# Perfil de Protección HSM Realia Technologies S.L.

11-04-2011

Versión 2.0

## Hoja de Información General

CONTROL DOCUMENTAL

| | |
|---|---|
| PROYECTO: | |
| TÍTULO: | Perfil de Protección HSM Realia Technologies S.L. |
| VERSIÓN | 2.0 |
| FECHA DE EDICIÓN: | 11-04-2011 |
| FICHERO: | Perfil de Protección HSM REALSEC |
| HERRAMIENTAS DE EDICIÓN: | MICROSOFT WORD 2003 |
| AUTORES: | REALSEC |
| COMPAÑÍA: | REALSEC |

## Control de Versiones

| Versión | Fecha | Afecta | Breve descripción del cambio |
|---|---|---|---|
| 1.0 | 03/12/2010 | Todo | Versión inicial |
| 1.1 | 23/12/2010 | Todo | - Solución a OR-001, OR-002 y OR-003<br>- Eliminación de requisito de canal seguro.<br>- Requisito extendido para FPT FSM (eliminar la política de control de acceso a la variable de estado) y FCS entrada de claves<br>- Especificación de notas de aplicación de SARs<br>- Refinar las políticas de control de acceso a CLAVES y SERVICIOS<br>- Refinar las funciones de gestión<br>- Incluir la dependencia de FPT_TDC que tiene FDP_ITC.2 |
| 2.0 | 11/04/2011 | Política de control de acceso a claves<br><br>Rol de usuario no identificado | Las operaciones de gestión sobre los atributos de seguridad de la política de acceso a claves se restringen a los roles que defina el autor de la declaración de seguridad que declara conformidad con este PP.<br><br>Se incluye el rol de usuario son identificado en la OSP P-ROLES y en el objetivo de seguridad del TOE O.ROLEs |

# Índice

# 1 Introducción

1 Este documento es el Perfil de Protección que describe los requisitos de seguridad de un módulo criptográfico tipo Hardware Security Module (HSM) genérico que proporciona servicios criptográficos y de protección de material criptográfico al sistema que trabaja conjuntamente con el TOE que declare cumplimiento con este PP.

2 Las funciones de seguridad que se implementan, ya sean servicios exportados o mecanismos internos de protección, deberán ser funciones aprobadas por FIPS o recomendadas por el NIST, conforme a [FIPS-ANEXOS].

## 1.1 Identificación del PP

| | |
|---|---|
| **Título** | Perfil de Protección HSM Realia Technologies S.L. |
| **Versión** | Versión 2.0 |
| **Autor** | Realia Technologies S.L. |
| **Fecha de publicación** | 11-04-2011 |

## 1.2 Resumen del TOE

### 1.2.1 Tipo de TOE

3 El TOE es un modulo criptográfico del tipo HSM que implementa funciones criptográficas cuyo objetivo es la protección de la confidencialidad, integridad de la información procesada, almacenada y trasmitida (datos de usuario) de acuerdo con una política de seguridad.

4 Así mismo, el TOE deberá gestionar y proteger el material criptográfico usado en las funciones de seguridad. El PP aplica a módulos HSM que implementan criptografía simétrica y/o asimétrica, por lo que protegerá tanto claves secretas como privadas.

1.2.1.1 Características de seguridad físicas

5 El TOE se define desde el punto de vista físico, como un conjunto de HW con su correspondiente SW y/o FW, que implementa funciones criptográficas y está contenido dentro de unos límites criptográficos

definidos. El TOE es un HSM en cualquier forma o configuración, formado un por único chip (**single-chip**) o por múltiples chips ensamblados en una placa (**multi-chip stand alone** o **embedded**).

6 Desde el punto de vista de propiedades de seguridad físicas, el TOE proporciona los mecanismos HW de protección contra manipulaciones físicas y sondado de canales, proporcionando evidencia de la manipulación ("*tamper evidence*") y respondiendo automáticamente de forma que no se comprometan los activos que se protegen: mecanismos "*tamper response*" que deberán destruir inmediatamente el material criptográfico y demás CSPs en cuanto se detecte la manipulación física ("*zeroization*"). Estos mecanismos se aplican especialmente cuando existen tapas que se puedan eliminar o interfaces para la realización de operaciones de mantenimiento del módulo (TOE).

7 Para todas las categorías de módulos criptográficos mencionadas, se implementan mecanismos de protección físicos:

- módulos single-chip: recubrimiento del chip mediante una capa dura (tipo epoxy) resistente a su eliminación o penetración y cuyo intento de manipulación deje evidencias ("*tamper-evident*") y tenga altas probabilidades de causar daños irreparables al módulo (TOE);

- módulos multi-chip: encapsulado del módulo con una capa dura o con material duro y opaco (tipo epoxy), o bien un cierre opaco tamper-evident que evite la observación directa, sondado o manipulación de los componentes del módulo, en el que los intentos de manipulación o penetración provoquen daños graves y proporcionen evidencia del intento de manipulación.

8 En el caso de existir ranuras de ventilación, éstas deberán construirse de forma que se evite la posibilidad de sondar o explorar internamente el módulo (TOE) sin ser detectado y estarán bloqueadas mecánicamente o mediante claves lógicas o protegidas mediante etiquetas tamper-evident.

1.2.1.2 Características de seguridad lógicas

1.2.1.2.1 Funciones de seguridad

9 Desde el punto de vista lógico, el TOE queda definido por el conjunto de funciones de seguridad que se exportan dependiendo de los algoritmos criptográficos y protocolos implementados. Los algoritmos y protocolos implementados deberán proporcionar al menos alguna de las siguientes funciones de seguridad:

- Creación de firma digital, para dar soporte a servicios de autenticación en origen, integridad de datos y no repudio;
- Verificación de firma digital, para detectar modificaciones de en datos firmados, como prueba de origen;
- Cifrado, para proteger la confidencialidad de la información;
- Descifrado, para dar soporte a la protección de la confidencialidad de la información;
- Generación de resúmenes para su uso como algoritmo subyacente en otros procesos, o para control de integridad.
- Generación de números aleatorios necesarios en otros procesos criptográficos (RNG).
- Generación de claves usadas en las funciones criptográficas usando un RNG aprobado según [FIPS-ANEXOS].

10 Los algoritmos criptográficos que implementan las funciones de seguridad deberán estar aprobadas en FIPS o recomendadas por el NIST, por lo que deberán estar incluidas en los anexos correspondientes [FIPS-ANEXOS] de [FIPS1402]. El módulo criptográfico (TOE) deberá implementar al menos una función criptográfica aprobada usada en un modo de operación aprobado.

11 Las declaraciones de seguridad que declaren cumplimiento con este PP deberan especificar la versión de la normativa del NIST que se está cumpliendo con el objeto de definir las funciones aprobadas que se implementen.

#### 1.2.1.2.2 Protección del material criptográfico

12 El módulo (TOE) gestionará de manera eficiente el material criptográfico necesario en los algoritmos y protocolos implementados, controlando el acceso al mismo por parte de las funciones criptográficas aprobadas.

13 Para entrada y salida de claves:

- Si se usan métodos automáticos, las claves privadas y secretas entrarán y saldrán del TOE cifradas.
- Si se usan métodos manuales, las claves privadas y secretas entrarán y saldrán del módulo (TOE) cifradas o mediante la

implementación de algún procedimiento de conocimiento dividido (split-knowledge).

- Las claves públicas pueden entrar y salir del módulo (TOE) en claro.

14 El TOE asocia una clave (secreta, privada o pública) que entra o sale del módulo con la entidad correcta (persona, grupo o proceso) a la que se asocia la clave.

15 En caso de usarse algún esquema de acuerdo de claves entre el TOE y una entidad externa, el esquema deberá ser alguno de los aprobados conforme a [FIPS-ANEXOS].

1.2.1.2.3 Interfaces del TOE

16 El TOE proporcionará los siguientes tipos de interfaces o *puertos* (I/P):

- **I/P de entrada de datos**: para todos los datos (excepto los datos de control que entran por el I/P de entrada de control) que entren y sean procesados por el TOE (incluyendo datos en claro, datos cifrados, material criptográfico y CSPs, datos de autenticación e información de estado de otra entidad);
- **I/P de salida de datos**: para todos los datos (excepto los datos de estado que salen por el I/P de estado) que salen del TOE (incluyendo datos en claro, datos cifrados, material criptográfico y CSPs, datos de autenticación e información de control para otra entidad);
- **I/P de entrada de control:** para todos comandos de entrada, señales y datos de control (incluyendo llamadas a funciones, controles manuales, botones, teclado) usados para el control de la operación del TOE;
- **I/P de salida de estado:** para la salida de señales, indicadores y datos de estado (incluyendo códigos de retorno de las funciones, indicadores físicos como LEDs o pantallas) que se usan para indicar el estado del TOE;
- **I/P de alimentación:** fuentes de alimentación externas.

17 Los interfaces físicos usados para la entrada y salida de material criptográfico y CSPs en claro (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar físicamente separados de otros interfaces, o bien los interfaces lógicos usados para la

entrada y salida de material criptográfico y CSPs en claro (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar lógicamente separados utilizando un "*trusted path*".

18 El material criptográfico y CSPs en claro (incluyendo interfaces para la entrada de datos de autenticación confidenciales) debe entrar directamente al módulo (TOE) mediante, por ejemplo, un "*trusted path*" o un cable directamente conectado.

19 La salida de datos se inhibirá en los siguientes escenarios:

- Durante el proceso de generación de claves
- Entrada manual de claves a través de este puerto
- Self-test
- Estado de error
- Destrucción de claves
- Carga de software

1.2.1.2.4 Roles, servicios y autenticación

20 El TOE soportará, al menos, los siguientes roles: usuario y crypto-officer. En el caso de que se permita que operadores realicen labores de mantenimiento del módulo (TOE), se deberá incluir un rol a tal efecto.

21 El TOE deberá proporcionar, al menos, los siguientes servicios:

- mostrar el estado del TOE,
- realizar auto-testing y
- ejecutar las funciones de seguridad (aprobadas por FIPS o recomendadas por NIST según [FIPS-ANEXOS]).

22 El TOE implementará un mecanismo de autenticación basado en la identidad de los usuarios. Se garantizará la confidencialidad e integridad de los datos de autenticación de referencia almacenados.

1.2.1.2.5 Auto-tests

23 El TOE deberá realizar auto-tests durante el proceso de arranque (power-up), bajo demanda y pruebas condicionales. En caso de fallo de alguna de las pruebas, el TOE entrará en estado de error y se indicará por el **I/P de**

**salida de estado**, inhibiéndose su funcionalidad criptográfica y el **I/P de salida de datos.**

24 Se realizan auto-tests de los algoritmos criptográficos aprobados (mediante KAT), integridad del SW/FW, funciones críticas.

25 En cuanto a las pruebas condicionales: consistencia entre pares (de claves), integridad en carga de SW/FW, entrada manual de claves, RNG continuo.

1.2.1.2.6 Auditoría

26 El TOE proporciona la capacidad de detectar y registrar los eventos relevantes a la seguridad. La información registrada debe permitir asociar los eventos con usuarios.

27 El entorno en el que opera el TOE, deberá revisar los registros generados por el TOE con el objeto de detectar posibles violaciones de seguridad o negligencias, haciendo responsables de sus acciones a los usuarios autenticados.

### 1.2.2 Uso del TOE

28 El TOE se usa como módulo de seguridad HW que proporciona funciones de seguridad a un sistema que lo invoca para realizar operaciones criptográficas. El TOE protege de manera adecuada todo el material criptográfico involucrado en dichas operaciones.

29 El sistema usará el TOE para proteger los datos de usuario durante las transmisiones sobre canales para los que existen sujetos que no tienen permiso de acceso a los mismos. Se consideran usuarios del TOE a las aplicaciones del sistema que hacen uso de sus servicios. Las aplicaciones pueden ser del tipo autoridad de sellado de tiempo (TSA), autoridad de certificación (CA), en sistemas bancarios, como parte del sistema de verificación de transacciones, aplicaciones de firma electrónica, proxy de correo electrónico, etc…

30 El TOE, para su uso, proporciona, los interfaces especificados en la sección anterior:

- I/P de entrada de datos
- I/P de salida de datos
- I/P de entrada de control
- I/P de salida de estado
- I/P de alimentación

### 1.2.3 Hardware, software y firmware no incluido en el TOE

31 El TOE es un conjunto de HW con su correspondiente SW y/o FW, que implementa funciones criptográficas o procesos criptográficos (incluyendo algoritmos criptográficos y opcionalmente generación de claves) y que está contenido dentro de unos límites criptográficos definidos. El TOE debe implementar al menos una función de seguridad aprobada (ver [FIPS-ANEXOS]).

