TBS_ASFv4.1_Declaración_de_Seguridad_20080128_v1.9

Revisión:

v 1.9

Fecha última versión:

Enero de 2008

HOJA DE CONTROL DOCUMENTAL

Nombre del Documento	TBS_ASFv4.1_Declaración_de_Seguridad_20080128_v1.9		
Resumen	Declaración de Seguridad para Advanced Signature Framework v4.1.5		
Autor:	María Peleato/Óscar Flor	**Fecha Versión**	28/01/2008
Revisado por:	Óscar Flor/Miguel Ángel Sarasa	**Fecha :**	28/01/2008
Aprobado por:	Óscar Flor	**Fecha :**	28/01/2008
Anexos:	N/A	**Nº de páginas:**	96

CONTROL DE VERSIONES

Versión	Fecha	Realizado por	Descripción
1.0	23/02/2007	Óscar Flor	Primera versión
1.1	28/06/2007	Óscar Flor	Versión revisada I
1.2	02/07/2007	Óscar Flor	Versión revisada II
1.3	16/07/2007	Óscar Flor	Versión revisada III
1.4	14/09/2007	Óscar Flor	Versión revisada IV
1.5	26/10/2007	Óscar Flor	Versión revisada V
1.6	07/12/2007	Óscar Flor	Versión revisada VI
1.7	14/12/2007	Óscar Flor	Versión revisada VII
1.8	21/01/2008	Óscar Flor	Versión revisada VIII
1.9	28/01/2008	Óscar Flor	Versión final

Contenido

1_ Introducción 10
1.1_ Identificación 10
1.2_ Glosario 10
1.3_ Referencias 12
1.4_ TOE overview 12
1.5_ Descripción del TOE 13
1.6_ Configuración evaluada 19
1.6.1_ Componentes del TOE 20
1.6.2_ Arquitectura lógica 20
1.6.3_ Arquitectura física 22
1.6.4_ Requisitos de la configuración evaluada 24
2_ Conformidad 26
3_ Definición del problema de seguridad del TOE 27
3.1_ Activos a proteger 27
3.1.1_ Activo 01: Claves privadas 28
3.1.2_ Activo 02: Acceso a contraseñas almacenadas en base de datos 28
3.1.3_ Activo 03: Claves secretas generadas para el cifrado simétrico 28
3.1.4_ Activo 04: Integridad de los archivos de auditoría 28
3.1.5_ Activo 05: Respuestas del TOE a peticiones de aplicaciones cliente a webservices 29
3.1.6_ Activo 06: Servicio TOE 29
3.1.7_ Activo 07: Peticiones del TOE a OCSPs y TSAs externos 29
3.1.8_ Activo 08: Respuestas de entidades externas al TOE 29
3.2_ Amenazas 29
3.2.1_ Amenaza 01: Obtención de las claves privadas 30
3.2.2_ Amenaza 02: Uso no autorizado de las claves privadas 30
3.2.3_ Amenaza 03: Lectura de contraseñas almacenadas en base datos 30
3.2.4_ Amenaza 04: Obtención de la clave secreta 31
3.2.5_ Amenaza 05: Violación de la integridad de los archivos de auditoria 31
3.2.6_ Amenaza 06: Suplantación de identidad en las respuestas de los webservices 31
3.2.7_ Amenaza 07: Modificación de las respuestas de los webservices 31

3.2.8_ Amenaza 08: Violación del Servicio TOE 31
3.2.9_ Amenaza 09: Uso no autorizado del Servicio TOE 31
3.2.10_ Amenaza 10: Integridad de peticiones realizadas a OCSPs y TSAs 32
3.2.11_ Amenaza 11: Integridad de respuestas de entidades externas al TOE 32
3.3_ Mapeo de activos y amenazas 32
3.4_ Políticas de seguridad organizacional 33
3.4.1_ Política 01: Documentación guía de instalación y uso 33
3.4.2_ Política 02: Aplicación de procedimientos por administrador TOE 33
3.4.3_ Política 03: Revisión de auditorías 34
3.4.4_ Política 04: Cualificación de los usuarios del TOE 34
3.4.5_ Política 05: Disposición de datos de usuario y privilegios de acceso ... 34
3.4.6_ Política 06: Restricción de acceso al TOE 35
3.4.7_ Política 07: Seguimiento de política de seguridad 35
3.5_ Hipótesis de uso seguro 35
3.5.1_ Hipótesis 01: Administrador del sistema confiable 35
3.5.2_ Hipótesis 02: Administrador de la auditoría 36
3.5.3_ Hipótesis 03: Administrador de la base de datos 36
3.5.4_ Hipótesis 04: Usuarios del TOE responsables 36
3.5.5_ Hipótesis 05: Datos de usuario 36
4_ Objetivos de seguridad 37
4.1_ Objetivos de seguridad para el TOE 37
4.1.1_ Objetivo 01: Confidencialidad de claves privadas de certificados 37
4.1.2_ Objetivo 02: Confidencialidad de contraseñas almacenadas en BD 37
4.1.3_ Objetivo 03: Cifrado de clave secreta para cifrado simétrico 37
4.1.4_ Objetivo 04: Registro de las peticiones realizadas 38
4.1.5_ Objetivo 05: Firma y verificación de las respuestas de los webservices 38
4.1.6_ Objetivo 06: Control de acceso 38
4.1.7_ Objetivo 07: Detección de modificaciones de archivos de auditoría 38
4.1.8_ Objetivo 08: Firma de peticiones a TSAs y OCSPs externos 38
4.1.9_ Objetivo 09: Verificar firma de respuestas de entidades externas 38
4.2_ Objetivos de seguridad para el entorno 39
4.2.1_ Objetivo entorno 01: Acceso restringido 39
4.2.2_ Objetivo entorno 02: Formación 39
4.2.3_ Objetivo entorno 03: Proporcionar todos los entregables necesarios... 39

4.2.4_ Objetivo entorno 04: Revisión de auditorías 39
4.2.5_ Objetivo entorno 05: Formación en política de seguridad 39
4.2.6_ Objetivo entorno 06: Gestión de los datos de autenticación 40
4.3_ Razonamiento de objetivos de seguridad 40
5_ Requisitos de seguridad 49
5.1_ Requisitos funcionales de seguridad 49
5.1.1_ Relación de objetos 49
5.1.2_ Relación de sujetos y sus atributos 49
5.2_ Requisitos de control de acceso 50
5.2.1_ FDP_ACC.2 Complete access control 50
5.2.2_ FDP_ACF.1 Security attribute based access control 51
5.2.3_ FMT_MSA.1 Management of security attributes 56
5.2.4_ FMT_MSA.3 Static attribute initialisation 56
5.2.5_ FMT_SMR.1 Security roles 56
5.2.6_ FMT_SMF.1 Specification of Management Functions 57
5.2.7_ FIA_UID.2 User identification before any action 57
5.2.8_ FIA_UAU.2 User authentication before any action 57
5.2.9_ FIA_UAU.5 Multiple authentication mechanisms 57
5.2.10_ FIA_UAU.7 Protected authentication feedback 58
5.3_ Requisitos y servicios criptográficos 58
5.3.1_ FCS_CKM.1 Cryptographic key generation 58
5.3.2_ FCS_CKM.2 Cryptographic key distribution 59
5.3.3_ FCS_CKM.3 Cryptographic key access 59
5.3.4_ FCS_CKM.4 Cryptographic key destruction 59
5.3.5_ FCS_COP.1 Cryptographic operation 59
5.4_ Requisitos relativos a auditoría de eventos 61
5.4.1_ FAU_GEN.1 Audit data generation 61
5.4.2_ FAU_SAR.3 Selectable audit review 62
5.5_ Requisitos relativos a la tranferencia interna segura de datos 63
5.5.1_ FDP_ITT.1 Basic internal transfer protection 63
5.5.2_ FDP_ITT.3 Integrity monitoring 63
5.5.3_ FPT_ITT.1 Basic internal TSF data transfer protection 63
5.5.4_ FPT_ITT.3 TSF data integrity monitoring 63
5.6_ Requisitos de aseguramiento: Clase ASE - Security Target Evaluation 64
5.6.1_ ASE_INT.1 ST introduction 64

5.6.2_ ASE_CCL.1 Conformance claims 64
5.6.3_ ASE_SPD.1 Security problem definition 65
5.6.4_ ASE_OBJ.2 Security objectives 65
5.6.5_ ASE_ECD.1 Extended components definition 66
5.6.6_ ASE_REQ.2 Derived security requirements 67
5.6.7_ ASE_TSS.1 TOE summary specification 67
5.7_ Requisitos de aseguramiento: Clase ADV - Development 68
5.7.1_ ADV_FSP.3 Functional specification with complete summary 68
5.7.2_ ADV_ARC.1 Security architecture description 68
5.7.3_ ADV_TDS.2 Architectural design 69
5.8_ Requisitos de aseguramiento: Clase AGD - Guidance Documents 70
5.8.1_ AGD_OPE.1 Operational user guidance 70
5.8.2_ AGD_PRE.1 Preparative procedures 70
5.9_ Requisitos de aseguramiento: Clase ALC - Life-Cycle Support 71
5.9.1_ ALC_CMC.3 Authorisation controls 71
5.9.2_ ALC_CMS.3 Implementation representation CM coverage 71
5.9.3_ ALC_DEL.1 Delivery procedures 72
5.9.4_ ALC_DVS.1 Identification of security measures 72
5.9.5_ ALC_FLR.1 Basic flaw remediation 72
5.9.6_ ALC_LCD.1 Developer defined life-cycle model 73
5.10_ Requisitos de aseguramiento: Clase ATE - Tests 73
5.10.1_ ATE_COV.2 Analysis of coverage 73
5.10.2_ ATE_DPT.1 Testing: basic design 74
5.10.3_ ATE_FUN.1 Functional testing 74
5.10.4_ ATE_IND.2 Independent testing - sample 75
5.11_ Requisitos de aseguramiento: Clase AVA - Vulnerability Assessment 75
5.11.1_ AVA_VAN.2 Vulnerability analysis 75
5.12_ Razonamiento de requisitos 75
5.12.1_ Razonamiento de requisitos funcionales 75
5.12.2_ Razonamiento requisitos de aseguramiento 83
6_ Especificación resumida del TOE 84
6.1_ FDP_ACC.2 Complete access control 84
6.2_ FDP_ACF.1 Security attribute based access control 85
6.3_ FMT_MSA.1 Management of security attributes 87
6.3.1_ FMT_MSA.1.1/ Entidades externas 87

6.3.2_ FMT_MSA.1.1/Usuarios 89
6.4_ FMT_MSA.3 Static attribute initialisation 89
6.5_ FMT_SMR.1 Security roles 90
6.6_ FMT_SMF.1 Specification of Management Functions 90
6.7_ FIA_UID.2 User identification before any action 90
6.8_ FIA_UAU.2 User authentication before any action 91
6.9_ FIA_UAU.5 User authentication mechanism 91
6.10_ FIA_UAU.7 Protected authentication feedback 92
6.11_ FCS_CKM.1 Cryptographic key generation 92
6.12_ FCS_CKM.2 Cryptographic key distribution 92
6.13_ FCS_CKM.3 Cryptographic key access 92
6.14_ FCS_CKM.4 Cryptographic key destruction 93
6.15_ FCS_COP.1 Cryptographic operation 93
6.16_ FAU_GEN.1 Audit data generation 95
6.17_ FAU_SAR.3 Selectable audit review 95
6.18_ FDP_ITT.1 Basic internal transfer protection 95
6.19_ FDP_ITT.3 Integrity monitoring 96
6.20_ FPT_ITT.1 Basic internal TSF data transferprotection 96
6.21_ FPT_ITT.3 TSF data integrity monitoring 96

Figuras

Figura 01 – Arquitectura lógica de la configuración evaluada 21
Figura 02 – Arquitectura física de la configuración evaluada 23

Tablas

Tabla 01 – Identificación de ST y TOE 10
Tabla 02 – Glosario de términos 12
Tabla 03 – Mapeo de activos y amenazas 33
Tabla 04 – Razonamiento de los objetivos de seguridad del TOE 43
Tabla 05 – Razonamiento de los objetivos de seguridad del entorno 48

Tabla 06 – Razonamiento de los requisitos funcionales 80

1_ Introducción

1.1_ Identificación

Esta sección recoge la información de etiquetado para la identificación de la presente Declaración de Seguridad (ST), así como del Objeto de Evaluación (TOE) al que ésta hace referencia.

Identificador	Valor
Identificador del documento:	TBS_ ASFv4.1_Declaración de Seguridad_20080128_v1.9
Título:	Declaración de seguridad para Advanced Signature Framework v4.1.5
Autores	María Peleato Óscar Flor Luis Franco Miguel Ángel Sarasa
Estado del documento:	Finalizado
Fecha de publicación:	28 de Enero de 2008
Identificador del TOE:	*ASF* v4.1.5
Versión CC:	CC Version 3.1 Revision1
EAL:	EAL3+ (ALC-FLR.1)
Evaluación Declaración de Seguridad:	Epoche&Espri

Tabla 01 – Identificación de ST y TOE

1.2_ Glosario

Los siguientes términos y acrónimos son utilizados a lo largo del documento:

Término/Acrónimo	Descripción
Autorización	El proceso de aprobación de una solicitud de acuerdo con los criterios recogidos en una política de registro.
CA (Autoridad de Certificación)	Es la entidad de confianza, responsable de emitir y revocar los certificados digitales utilizados en firma electrónica.
Certificado	Es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Término/Acrónimo	Descripción
Certificados X-509	X.509 especifica formatos estándar para certificados de claves públicas y un algoritmo de validación de ruta de certificación.
CRL (Certificate Revocation List)	Lista firmada de certificados que han sido revocados y no son confiables (de acuerdo con el estándar para CRLs v2 como se define en X.509).
Firma Electrónica Avanzada	Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere, y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
HTTP/HTTPS (HyperText Transfer Protocol)	Protocolos usados en cada transacción de la Web.
HSM (Hardware Security Module)	Dispositivo criptografía basado en hardware que genera, almacena y protege claves criptográficas.
Keystore	Es un almacén de claves criptográficas.
LDAP (Lightweight Directory Access Protocol)	Protocolo de red que permite el acceso a un servicio de directorio ordenado y distribuido para buscar información en un entorno de red.
OCSP (Online Certificate Status Protocol)	Método que proporciona una prueba activa acerca del estado (activo, suspendido o revocado) de un certificado digital X.509, a diferencia de la prueba pasiva proporcionada por otros métodos como, por ejemplo, las CRLs (Listas de Revocación de Certificados).
PKI (Public Key Infraestructure)	Es una combinación de hardware, software, políticas y procedimientos que permiten asegurar la identidad de los participantes en un intercambio de datos usando criptografía pública.
PKCS7	Estándar sobre la sintaxis de mensajes criptográficos usado para firmar y/o cifrar mensajes en PKIs.
Servicio TOE	Conjunto de servicios y servlets del Objeto de Evaluación que se publican al exterior para ofrecer funcionalidades.
SOAP (Simple Object Access Protocol)	Protocolo estándar creado por Microsoft, IBM y otros, que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.
SSL (Secure Sockets Layer)	Protocolo criptográfico que proporciona comunicaciones seguras en Internet.
TOE (Target of Evaluation)	Objeto de Evaluación.

Término/Acrónimo	Descripción
TSA (Autoridad de Sellado de Tiempo)	Actúa como tercera parte de confianza testificando la existencia de unos datos electrónicos en una fecha y hora concretos.
Webservice	Colección de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

Tabla 02 – Glosario de términos

1.3_ Referencias

La presente Declaración de Seguridad se ha elaborado teniendo en cuenta las referencias que se indican a continuación:

[CC] Common Criteria for Information Technology Security Evaluation, version 3.1, Parts 1, 2 and 3.

1.4_ TOE overview

La plataforma de firma ASF constituye una solución completa para la integración de la Firma Electrónica Avanzada en la infraestructura informática de una entidad u organización. Una de sus características diferenciadoras es la posibilidad de operar simultáneamente con más de una Autoridad de Certificación (CA), liberando al resto de los sistemas de la complejidad añadida que supone la compatibilidad multi-CA.

Las principales funciones de seguridad ofrecidas por la plataforma ASF para garantizar la salvaguarda de las transacciones electrónicas son las siguientes:

- **Autenticación**. Permite la identificación fiable de usuarios remotos. La herramienta básica utilizada para ello es el certificado digital X.509v3.

- **Integridad**. La Firma Electrónica Avanzada de documentos digitales permite verificar que éstos no han sido modificados por un tercero tras la generación de los mismos.

- **No Repudio**. El sistema almacena en una base de datos las copias de los documentos firmados, de forma que éstas puedan ser utilizadas, si ello es necesario, como prueba de autoría.

- **Confidencialidad**. La generación de documentos cifrados permite garantizar que únicamente los destinatarios de los mismos pueden acceder a su contenido.

La plataforma ASF proporciona una solución de principio a fin para garantizar la seguridad de las comunicaciones, disponiendo para ello de funcionalidades que permiten el cifrado, la firma, el fechado, y la transmisión de documentos electrónicos de un modo seguro.

Para ello, ASF contempla todos los procedimientos necesarios para la creación de documentos firmados y/o cifrados, la validación y el control de la vigencia de los certificados utilizados, el registro de la información de firma necesaria para garantizar el no repudio, así como el establecimiento de políticas de firma.

El Target Of Evaluation (TOE) objeto de la presente Declaración de Seguridad está constituido por un subconjunto de los servicios que proporcionan la funcionalidad completa de la plataforma de firma ASF. En el apartado siguiente, se describirán de forma detallada qué componentes de la plataforma de firma ASF son necesarios para ofrecer los servicios y funcionalidades objeto de la presente evaluación (i.e., los servicios y funcionalidades que integran el TOE).

1.5_ Descripción del TOE

El Target Of Evaluation (TOE) objeto de la presente Declaración de Seguridad se encuentra constituido por un conjunto de servicios y servlets que se publican al exterior para ofrecer funcionalidades. En adelante, este conjunto será referido con la denominación de **Servicio TOE**. El TOE incluye además un componente adicional denominado **Consola de Administración**, que proporciona utilidades para la configuración del Servicio TOE.

Como se indicó en el apartado 1.4_TOE overview, el TOE no está conformado por la totalidad de los servicios proporcionados por la plataforma de firma ASF, sino únicamente por un subconjunto de los mismos. Dicho subconjunto es a su vez ofrecido por una parte de los módulos que integran la plataforma de firma ASF (a nivel de componente).

Teniendo en cuenta lo anterior, a continuación se presenta una breve descripción de la totalidad de los componentes que integran la plataforma de firma ASF, indicando cuáles de ellos son necesarios para proporcionar los servicios y utilidades que forman parte del TOE. El apartado se concluye con la descripción de dichos servicios.

