.2 User identification before any action

Los usuarios del TOE accederán a los servicios publicados por el TOE y deberán identificarse antes de poder realizar cualquier operación. Esta identificación puede ser mediante usuario y contraseña o firmando la petición mediante un certificado digital.

6.2.4 FIA_UAU.2 User authentication before any action

Los usuarios, una vez identificados, serán autenticados tal y como se define en el requisito FIA_UAU.5, mediante usuario y contraseña o mediante certificado. En cualquier caso, todas las peticiones a los servicios deberán pasar el proceso de autenticación antes de poder realizar cualquier operación.

6.2.5 FIA_UAU.5 Multiple authentication mechanisms

Los usuarios podrán autenticarse mediante dos métodos, usuario y contraseña o certificado digital. No existe ninguna limitación en cuanto al uso de un método u otro, los usuarios peticionarios del servicio podrán utilizar cualquiera de los dos métodos indistintamente según su preferencia. El único requisito existente es que se haya configurado el certificado con el que el usuario se autenticará.

- **Usuario y Contraseña**:

  Mediante usuario y contraseña los usuarios envían en la petición el nombre del usuario y la contraseña que previamente se ha configurado. En primer lugar, se determina si el usuario existe y, posteriormente, se compara la contraseña enviada con la contraseña que se encuentra cifrada en el fichero de configuración, asociada con su nombre de usuario. En caso de que el resultado sea positivo se le asocia el rol del usuario, para determinar el nivel de permisos del usuario.

- **Certificado**:

  La autenticación mediante certificado se realiza firmando la petición al servicio; de esta manera, se verifica que la firma de la petición es correcta y se procede a buscar un usuario que tenga asociado el certificado con el que se firmó la petición. Si se encuentra un usuario con el mismo certificado con el que se firmó la petición, se establece su rol para determinar el nivel de permisos del usuario.

6.3 Operaciones Criptográficas

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:

6.3.1 Descifrado simétrico de contraseñas

Las operaciones criptográficas para el descifrado de contraseñas almacenadas en los ficheros de configuración se componen de:

- **FCS_COP.1 Cryptographic operation descifrado simétrico de contraseñas**

  Las contraseñas de los usuarios y las contraseñas de acceso a los almacenes de claves, se guardan cifradas utilizando un algoritmo simétrico 3DES (192 bits).

  Esta operación se realiza tanto en la fase de autenticación del usuario para comprobar que la contraseña enviada por el usuario coincide con la almacenada en el fichero de configuración, como cuando se requiere acceder a las claves de usuarios almacenadas en los almacenes criptográficos, ya sean PKCS#12 o módulo criptográfico HSM para descifrar las contraseñas de acceso.

- **FCS_CKM.1 Cryptographic key generation descifrado simétrico de contraseñas**

Las contraseñas almacenadas en los ficheros de configuración son cifradas por el módulo de administración mediante una clave simétrica. Estas contraseñas se descifran por el TOE generando la misma clave a través de un proceso de generación a partir de una clave común incluida en el código, un identificador único que identifica la contraseña en la configuración y un 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. Con ella se realizan las operaciones de descifrado de las contraseñas.

6.3.2 Cifrado, Descifrado y Verificación políticas de control de acceso

Las operaciones criptográficas para el cifrado, descifrado y verificación de los ficheros de políticas de control de acceso son:

- **FCS_COP.1 Cryptographic operation cifrado/descifrado políticas de control de acceso**

  Los ficheros de políticas de control de acceso determinan los procesos a ejecutar y las reglas para determinar el acceso a los servicios del TOE. Estos ficheros forman parte de los ficheros de configuración que se importan desde el módulo de administración. En el proceso de importación a través del requisito *FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración* cuando el TOE recibe los ficheros de la configuración, antes de almacenarlos físicamente se cifran mediante un algoritmo XMLEncryption para proteger su confidencialidad.

  Una vez que el TOE ha cifrado y almacenado físicamente los ficheros, en el proceso de arranque del TOE se realiza la operación de descifrado para poder realizar la carga de la configuración. Este proceso de descifrado se realiza en memoria y no se vuelven a almacenar físicamente los ficheros descifrados.

- **FCS_COP.1 Cryptographic operation firma/verificación políticas control de acceso**

Los ficheros de políticas de control de acceso además de cifrarse para preservar su confidencialidad se firman para asegurar su integridad. De esta manera, una vez que se reciben los ficheros desde el módulo de administración, son firmados antes de ser guardados físicamente. En el proceso de carga de la configuración son verificados para comprobar si han sido alterados. En caso de que se detecte que han sido alterados y no se verifique correctamente la firma, se denegará la carga de la configuración quedando el TOE sin prestar servicio.

- **FCS_CKM.1 Cryptographic key generation políticas de control de acceso**

  Las claves utilizadas para el cifrado y descifrado de los ficheros de políticas de control de acceso son generadas por el TOE en el proceso de su activación desde el módulo de administración. En este momento, el TOE genera el par de claves que almacena en un keystore y se guarda físicamente en el misma máquina.