32 El perímetro físico establece los límites del TOE. Se consideran elementos HW, SW no incluidos en el TOE, todos aquellos fuera el perímetro físico definido. Estos elementos formarán parte del entorno operativo del TOE y deberán cumplir los requisitos de interfaces y operación expuestos en este PP.

33 Teniendo en cuenta los diferentes tipos de TOEs especificados en este perfil de protección, a la hora de definir el HW, SW y FW no incluido en el TOE , hay que tener en cuenta la capacidad del TOE de funcionar en modo "standalone" o bien que deba estar empotrado ("embedded") en un sistema para que pueda operar.

- En el caso de **TOEs single-chip,** si hablamos, por ejemplo de una smartcard, el entorno lógico de operación será cualquiera que sea capaz de comunicarse con el TOE con el que quiere operar y ejercitar sus servicios a través de los interfaces declarados en la sección 1.2.2 Uso del TOE: I/P de entrada de datos, I/P de salida de datos, I/P de entrada de control, I/P de salida de estado, I/P de alimentación. Si el módulo es un chip que hay que integrar en una placa que está fuera de los límites del módulo, además el entorno físico y que no forma parte del TOE será aquél que cumpla con los requisitos físicos de los interfaces necesarios para integrar el chip en la placa (pinout, separación física, alimentación - I/P de alimentación);

- **Multi-chip stand-alone**: el entorno de operación será cualquiera que sea capaz de comunicarse con el TOE con el que quiere operar y ejercitar sus servicios a través de los interfaces declarados en la sección 1.2.2 Uso del TOE: I/P de entrada de datos, I/P de salida de datos, I/P de entrada de control, I/P de salida de estado, I/P de alimentación.

- **TOEs multi-chip embedded:** como este tipo de TOEs necesitan, para su operación, un sistema que los aloje, el HW, SW y/o FW necesario en el entorno y que no forma parte del TOE será aquél que cumpla con:

1. los requisitos físicos de los interfaces necesarios para empotrar el TOE (slots, buses, separación física, alimentación - I/P de alimentación);

2. con los requisitos lógicos que le permiten comunicarse con el TOE con el que quiere operar y ejercitar sus servicios a través de los interfaces declarados en la sección 1.2.2 Uso del TOE: I/P de entrada de datos, I/P de salida de datos, I/P de entrada de control, I/P de salida de estado.

34 Se pueden excluir del TOE componentes HW, SW y FW que estén dentro del perímetro físico si el autor de la declaración de seguridad que declara conformidad con este PP, demuestra que no afectan a la seguridad del TOE.

# 2 Declaración de conformidad

## 2.1 Conformidad con respecto a la norma CC

35 Este perfil de protección se desarrolla conforme a la norma Common Criteria versión 3.1 R3 de Julio de 2009:

- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1 R3, Julio 2009, [CC31p2].
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1 R3, Julio 2009, [CC31p3].

según lo siguiente:

- [CC31p2] Parte 2 extendida;
- [CC31p3] Parte 3;
- Conforme al paquete de garantía EAL4 según [CC31p3].

36 Este Perfil de Protección, y las declaraciones de seguridad que declaren su cumplimiento, se deberán evaluar utilizando la metodología de evaluación definida en:

- Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1 R3, Julio 2009, [CEM31].

37 En la sección **5 Definición de componentes extendidos** de esta declaración de seguridad se incluyen los componentes extendidos definidos.

## 2.2 Conformidad con otros perfiles de protección

38 Este PP no declara el cumplimiento de ningún otro PP.

## 2.3 Declaraciones de conformidad con respecto a este PP

39 Este PP requiere que la conformidad al mismo se declare de manera estricta, tal como se define en la norma CC.

# 3 Definición del problema de seguridad (SPD)

40 Esta sección define el problema de seguridad que se quiere resolver. En lo que respecta a la norma CC, el problema de seguridad es axiomático en el sentido de que el proceso seguido para la derivación final del mismo, está fuera del alcance de la norma, es decir, no se valora.

## 3.1 Activos del TOE

41 Se tienen en cuenta los siguientes activos:

| Id | Descripción del Activo | Valor del activo |
|---|---|---|
| A.PLAIN | Datos de usuario que están en claro. | Confidencialidad<br>Integridad |
| A.CLAVES_SECRETAS | Claves secretas utilizadas en las funciones de seguridad y protocolos implementados mediante algoritmos criptográficos simétricos.<br><br>Se incluyen tanto claves usadas en los servicios que exporta el TOE para el sistema externo, como claves usadas internamente en los mecanismos de protección del TOE. | Confidencialidad<br>Integridad |
| A.CLAVES_PRIVADAS | Claves privadas utilizadas en las funciones de seguridad y protocolos implementados mediante algoritmos criptográficos asimétricos.<br><br>Se incluyen tanto claves usadas en los servicios que exporta el TOE para el sistema externo, como claves usadas internamente en los mecanismos de protección del TOE. | Confidencialidad<br>Integridad |
| A.CLAVES_PUBLICAS | Claves públicas utilizadas en las funciones de seguridad y protocolos implementados mediante algoritmos criptográficos asimétricos | Integridad<br>Autenticidad |
| A.RAD | Datos de autenticación de referencia almacenados por el TOE de forma permanente para la comprobación de autenticación de los usuarios. Se | Confidencialidad<br>Integridad |

| | | |
|---|---|---|
| | corresponde con los credenciales de un usuario o de un crypto-officer. | |

## 3.2 Amenazas

42 Se consideran las siguientes amenazas y valores del los activos afectados (C - Confidencialidad, I-integridad, A-Autenticidad):

| Id | Descripción | Activos afectados |
|---|---|---|
| T.CSP_CONF | Comprometer confidencialidad de parámetros críticos de seguridad (CSP). El atacante puede tener acceso físico al TOE o bien realizar el ataque en remoto tomando el control del sistema que interacciona con el TOE.<br><br>El agente es un **atacante no autorizado** a la organización con recursos y experiencia limitada. El potencial de ataque asociado al atacante es "**Enhanced basic**".<br><br>Este ataque permitiría en segundo orden comprometer los datos de usuarios protegidos. | A.CLAVES_SECRETAS (C)<br>A.CLAVES_ PRIVADAS (C)<br>A.RAD (C) |
| T.CSP_INTEG | Comprometer integridad o autenticidad de parámetros críticos de seguridad (CSP) o funciones de seguridad. El atacante puede tener acceso físico al TOE o bien realizar el ataque en remoto tomando el control del sistema que interacciona con el TOE.<br><br>El agente es un **atacante no autorizado** a la organización con recursos y experiencia. El potencial de ataque asociado al atacante es "**Enhanced basic**".<br><br>Este ataque permitiría en segundo orden comprometer los datos de usuarios protegidos. | A.CLAVES_ PUBLICAS (A)<br>A.CLAVES_SECRETAS (I)<br>A.CLAVES_ PRIVADAS (I)<br>A.RAD (I) |
| T.ABUSO | Abuso de las funciones de instalación, configuración o mantenimiento del TOE.<br>El atacante podría usar estas funciones para revelar o manipular CSPs operacionales o | A.PLAIN (CI)<br>A.CLAVES_SECRETAS (CI)<br>A.CLAVES_ PRIVADAS (CI)<br>A.CLAVES_ PUBLICAS (IA) |

| | | |
|---|---|---|
| | datos de usuario o para posibilitar ataques sobre la integridad o confidencialidad de CSPs operacionales o datos de usuario mediante la manipulación (exploración, bypass, cambio o desactivación) de mecanismos de seguridad o revelando o manipulando datos de la TSF.<br><br>El agente es un **atacante interno a la organización** con recursos y experiencia limitada. El potencial de ataque asociado al atacante es "**Enhanced basic**". | A.RAD (CI) |
| T.PHY_TAMPER | Modificación de las medidas de seguridad físicas de forma que el atacante pueda acceder a los CSPs y/o datos de usuarios almacenados y comprometer su confidencialidad o integridad.<br><br>El agente es un **atacante no autorizado con acceso físico al TOE** con recursos y experiencia limitada. El potencial de ataque asociado al atacante es "**Enhanced basic**". | A.PLAIN (CI)<br>A.CLAVES_SECRETAS (CI)<br>A.CLAVES_ PRIVADAS (CI)<br>A.CLAVES_ PUBLICAS (IA)<br>A.RAD (CI) |
| T.SUPLANTAR | El atacante se hace pasar por una fuente de datos autorizada o receptor autorizado para realizar operaciones de usuarios autorizado o acceder al TOE sin ser detectado comprometiendo la integridad y confidencialidad de los activos.<br><br>El agente es un **atacante no autorizado** con recursos y experiencia limitada. El potencial de ataque asociado al atacante es "**Enhanced basic**". | A.PLAIN (CI)<br>A.CLAVES_SECRETAS (CI)<br>A.CLAVES_ PRIVADAS (CI)<br>A.CLAVES_ PUBLICAS (IA)<br>A.RAD (CI) |

## 3.3 Políticas de seguridad organizativas (OSPs)

43 Esta sección detalla las políticas de seguridad organizativas en forma de reglas, prácticas o guías que se siguen en la empresa.

| Id | Descripción |
|---|---|
| P.FUN_APROBADAS | Las funciones de seguridad del módulo (TOE) deberán estar aprobadas en FIPS o recomendadas por el NIST, por lo que deberán estar incluidas en los anexos correspondientes |

| | |
|---|---|
| | [FIPS-ANEXOS] de [FIPS1402]. El módulo criptográfico (TOE) deberá implementar al menos una función de seguridad aprobada usada en un modo de operación aprobado. |
| P.IA | Todos los usuarios deberán identificarse y autenticarse frente al TOE antes de permitirse cualquier acción (excepto self-tests) presentando sus credenciales que serán de tipo individual y no por grupos de usuarios. |
| P.ROLES | Se separará y se distinguirá al menos entre los siguientes roles: usuarios y crypto-officer. En el caso de que se permita que operadores realicen labores de mantenimiento del módulo (TOE), se deberá incluir un rol a tal efecto. Antes de identificarse, los usuarios tendrán el rol de usuario no identificado.<br>Los roles deberán ser asignados a personas diferentes de la organización. |
| P.INTERFACES | Se proporcionarán los siguientes tipos de interfaces o *puertos* (I/P):<br><br>- I/P de entrada de datos;<br>- I/P de salida de datos;<br>- I/P de entrada de control;<br>- I/P de salida de estado;<br>- I/P de alimentación. |
| P.SERVICIOS | Se proporcionarán al menos los siguientes servicios: mostrar el estado del TOE, realizar auto-testing y ejecutar las funciones de seguridad (aprobadas por FIPS o recomendadas por NIST según [FIPS-ANEXOS]). |
| P.AUDIT | Se registrarán los eventos de seguridad del sistema de forma que se pueda asociar a los usuarios del TOE con sus acciones.<br><br>El entorno en el que opera el TOE deberá revisar los registros generados por el TOE con el objeto de detectar posibles violaciones de seguridad o negligencias, haciendo responsables de sus acciones a los usuarios autenticados. |

## 3.4 Hipótesis

44 Esta sección detalla hipótesis que se hacen sobre el entorno operacional en el que opera el TOE. Si el TOE opera en un entorno que no cumple estas

hipótesis, éste no será capaz de proporcionar su funcionalidad de seguridad.

| Id | Descripción |
|---|---|
| H.GENERACIÓN_CLAVES | Las claves generadas por el entorno e importadas dentro del TOE deberán cumplir los mismos requisitos que se exigen al material criptográfico generado internamente por el TOE. |
| H.DISPONIBILIDAD | El entorno (el sistema que usa el TOE), asegura la disponibilidad del material criptográfico necesario que depende de él. |

# 4 Objetivos de seguridad

45 Esta sección define los objetivos de seguridad que permiten resolver el problema de seguridad expuesto en la anterior sección. Se exponen los objetivos de seguridad para el TOE y los objetivos de seguridad para el entorno operacional.