A nivel de componente, la plataforma ASF se compone de catorce (14) módulos diferentes, que se relacionan entre sí para proporcionar la totalidad de las funcionalidades ofrecidas por la plataforma. En su caso, y dependiendo de las necesidades de integración, dichos módulos pueden a su vez trabajar de forma independiente. Los módulos referidos son los siguientes:

- **PolicyManager**: Proporciona servicios de configuración al resto de módulos de ASF, siendo el encargado de acceder a la base de datos

donde se almacena toda la información que define el comportamiento de la plataforma.

- **X509Validator**: Proporciona servicios para la verificación del estado en el que se encuentran los certificados X.509v3 utilizados por la plataforma ASF.

- **Consola de Administración**: Herramienta que proporciona utilidades a través de las cuales es posible establecer la configuración de cada uno de los módulos de la plataforma para su correcto funcionamiento.

- **SignatureServer**: Proporciona servicios para la firma digital de datos y documentos en diferentes formatos y con distintos algoritmos, así como servicios para la validación de firmas electrónicas.

- **EncryptionServer**: Proporciona servicios para realizar el cifrado y descifrado de documentos en distintos formatos y con diversos algoritmos.

- **NonRepudiationServer**: Registra en la base de datos de no repudio (incluida dentro de la base de datos de ASF) todas las firmas generadas y verificadas por el módulo SignatureServer, junto con la información necesaria para comprobar el estado de revocación de los certificados implicados en el proceso: CRLs (Certificate Revocation Lists), respuestas OCSP (On-line Certificate Status Protocol), etc.

- **X509SingleSignOn**: Posibilita la integración de varias aplicaciones Web en un único sistema de autenticación, de forma que una vez que el usuario se haya autenticado frente a una de ellas, no necesite autenticarse frente al resto.

- **TimeStampServer**: Permite a aplicaciones y componentes añadir sellos temporales a los documentos firmados, dotando así a las firmas de validez a lo largo del tiempo.

- **TimeStampClient**: Ofrece una sencilla interfaz basada en Web Services (SOAP: Simple Object Access Protocol) para obtener sellos de tiempo.

- **OCSPResponder**: Encargado de devolver la información relativa al estado (activo, suspendido o revocado) de los certificados incluidos en la invocación al servicio.

- **DSSProxy**: Permite realizar peticiones de firma y verificación de firma según el formato establecido en el estándar de firma DSS.

- **WebSigner**: Componente cliente de ASF diseñado para permitir la firma y el cifrado de documentos y formularios Web desde una página HTML enviada al servidor. El componente permite asimismo la verificación de firmas y el descifrado de documentos en la parte cliente.

- **DesktopSigner**: Aplicación de escritorio que ofrece la misma funcionalidad que WebSigner con un interfaz propio, por lo que no es necesario el uso de un navegador.

- **EasyCert**: Herramienta para la emisión y gestión completa de certificados digitales, basada en el Servicio de Certificación de Microsoft Windows 2000/2003 Server.

- **SecurityAgents**: Componentes cliente concebidos para simplificar la integración de las aplicaciones cliente J2EE con los módulos de ASF, haciendo transparentes al usuario las invocaciones a Web services y ofreciendo a las aplicaciones externas un sencillo API para interactuar con la plataforma ASF.

De entre todos los módulos anteriores, aquéllos requeridos para ofrecer el conjunto de servicios, herramientas y utilidades que integran el TOE objeto de la presente Declaración de Seguridad son los que se indican a continuación:

- **PolicyManager.**

- **X509Validator.**

- **Consola de Administración.**

- **SignatureServer.**

- **EncryptionServer.**

- **NonRepudiationServer.**

- **TimeStampServer.**

- **TimeStampClient.**

- **OCSPResponder.**

- **SecurityAgents.**

Así pues, quedan fuera del alcance de esta evaluación las funcionalidades ofrecidas por siguientes módulos de la plataforma de firma ASF:

- X509SingleSignOn.
- DSSProxy.
- WebSigner.
- DesktopSigner.
- EasyCert.

Una vez identificados los componentes de la plataforma ASF necesarios para ofrecer los servicios y funcionalidades que constituyen el TOE, éste puede ser descrito como una solución completa capaz de proporcionar todos los servicios de Firma Electrónica Avanzada a la infraestructura informática de una entidad u organización.

En concreto, el Servicio TOE permite firmar en multitud de formatos, verificar firmas, así como validar certificados (validez temporal, validez de la cadena de confianza y comprobación del estado de revocación). El TOE permite asimismo almacenar las firmas realizadas para garantizar el no repudio de las mismas, así como dotar a dichas firmas de sellos de tiempo (tanto en el momento de su generación como una vez que se encuentran almacenadas como garantía para no repudio). Además de lo anterior, el TOE permite establecer diferentes políticas de firma y proporcionar servicios de cifrado y descifrado.

Asimismo, el Objeto de Evaluación es capaz de acometer el registro de las invocaciones realizadas a los módulos que componen el Servicio TOE. La generación de auditorías la realiza un subsistema específico, que registra el comienzo y el fin de la ejecución de un método invocado por una aplicación usuaria en el archivo de auditoría correspondiente. Únicamente se registra la ejecución de estos métodos si son invocaciones remotas, es decir, desde una aplicación usuaria. En caso de que otro subsistema de los que componen el TOE llamara a un método de otro subsistema, aunque esté publicado al exterior, este hecho no se audita al tratarse de una invocación local.

El TOE dispone igualmente de la capacidad de controlar el acceso de las peticiones a los Webservices al TOE por parte de las aplicaciones uaurias, así como la de firmar las respuestas de éste a las mismas. Para ello, el TOE dispone de manejadores automáticos para la verificación de las peticiones y para la realización de la firma de las respuestas.

Por lo que respecta a la Consola de Administración, aparte de permitir configurar todo lo necesario para el uso del Servicio TOE, cuenta con una utilidad que permite la extracción de datos almacenados para garantizar el no repudio, así como la generación de informes sobre los mismos en formato PDF. La autenticación para el uso de la Consola de Administración puede hacerse por medio de usuario/contraseña o bien mediante certificados digitales.

Una de las características más relevantes del TOE es la de ofrecer un escenario multi-CA capaz de operar con más de una Autoridad de Certificación (CA). Así, el TOE permite dar de alta y configurar diferentes CAs de forma transparente a las aplicaciones que lo invocan. Concretamente, para cada CA dada de alta, se pueden configurar:

- **Métodos de comprobación de revocación**: Dado que la forma en la que cada Autoridad de Certificación permite consultar la revocación de sus certificados es diferente, estos métodos permiten unificar la comprobación del estado de los certificados emitidos por diferentes CAs, cada uno de ellos con su respectiva prioridad y datos de configuración. Los métodos de comprobación de revocación que pueden asociarse a una CA son: OCSP (On-line Certificate Status Protocol), HTTP (HyperText Transfer Protocol), LDAP (Lightweight Directory Access Protocol), DATABASE, CDP (Certificate Distribution Point) y AIA (Authority Information Access). Además, el usuario final de la plataforma puede crear sus propios métodos de comprobación de revocación conforme a sus necesidades, y posteriormente añadirlos a la plataforma sin necesidad de realizar cambios en ésta.

- **Editor de consultas**: Dado que cada Autoridad de Certificación define a su arbitrio los campos que incluye en sus certificados, el editor de consultas permite unificar la extracción de la información contenida en certificados emitidos por diferentes CAs. La forma en que se define la extracción de esta información es mediante el uso de patrones.

Como ya se ha indicado anteriormente, las funcionalidades ofrecidas por el Servicio TOE se encuentran proporcionadas por un conjunto de módulos que pueden interaccionar entre sí. Estos módulos pueden trabajar de forma independiente o incluso alguno de ellos puede no ser necesario dependiendo de la funcionalidad que se requiera. Los módulos pueden distribuirse en diferentes servidores, comunicándose entre sí a través de protocolos seguros SSL y/o mediante la firma de las invocaciones.

El TOE ofrece sus servicios a través de interfaces de tipo WebService (SOAP/XML), es decir, el TOE publica sus funcionalidades de manera que éstas pueden ser invocadas, bien desde el equipo en el que se aloja al TOE o bien desde cualquier otro equipo (incluso con un sistema operativo diferente al de la máquina en la que resida el TOE).

Si la aplicación que invoca al Servicio TOE se encuentra alojada en el mismo equipo que éste y en el mismo servidor de aplicaciones, entonces la aplicación puede efectuar las invocaciones a las funcionalidades del TOE mediante interfaces locales Java. Sin embargo, en el caso de que las invocaciones sean realizadas a través de WebServices o bien a través de HTTP o HTTPS, el cliente dispone de un componente capaz de firmar digitalmente dichas invocaciones, de manera que la autenticidad de origen y la integridad de las mismas queden garantizadas. De igual manera, el TOE puede firmar sus respuestas, garantizando para éstas los mismos principios (i.e., autenticidad de origen e integridad) garantizados por el cliente en el caso de las peticiones.

Asimismo, el TOE permite el establecimiento de reglas para restringir las IPs desde las que se aceptan peticiones.

En lo referente a la política del TOE concerniente al tratamiento de claves públicas y privadas, cabe reseñar los aspectos que se indican a continuación:

- Para realizar cualquier operación criptográfica que requiera el uso de una clave privada (es decir, firma y/o descifrado), el certificado asociado a dicha clave debe estar dado de alta en la Consola de Administración, y ha de estar asociado tanto a la aplicación que lo va a utilizar como a la operación concreta que se desea realizar con el mismo. Es decir, se ha de manifestar de forma explícita la confianza en el certificado de forma previa a la solicitud de la operación de que se trate.

- Para realizar cualquier operación criptográfica que requiera el uso de una clave pública (i.e., verificación de firma y/o cifrado), no es necesario que el certificado que contiene dicha clave esté dado de alta en la Consola de Administración, si bien puede estarlo si así se desea. Así, por ejemplo, el certificado que contiene la clave pública requerida para la verificación de una firma puede ser suministrado en la propia firma, o bien puede ser obtenido de un repositorio de datos para el que se disponga de la implementación del correspondiente componente de acceso. Por su parte, en el caso del cifrado, el certificado puede ser suministrado directamente en la invocación como una cadena de caracteres codificada. En los dos casos anteriores, la Autoridad de Certificación emisora de los certificados deberá estar dada de alta en la Consola de Administración. Asimismo, cada certificado deberá estar asociado a la aplicación que haya de utilizarlo, así como a la operación que se desee realizar con el mismo.

Por lo que respecta al almacenamiento de claves privadas por parte del TOE, existen dos posibilidades:

- Almacenamiento de las claves privadas en Base de Datos.

- Almacenamiento de las claves privadas en un módulo de Hardware Criptográfico de tipo HSM (Hardware Security Module).

En el caso de que las claves privadas sean almacenadas en Base de Datos, de forma previa al almacenamiento físico de la clave, ésta es introducida en un keystore por motivos de seguridad. Un keystore es una estructura de datos que permite almacenar múltiples claves y protegerlas mediante el uso de cifrado simétrico. Cada registro del keystore donde se almacena una clave privada está protegido por una clave simétrica diferente. Otra clave simétrica común protege la totalidad del keystore. A su vez, cada clave privada depositada en un registro del keystore se almacena cifrada con una clave diferente, generada automáticamente por el keystore en el momento del depósito. Existen diferentes tipos de keystores, todos ellos con un interfaz común. El uso de

un tipo u otro de keystore para el almacenamiento de las claves privadas es configurable mediante propiedades.

En el caso de almacenamiento en Base de Datos, el TOE es el encargado de acopiar, proteger y gestionar las claves de protección necesarias para poder utilizar las claves privadas del keystore.

En el caso de almacenamiento en hardware criptográfico, es el propio HSM el que se encarga de almacenar, proteger y gestionar las claves necesarias para el acceso y utilización de las claves privadas de sus keystores internos. Dependiendo de cómo se decida usar, también puede hacerse necesario que estas claves sean almacenadas por el TOE.

En el escenario propuesto para la configuración evaluada se considerará únicamente el almacenamiento de claves privadas en Base de Datos, quedando fuera de su alcance la evaluación del servidor de Base de Datos utilizado.

Con todo lo anterior, el TOE proporciona todos los servicios necesarios para poder garantizar los cuatro pilares básicos de la seguridad:

- **Autenticidad**: para garantizar la identidad del emisor del mensaje.
- **Integridad**: para demostrar que la información no ha sido modificada.
- **No Repudio**: para asegurar que el emisor del mensaje no pueda negar su emisión a posteriori.
- **Confidencialidad**: para garantizar que sólo los destinatarios legítimos de la información pueden tener acceso a ella.

Para ello, el TOE basa sus servicios en el uso de Criptografía Asimétrica, también conocida con la denominación de Criptografía de Clave Pública.

1.6_ Configuración evaluada

En esta sección se especifican las características y requerimientos de la configuración evaluada del TOE. En particular, se detallan:

- Módulos de la plataforma de ASF que se incluyen dentro de la configuración evaluada, indicados en 1.6.1_Componentes del TOE.
- Diagrama de la arquitectura lógica de componentes del TOE, descrito en el apartado 1.6.2_Arquitectura lógica del TOE.
- Diagrama de arquitectura física de componentes del TOE, descrito en el apartado 1.6.3_Arquitectura física del TOE.

- Relación de componentes de terceros que deben ser utilizados junto con el TOE en su configuración evaluada, referidos en el apartado 1.6.4_Requisitos de la configuración evaluada.

1.6.1_ Componentes del TOE

El conjunto de servicios que integran el TOE requiere que el escenario de la configuración evaluada contenga los siguientes componentes de la plataforma de firma ASF:

- PolicyManager.
- X509Validator.
- Consola de Administración.
- SignatureServer.
- EncryptionServer.
- NonRepudiationServer.
- TimeStampServer.
- TimeStampClient.
- OCSPResponder.
- SecurityAgents.

1.6.2_ Arquitectura lógica

La arquitectura lógica de la configuración evaluada se representa en la Figura 01 – Arquitectura lógica de la configuración evaluada. En dicha arquitectura se diferencian dos casos, dependiendo de quién invoca los servicios de la plataforma. Éstos son los siguientes:

- **Administrador del sistema**: Para configurar el TOE, el administrador del sistema utiliza el módulo Consola de Administración. En la configuración evaluada, la comunicación entre este tipo de usuario y la consola se realiza mediante el protocolo HTTP. El administrador indica los datos que quiere registrar y la consola es la encargada de almacenarlos en la base de datos. Además, la consola accede a la base de datos para obtener los datos que el administrador solicite en cada momento. Así, los únicos módulos

del TOE que se ven involucrados en este modo de uso son la Consola de Administración y el PolicyManager. En la configuración evaluada, éste último interviene cuando es invocado localmente por la Consola de Administración para refrescar en cachés los cambios de configuración que el administrador haya realizado.

- **Aplicaciones usuarias**: Las aplicaciones usuarias pueden interactuar con el Servicio TOE, pero no con la Consola de Administración. En la configuración evaluada, las invocaciones a los módulos OCSPResponder y TimeStampServer se realizan vía HTTP. Por lo que se refiere a los servicios publicados por los componentes SignatureServer, X509Validator, TimeStampClient, EncryptionServer, NonRepudiationService y PolicyManager, éstos son invocados mediante Webservices (a través de mensajes SOAP en formato XML).

  Independientemente de la manera que tengan de interaccionar con el exterior, todos estos módulos utilizan invocaciones locales Java para comunicarse entre ellos.

  Los únicos módulos utilizados por las aplicaciones usuarias que acceden a la base de datos son el NonRepudiationService y el PolicyManager. El primero almacena en la base de datos la información de no repudio y la extrae, teniendo sólo acceso a este tipo de información. Por su parte, el PolicyManager, que sólo tiene permiso para acceder a la base de datos en modo lectura, es el encargado de actuar de intermediario para el resto de los componentes del TOE ante cualquier dato solicitado excepto la información de no repudio, información para el cual se emplea el NonRepudiationServer.

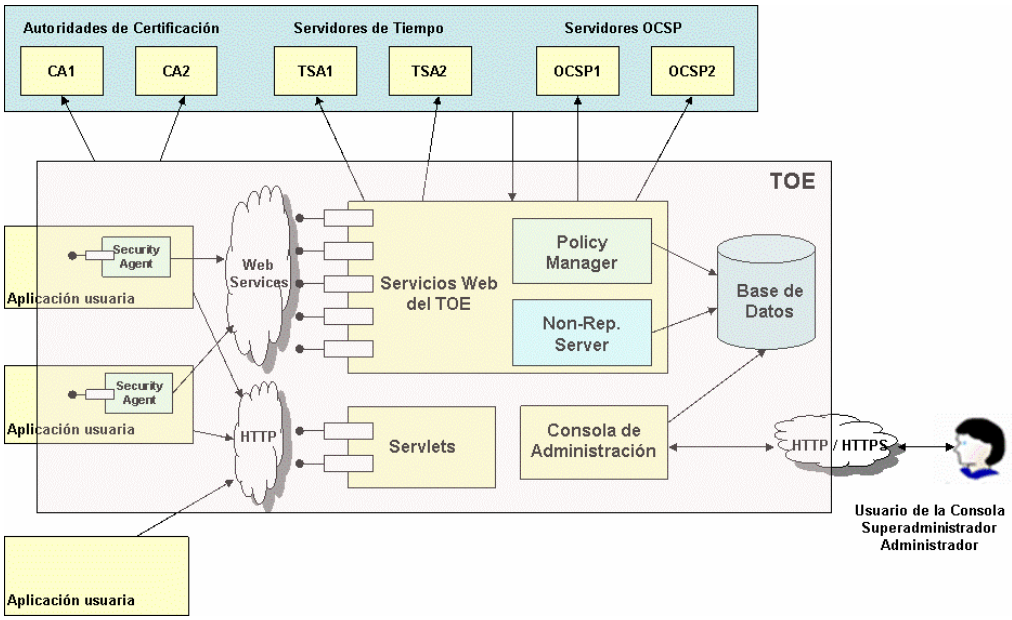

Figura 01 – Arquitectura lógica de la configuración evaluada

Como ya se ha indicado, cada módulo publica sus propios Webservices. Éstos podrían ser invocados directamente por una aplicación usuaria, es decir, la aplicación podría construir su propia invocación a cualquier Webservice publicado. No obstante, la configuración evaluada hace uso del módulo SecurityAgent para realizar las invocaciones al servidor, tal y como se indica en la Figura 01 – Arquitectura lógica de la configuración evaluada. El SecurityAgent es simplemente una facilidad que se proporciona a los clientes para la construcción de las invocaciones a los servicios Web (serialización de los parámetros, etc.), pero no es imprescindible, incluyéndose tan solo como una herramienta de integración.