6.3.2.1 Cifrado/descifrado datos de autenticación

Las operaciones criptográficas para el cifrado, descifrado de los datos de autenticación de los usuarios/aplicaciones en los servicios web son:

- **FCS_COP.1 Cryptographic operation cifrado/descifrado datos de autenticación**

  Existe la posibilidad de que en el proceso de autenticación de una petición a los servicios web del TOE el usuario envíe la contraseña cifrada. Bajo la especificación de utilización segura del TOE este proceso es obligatorio, por lo que, el usuario que realiza la llamada al servicio web debe cifrar la contraseña con la clave pública de la clave utilizada para este cometido y cuando la petición llega al servidor el TOE la descifra con la clave privada.

  Las claves utilizadas en estas operaciones son generadas por el módulo de administración y forman parte de los ficheros de configuración que se importan al TOE. En el proceso de importación a través del requisito *FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración* como parte de los ficheros de configuración importados, se recibe el keystore donde se encuentran las claves que se utilizarán para descifrar los datos de autenticación.

En el caso del API de Integración, la clave pública se establecerá manualmente configurando su localización en el fichero de propiedades. Entonces, se utilizará esta clave para cifrar los datos que enviará en la petición como parte de los datos de autenticación.

6.3.2.2 Verificación firma ficheros de configuración

Las operaciones criptográficas para la verificación de la firma de los ficheros de configuración son:

- **FCS_COP.1 Cryptographic operation verificación firma ficheros de configuración**

  La configuración del TOE está compuesta básicamente, por almacenes criptográficos donde se guardan las claves del TOE y ficheros que contienen la configuración funcional del TOE, entre ellos están los ficheros xml de configuración. En ellos se almacena la configuración lógica del TOE en cuanto a usuarios, contraseñas, roles, credenciales, políticas de validación, etc. La integridad de estos ficheros se mantiene al ser firmados por el módulo de administración que es el encargado de generar estos ficheros y enviárselos al TOE. El TOE en el proceso de carga de la configuración verifica su integridad comprobando que no han sido alterados.

  La administración firma con su clave privada los ficheros de configuración y el TOE verifica su integridad con el certificado de la administración. Este certificado o bien se establece en el momento de la instalación del TOE o bien es parte del proceso de importación de la configuración en el momento de la activación del TOE desde el módulo de administración a través del requisito *FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración.*

6.3.2.3 Verificación firma respuestas servidores externas

- **FCS_COP.1 Cryptographic operation verificación firma respuestas servidores externas**

  Las firmas de las respuestas emitidas por servidores externos al TOE, como servidores de sellos de tiempo o servidores de servicios de validación de certificados, son verificadas según dictamine la firma en cuanto al algoritmo y tamaño de clave establecido.

Los certificados utilizados para verificar la firma de las respuestas forman parte de los ficheros de configuración importados a través del requisito *FPT_CII.1 Basic confidentiality and integrity of imported data Ficheros de configuración.*

6.3.2.4 Acceso Claves de configuración

- **FCS_CKM.3 Cryptographic key access**

  El acceso a las claves para las operaciones criptográficas anteriormente descritas se realiza de la siguiente manera:

  - 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. Estas contraseñas se han cifrado desde el módulo de administración y son descifradas según establece el requisito *FCS_COP.1 Cryptographic operation descifrado simétrico de contraseñas.*
  - Las claves privadas se encuentran en almacenes criptográficos y su acceso y uso se realiza según establece el estándar PKCS#12.
  - Las claves públicas se encuentran en formato X509 v3.

6.4 Ficheros de auditoría

6.4.1 FAU_GEN.1 Audit data generation actividad del TOE

El TOE genera logs de actividad donde se refleja el funcionamiento del TOE. A través de estos ficheros de actividad se podrá determinar el correcto funcionamiento del TOE. Existe la posibilidad de configurar el grado de información que se escribirá en los ficheros de actividad pudiendo obtener más o menos información a partir de la siguiente tabla de configuración:

DEBUG	Información en máximo detalle de la actividad del TOE. Se detalla toda la actividad del TOE además de los mensajes de Error.
INFO	Informa de aquellos mensajes que tengan cierto nivel de información de actividad además de los mensajes de Error.
WARN	Informa de aquellos mensajes que tengan un nivel de peligro en la actividad del TOE

	sin llegar a considerarse error, además de aquellos considerados como errores de actividad.
ERROR	Informa de aquellos mensajes del TOE considerados como error de actividad.
FATAL	Solamente se informará de aquellos mensajes de error críticos para la actividad del TOE.

Tabla 1: Nivel de actividad

6.4.2 FAU_GEN.1 Audit data generation operaciones de los servicios del TOE

El TOE genera ficheros donde se reflejan las operaciones de sus servicios. En estos ficheros se observarán las operaciones realizadas por los usuarios a través de los servicios del TOE así como las operaciones realizadas a través de los servicios de configuración desde el módulo de administración.

Por cada operación realizada se reflejará una entrada en el fichero donde quedará constancia de la operación realizada, fecha de operación, usuario, IP y resultado de la operación.