## 4.1 Objetivos de seguridad para el TOE

| Id | Descripción |
|---|---|
| O.FUN_APROBADAS | El TOE debe implementar funciones de seguridad que estén aprobadas en FIPS o recomendadas por el NIST, por lo que deberán estar incluidas en los anexos correspondientes [FIPS-ANEXOS] de [FIPS1402]. El TOE deberá implementar al menos una función de seguridad aprobada usada en un modo de operación aprobado. |
| O.IA | EL TOE debe verificar y autenticar a todos los usuarios antes de permitirse cualquier acción (excepto self-tests). Los credenciales que verifica y autentica el TOE deberán ser de tipo individual y no por grupos de usuarios. |
| O.ROLES | El TOE soportará los siguientes roles: usuarios y crypto-officer. En el caso de que se permita que operadores realicen labores de mantenimiento del TOE, deberá incluir un rol a tal efecto.<br><br>Existirá un rol de usuario no identificado que será el que se asigne a los usuarios antes de identificarse. |
| O.INTERFACES | El TOE proporcionará los siguientes tipos de interfaces o *puertos* (I/P):<br><br>(A) **I/P de entrada de datos**: para todos los datos (excepto los datos de control que entran por el I/P de entrada de control) que entren y sean procesados por el TOE (incluyendo datos en claro, datos cifrados, material criptográfico y CSPs, datos de autenticación e información de estado de otra entidad);<br><br>(B) **I/P de salida de datos**: para todos los datos (excepto los datos de estado que salen por el I/P |

| | |
|---|---|
| | de estado) que salen del TOE (incluyendo datos en claro, datos cifrados, material criptográfico y CSPs, datos de autenticación e información de control para otra entidad);<br><br>(C) **I/P de entrada de control:** para todos comandos de entrada, señales y datos de control (incluyendo llamadas a funciones, controles manuales, botones, teclado) usados para el control de la operación del TOE;<br><br>(D) **I/P de salida de estado:** para la salida de señales, indicadores y datos de estado (incluyendo códigos de retorno de las funciones, indicadores físicos como LEDs o pantallas) que se usan para indicar el estado del TOE;<br><br>(E) **I/P de alimentación:** fuentes de alimentación externas. |
| O.SEP_INTERFACES | Los interfaces físicos usados para la entrada y salida de material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar físicamente separados de otros interfaces, o bien los interfaces lógicos usados para la entrada y salida de material criptográfico y CSPs en claro (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar lógicamente separados utilizando un "*trusted path*".<br><br>El material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales) debe entrar/salir directamente al módulo (TOE) mediante, por ejemplo, un "*trusted path*" o un cable directamente conectado.<br><br>Se aplica la definición del término "*trusted path*", según [FIPS1402] incluida en la sección 7.2 Definiciones, que considera un canal que proporciona la confianza necesaria para cumplir la política de seguridad del módulo y su operación. En este perfil de protección se considera que los requisitos de entrada/salida de material criptográfico y demás CSPs (cifrado y split knowledge) indicados, establecen la política de seguridad necesaria para confiar en el |

| | |
|---|---|
| | canal. |
| O.STATUS_FUN_APR | El TOE deberá proporcionar los servicios:<br>1. Mostrar el estado del TOE a través del interface de salida de estado;<br>2. Ejecutar las funciones de seguridad (aprobadas por FIPS o recomendadas por NIST según [FIPS-ANEXOS]). |
| O.SELF_TEST | El TOE deberá proporcionar el servicio de auto-test durante el proceso de arranque (power-up), bajo demanda y pruebas condicionales.<br><br>Se realizan auto-test de los algoritmos criptográficos aprobados (KAT), integridad del SW/FW, funciones críticas.<br><br>En cuanto a las pruebas condicionales: consistencia entre pares (de claves), integridad en carga de SW/FW, entrada manual de claves, RNG continuo.<br><br>La salida de datos se deberá inhibir cuando el TOE se encuentre en un estado de error o cuando esté en modo auto-testing. |
| O.CONTROL_ACCESO_SERVICIOS | El TOE deberá restringir el acceso a sus servicios dependiendo el rol del usuario. La asignación de los servicios a los roles deberá hacerse por defecto a bien por una acción explícita del administrador (crypto-officer). |
| O.GESTIÓN_CLAVES | El módulo (TOE) gestionará de manera eficiente y segura el material criptográfico necesario en los algoritmos y protocolos implementados y sus atributos de seguridad.<br><br>El TOE asociará atributos de seguridad de la entidad a la que es asignada la clave (secreta, privada o pública), de forma que las claves se puedan asociar con la entidad correcta (persona, grupo o proceso). |
| O.CONTROL_ACCESO_CLAVES | El TOE deberá restringir el acceso al material criptográfico y otros CSPs en base a sus atributos de seguridad. |
| O.IO_CLAVES | Para entrada y salida de claves:<br><br>(A) Si se usan métodos automáticos, las claves |

| | |
|---|---|
| | privadas y secretas entrarán y saldrán del TOE cifradas.<br>(B) Si se usan métodos manuales, las claves privadas y secretas entrarán y saldrán del módulo (TOE) cifradas o mediante la implementación de algún procedimiento de conocimiento dividido (split-knowledge).<br>(C) Las claves públicas pueden entrar y salir del módulo (TOE) en claro.<br><br>La exportación e importación de claves se realiza con sus atributos de seguridad. Se protege la integridad de las claves y sus atributos.<br><br>La salida de datos se inhibe durante el proceso de generación de claves, entrada manual de claves a través de este puerto, Self-test, estado de error, destrucción de claves y carga de software. |
| O.GENERACIÓN_CLAVES | EL TOE deberá generar claves utilizando algoritmos criptográficos de generación de claves y RNGs aprobados, según [FIPS-ANEXOS]. |
| O.DESTRUCCIÓN_CLAVES | El TOE deberá destruir todo el material criptográfico y otros CSPs por demanda del crypto-officer o como caso de tamper-response en caso de que el TOE se vea comprometido físicamente. |
| O.PHYSICAL_PROTECCIÓN | El TOE debe resistir ataques físicos de un atacante con potencial de ataque **Enhanced Basic.**<br><br>El TOE debe implementar mecanismos HW de protección contra manipulaciones físicas y sondado de canales, proporcionando evidencia de la manipulación ("*tamper evidence*") y respondiendo automáticamente de forma que no se comprometan los activos que se protegen: mecanismos "*tamper response*" que deberán destruir inmediatamente el material criptográfico y demás CSPs en cuanto que se detecte la manipulación física ("*zeroization*"). Estos mecanismos se aplican especialmente cuando existen tapas que se puedan eliminar o interfaces para la realización de operaciones de mantenimiento del módulo (TOE). |
| O.AUDITORÍA | El TOE debe proporcionar la capacidad de detectar y registrar los eventos relevantes a la seguridad. La |

| | |
|---|---|
| | información registrada deberá permitir asociar los eventos con usuarios. |



## 4.2 Objetivos de seguridad para el entorno operacional

| Id | Descripción |
|---|---|
| OE.GENERACIÓN_CLAVES | Las claves generadas por el entorno e importadas dentro del TOE deberán cumplir los mismos requisitos que se exigen al material criptográfico generado internamente por el TOE. |
| OE.DISPONIBILIDAD | El entorno (el sistema que usa el TOE), deberá asegurar la disponibilidad del material criptográfico necesario que depende de él. |
| OE.PERSONAL | El entorno del TOE deberá asegurar que el rol de administrador (Crypto-officer), el rol de usuario y, en caso de existir, el rol de mantenimiento, deberán ser asignados a personas diferentes de la organización.<br><br>El entorno del TOE deberá asegurar que los administradores del TOE (Crypto-officer, rol de mantenimiento) son confiables y cuidan de la seguridad y correcto funcionamiento del TOE. |
| OE.AUDITORÍA | El entorno del TOE deberá revisar los registros de auditoría generados por el TOE para detectar posibles violaciones, pudiéndose asociar las acciones a los usuarios del TOE.<br>El administrador (crypto-officer) es responsable de configurar la auditoría. |

## 4.3 Justificación de los objetivos de seguridad

| | T.CSP_CONF | T.CSP_INTEG | T.ABUSO | T.PHY_TAMPER | T.SUPLANTAR | P.FUN_APROBADAS | P.IA | P.ROLES | P.INTERFACES | P.SERVICIOS | P.AUDIT | H.GENERACIÓN_CLAVES | H.DISPONIBILIDAD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **O. FUN_APROBADAS** | | | | | | X | | | | | | | |
| **O.IA** | X | X | | | X | | X | | | | X | | |
| **O.ROLES** | | | X | | | | | X | | | | | |
| **O.INTERFACES** | | | | | | | | | X | | | | |
| **O.SEP_INTERFACES** | X | X | | | X | | | | | | | | |
| **O.STATUS_FUN_APR** | | | | | | | | | | X | | | |
| **O.SELF_TEST** | | X | | | | | | | | X | | | |
| **O.CONTROL_ACCESO_SERVICIOS** | | | X | | X | | | | | | | | |
| **O.GESTIÓN_CLAVES** | X | X | | | | | | | | | | | |
| **O.CONTROL_ACCESO_CLAVES** | X | X | | | X | | | | | | | | |
| **O.IO_CLAVES** | X | X | | | | | | | | | | | |
| **O.GENERACIÓN_CLAVES** | X | | | | | | | | | | | | |
| **O.DESTRUCCIÓN_CLAVES** | X | | | X | | | | | | | | | |
| **O.PHYSICAL_PROTECCIÓN** | | | | X | | | | | | | | | |
| **O.AUDITORÍA** | | | | | | | | | | | X | | |
| **OE. GENERACIÓN_CLAVES** | | | | | | | | | | | | X | |
| **OE.DISPONIBILIDAD** | | | | | | | | | | | | | X |
| **OE.PERSONAL** | | | X | | | | | X | | | | | |
| **OE. AUDITORÍA** | | | | | | | | | | | X | | |

**Correspondencia de los objetivos de seguridad**

46 A continuación se justifica la necesidad y suficiencia de cada objetivo de seguridad para contrarrestar las amenazas, cumplir las políticas organizativas y soportar las suposiciones de entorno.

47 La amenaza T.CSP_CONF, compromete la confidencialidad o autenticidad de parámetros críticos de seguridad (CSP) pudiendo el atacante realizar ataque contra la confidencialidad o integridad de los datos de usuario. El objetivo de seguridad del TOE O.IA, requiere que el TOE verifique y autentique a todos los usuarios antes de permitirse cualquier acción (excepto self-tests). El objetivo de seguridad del TOE O.CONTROL_ACCESO_CLAVES requiere que el TOE restrinja el acceso al material criptográfico y otros CSPs en base a sus atributos de seguridad.

El objetivo de seguridad del TOE O.GESTIÓN_CLAVES asegura que los atributos de seguridad asociados a las claves se gestiona de manera eficiente y segura. El objetivo de seguridad del TOE O.IO_CLAVES obliga a que la entrada salida de claves se haga cifrada o mediante métodos split-knowledge. El objetivo de seguridad del TOE O.GENERACIÓN_CLAVES asegura que el TOE genera claves utilizando algoritmos criptográficos de generación de claves y RNGs aprobados, según [FIPS-ANEXOS], por lo que se asegura su fortaleza. El objetivo de seguridad del TOE O.DESTRUCCIÓN_CLAVES requiere la destrucción de todo el material criptográfico y otros CSPs por demanda del crypto-officer. El objetivo de seguridad del TOE O.SEP_INTERFACES protege la confidencialidad de CSPs al requerir una separación física o lógica de los interfaces para CSPs de otros interfaces.

48 La amenaza T.CSP_INTEG, compromete la integridad de parámetros críticos de seguridad (CSP) o funciones de seguridad pudiendo el atacante realizar ataque contra la confidencialidad o integridad de los datos de usuario. El objetivo de seguridad del TOE O.IA, requiere que el TOE verifique y autentique a todos los usuarios antes de permitirse cualquier acción (excepto self-tests). El objetivo de seguridad del TOE O.CONTROL_ACCESO_CLAVES requiere que el TOE restrinja el acceso al material criptográfico y otros CSPs en base a sus atributos de seguridad. El objetivo de seguridad del TOE O.GESTIÓN_CLAVES asegura que los atributos de seguridad asociados a las claves se gestiona de manera eficiente y segura. El objetivo de seguridad del TOE O.IO_CLAVES obliga a que la entrada salida de claves se haga cifrada o mediante métodos split-knowledge. El objetivo de seguridad del TOE O.SEP_INTERFACES protege la confidencialidad de CSPs al requerir una separación física o lógica de los interfaces para CSPs de otros interfaces. El objetivo de seguridad del TOE O.SELF_TEST requiere que el TOE realice chequeos regulares para verificar que sus componentes operan correctamente.

49 La amenaza T.ABUSO se basa en el mal uso de las funciones de instalación, configuración o mantenimiento del TOE. El objetivo de seguridad del TOE O.ROLES requiere que el TOE soporte los siguientes roles: usuarios, crypto-officer y, en el caso de que se permita que operadores realicen labores de mantenimiento del TOE, incluirá un rol a tal efecto. Con el objetivo del entorno OE.PERSONAL se asegura que el rol de administrador (Crypto-officer), el rol de usuario y, en caso de existir, el rol de mantenimiento, sean asignados a personas diferentes de la organización y los administradores del TOE (Crypto-officer, rol de mantenimiento) son confiables y cuidan de la seguridad y correcto funcionamiento del TOE. El objetivo de seguridad del TOE O.CONTROL_ACCESO_SERVICIOS requiere que el TOE restrinja el acceso a sus servicios dependiendo el rol del usuario.