1.6.3_ Arquitectura física

La arquitectura física de la configuración a evaluar es la indicada en la Figura 02 – Arquitectura física de la configuración evaluada. En dicha arquitectura, los módulos PolicyManager, X509Validator, Consola de Administración, SignatureServer, EncryptionServer, NonRepudiationService, TimeStampServer, TimeStampClient y OCSPResponder estarán ubicados en un mismo equipo, y se comunicarán entre ellos por medio de invocaciones locales Java.

Por lo que respecta a las aplicaciones usuarias, éstas se alojarán en un equipo diferente al anteriormente referido. Este segundo equipo alojará igualmente a los respectivos Security Agents, utilizados por las aplicaciones usuarias para integrarse con el resto del TOE. Lo anterior queda reflejado igualmente en la Figura 02 – Arquitectura física de la configuración evaluada. De esta forma, la configuración evaluada incluirá únicamente las invocaciones remotas, permitiendo la simulación de posibles ataques de tipo man-in-the-middle.

El administrador se comunica con el TOE a través del protocolo HTTP. La interacción entre las aplicaciones usuarias y el TOE se efectúa mediante la invocación a un servicio web o bien por medio de HTTP, dependiendo de a qué módulo pertenezca el servicio solicitado. Las comunicaciones con los módulos que integran esta configuración se realizan a través de HTTP o bien por medio de Webservices, dependiendo del componente del que se trate. Así, por ejemplo:

- En el caso de los componentes OCSPResponder, Consola de Administración y TSAServer la comunicación se realiza vía HTTP.

- Para establecer comunicación con los módulos TimeStampClient, PolicyManager, SignatureServer, Encryption Server, NonRepudiationService y X509Validator se utilizan los Webservices.

El módulo PolicyManager es el encargado de gestionar las consultas a la base de datos de ASF de todos los módulos del TOE pertenecientes a la configuración evaluada, a excepción de la Consola de Administración. Esto implica que si un componente diferente de éste último requiere infor-

mación de la base de datos, ha de invocar al PolicyManager, que es el encargado de devolver los datos al módulo invocante. Debe tenerse en cuenta que la Base de Datos no es un componente que pertenezca al TOE, sino un software de terceros.

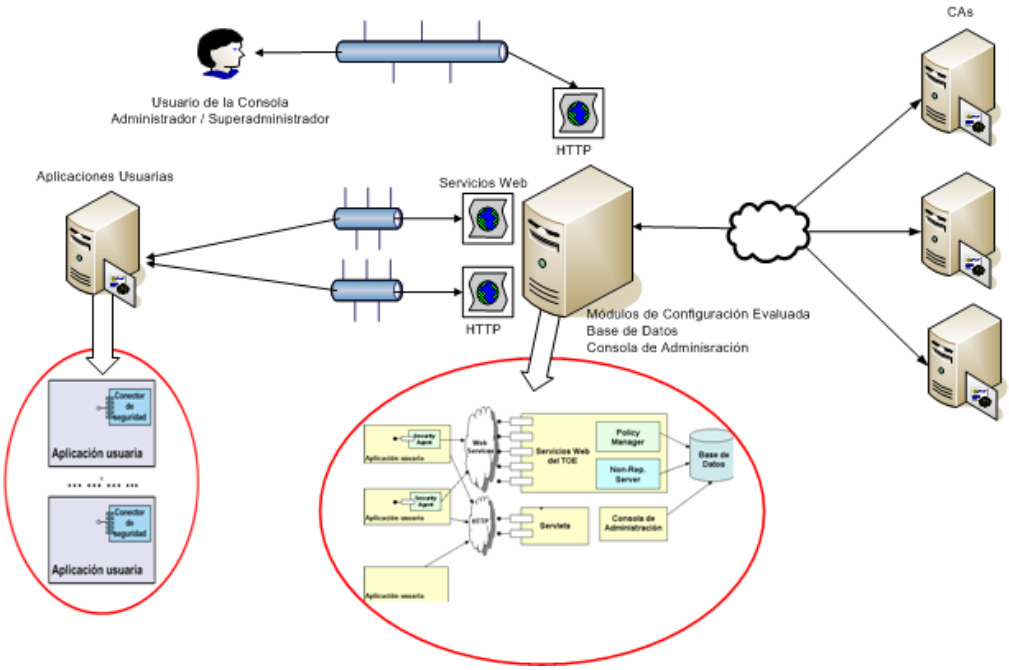

Figura 02 – Arquitectura física de la configuración evaluada

La Consola de Administración es el módulo a través del cual se realiza la inserción y/o edición de la información alojada en la base de datos de la plataforma de ASF. El módulo Consola de Administración es utilizado únicamente por el administrador del sistema, y se comunica únicamente con el módulo PolicyManager. Aun siendo posible la autenticación remota del usuario administrador ante el módulo Consola de Administración, en la configuración evaluada se considera únicamente el caso de la autenticación local de dicho usuario ante el referido módulo (bien sea mediante usuario y contraseña o bien utilizando un certificado digital).

Otro módulo que trata con la base de datos es el componente NonRepudiatonServer, que se encarga tanto de almacenar las firmas generadas y verificadas por la plataforma (dispone de permisos de escritura en la base de datos) como de consultar los datos relacionados con los objetos firmados (a través del módulo PolicyManager).

Dos de los módulos del TOE, el X509Validator y el TSAClient, se comunican con entidades externas. En concreto, el X509Validator debe interactuar con Autoridades de Certificación para obtener el estado de revocación de los certificados. Así, dependiendo de cuáles sean los métodos establecidos para dichas Autoridades de Certificación, se realizará la consulta a una de las entidades indicadas a continuación:

- A un servidor de estados (Web HTTP u OCSP).

- A la Base de Datos del TOE, donde se encuentra la información acerca del estado de revocación.

Por su parte, el componente TSAClient requiere establecer comunicación con TSA's externas para obtener sellos de tiempo. Así, el módulo TSA-Client es el encargado de obtener (a través del componente PolicyManager) las Autoridades de Sellado de Tiempos disponibles, y posteriormente invocar a dichas TSAs.

El almacén de claves (en adelante, keystore) de la configuración evaluada residirá en la base de datos del TOE. Esta opción de configuración será establecida mediante la edición de las propiedades requeridas de los archivos de propiedades del TOE.

El resto de componentes de terceros requeridos para el funcionamiento de la configuración base (Servidor de Aplicaciones, Servidor de Directorio, Servidor OCSP, Servidor Web, Servidor Base de Datos, JDK) se instalarán siguiendo las indicaciones recogidas en el apartado 1.6.4_Requisitos de la configuración evaluada.

1.6.4_ Requisitos de la configuración evaluada

A continuación se detallan los requisitos necesarios para la instalación en un entorno seguro de la configuración evaluada del TOE presentada en el apartado 1.6_Configuración evaluada.

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento de ASF es necesario disponer de los siguientes componentes software:

- **Servidor de aplicaciones**. El servidor de aplicaciones ha de soportar una máquina virtual Java J2SE 1.4.2. o superior.

- **Servidor base de datos**. El servidor de base de datos ha de tener disponible un driver de tipo JDBC.

- **Sistema operativo**. El sistema operativo de los equipos donde se ejecuta ASF ha de permitir la ejecución de una máquina virtual Java J2SE 1.4.2 o superior.

- **Java Runtime Enviroment**. Respecto a la versión del runtime Java (J2SE) sobre el que se ejecutará el servidor de aplicaciones, se recomienda utilizar la máquina virtual JRE 1.5.0 o superior de Sun. Como mínimo, es necesario la J2SE 1.4.2.

- **Navegadores**. Cualquiera de los siguientes es válido.
    - Microsoft Internet Explorer v6.0 Service Pack 2 o superior.
    - Netscape Comunicator v6 o superior.
    - Mozilla v4.1 o superior.

En cuanto a los componentes hardware, el único requisito es que soporten los elementos software detallados previamente.

Dentro de todas las posibilidades que ofrecen estos requisitos software, la configuración que se ha elegido para su evaluación es la siguiente:

- **Servidor de aplicaciones**. Apache Tomcat 5.5.
- **Servidor base de datos**. SQLServer 2000.
- **Sistema operativo**: Windows XP
- **Java Runtime Enviroment**. JRE 1.5.0.12
- **Navegadores**. Microsoft Internet Explorer v6.0.

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 1), de Septiembre de 2006. En concreto, con:

- Requerimientos Funcionales de seguridad de la Parte 2 de CC Version 3.1. Revision 1.

- Requerimientos de Garantía de Seguridad de la Parte 3 de CC Version 3.1 Revision 1 para el Nivel de Certificación EAL3+ (ALC-FLR.1).

- RI # 145 - FCS component dependencies on FMT_MSA.2:

  Problem: Each of the components in the FCS class has a dependency on FMT_MSA.2.

  In cases where FMT_MSA.2 is included in the ST only as a consequence of satisfying the dependency from components from the FCS class, **is it necessary for FMT_MSA.2 to apply to all security attributes, or is it acceptable to include just those that pertain to cryptographic functionality?**

  FMT_MSA.2.1 reads: "The TSF shall ensure that only secure values are accepted for security attributes."First of all, it is not absolutely certain from the wording of FMT_MSA.2.1 as to the scope of those security attributes that must be covered by it. In the absence of any assignment operation, it would seem to be the case that FMT_MSA.2 applies to all security attributes whenever it is included in the ST. If this is the case, then this appears to be a case where there is insufficient flexibility in requirements.

  Specific Changes: (specified from v3.1)

  Replace FMT_MSA.2.1 with: FMT_MSA.2.1 The TSF shall ensure that secure values are accepted for [assignment: list of security attributes]. Following for 1015, insert:

  Operations:

  Assignment: In FMT_MSA.2.1, the PP/ST author should specify the list of security attributes that require only secure values to be provided.

  Remove FCS dependencies on MSA.

  Accepted

La Metodología de Evaluación asociada a la presente Declaración de Seguridad será Common Methodology for Information Technology Security Evaluation CEM v3.1 (Revisión 1) de Septiembre de 2006.

3_ Definición del problema de seguridad del TOE

Este capítulo contiene la definición del entorno de seguridad del TOE. Se describen los aspectos de seguridad del entorno en el que el TOE será utilizado, así como la forma en la que se espera que el TOE sea gestionado. Se considera natural que sea el propio Objeto de Evaluación el responsable de proporcionar unas medidas de seguridad acordes con los distintos escenarios de uso en los que se haya de utilizar, y que éstas aporten la suficiente seguridad a los servicios y aplicaciones que así lo requieran. Con todo ello, las principales características que se deben asegurar son:

- **Autenticación**: garantiza la identidad de los usuarios remotos mediante el uso de certificados digitales X.509 v3.
- **Integridad**: avala que los documentos no han sido modificados por un tercero, empleando para ello la Firma Electrónica Avanzada.
- **No Repudio**: aporta pruebas de la procedencia de los documentos. Para ello, éstos se almacenan firmados en base de datos, de manera que puedan ser empleados, si es necesario, como prueba de autoría.
- **Confidencialidad**: garantiza que sólo los destinatarios fidedignos de la información pueden acceder a ella.
- **Disponibilidad**: asegura que la información, así como los procedimientos asociados a su generación y uso, puedan ser recuperados en el momento en el que se necesiten, quedando accesibles a los usuarios autorizados de acuerdo al cargo y funciones que desempeñan en la organización.

3.1_ Activos a proteger

Para el aseguramiento de las cinco características arriba mencionadas, existe una serie de activos que el TOE debe proteger, garantizando el cumplimiento de dichas características para cada uno de ellos. Se presenta a continuación la enumeración y descripción de estos activos.

3.1.1_ Activo 01: Claves privadas

Al tratarse de un sistema basado en criptografía de clave pública, el TOE ha de almacenar tanto certificados digitales como sus correspondientes claves privadas asociadas, debiendo éstas últimas ser custodiadas de forma segura.

3.1.2_ Activo 02: Acceso a contraseñas almacenadas en base de datos

Existen varias contraseñas que han de ser almacenadas en base de datos de manera confidencial (es decir, cifradas), y protegidas de lecturas no permitidas. Éstas son las siguientes:

- Contraseñas de los keystores: protegen el acceso a los almacenes de las claves privadas.
- Contraseñas de protección de cada registro del keystore: corresponden a las contraseñas de acceso a cada uno de los registros del almacén.
- Contraseñas de acceso a LDAPs: con ellas se accede al correspondiente repositorio LDAP, en el caso de que el acceso no sea anónimo.
- Contraseñas de métodos de comprobación de revocación: tales como las claves requeridas en los métodos de tipo Database.

3.1.3_ Activo 03: Claves secretas generadas para el cifrado simétrico

El intercambio de la clave secreta utilizada para el cifrado simétrico del canal entre el TOE y el usuario final ha de realizarse de manera segura, garantizando la confidencialidad de la clave intercambiada.

3.1.4_ Activo 04: Integridad de los archivos de auditoría

El TOE cuenta con diferentes componentes de auditoría que registran todas las operaciones realizadas, junto con el usuario responsable de las mismas. Así, por ejemplo, existe un componente de auditoría para la Consola de Administración, otro para el módulo OCSPResponder y un tercero para el resto de servicios. Cada uno de estos componentes de auditoría genera un archivo diferente con las respectivas trazas de las operaciones, detallando la operación efectuada, el autor de la misma y el momento de su realización. De esta forma, garantizando la integridad del

contenido de los archivos de auditoría, se garantiza igualmente la posibilidad de reconstruir la totalidad de la secuencia de operaciones realizadas por el TOE para, en su caso, poder devolverlo a un estado previo.

3.1.5_ Activo 05: Respuestas del TOE a peticiones de aplicaciones cliente a webservices

Cuando se procesa una petición generada por una aplicación cliente, se debe garantizar que no se suplante la identidad del TOE en la respuesta a la misma, así como que su contenido no pueda ser modificado por agentes externos.

3.1.6_ Activo 06: Servicio TOE

El Servicio TOE han de encontrarse siempre disponible y protegido de cualquier amenaza que pueda comprometa la confidencialidad, integridad, autenticidad o disponibilidad de los componentes del TOE. El Servicio TOE ha de encontrarse igualmente libre de invocaciones no autorizadas.

3.1.7_ Activo 07: Peticiones del TOE a OCSPs y TSAs externos

Las peticiones realizadas por el TOE a servidores TSA y servidores OCSP deben ser protegidas de posibles ataques que comprometan su integridad.

3.1.8_ Activo 08: Respuestas de entidades externas al TOE

Las respuestas recibidas por el TOE ante peticiones realizadas a entidades externas tales como servidores OCSP, servidores de Sellado de Tiempo (TSAs) y Autoridades de Certificación, deben ser protegidas de posibles ataques que comprometan su integridad.

3.2_ Amenazas

Cada uno de los activos a proteger del TOE se encuentra expuesto a series de amenazas contra una o a varias de las cinco características de seguridad referidas al comienzo del Capítulo 3_Definición del problema de seguridad del TOE (i.e., autenticación, integridad, no repudio, confidencialidad y disponibilidad). Cada amenaza tiene asociado un agente responsable de la misma, pudiendo dicho agente ser clasificado en uno de los siguientes tipos:

- **Atacante**: en este tipo se incluyen todos aquellos agentes, tanto externos como internos al sistema, que estando o no autorizados a acceder al TOE, intentan realizar acciones con el fin de violar algunas de sus características de seguridad.

- **Administrador de la Base de Datos**: es el responsable de la base de datos del TOE.

- **Agente externo**: bajo esta denominación, se incluye a toda persona o entidad que no desempeñando ningún rol dentro de la organización del TOE ni estando autorizado a su uso, intente cualquier acción para vulnerar alguna de sus características de seguridad.

- **Administrador del registro de ficheros antiguos de auditoría**: esta figura es la del responsable de la administración del soporte físico-lógico donde se archivan periódicamente los ficheros de auditoría, para evitar el desbordamiento del almacén inicial de los mismos.

A continuación se presenta un listado de las amenazas identificadas que pueden afectar a los activos a proteger del TOE. El listado se acompaña de una breve descripción de cada una de ellas, así como de la indicación de sus posibles agentes.

3.2.1_ Amenaza 01: Obtención de las claves privadas

Un atacante podría conseguir el acceso a alguna de las claves privadas de los certificados almacenados si lograse vulnerar las medidas de seguridad que las protegen, comprometiendo de esa forma la confidencialidad de las mismas.

3.2.2_ Amenaza 02: Uso no autorizado de las claves privadas

Un atacante podría utilizar las claves privadas almacenadas y registradas para uso de una determinada aplicación, realizando con ellas operaciones que no le estuvieran permitidas.

3.2.3_ Amenaza 03: Lectura de contraseñas almacenadas en base datos

El administrador de la base de datos podría acceder a la totalidad de las contraseñas almacenadas en ella, puesto que dispone de permiso de lectura para toda la base de datos. Al encontrarse las contraseñas cifradas, el administrador podría descifrarlas si fuese capaz de vulnerar el algoritmo criptográfico de cifrado utilizado para protegerlas.

3.2.4_ Amenaza 04: Obtención de la clave secreta

Durante el proceso de intercambio de la clave secreta, un agente externo podría interceptar la información negociada mediante un ataque de tipo “man-in-the-middle” y posteriormente leer la clave secreta. Si esto ocurriese, el atacante sería capaz de descifrar la información intercambiada entre el TOE y la aplicación usuaria, la cual debería ser confidencial.

3.2.5_ Amenaza 05: Violación de la integridad de los archivos de auditoria

La violación de la integridad de los archivos de auditoría podría no ser detectada una vez que los ficheros de auditoría más antiguos hubiesen sido archivados en un almacén externo gestionado por personal ajeno a la administración del TOE.

3.2.6_ Amenaza 06: Suplantación de identidad en las respuestas de los webservices

Un atacante podría interceptar una petición realizada al TOE por una aplicación cliente y responder a ésta suplantando la identidad del TOE.

3.2.7_ Amenaza 07: Modificación de las respuestas de los webservices

Durante el proceso de envío de la respuesta del TOE a una petición realizada por una aplicación cliente, dicha respuesta podría ser interceptada y modificada por un atacante.

3.2.8_ Amenaza 08: Violación del Servicio TOE

Los intentos por parte de un atacante de realizar operaciones no permitidas (introduciendo parámetros erróneos, realizando ataques de repetición, etc.) capaces de comprometer la confidencialidad, integridad, disponibilidad y/o autenticidad del TOE podrían no ser detectados.

3.2.9_ Amenaza 09: Uso no autorizado del Servicio TOE

Un atacante podría realizar invocaciones a los servicios del TOE sin estar autorizado a ello, comprometiendo con ello la confidencialidad y la disponibilidad del mismo.

3.2.10_ Amenaza 10: Integridad de peticiones realizadas a OCSPs y TSAs

Un atacante podría interceptar y modificar la petición realizada por el TOE a una Autoridad de Sellado de Tiempos (TSA) y/o Servidor de Estados (OCSP) sin que dicha modificación fuese detectada.

3.2.11_ Amenaza 11: Integridad de respuestas de entidades externas al TOE

Un atacante podría interceptar y modificar la respuesta del TOE a una petición de una TSA, un servidor OCSP o una Autoridad de Certificación sin que dicha modificación fuese detectada.

3.3_ Mapeo de activos y amenazas

A continuación se presenta una tabla relacionando cada uno de los activos a proteger del TOE con las amenazas que les pueden afectar, así como con los respectivos tipos de agentes de las mismas.

Activo a proteger	Amenazas al activo	Tipo de agente
Activo 01: Claves privadas	Amenaza 01: Obtención de las claves privadas Amenaza 02: Uso no autorizado de las claves privadas	Atacante
Activo 02: Acceso a contraseñas almacenadas en base de datos	Amenaza 03: Lectura de contraseñas almacenadas en base datos	Administrador de la Base de Datos
Activo 03: Claves secretas generadas para el cifrado simétrico	Amenaza 04: Obtención de la clave secreta	Agente externo
Activo 04: Integridad de los archivos de auditoría	Amenaza 05: Violación de la integridad de los archivos de auditoria	Administrador del registro de ficheros antiguos de auditoría

Activo a proteger	Amenazas al activo	Tipo de agente
Activo 05: Respuestas a peticiones de aplicaciones cliente a webservices	Amenaza 06: Suplantación de identidad en las respuestas de los webservices Amenaza 07: Modificación de las respuestas de los webservices	Atacante
Activo 06: Servicio TOE	Amenaza 08: Violación del Servicio TOE Amenaza 09: Uso no autorizado del Servicio TOE	Atacante
Activo 07: Peticiones del TOE a OCSPs y TSAs externos	Amenaza 10: Integridad de peticiones realizadas a OCSPs y TSAs	Atacante
Activo 08: Respuestas de entidades externas al TOE	Amenaza 11: Integridad de respuestas de entidades externas al TOE	Atacante

Tabla 03 – Mapeo de activos y amenazas

3.4_ Políticas de seguridad organizacional

En esta sección se abordan las políticas de seguridad organizacional que deben aplicarse para asegurar el correcto funcionamiento del TOE.

3.4.1_ Política 01: Documentación guía de instalación y uso

En el momento de la entrega del TOE se proporcionará la documentación guía de instalación y de uso necesaria para que el propietario del TOE sepa cómo instalarlo y gestionarlo de modo seguro. La documentación será inequívoca y contendrá la suficiente información para garantizar la instalación y operación seguras del TOE.

3.4.2_ Política 02: Aplicación de procedimientos por administrador TOE

El administrador del sistema seguirá todos los procedimientos y normas establecidas en la documentación guía que se le entregará, definiendo y

manteniendo los permisos de acceso establecidos para los archivos críticos del TOE. Éstos son los archivos de auditoría, las trazas de eventos del servidor de aplicaciones (en los que podría aparecer información sensible acerca de las conexiones a base de datos) y el archivo en el que se encuentra la clave secreta con la que se cifran las contraseñas almacenadas.

3.4.3_ Política 03: Revisión de auditorías

Existirá un auditor interno del TOE, diferente del administrador del sistema, que será el encargado de revisar periódicamente el HMAC de cada archivo de auditoria, para comprobar así que dichos ficheros no han sido modificados. Además, el auditor interno del TOE asegurará que los datos auditados se archivan regularmente, para de esta forma prevenir posibles problemas de sobrecarga en los almacenes de registros de auditoría.

3.4.4_ Política 04: Cualificación de los usuarios del TOE

Los usuarios del TOE deberán estar suficientemente cualificados para realizar sus funciones. El propietario del TOE proporcionará a los usuarios y administradores del mismo el entrenamiento y formación necesarios para que adquieran el conocimiento y la experiencia requeridos para la utilización del sistema de manera segura.

3.4.5_ Política 05: Disposición de datos de usuario y privilegios de acceso

El propietario del TOE garantizará la confidencialidad y protección de los datos de autenticación de los usuarios del mismo. Ningún usuario podrá acceder al sistema sin acreditarse previamente con ellos. Asimismo, en el momento en el que un usuario sea dado de alta se le asignará un rol, en función del cual tendrá unos permisos asociados para realizar determinadas acciones. El propietario del TOE habrá de cerciorarse de que estas acciones corresponden realmente con aquellas operaciones para las que el usuario esté realmente autorizado.

Asimismo, el propietario del TOE deberá gestionar los keystores definidos para almacenar las claves privadas utilizadas para firmar las peticiones o para procedimientos de autenticación, de manera que las contraseñas de acceso a los almacenes estén libres de accesos indebidos y almacenadas en un lugar seguro. Además, estos keystores deben ser de tipo JCEKS para que de esta forma las claves privadas en ellos depositadas puedan almacenarse cifradas.

El propietario del TOE se asegurará igualmente de que existan procedimientos apropiados para asegurar la destrucción de los datos de autenticación, así como la eliminación de los privilegios asociados, una vez que

el acceso haya sido eliminado o bien en el caso de que las reglas de control de acceso hayan sido redefinidas. Esto se aplica tanto a los administradores como a los usuarios del TOE.

3.4.6_ Política 06: Restricción de acceso al TOE

El propietario del TOE será el responsable de asignar las debidas restricciones de acceso al mismo para cada una de las aplicaciones registradas en el sistema. De esta forma, se definirán los usuarios autorizados a acceder al TOE mediante cada aplicación. Asimismo, deberán asignarse restricciones de acceso a los módulos OCSPResponder y TSAServer.

3.4.7_ Política 07: Seguimiento de política de seguridad

Existe una Política de Seguridad Organizacional del Sistema, en la que se identifican y documentan adecuadamente los riesgos y amenazas al sistema, así como los objetivos de seguridad deseados, proporcionando unas pautas a seguir para garantizar los servicios y propiedades de seguridad declarados. Asimismo, en dicha política se especifica un plan de actuación ante posibles contingencias o incidentes no deseados. Todos los usuarios del TOE, y especialmente los administradores del mismo, deberán estar al corriente de dicha política de seguridad organizacional y cumplir los requisitos en ella marcados.

3.5_ Hipótesis de uso seguro

Para garantizar el uso seguro del TOE, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

3.5.1_ Hipótesis 01: Administrador del sistema confiable

Se supone que el equipo en el que se encuentran instalados tanto los archivos de propiedades utilizados para la configuración del sistema como los archivos de servidor en los que puede aparecer información sensible (por ejemplo, la relativa a las conexiones a bases de datos) tendrá su acceso restringido, de forma que el administrador del sistema será la única entidad que dispondrá de los permisos necesarios para acceder a los mencionados archivos. Además, se supone que dicho administrador no actuará de manera malintencionada ni proporcionará permisos de acceso indebidos.

3.5.2_ Hipótesis 02: Administrador de la auditoría

Se supone que existirá un administrador de archivos de auditoría que revisará periódicamente dichos archivos en busca de posibles intentos de ataque al TOE. En el caso de encontrar algún intento de ataque, el administrador de archivos de auditoría realizará las acciones que defina el usuario del producto.

3.5.3_ Hipótesis 03: Administrador de la base de datos

Se supone que el administrador de la base de datos será confiable, que no otorgará a la misma permisos de acceso indebidos (ni de lectura ni de escritura), así como que mantendrá en secreto los datos de las conexiones establecidas.

3.5.4_ Hipótesis 04: Usuarios del TOE responsables

El personal que administra, gestiona y utiliza el Objeto de Evaluación será suficientemente competente para desarrollar sus funciones, de forma que no realizará un uso incorrecto del TOE, a la vez que respetará la seguridad y confidencialidad de los datos sensibles contenidos en el mismo. Para ello, se supone que dicho personal poseerá el conocimiento necesario acerca de principios básicos de seguridad computacional. Asimismo, se presume que dicho personal leerá, entenderá y seguirá la documentación que le sea relevante para el desempeño de sus funciones.

3.5.5_ Hipótesis 05: Datos de usuario

El personal que administra, gestiona y utiliza el TOE será suficientemente responsable para evitar que sus contraseñas de acceso sean accesibles a personas o entidades no autorizadas. Además, dicho personal deberá asegurarse de poder disponer de estas contraseñas cuando éstas se le requieran para llevar a cabo la autenticación. Lo mismo habrá de ser tenido en cuenta para el caso de los certificados digitales con los que se realizan autenticaciones de cliente en la consola. Respecto a las claves privadas almacenadas en los keystores de aplicaciones cliente, se supone que el personal encargado de gestionar los keystores será lo suficientemente responsable como para mantener las contraseñas de acceso a los mismos libres de accesos indebidos y almacenadas en lugar seguro.

4_ Objetivos de seguridad

4.1_ Objetivos de seguridad para el TOE

Se definen a continuación los objetivos de seguridad que son satisfechos por el TOE. Dichos objetivos se plantean para hacer frente a las posibles amenazas identificadas. Cada amenaza es cubierta por al menos uno de los objetivos de seguridad que se recogen a continuación.

4.1.1_ Objetivo 01: Confidencialidad de claves privadas de certificados

Se garantizará la confidencialidad de las claves privadas correspondientes a los certificados digitales mediante su almacenamiento en keystores de tipo JCEKS. Estos almacenes de claves desarrollados por la plataforma Java Sun protegen el acceso a las claves mediante dos contraseñas: una global, correspondiente al keystore y otras correspondientes a cada uno de los registros del mismo en los que se almacena una clave. Además, este tipo de almacenes guarda las claves privadas cifradas de manera automática, de forma que en el caso de que se consiga acceder a las mismas, estén protegidas de lecturas no autorizadas.

4.1.2_ Objetivo 02: Confidencialidad de contraseñas almacenadas en BD

Las contraseñas de protección de acceso a los keystores, de protección de cada registro de los mismos, de acceso a los LDAPs, así como las implicadas en los métodos de consulta de revocación (como, por ejemplo, las de métodos Database), se almacenarán cifradas en la base de datos. Para ello, se utilizarán algoritmos de cifrado robustos, basados en criptografía de clave simétrica, junto con una clave de tamaño mínimo de 128 bits. La clave privada con la que se cifran las contraseñas será guardada debidamente en secreto para protegerlas de lecturas no autorizadas, garantizando así su confidencialidad.

4.1.3_ Objetivo 03: Cifrado de clave secreta para cifrado simétrico

La clave secreta generada para el cifrado simétrico será cifrada mediante algoritmos basados en criptografía de clave pública para garantizar su transmisión en modo seguro. De esta manera se protegerá la confidencialidad de la misma, en el caso de que alguien intercepte su envío.

4.1.4_ Objetivo 04: Registro de las peticiones realizadas

Se efectuará un registro de todas las peticiones realizadas a los servicios publicados por el TOE en el archivo de auditoría que corresponda. De esta manera, cuando un administrador autorizado los revise, será capaz de identificar los posibles ataques acontecidos.

4.1.5_ Objetivo 05: Firma y verificación de las respuestas de los webservices

Las respuestas del TOE a peticiones realizadas a sus servicios web por aplicaciones cliente se firmarán digitalmente. Una vez en el componente cliente del TOE estas respuestas se verificaránpara de esta forma garantizar a la entidad invocante la integridad y autenticidad de las mismas.

4.1.6_ Objetivo 06: Control de acceso

Se asociarán restricciones de acceso para cada una de las aplicaciones registradas en el sistema, que delimiten los usuarios autorizados a acceder al TOE mediante dichas aplicaciones.

4.1.7_ Objetivo 07: Detección de modificaciones de archivos de auditoría

Se asegurará la detección de la violación de la integridad de los archivos de auditoría mediante el almacenamiento de los correspondientes HMACs.

4.1.8_ Objetivo 08: Firma de peticiones a TSAs y OCSPs externos

Las peticiones del TOE a Autoridades de Sellado de Tiempos (TSAs) y servidores OCSP para solicitar un sello temporal o realizar consultas relacionadas con el estado de revocación de certificados serán firmadas digitalmente por el TOE.

4.1.9_ Objetivo 09: Verificar firma de respuestas de entidades externas

Las posibles respuestas recibidas por el TOE procedentes de entidades externas (i.e., Autoridades de Certificación, Autoridades de Sellado de Tiempos o Servidores OCSP) habrán de estar firmadas digitalmente por la entidad emisora.

4.2_ Objetivos de seguridad para el entorno

Los objetivos de seguridad para el entorno que se refieren a continuación se plantean para contrarrestar las amenazas y/o hacer cumplir las políticas de seguridad organizacional que no hayan sido cubiertas, bien por los objetivos de seguridad del TOE o bien por las hipótesis de uso seguro del mismo.

4.2.1_ Objetivo entorno 01: Acceso restringido

El entorno operacional del TOE debe permitir el acceso al TOE o partes del TOE únicamente al personal autorizado al mismo.

4.2.2_ Objetivo entorno 02: Formación

El entorno operacional del TOE debe asegurar que todos los usuarios humanos del TOE (i.e., personas físicas) hayan recibido previamente la formación e instrucción adecuadas para permitirles trabajar con el TOE siguiendo todos los procedimientos que impliquen el funcionamiento seguro del mismo.

4.2.3_ Objetivo entorno 03: Proporcionar todos los entregables necesarios

El entorno operacional del TOE debe garantizar que la entrega del mismo se haga acompañada de toda la información y documentación guía necesarias para una correcta instalación y uso del TOE.

4.2.4_ Objetivo entorno 04: Revisión de auditorías

El entorno operacional del TOE debe garantizar la realización de auditorías periódicas que permitan la detección de posibles intentos de violación al TOE, para de esta forma poder tomar las medidas oportunas, definidas por el propietario del TOE, en el caso de que dichos intentos sean identificados.

4.2.5_ Objetivo entorno 05: Formación en política de seguridad

En el entorno operacional del TOE debe existir un responsable encargado de formar a los administradores y usuarios del mismo, para asegurarse de que éstos conocen las políticas de seguridad del TOE y de que las aplican.

4.2.6_ Objetivo entorno 06: Gestión de los datos de autenticación

El entorno operacional del TOE debe garantizar la confidencialidad de los datos de autenticación de los distintos usuarios, así como la destrucción de los mismos en caso de su redefinición.

Asimismo, el entorno operacional del TOE debe garantizar que las restricciones de acceso no tendrán asociados certificados cuya seguridad pueda haberse visto comprometida.

4.3_ Razonamiento de objetivos de seguridad

En esta sección se demuestra que el problema de seguridad planteado es completo y su solución también lo es, relacionando los objetivos de seguridad definidos con las amenazas, políticas e hipótesis establecidas.

En un primer lugar se relacionan los objetivos de seguridad del TOE con las amenazas que resuelven y las políticas a aplicar para su consecución. Tras cada amenaza, política o hipótesis aparece una breve explicación que reseña su implicación con el objetivo con el que se le relaciona. El resultado se muestra en la Tabla 04 – Razonamiento de los objetivos de seguridad.

Objetivos TOE	Amenazas	Políticas
Objetivo 01: Confidencialidad de claves privadas de certificados	Amenaza 01: Obtención de las claves privadas Un usuario no autorizado no podrá acceder a las claves privadas al estar su acceso protegido	
Objetivo 02: Confidencialidad de contraseñas almacenadas en BD	Amenaza 03: Lectura de contraseñas almacenadas en base datos Al cifrarse las contraseñas. el administrador de la base de datos no podrá leerlas, puesto que no estará en posesión de la clave de cifrado	

Objetivos TOE	Amenazas	Políticas
Objetivo 03: Cifrado de clave secreta para cifrado simétrico	Amenaza 04: Obtención de la clave secreta Al cifrarse la clave secreta transmitida, alguien que no tenga la clave privada de descifrado no podrá acceder a ella	
Objetivo 04: Registro de las peticiones realizadas	Amenaza 08: Violación del Servicio TOE Se registran todas las peticiones quedando así también reflejados los posibles ataques	
Objetivo 05: Firma y verificaciónde las respuestas de los webservices	Amenaza 06: Suplantación de identidad en las respuestas de los web-services Al firmarse las respuestas de los webservices se garantiza que el TOE es el emisor ---------- Amenaza 07: Modificación de las respuestas de los webservices Al firmarse las respuestas de los webservices se garantiza la integridad de las mismas	

Objetivos TOE	Amenazas	Políticas
Objetivo 06: Control de acceso	Amenaza 02: Uso no autorizado de las claves privadas Al controlar el acceso, sólo usuarios autorizados podrán utilizar las claves privadas registradas --- Amenaza 09: Uso no autorizado del Servicio TOE Al controlar el acceso, sólo usuarios autorizados podrán realizar invocaciones al Servicio TOE	
Objetivo 07: Detección de modificaciones de archivos de auditoría	Amenaza 05: Violación de la integridad de los archivos de auditoria Al almacenarse las peticiones junto con su HMAC (encadenado con el HMAC anterior), se garantiza que ningún usuario con permisos de escritura en la máquina en la que se almacenan los ficheros de auditoría antiguos podrá modificarlos violando su integridad, sin que el revisor de auditorías detecte esos cambios	
Objetivo 08: Firma de peticiones a TSAs y OCSPs externos	Amenaza 10: Integridad de peticiones realizadas a OCSPs y TSAs Al firmarse las peticiones realizadas por el TOE se garantiza que las entidades receptoras serán capaces de detectar si éstas han sido modificadas	

Objetivos TOE	Amenazas	Políticas
Objetivo 09: Verificar firma de respuestas de entidades externas	Amenaza 11: Integridad de respuestas de entidades externas al TOE Al firmarse las respuestas realizadas por entidades externas al TOE se garantiza que el TOE será capaz de detectar cualquier modificación realizada al verificar siempre esta firma antes de dar como válida la información recibida.	

Tabla 04 – Razonamiento de los objetivos de seguridad del TOE

Para los objetivos de entorno se realiza la misma asociación, salvo que además se relacionan las suposiciones de entorno que tienen que darse para que los objetivos puedan alcanzarse. El resultado se muestra en la Tabla 05 – Razonamiento de los objetivos de seguridad del entorno.