50 La amenaza T.PHY_TAMPER consiste en la modificación de las medidas de seguridad físicas de forma que el atacante pueda acceder a los CSPs y/o datos de usuarios almacenados y comprometer su confidencialidad o integridad. El objetivo de seguridad de TOE O.PHYSICAL_PROTECCIÓN requiere que el TOE resista a ataques físicos de un atacante con potencial de ataque **Enhanced Basic y define los mecanismos HW que debe implementar para la** protección contrarrestar directamente la amenaza. Además, el objetivo de seguridad del TOE O.DESTRUCCIÓN_CLAVES requiere que el TOE destruya todo el material criptográfico y otros CSPs por demanda del crypto-officer o como caso de tamper-response en caso de que el TOE se vea comprometido físicamente.

51 La amenaza T.SUPLANTAR, describe que el atacante se hace pasar por una fuente de datos autorizada o receptor autorizado para realizar operaciones de usuarios autorizado o acceder al TOE sin ser detectado comprometiendo la integridad y confidencialidad de los activos. El objetivo de seguridad del TOE O.IA, requiere que el TOE verifique y autentique a todos los usuarios antes de permitirse cualquier acción (excepto self-tests). El objetivo de seguridad del TOE O.CONTROL_ACCESO_SERVICIOS requiere que el TOE restrinja el acceso a sus servicios dependiendo el rol del usuario. El objetivo de seguridad del TOE O.CONTROL_ACCESO_CLAVES requiere que el TOE restrinja el acceso al material criptográfico y otros CSPs en base a sus atributos de seguridad. El objetivo de seguridad del TOE O.SEP_INTERFACES protege la confidencialidad de CSPs al requerir una separación física o lógica de los interfaces para CSPs de otros interfaces.

52 La política P.FUN_APROBADAS especifica que las funciones de seguridad del módulo (TOE) sean funciones aprobadas en FIPS o recomendadas por el NIST. La política se cumple directamente por el objetivo de seguridad del TOE O.FUN_APROBADAS.

53 La política P.IA especifica que todos los usuarios deberán identificarse y autenticarse frente al TOE antes de permitirse cualquier acción presentando sus credenciales que serán de tipo individual y no por grupos de usuarios. Esto se asegura directamente mediante el objetivo de seguridad del TOE O.IA.

54 La política P.ROLES, especifica que se separará y se distinguirá entre los roles usuario, crypto-officer y, en el caso de que se permita que operadores realicen labores de mantenimiento del módulo (TOE), se deberá incluir un rol a tal efecto. Los roles serán asignados a personas diferentes de la organización. El objetivo de seguridad del TOE O.ROLES requiere que el TOE soporte los siguientes roles: usuarios, crypto-officer y, en el caso de que se permita que operadores realicen labores de

mantenimiento del TOE, incluirá un rol a tal efecto. Con el objetivo del entorno OE.PERSONAL se asegura que el rol de administrador (Crypto-officer), el rol de usuario y, en caso de existir, el rol de mantenimiento, sean asignados a personas diferentes de la organización.

55 La política P.INTERFACES, especifica que el TOE proporcionará los siguientes tipos de interfaces o *puertos* (I/P): I/P de entrada de datos, I/P de salida de datos, I/P de entrada de control, I/P de salida de estado y I/P de alimentación. Esto se asegura directamente mediante el objetivo de seguridad del TOE O.INTERFACES.

56 La política P.SERVICIOS especifica que el TOE proporcionará al menos los siguientes servicios: mostrar el estado del TOE, realizar auto-testing y ejecutar las funciones de seguridad (aprobadas por FIPS o recomendadas por NIST según [FIPS-ANEXOS]). El objetivo de seguridad del TOE O.SELF_TEST requiere que el TOE realice chequeos regulares para verificar que sus componentes operan correctamente. El objetivo de seguridad del TOE O.STATUS_FUN_APR requiere que el TOE proporcione los servicios "mostrar el estado del TOE a través del interface de salida de estado" y "ejecutar las funciones de seguridad (aprobadas por FIPS o recomendadas por NIST según [FIPS-ANEXOS])".

57 La política P.AUDIT describe que se registrarán los eventos de seguridad del sistema de forma que se pueda asociar a los usuarios del TOE con sus acciones. Se requiere que el TOE identifique y autentique a los usuarios (objetivo de seguridad del TOE O.IA) y que se proporcione la capacidad de detectar y registrar los eventos relevantes a la seguridad y que la información registrada deberá permitir asociar los eventos con usuarios (objetivo de seguridad del TOE O.AUDITORÍA). El objetivo de seguridad del entorno OE.AUDITORÍA requiere que el entorno del TOE revise los registros de auditoría generados por el TOE para detectar posibles violaciones, pudiéndose asociar las acciones a los usuarios del TOE.

58 La hipótesis H.GENERACIÓN_CLAVES supone que las claves generadas por el entorno (el sistema que usa el TOE) e importadas dentro del TOE tienen la fortaleza suficiente para su uso y atributos seguros. Esta suposición es directamente cubierta por el objetivo del entorno OE. GENERACIÓN_CLAVES.

59 La hipótesis H.DISPONIBILIDAD supone que el entorno (el sistema que usa el TOE), asegura la disponibilidad del material criptográfico necesario que depende de él. Esta suposición es directamente cubierta por el objetivo del entorno OE. DISPONIBILIDAD.

# 5 Definición de componentes extendidos

## 5.1 Definición de la familia FCS_RNG Random Number Generation

60 Se define el componente extendido FCS_RNG.1 para especificar requisitos de generación de números aleatorios en los que los números aleatorios se usan para propósitos criptográficos.

61 La especificación del componente requiere la definición de una nueva familia dentro de la clase FCS de soporte a las funciones criptográficas, ya que no existen SFRs específicos en [CC31p2] que permitan expresar requisitos de uso y métricas de calidad para RNGs.

**62 Family behaviour**

This family defines requirements for the generation of random numbers where the random numbers are used for cryptographic purposes.

**63 Component Levelling**


The family presents a single component.

FCS_RNG.1 Generation of random numbers requires that the random numbers meet a defined quality metric.

**64 Management: FCS_RNG.1**

There are no management activities foreseen.

**65 Audit: FCS_RNG.1**

There are no actions to be auditable.

**66 FCS_RNG.1 Random Number Generation**

Hierarchical to: No other components.

Dependencies: FPT_TST.2.

FCS_RNG.1.1 The TSF shall provide a [*selection: deterministic RNG (DRNG), non-deterministic RNG (NDRNG)* **(*)**] random number generator that meet [*assignment: list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [*assignment: a defined quality metric*].

**(*)** as defined in [FIPS1402]

**Application notes:**

(A) Nondeterministic RNGs may be only used for key generation or to seed Approved deterministic RNGs (see [FIPS_ANEXOS]) used in key generation. Commercially available nondeterministic RNGs may be used for the purpose of generating seeds for Approved deterministic RNGs.

(B) An Approved RNG (see [FIPS_ANEXOS]) shall be used for the generation of cryptographic keys used by an Approved security function.

(C) The output from a non-Approved RNG may be used 1) as input (e.g., seed, and seed key) to an Approved deterministic RNG or 2) to generate initialization vectors (IVs) for Approved security function(s). The seed and seed key shall not have the same value.

(D) The quality metric of the random numbers should be chosen depending on the RNG type and the intended application of the random numbers.

(E) If the seed of a DRNG is entered during key generation, shall be entered as key according with FCS_CKM.5

## 5.2 Definición del componente funcional FPT_TST.2 TSF self test

67 Se define el componente extendido FPT_TST.2 con el objeto de especificar los requisitos de autotesting que permitan satisfacer el objetivo de seguridad del TOE O.SELF-TEST.

68 Se justifica la necesidad del componente extendido ya que el TOE deberá proporcionar el servicio de auto-test durante el proceso de arranque (power-up), bajo demanda y pruebas condicionales.

69 Se utiliza la familia FPT_TST definida en [CC31p2] que proporciona el componente FPT_TST.1 en el que se requiere que el TOE chequee la

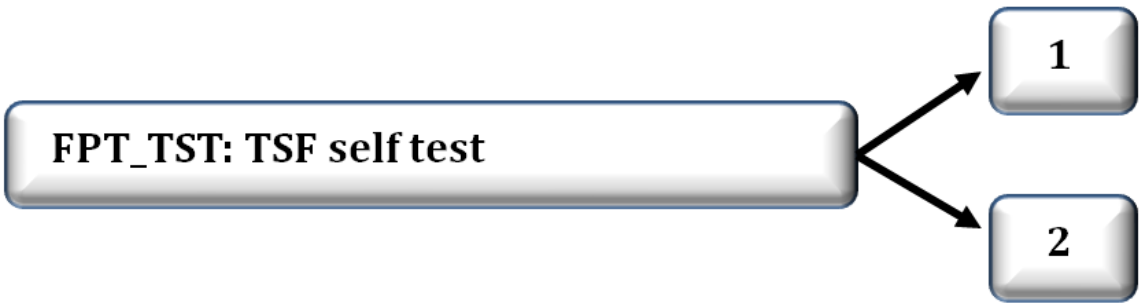
funcionalidad de seguridad (TSF) y la integridad de datos de la TSF y código ejecutable. El nuevo componente incluye la realización de nuevos tipos de autotests cuyos resultados condicionan el comportamiento de TOE. Esta funcionalidad no se contempla con el requisito FPT_TST.1.

70 **Family behaviour**

[*In addition to what is expressed in [CC31p2]* ]:

The family defines the requirements for the self-testing of the TSF with respect to some expected correct operation (an example is an approved security functions self-tested with a KAT (Know Answer Test) approach). These tests can be carried out at start-up, periodically, at the request of the authorised user, or when other conditions are met. The actions to be taken by the TOE as the result of self testing are defined in other families. The requirements of this family are also needed to detect the corruption of TSF executable code (i.e. TSF SW/FW) and critical functions.

71 **Component Levelling**




The family presents two independent components.

[CC31p2]: *"FPT_TST.1 TSF testing, provides the ability to test the TSF's correct operation. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and TSF itself*".

FPT_TST.2 TSF self-testing requires self-testing capabilities of the TSF correct operation. These tests must be performed at start-up. Conditional and on demand by a user self-testing may be required. Particular TSF behaviour during self-testing and TSF-actions after self-testing are required.

72 **Management: FPT_TST.2**

There are no management activities foreseen.

73 **Audit: FPT_TST.2**

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Execution of the TSF self tests and the results of the tests.

74 **FPT_TST.2 Self Testing**

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state.

FPT_TST.2.1 The TSF shall perform self-testing at power-up to verify the correctness of [*assignment: list of cryptographic algorithms approved [FIPS-ANEXOS]*] and of [*assignment: list of critical TSF*], and to verify the integrity of the TSF-software/firmware.

FPT_TST.2.2 The TSF shall perform self-testing at the conditions [*assignment: list of conditions*] to verify the correctness of [*assignment: list of critical cryptographic algorithms*].

FPT_TST.2.3 The TSF shall provide [*assignment: list of users*] with the capability to invoke the following self-tests [*assignment: list of self-tests*].

FPT_TST.2.4 During [*assignment: list of self-tests*] the TSF shall [*assignment: list of actions to be performed*].

FPT_TST.2.5 After completion of self-testing the TSF shall [*assignment: list of actions to be performed*].

FPT_TST.2.6 If the self-testing result is fail the TSF shall [*assignment: list of actions to be performed*].

## 5.3 Definición de la familia FPT_SEP Interfaces Separation

75 Se define el componente extendido “FPT_SEP.1 TSF Interfaces Separation” para especificar requisitos de implementación de interfaces de entrada y salida del TOE concretos y que cumplan unas especificaciones respecto a la separación física y lógica de los mismos basada en la entrada/salida del material criptográfico y demás CSPs.

76 La separación de dominios y garantía de que éstos sean estancos es una propiedad de la arquitectura de seguridad que se exige al diseño del TOE, tal y como se especifica en el componente de garantía ADV_ARC.1. En este caso, se habla de separación de interfaces de entrada y salida de material

criptográfico y demás CSPs que no implica la creación de dominios estancos dentro del TOE.

77 El componente se utiliza para expresar un requisito del TOE que permite dar cumplimiento a los objetivos de seguridad O.INTERFACES y O.SEP_INTERFACES que implican la implementación de interfaces concretos y la garantía de su separación. Estos objetivos hacen cumplir de la política P.INTERFACES y contrarrestan las amenazas T.CSP_CONF, T.CSP_INTEG , T.SUPLANTAR.