Objetivos entorno	Amenazas	Hipótesis	Políticas
Objetivo entorno 01: Acceso restringido			Política 05: Disposición de datos de usuario y privilegios de acceso Mediante la restricción de acceso para cada aplicación (objetivo), aseguramos el cumplimiento de la política de restricción de acceso evitando que usuarios que no cuenten con los suficientes privilegios podrán acceder al TOE. --- Política 06: Restricción de acceso al TOE Al asociarse restricciones de acceso sólo personal autorizado podrá acceder al TOE a través de aplicaciones.

Objetivos entorno	Amenazas	Hipótesis	Políticas
Objetivo entorno 02: Formación		Hipótesis 01: Administrador del sistema confiable Hipótesis 02: Administrador de la auditoría Hipótesis 03: Administrador de la base de datos Hipótesis 04: Usuarios del TOE responsables Hipótesis 05: Datos de usuario --- Al haber recibido la formación necesaria se garantiza que ningún miembro usuario o administrador del TOE del TOE realizará acciones malintencionadas contrarias a la formación recibida	Política 04: Cualificación de los usuarios del TOE Al estar convenientemente formado, se garantiza que los usuarios del TOE estarán convenientemente cualificados en todo momento. --- Política 05: Disposición de datos de usuario y privilegios de acceso Al haber recibido la formación adecuada, los usuarios del TOE responsables de autorizar el acceso a otros usuarios no concederán permisos indebidos y gestionarán los datos de estos adecuadamente.
Objetivo entorno 03: Proporcionar todos los entregables necesarios			Política 01: Documentación guía de instalación y uso Al haberse entregado toda la documentación guía necesaria, el propietario del TOE será capaz de instalar y utilizar el TOE de un modo seguro.

Objetivos entorno	Amenazas	Hipótesis	Políticas
Objetivo entorno 04: Revisión de auditorías	Amenaza 05: Violación de la integridad de los archivos de auditoria Al revisarse periódicamente las auditorías se detectarán las violaciones de integridad si las hay. --- Amenaza 08: Violación del Servicio TOE Al revisarse periódicamente las auditorías se encontrarán, si los hay, los posibles ataques	Hipótesis 02: Administrador de la auditoría Al revisarse periódicamente los ficheros de auditoría se garantiza que cualquier anomalía existente en ellos será detectada por el administrador de los mismos y que éste ejecutará las acciones definidas para cada caso.	Política 03: Revisión de auditorías Al revisarse periódicamente los ficheros de auditorías, se detectará siempre cualquier modificación ocurrida en ellos.

Objetivos entorno	Amenazas	Hipótesis	Políticas
Objetivo entorno 05: Formación en política de seguridad		Hipótesis 01: Administrador del sistema confiable Al haber recibido la formación necesaria en materia de política de seguridad del TOE, se garantiza que el administrador del sistema actuará de acuerdo a ella y no realizará acciones no acordes a esta política. --- Hipótesis 02: Administrador de la auditoría Al haber recibido la formación necesaria en política de seguridad, se garantiza que el administrador de las auditorías será capaz de detectar cualquier anomalía y que siempre ejecutará las acciones adecuadas --- Hipótesis 03: Administrador de la base de datos Al haber recibido la formación en política de seguridad necesaria, se garantiza que el usuario de la Base de datos actuará de acuerdo a ella no dando accesos indebidos ni publicando los datos de las conexiones. --- Hipótesis 04: Usuarios del TOE responsables Al haber recibido todos los usuarios y administradores del TOE la formación necesaria previa al uso del mismo, estarán capacitados para realizar sus funciones correctamente.	Política 02: Aplicación de procedimientos por administrador TOE Al estar convenientemente formado en materia de seguridad, el administrador del TOE aplicará los procedimientos convenientes en cada ocasión. --- Política 04: Cualificación de los usuarios del TOE Al estar convenientemente formado en materia de seguridad, se garantiza que los usuarios del TOE estarán convenientemente cualificados en todo momento. --- Política 07: Seguimiento de política de seguridad Al estar convenientemente formados en la política de seguridad a seguir, los usuarios del TOE serán siempre capaces de actuar de acuerdo a ella.

Objetivos entorno	Amenazas	Hipótesis	Políticas
Objetivo entorno 06: Gestión de los datos de autenticación		Hipótesis 03: Administrador de la base de datos Al garantizarse la confidencialidad de los datos de autenticación se asegura que el administrador de la base de datos no actuará contrario a su labor extrayendo datos sin autorización o permitiendo conexiones indebidas	Política 05: Disposición de datos de usuario y privilegios de acceso Al estar convenientemente gestionados los datos de usuarios del TOE, se garantiza que sólo personal autorizado accederá a él.

Tabla 05 – Razonamiento de los objetivos de seguridad del entorno

Como se puede observar, todos los requisitos están relacionados con alguna amenaza o política, quedando patente que todos ellos son necesarios. Igualmente, todas las amenazas, políticas e hipótesis tienen relación con algún objetivo. De esta manera, se concluye que la solución al problema de seguridad planteado es una solución completa.

5_ Requisitos de seguridad

5.1_ Requisitos funcionales de seguridad

5.1.1_ Relación de objetos

Para la formulación de los requisitos funcionales de seguridad, se consideran como objetos los siguientes activos del TOE:

- Claves privadas
- Acceso a contraseñas almacenadas en base de datos
- Claves secretas generadas para el cifrado simétrico
- Integridad de los archivos de auditoría
- Respuestas a peticiones de aplicaciones cliente
- Servicio TOE
- Peticiones del TOE a entidades externas
- Respuestas de entidades externas al TOE

5.1.2_ Relación de sujetos y sus atributos

Para la formulación de los requisitos funcionales de seguridad, se consideran los siguientes sujetos:

- **Aplicaciones usuarias**: Aplicaciones usuarias que acceden a los servicios de ASF. El acceso se lleva a cabo a través de servicios web publicados o bien realizando peticiones HTTP cuando así sea requerido. Sus atributos de seguridad son los que se indican a continuación, dependiendo de qué tipo de invocación realicen:
    - Acceso a un Webservice:
        - La identidad de la aplicación invocante: código que identifica la aplicación que realiza la invocación.
        - Dirección IP desde la que se realiza la invocación.

- La firma de la petición efectuada.

Además, en caso de que se supere el control de acceso al Webservice y se permita la ejecución de éste, si el método que se está solicitando corresponde a uno de firma o descifrado, se ven involucrados también los siguientes atributos de seguridad:

- La identidad de la aplicación y de la operación para la que se solicita el servicio.
- El alias del certificado que va a ser utilizado en esa operación. En este último caso, en el de descifrado, este atributo es sólo necesario si no se está adjuntando el certificado en los parámetros enviados.

o Petición por HTTP:

- Dirección IP desde la que se realiza la invocación.
- La firma de la petición efectuada.

- **Usuarios locales**: Los usuarios de la consola. Su único atributo de seguridad es el identificador de rol, que puede tomar los valores siguientes: <administrador, super-administrador>.

5.2_ Requisitos de control de acceso

5.2.1_ 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_ASF] on [assignment:

- Lista de objetos:
  - Claves privadas
  - Acceso a contraseñas almacenadas en base de datos
  - Claves secretas generadas para el cifrado simétrico
  - Respuestas a peticiones de aplicaciones cliente
  - Servicio TOE
  - Peticiones del TOE a entidades externas

- Respuestas de entidades externas al TOE

- Lista de sujetos:
  - Aplicaciones usuarias
  - Usuarios locales de la consola

] 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.

5.2.2_ FDP_ACF.1 Security attribute based access control

Dependencies: FDP_ACC.2 Complete access control
FMT_MSA.3 Static attribute initialisation

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

- Objetos:
  - Claves privadas
  - Acceso a contraseñas almacenadas en base de datos
  - Claves secretas generadas para el cifrado simétrico
  - Respuestas a peticiones de aplicaciones cliente
  - Servicio TOE
  - Peticiones del TOE a entidades externas
  - Respuestas de entidades externas al TOE
- Atributos de objetos: ninguno.
- Sujetos:
  - Aplicaciones usuarias
    - Atributos para invocación a un Webservice:
      - La identidad de la aplicación invocante
      - La dirección IP desde la que se realiza la invocación.
      - La firma de la petición efectuada

    Además, en caso de que se supere el control de acceso al Webservice y se permita la ejecución de éste, si el método que solicitado corresponde a uno de firma o descifrado, se ven involucrados también los siguientes atributos:

- La identidad de la aplicación y de la operación para la que se solicita el servicio.
- El alias del certificado que va a ser utilizado en esa operación. En este último caso, en el de descifrado, este atributo es sólo necesario si no se está adjuntando el certificado en los parámetros enviados.

▪ Atributos para petición HTTP:

- La dirección IP desde la que se realiza la invocación.
- La firma de la petición efectuada

o Usuarios locales de la consola

▪ Atributos:

- Identidad de rol <Admin, Super-admin>

].

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 <Aplicaciones usurias>

o A.1) Invocación a un Webservice:

Al recibir el TOE una petición a uno de sus servicios web publicados por parte de una entidad externa, éste comprueba que la aplicación invocante existe en el sistema. Si existe, pasa a verificar las restricciones de acceso que han debido de ser definidas previamente desde la consola de administración. En caso de que así sea, habrá que verificar que la petición venga firmada con alguno de los certificados asociados para una de las restricciones registradas para esa aplicación, pues significa que sólo se permite el acceso para peticiones realizadas con dichos certificados.

Si todas estas comprobaciones dan un resultado positivo el acceso le será permitido al servicio del TOE (objeto definido para el que se controla el acceso), el cual, para desarrollar las acciones correspondientes para construir la respuesta que se envía al cliente (objeto "Respuestas a peticiones de aplicaciones cliente") y, dependiendo del método solicitado, puede acceder a los siguientes objetos:

▪ Activo 02. Acceso a contraseñas almacenadas en base de datos: Si se está solicitando un servicio que necesita de un método de comprobación de revocación por database o de un LDAP, obtiene la contraseña para la conexión a esa base de datos o a ese LDAP, de la base de datos.

▪ Activo 06: Servicio TOE. Cada petición que realiza una aplicación usuaria y que supere el control de acceso aquí definido, accede a un servicio del TOE.

▪ Activo 07: Peticiones del TOE a OCSPs y TSAs externos. Si la petición realizada al TOE solicita la comprobación

de revocación a un servidor OCSP externo o un sello de tiempo a una TSA, el TOE ha de realizar la correspondiente petición al servidor involucrado.

- Activo 08: Respuestas de entidades externas al TOE. En caso de que la petición de la aplicación supusiera que el TOE requiriese del servicio de una entidad externa, tras realizar la petición correspondiente, el TOE esperaría la respuesta de la misma antes de dar una respuesta a la aplicación invocante.

Si el control acceso ha sido superado y el servicio solicitado corresponde a uno de cifrado o descifrado, se ha de superar una de las siguientes reglas dependiendo del servicio:

- A.1.1) Servicio de verificación:

  Si la invocación es a un Webservice cuya funcionalidad es la de verificar, se comprobará que la aplicación invocante existe en el sistema. En caso de que así sea, se verificará que existe una operación asociada a la misma con ese código de operación y definida como una operación del mismo tipo que el servicio. Es decir, al estarse realizando una petición a un servicio de verificación, la operación para esa aplicación debe estar definida como una de verificación.

- A.1.2) Servicio de cifrado:

  En el caso de que la petición sea a un servicio de cifrado, se realizarán las mismas comprobaciones en cuanto a los atributos de identificador de aplicación y de operación, pero teniendo que estar definidas como operación de cifrado. Además, si se está indicando el alias del certificado que se quiere utilizar para cifrar, se ha de verificar que está asociado a esa aplicación-operación, permitiéndose su acceso en caso que lo esté y denegándose en caso contrario. Si, por el contrario, no se indica el alias del certificado con el que se desea cifrar sino que éste se adjunta, se han de realizar dos comprobaciones para permitir cifrar.

- A.1.3) Servicio de firma o descifrado:

  Si la invocación es a un Webservice cuya funcionalidad es firmar o descifrar, se comprobará que la aplicación invocante existe en el sistema. En caso de que así sea, se verificará que existe una operación asociada a la misma con ese código de operación y definida como una operación del mismo tipo que el servicio. Es decir, al estarse realizando una petición a un servicio de firma, la operación para esa aplicación debe estar definida como una operación de firma. En caso del descifrado sería de descifrado. Si estas comprobaciones resultan satisfactorias, queda comprobar si está permitido emplear el certificado correspondiente al alias enviado como parámetro para ese certificado. En caso afirmativo, se autoriza el acceso al certificado para la aplicación que solicita ese servicio.

  Un caso especial dentro de esta regla de acceso corresponde a los servicios de descifrado que en lugar de incluir el alias del certificado registrado en el sistema para descifrar, adjuntan el certificado. En este caso, la segunda parte de esta comprobación, la correspondien-

te al certificado no se realiza y, en su lugar, se comprueba que el certificado enviado ha sido emitido por una de las Autoridades de Certificación consideradas de confianza para esa aplicación-operación.

La totalidad los servicios anteriormente indicados ha de superar el control de acceso. Posteriormente, todos a excepción del servicio de descifrado en el que se adjunta el certificado para descifrar, han de acceder a los siguientes activos (en adición de a los activos permitidos para todos los servicios autorizados) para poder realizar sus acciones asociadas:

- Activo 01: Claves privadas de los certificados de los almacenes. Una aplicación, al solicitar la realización de una operación de firma, cifrado, descifrado o cualquier otra que involucre el uso de una clave privada que está autorizada a usar, accede a ella para utilizarla en la operación pero no puede obtenerla en ningún momento.

- Activo 02: Acceso a contraseñas almacenadas en base de datos. Cuando una entidad externa va a usar una clave privada a la que está autorizada, obtiene previamente las claves correspondientes al keystore y al registro donde se encuentra la clave privada en cuestión.

o A.2) Petición por HTTP al OCSPResponder:

Cuando el servidor OCSPResponder recibe una petición HTTP de una aplicación externa comprueba que está autorizada a ello. Para eso, el TOE verifica que la firma de la petición es realizada con un certificado asociado a alguna de las restricciones de acceso impuestas al OCSPResponder. Si esta verificación resulta satisfactoria el acceso le será permitido al servicio del TOE (objeto definido para el que se controla el acceso), el cual, para desarrollar las acciones correspondientes para construir la respuesta que se envía al cliente (objeto "Respuestas a peticiones de aplicaciones cliente") y, dependiendo del método solicita ha de acceder a los siguientes objetos:

- Activo 01: Claves privadas de los certificados de los almacenes. Al tener que firmar el OCSPResponder la respuesta a la aplicación ha de acceder al keystore para obtener la clave privada con el que la firmará.

- Activo 02: Acceso a contraseñas almacenadas en base de datos. Al firmar la respuesta a la aplicación y tener que acceder a la clave privada con la que realizará la firma, ha de acceder previamente a las contraseñas que protegen tanto el keystore donde se encuentra almacenada como del correspondiente registro del mismo, estando contenidas ambas en la base de datos cifradas. En caso de que la petición realizada al OCSPResponder, involucre a su vez que éste deba hacer una solicitud de comprobación de revocación a una base de datos o a un servidor de directorios LDAP, ha de acceder también a la contraseña almacenada en base de datos que protege el acceso a cada uno de ellos. Similar situación se da cuando la petición que ha de realizar el TOE a raíz de una solicitud de la aplicación es a un servidor OCSP externo. En este caso ha de obtener de la base de datos las contraseñas (tanto la de protección del almacén como la del registro individual) que protegen la clave privada con la que ha de firmar la petición.

- Activo 06: Servicio TOE. Cada petición que realiza una aplicación usuaria y que supere el control de acceso aquí definido, accede a un servicio del TOE.

- Activo 07: Peticiones del TOE a OCSPs y TSAs externos. Si la petición realizada al TOE solicita la comprobación de revocación a un servidor OCSP externo,, el TOE ha de realizar la correspondiente petición al servidor involucrado firmando la misma.

- Activo 08: Respuestas de entidades externas al TOE. En caso de que la petición de la aplicación involucrara que el TOE requiriera del servicio de una entidad externa, tras realizar la petición correspondiente, el TOE espera la respuesta del mismo antes de dar una respuesta a la aplicación invocante.

o A.3) Petición por HTTP al TSAServer

Cuando el servidor TSAServer recibe una petición HTTP de una aplicación externa comprueba que está autorizada a ello. Para eso, el TOE verifica que la firma de la petición es realizada con un certificado asociado a una de estas restricciones. Si esta verificación resulta satisfactoria le será permitido al servicio del TOE (objeto definido para el que se controla el acceso), el cual, para desarrollar las acciones correspondientes para construir la respuesta que se envía al cliente (objeto "Respuestas a peticiones de aplicaciones cliente") y, dependiendo del método ha de acceder a los siguientes objetos:

- Activo 01: Claves privadas de los certificados de los almacenes. Al tener que firmar el TSAServer la respuesta a la aplicación ha de acceder al keystore para obtener la clave privada del certificado con el que la firmará.

- Activo 02: Acceso a contraseñas almacenadas en base de datos. Al firmar la respuesta a la aplicación y tener que acceder a la clave privada con la que realizará la firma, ha de acceder previamente a las contraseñas que protegen tanto el keystore donde se encuentra almacenada como del correspondiente registro del mismo, estando contenidas ambas en la base de datos cifradas.

- Activo 06: Servicio TOE. Cada petición que realiza una aplicación usuaria y que supere el control de acceso aquí definido, accede a un servicio del TOE.

- Caso de los usuarios locales de la consola

El control de acceso definido para un usuario local de la consola está basado en el atributo que indica el rol que desempeña. Para superarlo ha de tener asignado el rol de administador o de superadministrador (obteniendo uno de estos valores en el momento de su autenticación). Pueden acceder al siguiente activo:

- Activo 02: Acceso a contraseñas almacenadas en base de datos. Al insertar un nuevo registro en un keystore, lo que ocurre en el momento de registrar un nuevo certificado en el TOE, el usuario local de la consola accede a la contraseña del keystore en lectura. La contraseña propia a cada registro es insertada en el momento del registro del certificado, con lo cual, estos usuarios no acceden a este tipo de contraseñas cuando están almacenadas en base de datos nunca. A las otras contraseñas almacenadas en base de datos, las correspondientes a los métodos de

comprobación de revocación por Database, o las asociadas a un LDAP, los usuarios locales de la consola acceden en el momento en que se muestran los datos de uno de estos métodos o del LDAP en cuestión respectivamente, pudiendo modificarlas.

].

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].

5.2.3_ FMT_MSA.1 Management of security attributes

Dependencies: FDP_ACC.2 Complete access control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Apps The TSF shall enforce the [assignment:CONTROL ACCESO_ASF] to restrict the ability to [selection: modify, delete] the security attributes [assignment: atributos de los sujetos entidades externas] to [assignment: administrador].