78 La especificación del componente requiere la definición de una nueva familia dentro de la clase FPT de protección de la TSF.

**79 Family behaviour**

The component of this family specifies a set of interfaces categories and their use, that shall be implemented by the TOE. It ensures also the existence of separation between those interfaces used for I/O of key material and the interfaces used for user data, control or displaying the status of the TOE.

Satisfying the requirements of this family makes the TSF self-protecting, meaning that an untrusted subject cannot modify or damage the TSF.

**80 Component Levelling**


The family presents a single component.

FPT_SEP.1 TSF interface separation, implements a set of specific interfaces for I/O of key material and other CSPs, user data, control, TOE status and power supply and provides physical and logical separation specifications between these interfaces within the TSF.

**81 Management: FPT_SEP.1**

There are no management activities foreseen.

**82 Audit: FPT_SEP.1**

There are no actions to be auditable.

**83 FPT_SEP.1 TSF Interfaces separation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SEP.1.1 The TSF shall implement the following interfaces or ports: **I/P de entrada de datos, I/P de salida de datos, I/P de entrada de control, I/P de salida de estado, I/P de alimentación.**

FPT_SEP.1.2 The TSF shall enforce the separation between the I/O interfaces or ports according to the following rules:

(A) Los interfaces físicos usados para la entrada y salida de material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar físicamente separados de otros interfaces,
(B) o bien los interfaces lógicos usados para la entrada y salida de material criptográfico y CSPs en claro (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar lógicamente separados utilizando un "trusted path".
(C) El material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales) debe entrar/salir directamente al módulo (TOE) mediante, por ejemplo, un "trusted path" o un cable directamente conectado.

## 5.4 Definición de la familia FPT_FSM Finite State Model

84 Se define el componente extendido "FPT_FSM.1 Finite State Model Operation" para especificar requisitos de implementación de un modelo de estados que definen las restricciones de la operación del módulo conforme a un patrón preestablecido.

85 El modelo de estados finitos se desarrolla como parte de la arquitectura de seguridad (ADV_ARC.1) definiéndose como parte de las propiedades de separación de dominios. Los dominios se describen en términos de los estados del modelo. Se tendrán en cuenta, al menos los siguientes estados operacionales y de error (ver requisitos de documentación de ADV_ARC.1):

i. Power on/off. Estados que definen el arranque y la parada del TOE.

ii. Crypto officer. Refleja los estados en los que se ejecutan los servicios del crypto officer (por ejemplo., inicialización y gestión de claves).

iii. Entrada de claves/CSP. Refleja estados en los que se puede importar claves y CSPs al TOE.

iv. Usuarios. Estados en los que los usuarios autorizados acceden a los servicios, realizan operaciones criptográficas u otras funciones aprobadas o no aprobadas.

v. Self-test. Reflejan los estados en los que el modulo está realizando self-tests.

vi. Error. Estados en los que se ha producido un error (por ejemplo por fallo en self-test o intento de cifrado sin encontrar la clave o CSP adecuado).

Opcionales:

vii. Bypass. Reflejan estados en los que se active la capacidad de bypass y se proporcionan servicios sin procesamiento criptográfico (por ejemplo transferencia del datos en claro a través del TOE);

viii. Mantenimiento. Estados para el mantenimiento del TOE incluyendo pruebas locales físicas y lógicas. En el caso de existir el rol de mantenimiento, deberá existir un estado de mantenimiento.

86 El componente se utiliza para expresar un requisito del TOE que permite dar cumplimiento a los objetivos de seguridad O.STATUS_FUN_APR y O.CONTROL_ACCESO_SERVICIOS permitiendo controlar los modos operacionales que limitan los servicios disponibles.

87 Los requisitos de la operación de módulo conforme al modelo de estado, además de los estados operativos mínimos que debe contemplar el módulo, establecen:

(A) El modelo se establece en base a transiciones entre estados teniendo en cuenta las entradas, los eventos internos y condiciones internas que causan las transiciones, los eventos de salida generados en cada transición.

(B) El modelo no debe permitir que el TOE se encuentre operativo en dos estados a la vez.

(C) Si existe estado de bypass, se deberá demostrar que para entrar en ese estado deberán existir dos eventos independientes.

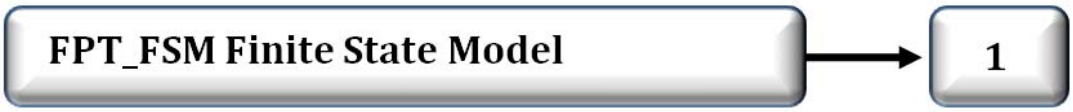
88 La especificación del componente requiere la definición de una nueva familia dentro de la clase FPT de protección de la TSF.

**89 Family behaviour**

The component of this family specifies the requirements for the operation of the module specified through a semi formal method called Finite State Model. The requirements define the minimum set of states to be implemented (and documented) by the module, and the constraints for the transitions and the status of the module.

Satisfying the requirements of this family helps to achieve the TSF domain separation property.

**90 Component Levelling**




The family presents a single component.

FPT_FSM.1 Finite State Model Operation to express the FSM implementation requirements, including the restrictions of the module operation according to the model.

**91 Management: FPT_FSM.1**

There are no management activities foreseen.

**92 Audit: FPT_FSM.1**

There are no actions to be auditable.

**93 FPT_ FSM.1 Finite State Model Operation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FSM.1.1 The TSF shall implement its operation according to the following operational and error states:

(A) Power on/off states. States for primary, secondary, or backup power. These states may distinguish between power sources being applied to a cryptographic module.
(B) Crypto officer states. States in which the crypto officer services are performed (e.g., cryptographic initialization and key management).

(C) Key/CSP entry states. States for entering cryptographic keys and CSPs into the cryptographic module.
(D) User states. States in which authorized users obtain security services, perform cryptographic operations, or perform other Approved or non-Approved functions.
(E) Self-test states. States in which the cryptographic module is performing self-tests.
(F) Error states. States when the cryptographic module has encountered an error (e.g., failed a self-test or attempted to encrypt when missing operational keys or CSPs). Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service or repair of the cryptographic module, or recoverable "soft" errors that may require initialization or resetting of the module. Recovery from error states shall be possible except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.
(G) [*assignment: list and definition of other states*]

FPT_FSM.1.2 The TSF shall fulfil the following restrictions on its operation according to the defined operational and error states:

(A) The operation shall not permit the model to operate in two states at the same time;
(B) To transit to a bypass state (if applicable), the operation shall guarantee the occurrence of two independent events.

## 5.5 Definición del componente funcional FCS_CKM.5 Cryptographic key entry

94 Se define el componente extendido FCS_CKM.5 Cryptographic key entry con el objeto de especificar los requisitos criptográficos para la entrada de claves al TOE.

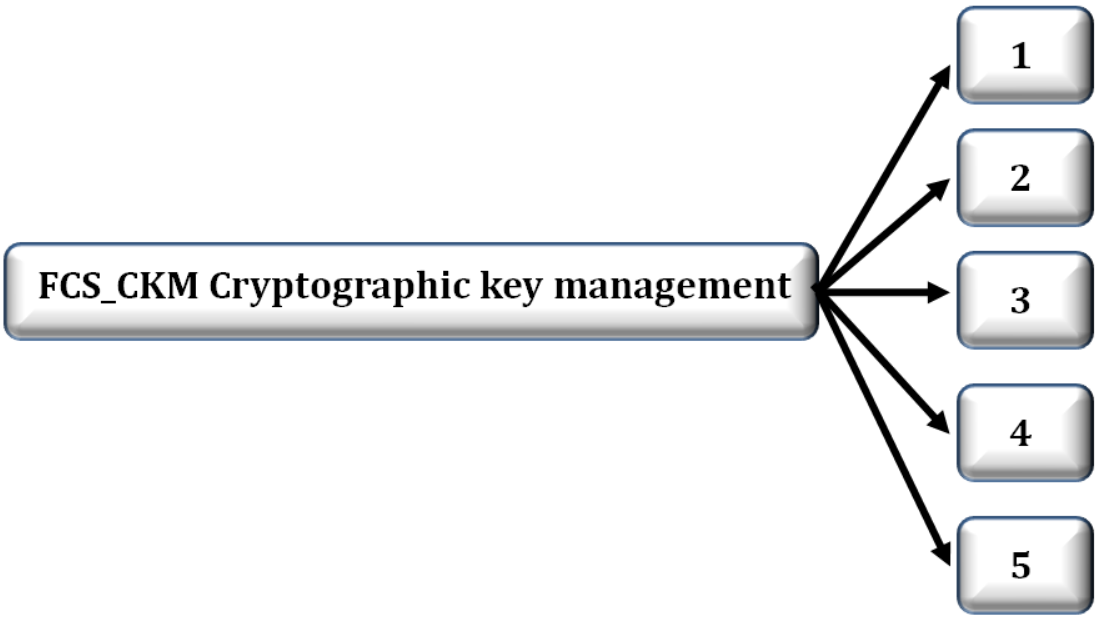
95 Se utiliza la familia FCS_CKM definida en [CC31p2] que especifica componentes para la gestión de claves: generación, acceso, distribución (salida) y destrucción. Este componente nuevo permitirá definir requisitos criptográficos para la entrada de claves y contribuirá a definir una política de importación junto con el componente FDP_ITC.2. El TOE no aceptará claves que no entren protegidas con una función de seguridad aprobada según [FIPS-ANEXOS].

96 **Family behaviour**

[*In addition to what is expressed in [CC31p2]*]:

The family defines the requirements for key entry to the TOE in accordance with a specified cryptographic key entry method that meets approved security functions including in [FIPS-ANEXOS]. This component may be used to define an import policy in conjunction with FDP_ITC.2 component.

97 **Component Levelling**




The family presents five independent components.

[*In addition to what is expressed in [CC31p2]* ]:

FCS_CKM.5 The TSF shall meet the security requirements for key entry when using automated or manual methods. The mechanisms used to implement the security requirements shall be approved in accordance with [FIPS-ANEXOS].

98 **Management: FCS_CKM.5**

There are no management activities foreseen.

99 **Audit: FCS_CKM.5**

There are no actions to be auditable.

100 **FCS_CKM.5 Cryptographic key entry**

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key destruction

**FCS_CKM.5.1** The TSF shall accept only cryptographic keys entered into the TOE in accordance with a specified cryptographic key entry method that meets the following:

(A) Si se usan métodos automáticos, las claves privadas y secretas entrarán en el TOE cifradas.
(B) Si se usan métodos manuales, las claves privadas y secretas entrarán en el módulo (TOE) cifradas o mediante la implementación de algún procedimiento de conocimiento dividido (split-knowledge). Si se usa split knowledge:
    a. El TOE deberá autenticar de manera separada al operador que meta cada componente de la clave;
    b. Se necesitarán al menos dos componentes de la clave para reconstruir la clave criptográfica original
    c. Si se necesita conocer n componentes de la clave para reconstruir la clave original, el conocimiento de cualquier n-1 componente no proporcionará información acerca de la clave original distinta de su longitud.

(C) Las claves públicas pueden entrar en el módulo (TOE) en claro.
**(D)** La protección de las claves y sus atributos se hará con [*assignment: lista de funciones aprobadas [FIPS-ANEXOS]*].

# 6 Requisitos de seguridad del TOE

## 6.1 Requisitos funcionales de seguridad

### 6.1.1 Operaciones criptográficas y gestión de claves

#### 101 FCS_CKM.1 Cryptographic key generation

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

**FCS_CKM.1.1** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: lista de funciones aprobadas [FIPS-ANEXOS]*].

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá realizar las operaciones teniendo en cuenta el uso de funciones de seguridad aprobadas, modos aprobados y tamaños de claves aprobados según [FIPS-ANEXOS].

#### 102 FCS_CKM.5 Cryptographic key entry

Hierarchical to: No other components.

Dependencies: FCS_CKM.4 Cryptographic key destruction

**FCS_CKM.5.1** The TSF shall accept only cryptographic keys entered into the TOE in accordance with a specified cryptographic key entry method that meets the following:

***(A) Si se usan métodos automáticos, las claves privadas y secretas entrarán en el TOE cifradas.***
***(B) Si se usan métodos manuales, las claves privadas y secretas entrarán en el módulo (TOE) cifradas o mediante la implementación de algún procedimiento de conocimiento dividido (split-knowledge). Si se usa split knowledge:***
***a. El TOE deberá autenticar de manera separada al operador que meta cada componente de la clave;***

***b. Se necesitarán al menos dos componentes de la clave para reconstruir la clave criptográfica original***

***c. Si se necesita conocer n componentes de la clave para reconstruir la clave original, el conocimiento de cualquier n-1 componente no proporcionará información acerca de la clave original distinta de su longitud.***

***(C) Las claves públicas pueden entrar en el módulo (TOE) en claro.***

**(D)** ***La protección de las claves y sus atributos se hará con*** [*assignment: lista de funciones aprobadas [FIPS-ANEXOS]*].