FMT_MSA.1.1/Users The TSF shall enforce the [assignment:CONTROL_ACCESO_ASF] to restrict the ability to [selection: modify, delete] the security attributes [assignment: atributos de los sujetos usuarios] to [assignment: super-administrador].

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.2.4_ FMT_MSA.3 Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment:CONTROL_ACCESO_ASF] to provide [selection, choose one of: valores nulos]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: administrador, super-administrador] to specify alternative initial values to override the default values when an object or information is created.

5.2.5_ FMT_SMR.1 Security roles

Dependencies: **FIA_UID.1 Timing of identification**

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: administrador, super-administrador].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.6_ FMT_SMF.1 Specification of Management Functions

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: edición de las reglas de acceso a los activos, gestión de los administradores].

5.2.7_ 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.

5.2.8_ 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.

5.2.9_ FIA_UAU.5 Multiple authentication mechanisms

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [assignment: Autenticación por nombre de usuario y contraseña, Autenticación por certificado] to support user authentication.

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

- Por nombre de usuario y contraseña: el usuario debe introducir su nombre de usuario y contraseña asociada. Si el usuario ha sido identificado previamente (el nombre de usuario existe), se calcula el hash de la contraseña y se compara con el hash almacenado en base de datos de la contraseña con la que se registró como usuario autorizado ese usuario. En caso de que estos dos coincidan, se le permitirá el acceso a la consola de administración, asignándole a la vez el rol correspondiente, administrador o super-administrador, según qué tipo de usuario se le hubiese asignado en el momento de darle de alta.

- Por certificado: para autenticarse mediante la presentación de un certificado, la parte pública del mismo debe haber sido registrada para la

identificación de un usuario en la consola previamente. Tras esto, el proceso de autenticación se realiza a través del proceso conocido como desafío: la consola envía al cliente una frase para que la firme con la clave privada correspondiente a la parte privada del certificado en cuestión. Una vez firmada, el cliente la envía y, el TOE intenta verificar la firma con la parte pública registrada en él. En caso de que el proceso de verificación resulte satisfactorio, se permitirá el acceso al TOE, asignándole asimismo el rol de administrador o superadministrador en función de cómo fue ese usuario registrado en el momento de darle de alta].

5.2.10_ FIA_UAU.7 Protected authentication feedback

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [assignment: asteriscos '*'] to the user while the authentication is in progress.

5.3_ Requisitos y servicios criptográficos

5.3.1_ FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/3DES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: 3DES] and specified cryptographic key sizes [assignment: 192 bits] that meet the following: [assignment: FIPS 46-3 Data Encryption Standard].

FCS_CKM.1.1/AES1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: AES] and specified cryptographic key sizes [assignment: 128 bits] that meet the following: [assignment: FIPS PUB 197].

FCS_CKM.1.1/AES2 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: AES] and specified cryptographic key sizes [assignment: 192 bits] that meet the following: [assignment: FIPS PUB 197].

FCS_CKM.1.1/AES3 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: AES] and specified cryptographic key sizes [assignment: 256 bits] that meet the following: [assignment: FIPS PUB 197].

FCS_CKM.1.1/IDEA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: IDEA] and specified cryptographic key sizes

[assignment: 128 bits] that meet the following: [assignment: none].

5.3.2_ FCS_CKM.2 Cryptographic key distribution

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.2.1/SKeys The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: Diffie-Hellman Key Agreement Method] that meets the following: [assignment: PKCS #3: Diffie-Hellman Key Agreement Standard].

5.3.3_ FCS_CKM.3 Cryptographic key access

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

FCS_CKM.3.1 The TSF shall perform [assignment: todos los accesos a claves criptográficas] in accordance with a specified cryptographic key access method [assignment: PKCS#11 ó PKCS#12] that meets the following: [assignment: estándar PKCS#11 ó PKCS#12].

5.3.4_ FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: destrucción física de la clave] that meets the following: [assignment: baja del certificado o eliminación del mismo del keystore mediante un borrado físico]

5.3.5_ FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1/Sim The TSF shall perform [assignment: cifrado de contraseñas] in accordance with a specified cryptographic key generation algorithm [assignment: 3DES] and specified cryptographic key sizes [assignment: 192] that meet the following: [assignment: FIPS 46-3 Data Encryption Standard].

FCS_COP.1.1/Desc The TSF shall perform [assignment: descifrado de contraseñas] in accordance with a specified cryptographic key generation algorithm [assignment: 3DES] and specified cryptographic key sizes [assignment: 192] that meet the following: [assignment: FIPS 46-3 Data Encryption Standard].

FCS_COP.1.1/Asim1 The TSF shall perform [assignment: cifrado y descifrado de la clave simétrica que cifra los datos] in accordance with a specified cryptographic algorithm [assignment: RSA] and cryptographic key sizes [assignment: 1024, 2048] that meet the following: [assignment: PKCS #1 - RSA Encryption Standard (RSA)].

FCS_COP.1.1/Asim2 The TSF shall perform [assignment: cifrado y descifrado de la clave simétrica que cifra los datos] in accordance with a specified cryptographic algorithm [assignment: DSA] and cryptographic key sizes [assignment: 1024, 1536, 2048 bits] that meet the following: [assignment: FIPS PUB 186-2 (DSA)].

FCS_COP.1.1/Fir1 The TSF shall perform [assignment: firma electrónica] in accordance with a specified cryptographic algorithm [assignment: RSA signature with SHA-1 and SHA-2 hashing] and cryptographic key sizes [assignment: RSA 1024, SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment: PKCS #1 - RSA Encryption Standard (RSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Fir2 The TSF shall perform [assignment: firma electrónica] in accordance with a specified cryptographic algorithm [assignment: RSA signature with SHA-1 and SHA-2 hashing] and cryptographic key sizes [assignment: RSA 2048, SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment: PKCS #1 - RSA Encryption Standard (RSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Fir3 The TSF shall perform [assignment: firma electrónica] in accordance with a specified cryptographic algorithm algorithm [assignment: DSA signature with SHA-1 hashing] and cryptographic key sizes [assignment: DSA 1024 and SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment: FIPS PUB 186-2 (DSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Fir4 The TSF shall perform [assignment: firma electrónica] in accordance with a specified cryptographic algorithm algorithm [assignment: DSA signature with SHA-1 hashing] and cryptographic key sizes [assignment: DSA 1536 and SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment: FIPS PUB 186-2 (DSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Fir5 The TSF shall perform [assignment: firma electrónica] in accordance with a specified cryptographic algorithm algorithm [assignment: DSA signature with SHA-1 hashing] and cryptographic key sizes [assignment: DSA 2048 and SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment: FIPS PUB 186-2 (DSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Veri1 The TSF shall perform [assignment: verificación de firma electrónica] in accordance with a specified cryptographic algorithm [assignment: RSA signature with SHA-1 and SHA-2 hashing] and cryptographic key sizes [assignment: RSA 1024, SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment: PKCS #1 - RSA Encryption Standard (RSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Veri2 The TSF shall perform [assignment: verificación de firma electrónica] in accordance with a specified cryptographic algorithm [assignment: RSA signature with SHA-1 and SHA-2

hashing] and cryptographic key sizes [assignment: RSA 2048, SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment: PKCS #1 - RSA Encryption Standard (RSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Veri3 The TSF shall perform [assignment: verificación de firma electrónica] in accordance with a specified cryptographic algorithm algorithm [assignment: DSA signature with SHA-1 hashing] and cryptographic key sizes [assignment: DSA 1024 and SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment: FIPS PUB 186-2 (DSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Veri4 The TSF shall perform [assignment: verificación de firma electrónica] in accordance with a specified cryptographic algorithm algorithm [assignment: DSA signature with SHA-1 hashing] and cryptographic key sizes [assignment: DSA 1536 and SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment FIPS PUB 186-2 (DSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Veri5 The TSF shall perform [assignment: verificación de firma electrónica] in accordance with a specified cryptographic algorithm algorithm [assignment: DSA signature with SHA-1 hashing] and cryptographic key sizes [assignment: DSA 2048 and SHA-1 160 bits and SHA-2 256 bits] that meet the following: [assignment FIPS PUB 186-2 (DSA), FIPS PUB 180-1 (SHA1), FIPS PUB 180-2 (SHA2)].

FCS_COP.1.1/Hash1 The TSF shall perform [assignment: hash seguro] in accordance with a specified cryptographic algorithm [assignment: DES] and cryptographic key sizes [assignment: 160 bits] that meet the following: [assignment: FIPS PUB 180-1 (SHA1)].

FCS_COP.1.1/Hash2 The TSF shall perform [assignment: hash seguro] in accordance with a specified cryptographic algorithm [assignment: SHA-1] and cryptographic key sizes [assignment: 160 bits] that meet the following: [assignment: FIPS PUB 180-1 (SHA1)].

FCS_COP.1.1/Der1 The TSF shall perform [assignment: derivación de clave] in accordance with a specified cryptographic algorithm [assignment: 3DES] and cryptographic key sizes [assignment: 192 bits] that meet the following: [assignment: FIPS 46-3 Data Encryption Standard].

FCS_COP.1.1/Der2 The TSF shall perform [assignment: derivación de clave] in accordance with a specified cryptographic algorithm [assignment: DES] and cryptographic key sizes [assignment: 64 bits] that meet the following: [assignment: FIPS 46-3 Data Encryption Standard].

5.4_ Requisitos relativos a auditoría de eventos

5.4.1_ FAU_GEN.1 Audit data generation

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: Todas las invocaciones a un servicio publicado por el TOE].

FAU_GEN.1.2/Cons 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: Parámetros del servicio invocado, Valor de retorno del servicio invocado, HMAC del registro de este evento en combinación con el HMAC de los eventos hasta entonces registrados en ese fichero].

FAU_GEN.1.2/OCSP 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: Parámetros del OCSPRequest, Valor del OCSPResponse, HMAC del registro de este evento en combinación con el HMAC de los eventos hasta entonces registrados en ese fichero].

FAU_GEN.1.2/Rest 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: Parámetros del servicio invocado, Valor de retorno del servicio invocado, HMAC del registro de este evento en combinación con el HMAC de los eventos hasta entonces registrados en ese fichero].

5.4.2_ FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: searches] of audit data based on [assignment: HMAC correcteness == true].

5.5_ Requisitos relativos a la tranferencia interna segura de datos

5.5.1_ FDP_ITT.1 Basic internal transfer protection

Dependencies: FDP_ACC.1 Subset access control

FDP_ITT.1.1 The TSF shall enforce the [assignment:CONTROL_ACCESO_ASF] to prevent the [selection: modification] of user data when it is transmitted between physically-separated parts of the TOE.

5.5.2_ FDP_ITT.3 Integrity monitoring

Dependencies: FDP_ACC.1 Subset access control
FDP_ITT.1 Basic internal transfer protection

FDP_ITT.3.1 The TSF shall enforce the [assignment: CONTROL_ACCESO_ASF] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors].

FDP_ITT.3.2 Upon detection of a data integrity error, the TSF shall [assignment: registrar petición autenticación, error obtenido, y notificar a los usuarios].

5.5.3_ FPT_ITT.1 Basic internal TSF data transfer protection

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: modification] when it is transmitted between separate parts of the TOE.

5.5.4_ FPT_ITT.3 TSF data integrity monitoring

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.3.1 The TSF shall be able to detect [selection: modification of data]] for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: registrar la petición y el error obtenido, y notificárselo al origen].

En los siguientes apartados se definen los requisitos de garantía de aseguramiento satisfechos por el TOE para la obtención del nivel de certificación EAL3 (Evaluation Assurance Level 3). Todo ello, de acuerdo con los términos especificados en el Catálogo de Componentes de Garantía de Common Criteria Parte 3.

5.6_ Requisitos de aseguramiento: Clase ASE - Security Target Evaluation

5.6.1_ 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 summarise 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.

5.6.2_ 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.

5.6.3_ ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

5.6.4_ ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

5.6.5_ 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.

5.6.6_ ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C 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.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

5.6.7_ ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements

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.

5.7_ Requisitos de aseguramiento: Clase ADV - Development

5.7.1_ ADV_FSP.3 Functional specification with complete summary

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For SFR-enforcing TSFIs, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarise the non-SFR-enforcing actions associated with each TSFI.

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

5.7.2_ ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

5.7.3_ ADV_TDS.2 Architectural design

Dependencies: ADV_FSP.3 Functional specification with complete summary

Developer action elements:

ADV_TDS.2.1D The developer shall provide the design of the TOE.

ADV_TDS.2.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.2.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.2.2C The design shall identify all subsystems of the TSF.

ADV_TDS.2.3C The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.

ADV_TDS.2.4C The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.5C The design shall summarise the non-SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarise the behaviour of the SFR-supporting subsystems.

ADV_TDS.2.7C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

5.8_ Requisitos de aseguramiento: Clase AGD - Guidance Documents

5.8.1_ 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.

5.8.2_ 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.

5.9_ Requisitos de aseguramiento: Clase ALC - Life-Cycle Support

5.9.1_ ALC_CMC.3 Authorisation controls

Dependencies: ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures

Developer action elements:

ALC_CMC.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.3.1C The TOE shall be labelled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ALC_CMC.3.5C The CM documentation shall include a CM plan.

ALC_CMC.3.6C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

5.9.2_ ALC_CMS.3 Implementation representation CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.3.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.3.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.

ALC_CMS.3.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.3.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

5.9.3_ ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

5.9.4_ ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

5.9.5_ ALC_FLR.1 Basic flaw remediation

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.1.1D The developer shall document 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.

5.9.6_ ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

5.10_ Requisitos de aseguramiento: Clase ATE - Tests

5.10.1_ ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

5.10.2_ ATE_DPT.1 Testing: basic design

Dependencies: ADV_ARC.1 Security architecture description
ADV_TDS.2 Architectural design
ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

5.10.3_ ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

5.10.4_ ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.11_ Requisitos de aseguramiento: Clase AVA - Vulnerability Assessment

5.11.1_ AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

5.12_ Razonamiento de requisitos

5.12.1_ Razonamiento de requisitos funcionales

En esta sección se demuestra que todos los requisitos funcionales expuestos son necesarios, pues todos y cada uno de ellos son necesarios para el cumplimiento de un objetivo, y viceversa, que todos los objetivos están cubiertos por al menos un requisito. Asimismo, se expone porque alguna de las dependecias entre los requisitos funcionales detallados no se cumplen.

La dependencia existente entre los requisitos FCS_CKM.1 y FCS_CKM.4 no se cumple para las claves simétricas, puesto que éstas se almacenan de forma temporal en memoria dinámica y no se destruyen de forma explícita, sino que son sobreescritas.

La dependencia existente entre los requisitos FCS_COP.1 y FCS_CKM.1 no se cumple para ninguna operación basada en criptografía asimétrica, puesto las claves utilizadas provienen del exterior y por tanto no fueron generadas previamente.

La dependencia existente entre los requisitos FCS_COP.1 y FCS_CKM.4 no se cumple para el cifrado simétrico, puesto las claves utilizadas no son borradas de forma explícita.

La dependencia existente entre los requisitos FAU_GEN.1 y FPT_STM.1 no se cumple puesto que la fecha y hora registrada en los ficheros de auditoría no pertenece a la funcionalidad de seguridad del TOE, sino que simplemente es un dato más a registrar en ellos.

Asimismo, la dependencia entre FAU_SAR.1 y FAU_SAR.3 tampoco es satisfecha puesto que la capacidad de leer los los ficheros de auditoría no es proporcionada por el TOE si no que la delega en el entorno (mediante un editor de textos), no siendo por tanto necesario el requisito FAU_SAR.1.

La última dependencia no satisfecha corresponde a la que hay entre el requisito FCS_CKM.2 y FMT_MSA.2. Sin embargo, ésta queda resuelta al ajustarse el presente documento al "*RI # 145 - FCS component dependencies on FMT_MSA.2".*

A continuación, se muestra la correspondencia entre requisitos funcionales y objetivos de seguridad en ambos sentidos: primero qué objetivos satisface cada requisito y, posteriormente, con qué requisitos es cubierto cada objetivo:

Requisito funcional	Objetivos de seguridad
FDP_ACC.2	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06, Objetivo 07, Objetivo 08, Objetivo 09 Establece qué usuarios están autorizados a acceder a alguno de los activos involucrados en estos objetivos.

Requisito funcional	Objetivos de seguridad
FDP_ACF.1	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06, Objetivo 07, Objetivo 08, Objetivo 09 Establece las reglas para que ningún usuario no autorizado acceda a alguno de los activos involucrados en estos objetivos.
FMT_MSA.1	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06, Objetivo 07, Objetivo 08, Objetivo 09 Gestiona los atributos que autorizarán o denegarán a un sujeto el acceso a los activos que protegen estos objetivos.
FMT_MSA.3	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06, Objetivo 07, Objetivo 08, Objetivo 09 Inicializa los atributos que autorizarán o denegarán a un sujeto el acceso a los activos que protegen estos objetivos.
FMT_SMR.1	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06, Objetivo 07, Objetivo 08, Objetivo 09 Asocia el rol correspondiente al usuario que acceden a los activos que protegen al sujeto que operará con ellos.
FMT_SMF.1	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06, Objetivo 07, Objetivo 08, Objetivo 09 Establece las reglas de control de acceso tanto para las entidades externas como los roles para los usuarios. Todos estos sujetos son los que accederán a los activos que protegen estos objetivos, dependiendo pues de estas reglas quién tendrá permiso para acceder.
FIA_UID.2	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06, Objetivo 07, Objetivo 08, Objetivo 09 Establece que los usuarios del TOE deben ser identificados antes de poder realizar cualquier acción.
FIA_UAU.2	Objetivo 01, Objetivo 02, Objetivo 04, Objetivo 07 Establece que los usuarios locales de la consola han de ser autenticados antes de poder acceder al TOE.

	Requisito funcional	Objetivos de seguridad
	FIA_UAU.5	Objetivo 01, Objetivo 02, Objetivo 04, Objetivo 07 Establece que los usuarios locales de la consola tienen dos mecanismos de autenticación: por usuario y contraseña o por certificado.
	FIA_UAU.7	Objetivo 01, Objetivo 02, Objetivo 04, Objetivo 07 Establece que la contraseña introducida por los usuarios locales de la consola al autenticarse no aparecerá en claro.
	FCS_CKM.1	Objetivo 03: se ha de generar una clave para el cifrado de la clave simétrica intercambiada.
	FCS_CKM.2	Objetivo 03: se ha de generar una clave para el cifrado de la clave simétrica intercambiada.
	FCS_CKM.3	Objetivo 01: para acceder a las claves privadas de los keystores hay que seguir el método de acceso definido en este requisito. Objetivo 05: para acceder a las claves privadas de los keystores con las que se van a firmar las respuestas hay que seguir el método de acceso definido en este requisito. Objetivo 08: para acceder a la clave privada para firmar las peticiones a Autoridades de Certificación o a LDAPS hay que seguir el método de acceso definido en este requisito.
	FCS_CKM.4	Objetivo 01: destruye las claves privadas cuando éstas se vean comprometidas. Objetivo 08: para destruir la clave privada para firmar las peticiones a Autoridades de Certificación o a LDAPS hay que seguir el método de acceso definido en este requisito. Objetivo 03: se ha de generar una clave para el cifrado de la clave simétrica intercambiada.