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá realizar las operaciones teniendo en cuenta el uso de funciones de seguridad aprobadas, modos aprobados y tamaños de claves aprobados según [FIPS-ANEXOS].

**103** **FCS_CKM.2 Cryptographic key distribution**

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

**FCS_CKM.2.1** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **(*)** that meets the following: [*assignment: lista de funciones aprobadas [FIPS-ANEXOS]*].

**(*) Refinamiento.** Salida de claves:

(A) Si se usan métodos automáticos, las claves privadas y secretas saldrán del TOE cifradas.
(B) Si se usan métodos manuales, las claves privadas y secretas saldrán del módulo (TOE) cifradas o mediante la implementación de algún procedimiento de conocimiento dividido (split-knowledge). Si se usa split knowledge:
   a. El TOE deberá autenticar de manera separada al operador que meta cada componente de la clave;
   b. Se necesitarán al menos dos componentes de la clave para reconstruir la clave criptográfica original

c. Si se necesita conocer n componentes de la clave para reconstruir la clave original, el conocimiento de cualquier n-1 componentes no proporcionará información acerca de la calve original distinta de su longitud.

(C) Las claves públicas pueden salir del módulo (TOE) en claro.
(D) La protección de las claves y sus atributos se hará con funciones aprobadas [FIPS-ANEXOS].

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá realizar las operaciones teniendo en cuenta el uso de funciones de seguridad aprobadas, modos aprobados y tamaños de claves aprobados según [FIPS-ANEXOS]. Lo mismo aplica para el caso de transporte de claves o key wrapping.

104 **FCS_CKM.4 Cryptographic key destruction**

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

**FCS_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: cryptographic key destruction method*] that meets the following: [*assignment: list of standards*].

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá realizar las operaciones teniendo en cuenta lo mecanismos de destrucción de material criptográfico definidos en [FIPS1402].

El TOE deberá destruir todo el material criptográfico y demás CSPs cuando se entra en modo mantenimiento (si aplica), por demanda del crypto-officer o como caso de tamper-response en caso de que el TOE se vea comprometido físicamente. Así mismo, el material criptográfico utilizado en el proceso de mantenimiento (claves específicas para tal proceso) deberán ser zeroizadas cuando se salga del modo mantenimiento.

105 **FCS_COP.1 Cryptographic operation**

Hierarchical to: No other components.
Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

**FCS_COP.1.1** The TSF shall perform [*assignment: list of cryptographic operations*] in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: lista de funciones aprobadas [FIPS-ANEXOS]*].

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá realizar las operaciones teniendo en cuenta el uso de funciones de seguridad aprobadas, modos aprobados y tamaños de claves aprobados según [FIPS-ANEXOS].

106 **FCS_RNG.1 Random Number Generation**

Hierarchical to: No other components.
Dependencies: FPT_TST.2.

**FCS_RNG.1.1** The TSF shall provide a [*selection: deterministic RNG (DRNG), non-deterministic RNG (NDRNG)* **(*)**] random number generator that meet [*assignment: list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [*assignment: a defined quality metric*].

**(*)** as defined in [FIPS1402]

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá describir los requisitos de todos los RNGs usados en el TOE conforme a la nota de aplicación en la definición del componente extendido.

(A) Nondeterministic RNGs may be only used for key generation or to seed Approved deterministic RNGs (see [FIPS_ANEXOS]) used in key generation. Commercially available nondeterministic RNGs may be used for the purpose of generating seeds for Approved deterministic RNGs.

(B) An Approved RNG (see [FIPS_ANEXOS]) shall be used for the generation of cryptographic keys used by an Approved security function.

(C) The output from a non-Approved RNG may be used 1) as input (e.g., seed, and seed key) to an Approved deterministic RNG or 2) to generate initialization vectors (IVs) for Approved security function(s). The seed and seed key shall not have the same value.

(D) The quality metric of the random numbers should be chosen depending on the RNG type and the intended application of the random numbers.

(E) If the seed of a DRNG is entered during key generation, shall be entered as key according with FCS_CKM.2.

### 6.1.2 Separación de interfaces

**107 FPT_SEP.1 TSF interfaces separation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SEP.1.1 The TSF shall implement the following interfaces or ports: **I/P de entrada de datos, I/P de salida de datos, I/P de entrada de control, I/P de salida de estado, I/P de alimentación.**

FPT_SEP.1.2 The TSF shall enforce the separation between the I/O interfaces or ports according to the following rules:

(A) Los interfaces físicos usados para la entrada y salida de material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar físicamente separados de otros interfaces,
(B) o bien los interfaces lógicos usados para la entrada y salida de material criptográfico y CSPs en claro (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar lógicamente separados utilizando un “trusted path”.
(C) El material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales) debe entrar/salir directamente al módulo (TOE) mediante, por ejemplo, un “trusted path” o un cable directamente conectado.

**Nota de Aplicación:**

El TOE proporcionará los siguientes tipos de interfaces o *puertos* (I/P):

a. **I/P de entrada de datos**: para todos los datos (excepto los datos de control que entran por el I/P de entrada de control) que entren y sean procesados por el TOE (incluyendo datos en claro, datos cifrados, material criptográfico y CSPs, datos de autenticación e información de estado de otra entidad);

b. **I/P de salida de datos**: para todos los datos (excepto los datos de estado que salen por el I/P de estado) que salen del TOE (incluyendo datos en claro, datos cifrados, material criptográfico y CSPs, datos de autenticación e información de control para otra entidad);

c. **I/P de entrada de control:** para todos comandos de entrada, señales y datos de control (incluyendo llamadas a funciones, controles manuales, botones, teclado) usados para el control de la operación del TOE;

d. **I/P de salida de estado:** para la salida de señales, indicadores y datos de estado (incluyendo códigos de retorno de las funciones, indicadores físicos como LEDs o pantallas) que se usan para indicar el estado del TOE;

e. **I/P de alimentación:** fuentes de alimentación externas.

### 6.1.3 Modelo de Estados Finitos (FSM)

**108** **FPT_ FSM.1 Finite State Model Operation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FSM.1.1 The TSF shall implement its operation according to the following operational and error states:

(A) Power on/off states. States for primary, secondary, or backup power. These states may distinguish between power sources being applied to a cryptographic module.
(B) Crypto officer states. States in which the crypto officer services are performed (e.g., cryptographic initialization and key management).
(C) Key/CSP entry states. States for entering cryptographic keys and CSPs into the cryptographic module.

(D) User states. States in which authorized users obtain security services, perform cryptographic operations, or perform other Approved or non-Approved functions.
(E) Self-test states. States in which the cryptographic module is performing self-tests.
(F) Error states. States when the cryptographic module has encountered an error (e.g., failed a self-test or attempted to encrypt when missing operational keys or CSPs). Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service or repair of the cryptographic module, or recoverable "soft" errors that may require initialization or resetting of the module. Recovery from error states shall be possible except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.
(G) [*assignment: list and definition of other states*]

FPT_FSM.1.2 The TSF shall fulfil the following restrictions on its operation according to the defined operational and error states:

(A) The operation shall not permit the model to operate in two states at the same time;
(B) To transit to a bypass state (if applicable), the operation shall guarantee the occurrence of two independent events.

**Nota de Aplicación:**

FPT_FSM.1.1 La operativa del TOE se debe representar mediante un modelo de estados finitos (ver ADV_ARC.1) con las restricciones especificadas en los requisitos anteriores. El autor de la declaración de seguridad puede incluir más estados de los mínimos definidos resolviendo la operación.

FPT_FSM.1.2 En el caso de no existir un estado bypass, el requisito se considera satisfecho en lo que ese aspecto se refiere.

### 6.1.4 Identificación y Autenticación

**109** **FIA_ATD.1 User attribute definition**

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

**FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users:

***(A) Identidad;***

***(B) Rol;***

(C) [*assignment: otros atributos*].

**Nota de Aplicación:**

El autor de la declaración de seguridad podrá incluir atributos adicionales.

110 **FIA_UID.1 Timing of identification**

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

**FIA_UID.1.1** The TSF shall allow

***(A) Self tests de acuerdo con FPT_TST.2;***

(B) [*assignment: otras acciones*]

on behalf of the user to be performed before the user is identified.

**FIA_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

111 **FIA_UAU.1 Timing of authentication**

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

**FIA_UAU.1.1** The TSF shall allow

***(A) Self tests de acuerdo con FPT_TST.2;***

***(B) Identificación según FIA_UID.1***

(C) [*assignment: otras acciones*]

on behalf of the user to be performed before the user is authenticated.

**FIA_UAU.1.2** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

**Nota de Aplicación:**

La fortaleza del mecanismo de autenticación deberá cumplir con la siguiente especificación:

(A) Por cada intento de uso del mecanismo, la probabilidad deberá ser menor de 1 entre 1.000.000 de que se de un falso positivo o intento aleatorio con éxito;

(B) Para intentos múltiples de uso durante un periodo de 1 minuto, la probabilidad deberá ser menor de 1 entre 100.000 de que se de un falso positivo o intento aleatorio con éxito;

112 **FIA_UAU.6 Re-authenticating**

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

**FIA_UAU.6.1** The TSF shall re-authenticate the user under the conditions

***(A) Reseteo del TOE;***

***(B) Fin de sesión autenticada y Entrada en nueva sesión;***

(C) [*assignment: otras condiciones en las que se requiere re-autenticación*]

**Nota de Aplicación:**

Se requiere re-autenticación cuando el usuario salga de su sesión y se pretenda arrancar una nueva del mismo usuario (con el mismo u otro rol) o de un nuevo usuario.

113 **FIA_UAU.7 Protected authentication feedback**

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

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

**Nota de Aplicación:**

La realimentación al usuario durante el proceso de autenticación no deberá ser visible cuando se introduzca la contraseña y no deberá debilitar la fortaleza del mecanismo de autenticación (información de fallo o éxito antes de finalizar el proceso).

114 **FIA_AFL.1 Authentication failure handling**

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

**FIA_AFL.1.1** The TSF shall detect when [*selection: [assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values*]] unsuccessful authentication attempts occur related to [*assignment: list of authentication events*].

**FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been [*selection: met, surpassed], the TSF shall [assignment: list of actions*].

**115** **FIA_USB.1 User-subject binding**

Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

**FIA_USB.1.1** The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

***(A) Identidad;***

***(B) Rol;***

(C) [*assignment: otros atributos*].

**FIA_USB.1.2** The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: ***antes de identificarse el sujeto tendrá el rol Usuario no identificado.***

**FIA_USB.1.3** The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

***(A) Antes de identificarse el sujeto tendrá el rol Usuario no identificado. Después de identificarse y autenticarse (o re-autenticarse) se le asignará el rol asignado a ese usuario.***

(B) [*assignment: otras reglas*].

### 6.1.5 Políticas de control de acceso

6.1.5.1 Control de acceso a claves

**116** **FDP_ACC.2 Complete access control / CLAVES**

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

**FDP_ACC.2.1** The TSF shall enforce the ***Política de control de acceso a CLAVES*** on

***(A) Objetos: material criptográficos, CSPs;***

***(B) Sujetos: usuarios o sujetos que los representan;***

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.

117 **FDP_ACF.1 Security attribute based access control / CLAVES**

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

**FDP_ACF.1.1** The TSF shall enforce the ***Política de control de acceso a CLAVES*** to objects based on the following:

***(A) Objetos:***

***a. material criptográfico; atributos: identidad, entidad a la que está ligada, permisos de control de acceso;*** [*assignment: otros atributos de los objetos que pudieran derivar en reglas adicionales*]

***b. CSPs; Atributos: identidad, permisos de control de acceso ;***[*assignment: otros atributos de los objetos que pudieran derivar en reglas adicionales*]

***(B) Sujetos: usuarios o sujetos que los representan; Atributos: la identidad del usuario al que se ha ligado, rol del usuario;***

**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: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

**FDP_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects*]**.**

**FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*assignment: rules, based on security attributes, that explicitly deny access of subjects to objects*].

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá definir las reglas de la política de control de acceso teniendo en cuenta:

- La protección de las claves secretas, claves privadas y CSPs dentro del TOE frente al revelado, modificación y sustitución;
- La protección de las claves públicas dentro del TOE frente a modificación o sustitución no autorizada.

Las reglas de política deberán tener en cuenta el rol del usuario:

- El cryto-officer puede importar claves secretas y privadas cifradas y demás material criptográfico y CSPs si éstos tienen el atributo de seguridad que permite importarlas;
- El cryto-officer puede exportar claves secretas y privadas cifradas y demás material criptográfico y CSPs si éstos tienen el atributo de seguridad que permite exportarlas;
- El cryto-officer puede destruir claves secretas y privadas cifradas y demás material criptográfico y CSPs;
- Un usuario en rol de mantenimiento puede importar y destruir material criptográfico necesario para el proceso de mantenimiento;
- Nadie puede exportar claves secretas o privadas en claro (ver **FCS_CKM.2)**;
- Nadie puede usar una clave para una operación distinta a la especificad en sus atributos de seguridad.
- Reglas de exportación de claves públicas.

El autor de la declaración de seguridad podrá definir reglas adicionales en base nuevos atributos, por ejemplo de las claves:

- Atributo de USO de la clave;

- PERIODO DE VALIDEZ: si se establece un periodo de validez (comprobar con FPT_STM), no se concede el acceso para claves caducadas;

- Se puede fijar el atributo de clave EXPORTABLE que concederá acceso a la clave para realizar la operación; etc.

118 **FMT_MSA.1 Management of security attributes / CLAVES**

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

**FMT_MSA.1.1** The TSF shall enforce the ***Política de control de acceso a CLAVES*** to restrict the ability to [*selection: change_default, query, modify, delete, [assignment: other operations*]] the security attributes [*assignment: list of security attributes*] to *[assignment: the authorised identified roles*].

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá definir las operaciones que se pueden hacer sobre los atributos de los objetos declarados en dicha política y quién las puede hacer. Los usuarios pueden modificar atributos de sus claves. El crypto-officer puede modificar los atributos de seguridad de las claves del sistema. El autor de la declaración de seguridad definirá qué roles pueden realizar las operaciones especificadas sobre los atributos de seguridad. En el caso de no poderse modificar ningún atributo de seguridad del material criptográfico y demás CSPs (es decir, viene fijado en la inicialización del HSM), se incluirá "none" en la operación [*assignment: list of security attributes*] y se considerará este requisito satisfecho.

(A) atributos del material criptográfico que se podrían modificar: entidad a la que está ligada, permisos de control de acceso;

(B) atributos de CSPs: permisos de control de acceso;

119 **FMT_MSA.3 Static attribute initialisation / CLAVES**

Hierarchical to: No other components.
Dependencies:
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

**FMT_MSA.3.1** The TSF shall enforce the ***Política de control de acceso a CLAVES*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2** The TSF shall allow the *[assignment: the authorised identified roles]* to specify alternative initial values to override the default values when an object or information is created.

**Nota de Aplicación:**

(A) Los roles autorizados serán ***Crypto-officer y usuario***

(B) En el caso de no poderse modificar ningún atributo de seguridad del material criptográfico y demás CSPs (es decir, viene fijado en la inicialización del HSM), ver requisito FMT_MSA.1 /CLAVES, se incluirá "none" en la operación *[assignment: the authorised identified roles*] y se considerará el requisito FMT_MSA.3.2 satisfecho.

6.1.5.2 Control de acceso a servicios

120 **FDP_ACC.2 Complete access control / SERVICIOS**

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

**FDP_ACC.2.1** The TSF shall enforce the ***Política de control de acceso a SERVICIOS*** on

***(A) Objetos:***

***a. servicios del TOE que serán (al menos) los siguientes: Mostrar estado del TOE, Realizar Self test, Ejecutar función de seguridad aprobada, funciones de administración (según FMT_SMF.1) y opcionalmente mantenimiento y bypass;***

***b. datos de usuario en claro o cifrados;***

***(B) Sujetos: usuarios o sujetos que los representan;***

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.

121 **FDP_ACF.1 Security attribute based access control / SERVICIOS**

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

**FDP_ACF.1.1** The TSF shall enforce the ***Política de control de acceso a SERVICIOS*** to objects based on the following:

***(B) Objetos:***

***a. servicios del TOE que serán (al menos) los siguientes: Mostrar estado del TOE, Realizar Self test, Ejecutar función de seguridad aprobada, funciones de administración (según FMT_SMF.1) y opcionalmente mantenimiento y bypass; Sus atributos: identificador, permisos de control de acceso;***

***b. datos de usuario en claro o cifrados sin atributos;***

***(C) Sujetos: usuarios o sujetos que los representan; Atributos: la identidad del usuario al que se ha ligado, rol del usuario;***

**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: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

**FDP_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects*]**.**

**FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*assignment: rules, based on security attributes, that explicitly deny access of subjects to objects*].

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá definir las reglas de la política de control de acceso teniendo en cuenta las siguientes especificaciones:

- El rol usuario, puede realizar servicios generales incluyendo operaciones criptográficas y otras funciones de seguridad aprobadas.

- El rol crypto-officer, puede realizar funciones de inicialización del TOE o de administración (por ejemplo, inicialización, entrada/salida de claves – según la política definida en la sección anterior, auditoría, gestión de usuarios, etc).

- Si existe rol de mantenimiento. Éste realizará funciones de mantenimiento físico y/o lógico (diagnósticos HW/SW). Todo el material criptográfico deberá ser zeroizado cuando se entre en modo mantenimiento.

- Si existe la capacidad de bypass, en la que los servicios se proporcionan sin proceso criptográfico, entonces se deberán realizar dos acciones internas independientes (crypto-officer) para activar bypass y el módulo deberá mostrarlo en el servicio de muestra del estado.

122 **FMT_MSA.1 Management of security attributes / SERVICIOS**

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

**FMT_MSA.1.1** The TSF shall enforce the ***Política de control de acceso a SERVICIOS*** to restrict the ability to [*selection: change_default, query, modify, delete, [assignment: other operations*]] the security attributes [*assignment: list of security attributes*] to ***Crypto-officer***.

**Nota de Aplicación:**

El autor de la declaración de seguridad deberá definir las operaciones que se pueden hacer sobre los atributos de los objetos declarados en dicha política. El crypto-officer puede modificar los atributos de seguridad de los servicios. En el caso de no poderse modificar ningún atributo de seguridad (es decir, vienen fijados en la inicialización del HSM), se incluirá "none" en la operación [*assignment: list of security attributes*] y se considerará este requisito satisfecho.

(A) atributos de los servicios del TOE que se podrían modificar: permisos de control de acceso;

123 **FMT_MSA.3 Static attribute initialisation / SERVICIOS**

Hierarchical to: No other components.

Dependencies:

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

**FMT_MSA.3.1** The TSF shall enforce the ***Política de control de acceso a SERVICIOS*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2** The TSF shall allow the *[assignment: the authorised identified roles]* to specify alternative initial values to override the default values when an object or information is created.

**Nota de Aplicación:**

(A) El rol autorizado será ***Crypto-officer***

(B) En el caso de no poderse modificar ningún atributo de seguridad (es decir, vienen fijados en la inicialización del HSM), ver requisito FMT_MSA.1/SERVICIOS, se incluirá "none" en la operación *[assignment: the authorised identified roles]* y se considerará el requisito FMT_MSA.3.2 satisfecho.

### 6.1.6 Importación y exportación de datos de usuario

**124 FDP_ITC.2 Import of user data with security attributes**

Hierarchical to: No other components.
Dependencies:

[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted path, or
FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

**FDP_ITC.2.1** The TSF shall enforce the ***Política de control de acceso a CLAVES*** when importing user data, controlled under the SFP, from outside of the TOE.

**FDP_ITC.2.2** The TSF shall use the security attributes associated with the imported user data.

**FDP_ITC.2.3** The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

**FDP_ITC.2.4** The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

**FDP_ITC.2.5** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

1. ***Las claves se importarán con los siguientes atributos de seguridad: identidad, entidad a la que está ligada; en caso de que la clave entre cifrada, se incluirá también como atributo, la identidad de clave con la que fue cifrada;***

2. ***Los CSPs se importarán con los siguientes atributos de seguridad: identidad;***

3. ***Si se usan métodos automáticos en la importación, las claves privadas y secretas entrarán en el TOE cifradas;***

4. ***Si se usan métodos manuales en la importación, las claves privadas y secretas entrarán en el TOE cifradas o mediante la implementación de algún procedimiento de conocimiento dividido (split-knowledge);***

5. ***Las claves públicas pueden entrar en el TOE en claro.***

*[assignment: otras reglas basadas en atributos de seguridad adicionales de las claves**]***

**Nota de Aplicación:**

El cifrado de las claves se realizará mediante funciones de seguridad aprobadas (ver [FIPS_ANEXOS]).

Se puede dar el caso de una importación de una clave que vaya acompañada por la clave que fue usada para cifrarla. Esta clave va a su vez cifrada con una clave de trasporte, previamente cargada en el módulo. En este caso, la importación no se realiza con el identificador de la clave con que fue cifrada, ya que lleva la propia clave.

125 **FPT_TDC.1 Inter-TSF basic TSF data consistency**

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

**FPT_TDC.1.1** The TSF shall provide the capability to consistently interpret ***los atributos de seguridad del material criptográfico y demás CSPs*** when shared between the TSF and another trusted IT product.

**FPT_TDC.1.2** The TSF shall use

***(A) El TOE asignará el material criptográfico y demás CSPs a la entidad especificada en la importación;***

***(B) El TOE no cambiará los atributos de seguridad del material criptográfico y demás CSPs cuando éstos sean importados;***

***(C)*** [*assignment: otras reglas de interpretación]*

when interpreting the TSF data from another trusted IT product.

126 **FDP_ETC.1 Export of user data without security attributes**

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

**FDP_ETC.1.1** The TSF shall enforce the ***Política de control de acceso a CLAVES*** when exporting user data, controlled under the SFP(s), outside of the TOE.

**FDP_ETC.1.2** The TSF shall export the user data without the user data's associated security attributes **(*)**

**(*) Refinamiento**

Se deberán observar las siguientes reglas de exportación de material criptográfico y demás CSPs:

(A) Si se usan métodos automáticos, las claves privadas y secretas saldrán del TOE cifradas.
(B) Si se usan métodos manuales, las claves privadas y secretas saldrán del módulo (TOE) cifradas o mediante la implementación de algún procedimiento de conocimiento dividido (split-knowledge). Si se usa split knowledge:
   a. El TOE deberá autenticar de manera separada al operador que meta cada componente de la clave;

b. Se necesitarán al menos dos componentes de la clave para reconstruir la clave criptográfica original
c. Si se necesita conocer n componentes de la clave para reconstruir la clave original, el conocimiento de cualquier n-1 componentes no proporcionará información acerca de la calve original distinta de su longitud.

(C) Las claves públicas pueden salir del módulo (TOE) en claro.
(D) El cifrado de las claves se realizará mediante funciones de seguridad aprobadas (ver [FIPS_ANEXOS]).
(E) Se deberá inhibir el interface I/P de salida de datos en los siguientes casos:
   a. Durante el proceso de generación de claves
   b. Entrada manual de claves a través de este puerto
   c. Self-test
   d. Estado de error
   e. Destrucción de claves
   f. Carga de software

### 6.1.7 Gestión de seguridad

**127** **FMT_SMF.1 Specification of Management Functions**

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

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

***(A) administración por el crypto-officer***

***a. gestión de atributos de seguridad de las políticas de control de acceso definidas: Política de control de acceso a CLAVES, Política de control de acceso a SERVICIOS según requisitos FMT_MSA definidos para ambas políticas;***

***b. gestión de datos de auditoría;***

***c. inicialización del TOE;***

***d. gestión de usuarios y sus datos de autenticación y atributos;***

***e. entrada / salida de claves;***

***f. activación de la capacidad de bypass (si aplica);***

***g. destrucción del material criptográfico y demás CSPs.***

***(B) Mantenimiento por el rol de mantenimiento (si aplica);***

(C) [*assignment: otras funciones de gestión que proporcione la TSF*].

**Nota de Aplicación:**

Si el TOE no proporciona funcionalidad de mantenimiento, ni la capacidad de bypass, el requisito, en lo que a estos aspectos se refiere, se considera satisfecho. Las funciones de mantenimiento pueden implicar la deshabilitación de mecanismos de seguridad tanto físicos como lógicos.

128 **FMT_SMR.2 Restrictions on security roles**

Hierarchical to: FMT_SMR.1 Security roles
Dependencies: FIA_UID.1 Timing of identification

**FMT_SMR.2.1** The TSF shall maintain the roles:

***(A) Rol de Usuario no identificado,***

***(B) Rol de Crypto-officer,***

***(C) Rol de Usuario,***

***(D) Rol de Mantenimiento, (si aplica);***

***(E)*** [*assignment: otros roles*].

**FMT_SMR.2.2** The TSF shall be able to associate users with roles.

**FMT_SMR.2.3** The TSF shall ensure that the conditions

***(A) Un usuario con el rol de "Usuario" no puede tener asignado el rol de "Crypto-officer" o el rol de "Mantenimiento";***

***(B) Un usuario con el rol de "Crypto-officer" o con el rol de "Usuario" no puede tener asignado el rol de "Mantenimiento";***

***(C) Antes de identificarse el usuario tendrá el rol "Usuario no identificado".***

***(D)*** [*assignment: otras condiciones para los roles*]

are satisfied.