Requisito funcional	Objetivos de seguridad
FCS_COP.1	Objetivo 02: cifra las contraseñas para garantizar su confidencialidad. Objetivo 03: cifra la clave secreta intercambiada para el cifrado simétrico. Objetivo 04: calcula el HMAC de una petición a registrar en la auditoría. Objetivo 05: firma las respuestas a enviar a los clientes y verifica esta firma una vez recibida en el cliente. Objetivo 07: calcula los HMACs de los registros de auditoría encadenadados con el anterior y los compara con los ya registrados. Objetivo 08: firma las peticiones a enviar a servidores OCSP o Autoridades de Sellado de Tiempos (TSAs). Objetivo 09: verifica la firma de las respuestas de un servidor OCSP, TSA o Autoridad de Certificación al TOE. Objetivo 10: verifica la firma de las respuestas del TOE a una aplicación usuaria que ha realizado una petición a un webservice..
FAU_GEN.1	Objetivo 04: genera los ficheros de auditoría con los datos necesarios para comprobar si alguna petición es un posible ataque y almacena el HMAC de la petición para garantizar la integridad.
FAU_SAR.3	Objetivo 07: proporciona las herramientas para buscar posibles ataques o fallos de integridad en los ficheros de auditoría.
FDP_ITT.1	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06 Proporciona una gestión segura de todos los datos de usuario transmitidos para la identificación previa a todos los objetivos..
FDP_ITT.3	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06 Monitoriza y avisa al usuario de cualquier error ocurrido durante la transmisión o recepción de los datos de usuario enviados por el primero.
FPT_ITT.1	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06 Proporciona una gestión segura de todos los datos de concernientes a la seguridad transmitidos en el control de acceso previo a todos los objetivos.

Requisito funcional	Objetivos de seguridad
FPT_ITT.3	Objetivo 01, Objetivo 02, Objetivo 03, Objetivo 04, Objetivo 05, Objetivo 06 Monitoriza y avisa al usuario de cualquier error ocurrido durante la transmisión o recepción de los datos de usuario enviados por el primero.

Tabla 06 – Razonamiento de los requisitos funcionales

Ahora se demostrará la suficiencia de los requisitos de seguridad para cumplir todos los objetivos establecidos:

Objetivo 01: Confidencialidad de claves privadas de certificados

Para este objetivo se asegura que sólo las entidades externas que hayan sido identificadas previamente en el TOE (FIA_UID.2) y superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) podrán acceder a las claves privadas de los certificados de los almacenes. Asimismo, se asegura una transmisión segura tanto de los datos de usuario como de los involucrados en la funcionalidad de seguridad desde las entidades externas al TOE (FDP_ITT.1 y FPT_ITT.1) y la monitorización de los errores de integridad de los mismos (FDP_ITT.3 y FPT_ITT.3).

Además, se garantiza que lo harán superando las restricciones impuestas por FCS_CKM.3 que explica el proceso de acceso al almacenamiento de estas claves. Asimismo, a través de FCS_CKM.4 se asegura la destrucción de estas claves cuando ya no deban ser accesibles.

Objetivo 02: Confidencialidad de contraseñas almacenadas en BD

Para este objetivo se asegura que sólo los usuarios que, tras cumplir los requisitos de identificación y autenticación a continuación expuestos, superen las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1), podrán leer las contraseñas almacenadas en base de datos y que las deberán descifrar por medio del requisito FCS_COP.1 correspondiente a los de cifrado/descifrado de los impuestos dependiendo de los parámetros de la operación. Para ello deberá utilizar la clave generada para el cifrado (FCS_CKM.1) con los parámetros correspondientes.

Los requisitos previos necesarios a cumplir por los usuarios que accedan a las contraseñas almacenadas en base de datos:

- **Entidades externas**: han debido de ser identificadas como expone el requisito (FIA_UID.2). Así, para su identificación, se ha de

comprobar que el identificador de aplicación con el que realizan la petición existe en el sistema.

- **Usuarios locales de la consola**: además de haberse identificado (FIA_UID.2), deben haber sido autenticados (FIA_UAU.2) bien mediante nombre de usuario y contraseña, no mostrándose ésta en claro por pantalla (FIA_UAU.7) y comparándose el hash de la misma con el almacenado en base de datos para ese usuario (FCS_COP.1) , o bien utilizando un certificado (FIA_UAU.5).

Para este objetivo se garantiza igualamente una transmisión segura de los datos de usuario a la Consola de Administración, mediante de las restricciones impuestas a través de requisitos (FDP_ITT.1 y FDP_ITT.3).

Asimismo, se asegura una transmisión segura tanto de los datos de usuario como de los involucrados en la funcionalidad de seguridad desde las entidades externas al TOE (FDP_ITT.1 y FPT_ITT.1) y la monitorización de errores de integridad de los mismos (FDP_ITT.3 y FPT_ITT.3).

Objetivo 03: Cifrado de clave secreta para cifrado simétrico

Para este objetivo se asegura que sólo usuarios correspondientes a entidades externas que se hayan identificado previamente en el TOE (FIA_UID.2) y superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) podrán acceder al servicio para cifrar la contraseña generada para el cifrado simétrico con FCS_CKM.1 por el TOE y distribuida por éste a las aplicaciones usuarias (FCS_CKM.2), mediante la función criptográfica requerida (FCS_COP.1).

Asimismo, se asegura una transmisión segura tanto de los datos de usuario como de los involucrados en la funcionalidad de seguridad desde las entidades externas al TOE (FDP_ITT.1 y FPT_ITT.1) y la monitorización de errores de integridad de los mismos (FDP_ITT.3 y FPT_ITT.3).

Objetivo 04: Registro de las peticiones realizadas

Para este objetivo se asegura que sólo los servicios accedidos por aplicaciones externas que hayan sido previamente identificadas (FIA_UID.2) y superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1), o la consola de administración, que ha debido ser accedida por usuarios identificados (FIA_UID.2), autenticados (FIA_UAU.1, FIA_UID.2, FIA_UAU.5 y FIA_UAU.7) y que hayan superado las restricciones de acceso impuestas por los mismo requisitos detallados para aquí para las aplicaciones externas, serán los únicos que registrarán en los ficheros de auditoría correspondientes, el de la consola para el segundo tipo de usuarios, y en el de servicios o en el del OCSP para las aplicaciones usuarias (FAU_GEN.1), los datos necesarios para cada tipo

de auditoría junto al HMAC del registro encadenado con el último HMAC (FCS_COP.1).

Asimismo, se asegura una transmisión segura tanto de los datos de usuario como de los involucrados en la funcionalidad de seguridad desde las entidades externas al TOE (FDP_ITT.1 y FPT_ITT.1) y la monitorización de errores de integridad de los mismos (FDP_ITT.3 y FPT_ITT.3).

Objetivo 05: Firma de las respuestas

Para este objetivo se asegura que sólo las entidades externas que se hayan identificado previamente en el TOE (FIA_UID.2) y superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) accederán al TOE y este firmará las respuestas (FCS_COP.1) a peticiones realizadas por uno de estos usuarios con un certificado definido por el administrador del sistema (FCS_CKM.3).

Asimismo, se asegura una transmisión segura tanto de los datos de usuario como de los involucrados en la funcionalidad de seguridad desde las entidades externas al TOE (FDP_ITT.1 y FPT_ITT.1) y la monitorización de errores de integridad de los mismos (FDP_ITT.3 y FPT_ITT.3).

Objetivo 06: Control de acceso

Para este objetivo se asegura que sólo las entidades externas que se hayan identificado previamente en el TOE (FIA_UID.2) y superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) accederán a los servicios publicados por el TOE.

Asimismo, para los usuarios locales de la consola se garantiza que sólo áquellos que hayan sido identificados (FIA_UID.2) y autenticados (FIA_UAU.1, FIA_UID.2, FIA_UAU.5 y FIA_UAU.7) y superado las restricciones de acceso impuestas por los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) estarán autorizados a acceder a la consola de administración.

Se asegura igualmente una transmisión segura tanto de los datos de usuario como de los involucrados en la funcionalidad de seguridad desde las entidades externas al TOE (FDP_ITT.1 y FPT_ITT.1) y la monitorización de errores de integridad de los mismos (FDP_ITT.3 y FPT_ITT.3).

Objetivo 07: Detección de modificaciones de ficheros de auditoría

Para este objetivo se asegura que sólo los usuarios de la consola de adminsitración que hayan sido previamente identificados (FIA_UID.2) y autenticados (FIA_UAU,2, FIA_UAU.5 y FIA_UAU.7) asignándoseles el rol

de superadministrador (FMT_SMR.1) y, que superen las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) podrán utilizar la herramienta de comprobación de los ficheros de auditoría (FAU_SAR.3) proveída por el TOE. Con ella detectarán si se ha violado la integridad de alguno de estos ficheros, ya que se almacena para cada nuevo registro su HMAC encadenado con el HMAC del último registro del fichero, siendo imposible modificar o eliminar algún registro sin ser detectado a través de la no corrección de los HMAC (FAU_SAR.3 y FCS_COP.1).

Objetivo 08: Firma de peticiones a TSAs y OCSPs externos

Para este objetivo se asegura que sólo las entidades externas que se hayan identificado previamente en el TOE (FIA_UID.2) y superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) podrán invocar servicios del TOE que tengan que realizar una petición a una servidor de sellado de tiempo o a un servidor OCSP, petición que deberá ir convenientemente firmada (FCS_CKM.3 y FCS_COP.1) para asegurar la integridad de la misma.

Objetivo 09: Verificar firma de respuestas de entidades externas

Para este objetivo se asegura que sólo los servicios del TOE que hayan sido solicitados por entidades externas que, previamente hubieran sido identificadas en el TOE (FIA_UID.2) y superado superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) podrán verificar la firma de las respuestas remitidas por entidades externas tales como servidores OCSP, TSAs o Autoridades de Certificación (FCS_COP.1) para asegurar su integridad.

Objetivo 09: Verificar firma de respuestas de entidades externas

Para este objetivo se asegura que sólo los servicios del TOE que hayan sido solicitados por entidades externas que, previamente hubieran sido identificadas en el TOE (FIA_UID.2) y superado superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 y FMT_SMF.1) podrán verificar la firma de las respuestas remitidas por entidades externas tales como servidores OCSP, TSAs o Autoridades de Certificación (FCS_COP.1) para asegurar su integridad.

5.12.2_ Razonamiento requisitos de aseguramiento

Los requisitos de aseguramiento se basan en la selección de áquellos necesarios para una evaluación EAL3 (descritos en las secciones 5.6, 5.7, 5.8, 5.9, 5.10 y 5.11 del presente documento), incrementados con

ALC_FLR.1 Basic flaw remediation, que describe cómo se gestionan las incidencias, desde su principio hasta su cierre.

Con este nivel de evaluación se provee una declaración de seguridad completa junto a un análisis de toda la funcionalidad de seguridad, aportando una especificación funcional de interfaces, documentación guía y una descripción funcional del diseño del TOE. El análisis es soportado por pruebas independientes de la funcionalidad de seguridad basadas en las aportadas por el desarrollador tanto sobre la especificación funcional como sobre su diseño así como con un análisis de vulnerabilidades que demuestra la resistencia del diseño.

Asimismo se provee seguridad sobre el entorno de desarrollo, la gestión de configuraciones y los procedimientos de entrega empleados.

6_ Especificación resumida del TOE

Esta sección define cómo se instancian en el TOE los requisitos de seguridad establecidos en el apartado anterior.

6.1_ FDP_ACC.2 Complete access control

El TOE controla el acceso por parte de cualquier tipo de sujeto (ya sea entidad externa o usuario con rol de administrador como superadministrador) a los siguientes objetos:

- Claves privadas
- Acceso a contraseñas almacenadas en base de datos
- Claves secretas generadas para el cifrado simétrico
- Respuestas a peticiones de aplicaciones cliente
- Servicio TOE
- Peticiones del TOE a entidades externas
- Respuestas de entidades externas al TOE

Asimismo, el TOE asegura que ninguno de los sujetos detallados antes realizará ningún tipo de operación no autorizada mediante las reglas descritas para el requisito presentado a continuación (FDP_ACF.1).

6.2_ FDP_ACF.1 Security attribute based access control

El TOE controla el acceso de los sujetos que representan entidades externas depende de si se está realizando una invocación a un Webservice o una petición mediante el protocolo HTTP, puesto que para cada uno de estos dos tipos el control se basa en unos atributos de seguridad. Dentro de este último tipo de peticiones también hay que diferenciar entre las realizadas al servidor OCSP o las efectuadas a su servidor de sellado de tiempo, siendo estos dos los únicos componentes del TOE a los que se puede acceder mediante dicho protocolo. La diferenciación entre el acceso a estos dos servidores es debida a que a partir de ellos se puede acceder a unos activos diferentes.

- **Invocación a un Webservice**: El módulo del TOE al que se invoca un servicio comprueba que la aplicación invocante existe en el sistema. Si existe, pasa a verificar las restricciones acceso que han debido de ser definidas previamente desde la Consola de Administración. En primer lugar, comprueba que exista alguna restricción de acceso asociada a esa aplicación con esa dirección IP. En caso de que así sea, habrá que verificar que la petición venga firmada con alguno de los certificados asociados para una de las restricciones registradas con esa dirección IP para esa aplicación, pues significa que sólo se permite el acceso para peticiones realizadas con dichos certificados.

  Si todas estas comprobaciones dan un resultado positivo el acceso les será permitido a los activos 02 (acceso a contraseñas almacenadas en base de datos), 06 (servicio del TOE), 07 (Peticiones del TOE a servidores OCSP y TSAs externos) y 08 (Respuestas de entidades externas al TOE).

  Además, si este control de acceso ha sido superado y el servicio solicitado corresponde a uno de firma o descifrado, se han de realizar las siguientes comprobaciones dependiendo del tipo de servicio:

- **Servicio de firma o descifrado:** Si la invocación es a un Webservice cuya funcionalidad es firmar o descifrar, ,se comprobará que la aplicación invocante existe en el sistema. En caso de que así sea, se verificará que existe una operación asociada a la misma con ese código y definida como una operación del mismo tipo que el servicio Es decir, si se está realizando una petición a un servicio de firma, la operación para esa aplicación debe estar definida como una operación de firma y lo mismo para descifrado.

  Si estas comprobaciones resultan satisfactorias, queda comprobar si está permitido emplear el certificado correspondiente al alias enviado como parámetro para ese certificado. En caso afirmativo, se autoriza el acceso al certificado para la aplicación que solicita ese servicio.

Un servicio de uno de estos dos tipos, en caso de superar todo el control de acceso, le está permitido el acceso a los activos 01 (claves privadas) y 02 (acceso a contraseñas almacenadas en base de datos), además de a los activos detallados anteriormente permitidos para todos los servicios autorizados.

Un caso especial dentro de esta regla de acceso corresponde a los servicios de descifrado que en lugar de incluir el alias del certificado registrado en el sistema para descifrar, adjuntan el certificado en sí mismo. En este caso, la segunda parte de esta comprobación, la correspondiente al certificado no se realiza y, en su lugar, se comprueba que el certificado enviado ha sido emitido por una de las Autoridades de Certificación consideradas de confianza para esa aplicación-operación. En esta situación, no se accede a ningún activo más al estar la clave privada con la que se va a descifrar en la propia petición.

- **Petición por HTTP al OCSPResponder:** Cuando el servidor OCSPResponder recibe una petición HTTP de una aplicación externa comprueba que está autorizada a ello. Para eso, lo primero que hacen es comprobar que existe alguna restricción de acceso a ellos registrada en el sistema en la que la dirección IP asociada a ella coincida con la dirección desde la que se realiza la invocación. En caso afirmativo, el TOE verifica que la firma de la petición es realizada con un certificado asociado a una de estas restricciones. Si esta verificación también resulta satisfactoria el acceso le está permitido a la aplicación, teniendo acceso a los siguientes activos dependiendo de lo solicitado por la aplicación:

  - Activo 01: Claves privadas de certificados de los almacenes.
  - Activo 02: Acceso a contraseñas almacenadas en BB.DD.
  - Activo 06: Servicio TOE.
  - Activo 07: Peticiones del TOE a OCSPs y TSAs externos.
  - Activo 08: Respuestas de entidades externas al TOE.

- **Petición por HTTP al TSAServer:** Cuando el servidor TSAServer recibe una petición HTTP de una aplicación externa comprueba que está autorizada a ello. Para eso, lo primero que hacen es comprobar que existe alguna restricción de acceso a ellos registrada en el sistema en la que la dirección IP asociada a ella coincida con la dirección desde la que se realiza la invocación. En caso afirmativo, el TOE verifica que la firma de la petición es realizada con un certificado asociado a una de estas restricciones. Si esta verificación también resulta satisfactoria el acceso le está permitido a la aplicación, teniendo acceso a los siguientes activos dependiendo de lo solicitado por la aplicación:

- Activo 01: Claves privadas de certificados de los almacenes.
- Activo 02: Acceso a contraseñas almacenadas en BB.DD.
- Activo 06: Servicio TOE.

El control de acceso definido para un usuario local de la consola está basado en el atributo que indica el rol que desempeña. Para superarlo ha de tener de tener asignado el rol de administador o de super-administrador permitiéndoseles entonces el acceso al activo 02 (contraseñas almacenadas en base de datos).

6.3_ FMT_MSA.1 Management of security attributes

6.3.1_ FMT_MSA.1.1/ Entidades externas

Los atributos de seguridad asociados a los sujetos de tipo entidad externa pueden ser modificados o borrados por un usuario administrador del TOE desde diferentes lugares de la consola de administración dependiendo de que tipo de petición se esté realizando al TOE:

Invocación a un Webservice

- **Identidad de la aplicación invocante**: al borrar una aplicación se está borrando también el código que correspondería para esa aplicación con este atributo.
- **Dirección IP y firma de la petición**: desde el menú restricciones de acceso pueden borrarse o modificarse restricciones ya existentes implicando, respectivamente, la eliminación o alteración de posibles valores que podría tomar el atributos dirección IP. El certificado con que el cliente firma las peticiones no puede ser eliminado o modificado por el usuario administrador pero dicho usuario puede borrar o modificar el certificado público correspondiente al certificado privado que debe usarse para la firma de las mismas, eliminando la posibilidad de acceso al cliente si es necesario. Es decir, aunque no se puede borrar el certificado con el que firma el cliente, éste se puede invalidar.
- **Firma de la petición**: la firma de la petición no puede ser modificada o eliminada directamente. La modificación requeriría el cambio del certificado asociado a la restricciones de acceso.

  En caso, además de solicitar un servicio de los siguientes tipos:

- Verificación o cifrado:

  - **Aplicación y operación para las que se solicita el servicio**: la parte de la consola dedicada a la administración de aplicaciones y sus operaciones realiza el mantenimiento de estos atributos.

- Firma o descifrado:

  - **Aplicación y operación para las que se solicita el servicio**: la parte de la consola dedicada a la administración de aplicaciones y sus operaciones realiza el mantenimiento de estos atributos.

  - **Alias del certificado con que se quiere operar**: en las secciones de la consola dedicadas a la gestión de certificados asociados a las distintas operaciones se pueden eliminar valores de este atributo ya definidos. Para modificar algún alias de un certificado, habrá que acceder al almacén correspondiente dependiendo de la operación a la que esté asociado y cambiar ahí el nombre del alias.

Las restricciones de acceso para las aplicaciones usuarias son definidas por un usuario administrador o superadministrador del TOE desde la consola de administración.

Petición por HTTP al OCSPResponder o al TSAServer

- Los atributos de seguridad referidos a una invocación por HTTP, independientemente del servidor del que se trate son los mismos: dirección IP desde la que se realiza la invocación y firma de la misma. Desde la consola, en la sección correspondiente al servidor del que se trate en ese momento, se pueden definir distintas restricciones de acceso o modificar las ya existentes. Así, pueden borrarse o modificarse restricciones ya existentes implicando, respectivamente, la eliminación o alteración de posibles valores que podría tomar el atributo dirección IP. La firma en sí misma no puede ser modificada, El certificado con que el cliente firma las peticiones no puede ser eliminado o modificado por el usuario administrador pero dicho usuario puede borrar o modificar el certificado público correspondiente al certificado privado que debe usarse para la firma de las mismas, eliminando la posibilidad de acceso al cliente si es necesario. Es decir, aunque no se puede borrar el certificado con el que firma el cliente, se puede invalidar.

6.3.2_ FMT_MSA.1.1/Usuarios

El único atributo de seguridad de los sujetos del TOE Usuarios es el rol que ocupan en el mismo. Éste puede ser modificado únicamente por usuarios <superadministradores> desde la consola de administración.

6.4_ FMT_MSA.3 Static attribute initialisation

Los valores que toman los atributos de seguridad son inicialmente nulos, hasta que un usuario de la consola, tanto administrador como superadministrador, los modifica de la siguiente manera:

Invocación a un Webservice

- **Identidad de la aplicación invocante**: al dar de alta una aplicación se está inicializando este valor.

- **Dirección IP y firma de la petición**: desde el menú restricciones de acceso pueden registrarse nuevas restricciones inicializándose así la dirección y certificado con el que se firmará.

  En caso, además de solicitar un servicio de los siguientes tipos:

  - Verificación o cifrado:

    - **Aplicación y operación para las que se solicita el servicio**: la parte de la consola dedicada a la administración de aplicaciones y sus operaciones realiza la inicialización de estos atributos realizándose al registrar nuevas aplicaciones y operaciones respectivamente.

  - Firma o descifrado:

    - **Aplicación y operación para las que se solicita el servicio**: la parte de la consola dedicada a la administración de aplicaciones y sus operaciones realiza la inicialización de estos atributos realizándose al registrar nuevas aplicaciones y operaciones respectivamente.

    - **Alias del certificado con el que se quiere operar**: al asociar certificados a operaciones de aplicaciones desde la consola de administración se está inicializando los valores que estos atributos pueden tomar.

Petición por HTTP al OCSPResponder o al TSAServer

Los atributos de seguridad referidos a una invocación por HTTP, independientemente del servidor del que se trate son los mismos: dirección IP desde la que se realiza la invocación y firma de la misma. Desde la consola, en la sección correspondiente al servidor del que se trate en ese momento, se pueden definir distintas restricciones de acceso que inicializan los valores de los atributos asociados a estos sujetos. Así, al registrar una nueva restricción se está dando valor a la IP y al certificado con el que puede firmarse esa petición.

Usuarios de la consola

El único atributo de seguridad de los sujetos del TOE Usuarios es el rol que ocupan en el mismo. Éste es inicializado desde la consola de administración cuando un usuario superadministrador registra un nuevo usuario.

6.5_ FMT_SMR.1 Security roles

Los usuarios administradores del TOE, que son los que acceden a la consola de administración, deben tener un rol asociado que sólo puede tomar los valores <administrador, superadministrador>.

6.6_ FMT_SMF.1 Specification of Management Functions

La funcionalidad del TOE proporciona la posibilidad de editar desde la consola de administración reglas de acceso para aplicaciones usuarias. Para ello, es posible asignar a una determinada aplicación parejas (dirección IP, certificado), de forma que se se restrinja el acceso desde dicha aplicación a todas las invocaciones realizadas desde las referidas IPs, y que se encuentren firmadas con los respectivos certificados asociados.

Los usuarios de la consola también pueden ser gestionados desde la propia consola por un usuario superadministrador, que puede bien registrar nuevos usuarios o bien modificar los ya existentes.

6.7_ FIA_UID.2 User identification before any action

Cuando un usuario administrador (correspondiente a un sujeto usuario) del TOE accede a la consola de administración, lo primero que debe hacer es introducir los datos que le identifican, sin tener posibilidad de realizar ninguna otra operación. La identificación puede llevarse a cabo bien presentando un nombre de usuario (que si deberá estar previamente registrado como usuario autorizado) o bien presentando un certificado digital, con el que le ocurrirá lo mismo: su existencia en el registro de usuarios autorizados le identifica.

Cuando los sujetos que solicitan un servicio web del TOE son entidades externas, las solicitudes deben incluir un atributo que las identifica. Este atributo debe comprobarse en el momento de la invocación mediante las reglas de restricción de acceso definidas previamente en la consola. Con todo ello, los sujetos de tipo entidades externas no pueden realizar ninguna acción previa a la identificación.

En caso de que las entidades externas estén realizando una petición por HTTP, tanto al Servidor OCSPResponder como al Servidor de Sellado de Tiempos, la petición se identifica previamente en el sistema mediante la comprobación de que la dirección IP desde la que se realiza existe en el sistema, siendo ésta la primera comprobación que se realiza en la petición.

6.8_ FIA_UAU.2 User authentication before any action

Cuando un usuario local de la consola que ya ha sido identificado debe ser autenticado por medio de uno de los mecanismos definidos en el requisito FIA_UAU.5 antes de poder realizar cualquier acción.

6.9_ FIA_UAU.5 User authentication mechanism

Un administrador de la consola, tanto administrador como superadministrador, tiene dos mecanismos para autenticarse pudiendo usar sólo aquél con el que fue registrado en el momento que fue dado de alta en el sistema. Éstos son:

- **Por nombre de usuario y contraseña**: una vez que se ha sido identificado tras comprobar que su nombre de usuario existe, se procede a autenticar comprobando la corrección de la contraseña asociada. Para ello, se calcula el hash de la contraseña asociada y se compara con el almacenado en base de datos para ese nombre de usuario. Si coinciden, el usuario es autenticado en el sistema y se le permite el acceso, asignándosele el rol de administrador o superadministrador en función de cómo fue definido ese usuario en el momento de darle de alta.

- **Por certificado**: se ha de comprobar que el certificado que presenta para su autenticación es correcto mediante el proceso de desafío en el que el TOE envía una frase para que la firme con su clave privada al usuario que está intentando acceder a la consola. En caso de que la firma realizada pueda ser verificada por el TOE con la clave pública asociada que le había identificado en el sistema, el usuario será autenticado y tendrá acceso al TOE asignándosele el rol de administrador o superadministrador en función de cómo fue definido ese usuario en el momento de darle de alta.

6.10_ FIA_UAU.7 Protected authentication feedback

Al autenticarse un usuario de la consola mediante nombre de usuario y contraseña, ésta no aparece en la pantalla en claro, sino que cada carácter es sustituido por una máscara (asterisco).

6.11_ FCS_CKM.1 Cryptographic key generation

El TOE permite generar claves criptográficas con los siguientes propósitos y de la siguiente manera:

- **Clave para el cifrado simétrico por invocación a Webservice**: Los encargados de generar esta clave son los proveedores criptográficos del TOE, utilizando como semilla aleatoria:
    - La fecha y hora del sistema o bien
    - Un vector de inicialización (IV) codificado en ANSI.1 y especificado como parámetro.

  Los algoritmos de cifrado disponibles son el 3DES (192 bits), bajo los modos de cifrado ECB y CBC, los algoritmos IDEA (128 bits) y AES (128, 192 y 256 bits), ambos bajo el modo CBC. La función “padding” utilizada por todos ellos es PKCS5#Padding.

6.12_ FCS_CKM.2 Cryptographic key distribution

El TOE distribuye la clave generada para el cifrado simétrico cifrando con la clave pública del receptor la misma. Una vez recibida, éste la puede descifrar con su correspondiente clave privada.

6.13_ FCS_CKM.3 Cryptographic key access

Para acceder a una clave que se encuentre almacenada en el TOE se deben seguir los siguientes pasos:

- Recupera el keystore de la clave de la base de datos.
- Obtener la clave de acceso al propio keystore. Ésta se encuentra cifrada en la base de datos con una contraseña especificada en archivos de propiedades.

- Obtener la clave del registro del keystore. Esta clave se obtiene de la base de datos y se descifra con una contraseña igualmente especificada en archivos de propiedades.

- Una vez que se dispone de las dos contraseñas anteriores, se obtiene la clave criptográfica que será utilizada por el proveedor.

6.14_ FCS_CKM.4 Cryptographic key destruction

La destrucción de las claves criptográficas se hace desde la Consola de Administración dando de baja el certificado en cuestión o bien eliminándolo directamente el keystore mediante un borrado físico.

6.15_ FCS_COP.1 Cryptographic operation

El soporte criptográfico requiere que las operaciones criptográficas se realicen de acuerdo a un algoritmo específico y con unas claves criptográficas de tamaños determinados. Los algoritmos y los tamaños de claves especificados pueden basarse en un estándar asignado. El TOE realiza las siguientes operaciones criptográficas de acuerdo a los algoritmos criptográficos y los tamaños de claves que se especifican a continuación:

- **Cifrado y descifrado simétrico de contraseñas**: Las contraseñas almacenadas en base de datos se cifran utilizando el algoritmo simétrico 3DES (192 bits) de manera que cada vez que desde la consola se inserta una nueva, ha de ejecutarse una operación de cifrado. Igualmente, las contraseñas almacenadas en base de datos se descifran utilizando el algoritmo simétrico 3DES (192 bits), de manera que cada vez que la aplicación necesita una de ellas, ha de ejecutarse una operación de descifrado.

- **Cifrado y descifrado asimétrico de la clave simétrica que cifra los datos**: Cada vez que se realiza una operación de cifrado de datos, el TOE genera una clave privada aleatoria con uno de los algoritmos de clave simétrica por él soportados: 3DES (192 bits), AES (192, 256 bits) o IDEA (128 bits). Esta clave recibe el nombre de clave de sesión, y es la utilizada para el cifrado de los datos. La clave de sesión se cifra asimétricamente con la clave pública del destinatario de los datos confidenciales, mediante uno de los algoritmos de clave pública soportados por el TOE: RSA (1024, 2048 bits) o DSA (1024, 1536, 2048 bits). Los datos cifrados con la clave de sesión, junto con ésta última cifrada con la clave pública del destinatario de los datos, se envían al receptor, constituyendo lo que se denomina un sobre digital. De esta forma, únicamente el destinatario de los datos confidenciales puede descifrar la clave de sesión (utilizando su clave asimétrica privada), y con ella recuperar dichoa datos.

- **Firma electrónica y verificación de firma electrónica**: El TOE tiene la posibilidad de firmar digitalmente datos, así como peticiones (tanto a Webservices como a servidores OCSP de estado de certificados y/o a servidores de tipo TimeStamp para sellado de tiempos) y respuestas (provenientes igualmente tanto de Webservices como de servidores OCSPs y/o servidores de TimeStamp. Las firmas de los objetos signados deben validarse como paso previo a a la toma de decisiones, disponiendo igulmente el TOE de la posibilidad de realizar esta tarea.

  La generación de datos, peticiones y/o respuestas firmadas por parte del TOE implica el cómputo de una firma digital asimétrica. El TOE dispone igualmente de funcionalidad para la validación de las firmas, para lo que se invoca a la función de verificación de firmas digitales. Evidentemente, los algoritmos que se utilizan para verificar firmas asimétricas dependen de los que se utilizaron en el proceso de generación de las mismas. La tecnología del TOE soporta los siguientes algoritmos en relación a la gestión (generación y/o verificación de firmas):

  - RSA (1024, 2048 bits) con SHA1 (160 bits) y SHA2 (256 bits)
  - DSA (1024, 1536, 2048 bits) con SHA1 (160 bits) y SHA2 (256 bits).

- **Hash seguro**: Las funciones criptográficas resumen (Hash) se aplican a las contraseñas de los usuarios para la generación de identificadores únicos de las mismas. El resumen de una contraseña obtenido mediante una función de este tipo tiene la propiedad de identificarla de forma unívoca, si bien no permite obtener información alguna acerca de la misma. Los resúmenes de las contraseñas de usuario se almacenan en base de datos, siendo ésta una forma segura de mantener un registro de referencias únicas a las contraseñas de los usuarios, sin necesidad de salvaguardar un registro local de dichas contraseñas. En estas condiciones, la función resumen SHA1 permite verificar si el resumen de la contraseña introducida por el usuario en el momento requerido coincide con el previamente registrado, pudiéndose adoptar las acciones necesarias en función del resultado obtenido. Los algoritmos y funciones criptográficas utilizados para el cómputo de resúmenes soportados por el TOE son: DES y SHA1.

- **Derivación de claves**: el TOE carga una clave indicada por fichero de propiedades y a partir de ésta deriva nuevas claves con las características requeridas por los algoritmos de cifrado a utilizar. Esto sucede en dos ocasiones:

  - **Clave para el cifrado de contraseñas**: La contraseña para el algoritmo de cifrado se genera a partir de una clave fija alojada en un archivo de texto, aplicándole funciones dependientes del algoritmo con el que haya de ser utilizada la clave generada. Así, para un determinado algoritmo, y manteniendo fijo el archivo referido (i.e., la clave para la generación de la contrase-

ña), siempre se obtiene la misma contraseña, ya que no se introduce ningún parámetro aleatorio adicional.

- **Clave asociada al HMAC**: Esta clave es utilizada para parametrizar una función criptográfica resumen, de forma que la salida de dicha función (contenido resumido) dependa de forma unívoca de la combinación del contenido a resumir y de dicha clave. Al igual que en el caso anterior, la clave asociada al HMAC se genera a partir de la clave fija alojada en un archivo de texto indicado por propiedades. Así pues, la clave asociada al HMAC será únicamente dependiente de la función criptográfica resumen subyacente utilizada en dicho HMAC.

6.16_ FAU_GEN.1 Audit data generation

Existen tres componentes de auditoría: el de la consola, el del OCSPResponder y otro para el resto de servicios. Cada vez que un servicio del TOE es invocado y, dependiendo de a que componente lógico del TOE corresponda éste, registra antes de realizar cualquier tipo de acción a través del componente de auditoría correspondiente (el primero de los nombrados para la consola, el segundo para el OCSPResponder y el tercero para el resto de los componentes) la petición antes de realizar cualquier tipo de operación la fecha en la que se realizó, el tipo de evento, el sujeto responsable de la invocación, la operación solicitada y sus parámetros. A todo ello le aplica una función resumen y registra su resultado también.

El mismo proceso es llevado a cabo al término de la operación del servicio invocado, sólo que en este caso además se registra el estado final de la misma: si ha tenido éxito o ha ocurrido algún error.

6.17_ FAU_SAR.3 Selectable audit review

En los ficheros de auditoría se almacena el HMAC de las peticiones registradas. Se puede comprobar la integridad de los mismos a través de la comprobación de la corrección del HMAC pudiendo buscar a través de él registros con fallos, es decir, aquellos en los que el registro no coincide con el resultado de aplicar una función resumen.

6.18_ FDP_ITT.1 Basic internal transfer protection

Para el control de acceso de las aplicaciones usuarias al TOE que invocan servicios web, se transfieren datos de usuario, como el identificador de la aplicación, que además es utilizado para la identificación de las mismas. Al estar firmadas todas las peticiones realizadas por estas aplicaciones a un webservice, se garantiza que cualquier modificación sobre ellas será detecta-

da por el TOE, asegurándose de esta manera la integridad de los datos de usuario recibidos.

6.19_ FDP_ITT.3 Integrity monitoring

En caso de que al verificar la firma de la petición a un Webservice de una aplicación usuaria, el TOE detecte un error de integridad sobre los datos de usuario transmitidos en ella, el TOE registra en los ficheros de log la traza de toda la ejecución con los errores detectados. Asimismo, el TOE devuelve a la aplicación usuaria el error detectado.

6.20_ FPT_ITT.1 Basic internal TSF data transferprotection

Para el control de acceso de las aplicaciones usuarias que invocan a un webservice al TOE, se transfieren datos de la funcionalidad de seguridad como son todos los atributos involucrados en el control de acceso que éstas han de superar al acceder al TOE, exceptuando el código de la aplicación invocante. Al estar firmadas todas las peticiones realizadas por estas aplicaciones, se garantiza que cualquier modificación sobre ellas será detectada por el TOE, asegurándose de esta manera la integridad de los datos relacionados con la funcionalidad de seguridad recibidos.

Asimismo, las respuestas que emiten los módulos que publican webservices son firmadas antes de ser enviadas al SecurityAgent garantizándose la posterior posibilidad de detectar cualquier error de integridad.

6.21_ FPT_ITT.3 TSF data integrity monitoring

En caso de al verificar la firma de la petición a un webservice de una aplicación usuaria, el TOE detecte un error de integridad sobre los datos de usuario transmitidos en ella, el TOE registra en los ficheros de log la traza de toda la ejecución con los errores detectados. Asimismo, el TOE devuelve a la aplicación usuaria el error detectado.