**Nota de Aplicación:**

Si el TOE no proporciona funcionalidad de mantenimiento, el requisito, en lo que a este aspecto se refiere, se considera satisfecho.

### 6.1.8 Seguridad física

**129** **FPT_PHP.3 Resistance to physical attack**

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

**FPT_PHP.3.1** The TSF shall resist ***Manipulaciones físicas y sondado de canales*** to the [*assignment: list of TSF devices/elements*] by responding automatically such that the SFRs are always enforced.

**Nota de Aplicación (1)**

El autor de la declaración deberá resolver la asignación definiendo la lista de dispositivos o componentes físicos que deberán resistir las ***Manipulaciones físicas y sondado de canales.*** Esta lista puede aplicar a un subconjunto de los componentes físicos de la TSF.

**Nota de Aplicación (2)**

**Descripción de medidas de seguridad según tipo de TOE que aplican en el cumplimiento de este requisito.**

El TOE es un HSM en cualquier forma o configuración, formado un por único chip (**single-chip**) o por múltiples chips ensamblados en una placa (**multi-chip stand alone** o **embedded**).

El TOE proporciona los mecanismos HW de protección contra manipulaciones físicas y sondado de canales, proporcionando evidencia de la manipulación ("tamper evidence") y respondiendo automáticamente de forma que no se comprometan los activos que se protegen: mecanismos "tamper response" que deberán destruir inmediatamente el material criptográfico y demás CSPs en cuanto que se detecte la manipulación física ("zeroization"). Estos mecanismos se aplican especialmente cuando existen tapas que se puedan eliminar o interfaces para la realización de operaciones de mantenimiento del módulo (TOE).

Para todas las categorías de módulos criptográficos mencionadas, se implementan mecanismos de protección físicos:

i. **módulos single-chip**: recubrimiento del chip mediante una capa dura (tipo epoxy) resistente a su eliminación o penetración y cuyo intento de manipulación deje evidencias ("*tamper-evident*") y tenga altas probabilidades de causar daños irreparables al módulo (TOE);

ii. **módulos multi-chip**: encapsulado del módulo con una capa dura o con material duro y opaco (tipo epoxy), o bien un cierre opaco tamper-evident que evite la observación directa, sondaje o manipulación de los componentes del módulo, en el que los intentos de manipulación o penetración provoquen daños graves y proporcionen evidencia del intento de manipulación.

En el caso de existir ranuras de ventilación, éstas deberán construirse de forma que se evite que se pueda sondar o explorar internamente el módulo (TOE) sin ser detectado y estarán bloqueadas mecánicamente o mediante claves lógicas o protegidas mediante etiquetas tamper-evident.

### 6.1.9 Self Tesing

**130 FPT_FLS.1 Failure with preservation of secure state**

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

**FPT_FLS.1.1** The TSF shall preserve a **secure state (*)** when the following types of failures occur: ***fallo en alguna de las siguientes pruebas:***

***(A) Pruebas en el arranque o bajo demanda***

***a. Algoritmos criptográficos aprobados según [FIPS-AENXOS]***

***b. Integridad SW / FW***

***c. Funciones críticas***

***(B) Pruebas condicionales (cuando se invoca***

***a. Pair-wise consistency test (for public and private keys).***

***b. Software/firmware load test.***

***c. Manual key entry test.***

***d. Continuous random number generator test.***

*e. Bypass test.*

**(*) Refinamiento**

El TOE deberá realizar auto-test durante el proceso de arranque (power-up), bajo demanda y pruebas condicionales. En caso de fallo de alguna de las pruebas anteriores y detalladas en FPT_TST.2, el TOE entrará en estado de error (excepto en apagado o mantenimiento) y se indicará por el I/P de salida de estado, inhibiéndose su funcionalidad criptográfica y el I/P de salida de datos.

**Nota de Aplicación:**

Si el TOE no proporciona la capacidad de bypass, o alguna otra funcionalidad que haga que no aplique la realización de alguna de las pruebas mencionadas en **FPT_FLS.1.1**, el requisito, en lo que a estos aspectos se refiere, se considera satisfecho.

131 **FPT_TST.2 Self Testing**

Hierarchical to: No other components.
Dependencies: FPT_FLS.1 Failure with preservation of secure state.

**FPT_TST.2.1** The TSF shall perform self-testing at power-up to verify the correctness of [*assignment: list of cryptographic algorithms approved [FIPS-ANEXOS]*] and of [*assignment: list of critical TSF*], and to verify the integrity of the TSF-software/firmware. **(*)**

**FPT_TST.2.2** The TSF shall perform self-testing at the conditions [*assignment: list of conditions*] to verify the correctness of [*assignment: list of critical cryptographic algorithms*]. **(*)**

**FPT_TST.2.3** The TSF shall provide [*assignment: list of users*] with the capability to invoke the following self-tests [*assignment: list of self-tests*].

**FPT_TST.2.4** During ***Power-up self-tests, self-tests at the request of the authorised user,*** [*assignment: other self-tests*] the TSF shall ***inhibit all output via the interface "*I/P de salida de datos", [*assignment: other actions to be performed*].

**FPT_TST.2.5** After completion of self-testing the TSF shall ***output the results of the self-test via the interface "*I/P de salida de estado", [*assignment: other actions to be performed*].

**FPT_TST.2.6** If the self-testing result is fail the TSF shall ***enter a secure state (see FPT_FLS.1 - refinamiento) and ouput an error indicator via***

***the interface* "I/P de salida de estado"**, [*assignment: other actions to be performed*].

**(*) Refinamientos**

For **FPT_TST.2.1**: Power-up tests shall be performed by the TOE when it is powered up (after being powered off, reset, rebooted, etc.). The power-up tests shall be initiated automatically and shall not require operator intervention. The TOE shall perform the following power-up tests:

(A) **Cryptographic algorithm test**. A cryptographic algorithm test using a known answer shall be conducted for all cryptographic functions (e.g., encryption, decryption, authentication, and random number generation) of each Approved cryptographic algorithm implemented by the TOE ([FIPS-ANEXOS]. A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known-answer test shall fail.

(B) **Software/firmware integrity test**. A software/firmware integrity test using an error detection code (EDC) or Approved authentication technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all validated software and firmware components within a cryptographic module when the TOE is powered up. If the calculated result does not equal the previously generated result, the software/firmware test shall fail. If an EDC is used, the EDC shall be at least 16 bits in length.

(C) **Critical functions test**. Other security functions critical to the secure operation of the TOE shall be tested when it is powered up as part of the power-up tests. Other critical security functions performed under specific conditions shall be tested as conditional tests.

In addition to performing the power-up tests when powered up, a cryptographic module shall permit operators to initiate the tests on demand for periodic testing of the module. Resetting, rebooting, and power cycling are acceptable means for the on-demand initiation of power-up tests.

For **FPT_TST.2.2**, regarding conditional tests, the following are to be performed:

(A) **Pair-wise consistency test** (for public and private keys). If TOE generates public or private keys, then pair-wise consistency tests for public and private keys shall be performed.

a. If the keys are used to perform an approved key transport method, then the public key shall encrypt a plaintext value. The resulting ciphertext value shall be compared to the original plaintext value. If the two values are equal, then the test shall fail. If the two values differ, then the private key shall be used to decrypt the ciphertext and the resulting value shall be compared to the original plaintext value. If the two values are not equal, the test shall fail.

b. If the keys are used to perform the calculation and verification of digital signatures, then the consistency of the keys shall be tested by the calculation and verification of a digital signature. If the digital signature cannot be verified, the test shall fail.

(B) **Software/firmware load test**. If software or firmware components can be externally loaded into the TOE, then software/firmware load tests using an approved authentication technique ([FIPS-ANEXOS]) shall be performed.

(C) **Manual key entry test**. If cryptographic keys or key components are manually entered into the TOE, then manual key entry tests shall be performed:

a. The cryptographic key or key components shall have an EDC applied, or shall be entered using duplicate entries.

b. If an EDC is used, the EDC shall be at least 16 bits in length.

c. If the EDC cannot be verified, or the duplicate entries do not match, the test shall fail.

(D) **Continuous random number generator test**. If TOE employs Approved or non-Approved RNGs in an Approved mode of operation, the TOE shall perform continuous random number generator test on each RNG that tests for failure to a constant value.

a. If each call to a RNG produces blocks of n bits (where n > 15), the first n-bit block generated after power-up, initialization, or reset shall not be used, but shall be saved for comparison with the next n-bit block to be generated. Each subsequent generation of an n-bit block shall be compared with the

previously generated block. The test shall fail if any two compared n-bit blocks are equal.

b. If each call to a RNG produces fewer than 16 bits, the first n bits generated after power-up, initialization, or reset (for some n > 15) shall not be used, but shall be saved for comparison with the next n generated bits. Each subsequent generation of n bits shall be compared with the previously generated n bits. The test fails if any two compared n-bit sequences are equal.

(E) **Bypass test**. If a cryptographic module implements a bypass capability where the services may be provided without cryptographic processing (e.g., transferring plaintext through the module), then bypass tests shall be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext.

a. A cryptographic module shall test for the correct operation of the services providing cryptographic processing when a switch takes place between an exclusive bypass service and an exclusive cryptographic service.

b. If the TOE can automatically alternate between a bypass service and a cryptographic service, providing some services with cryptographic processing and some services without cryptographic processing, then the TOE shall test for the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified.

**Nota de aplicación:**

Si el TOE no proporciona la capacidad de bypass, o alguna otra funcionalidad que haga que no aplique la realización de alguna de las pruebas mencionadas, el requisito, en lo que a estos aspectos se refiere, se considera satisfecho.

### 6.1.10 Auditoría de seguridad

**132 FAU_GEN.1 Audit data generation**

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

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*selection, choose one of: minimum, basic, detailed, not specified*] level of audit; and
c)
i. Power-up;
ii. Identificación y Autenticación (fallo y éxito) (FIA_UID.1, FIA_UAU.1);
iii. Fallo en self-tests (FPT_TST.2)
iv. Funciones de administración (FMT_SMF.1);
v. [*assignment: otros eventos auditables*].

**FAU_GEN.1.2** The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*assignment: other audit relevant information*].

133 **FAU_GEN.2 User identity association**

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

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

### 6.1.11 Sellado de tiempo

134 **FPT_STM.1 Reliable time stamps**

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

**FPT_STM.1.1** The TSF shall be able to provide reliable time stamps.

**Nota de aplicación:**

Este requisito se usa para la generación del sellado de tiempo incluido en los registros de auditoría (FAU_GEN.1).

En el caso de que el TOE implemente control de caducidad de las claves según el atributo de seguridad "periodo de validez" (FDP_ACF.1 ➔ si se incluye una regla en la política de control de acceso que obligue a chequear la validez de una clave antes de su uso) se utilizará esta fuente de tiempo.

## 6.2 Requisitos de garantía de seguridad

135 Los requisitos de garantía que se incluyen a continuación se corresponden con el nivel de garantía definido EAL4, conforme a [CC31p3].

### 6.2.1 Declaración de seguridad (ASE)

**136 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.

**Nota de aplicación**

El autor de la declaración de seguridad, deberá incluir en la sección TOE Description, la especificación de los componentes HW, SW y FW y los puertos e interfaces que definen los límites del TOE. También se deberá describir la configuración física del TOE.

Se listarán todas las funciones de seguridad, tanto las aprobadas según [FIPS-ANEXOS] como las que no lo está pero el módulo implementa.

137 **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.

138 **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.

139 **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.

140 **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.

141 **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.

**142** **ASE_TSS.1 TOE summary specification**

Dependencies:
ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements:
ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:
ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

### 6.2.2 Desarrollo (ADV)

**143** **ADV_FSP.4 Complete functional specification**

Dependencies: ADV_TDS.1 Basic design

Developer action elements:
ADV_FSP.4.1D The developer shall provide a functional specification.
ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:
ADV_FSP.4.1C The functional specification shall completely represent the TSF.
ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.
ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

**Nota de aplicación (1)**

La especificación funcional deberá identificar los interfaces lógicos y puertos físicos (I/P) y describir sus características:

(A) I/P de entrada de datos: para todos los datos (excepto los datos de control que entran por el I/P de entrada de control) que entren y sean procesados por el TOE (incluyendo datos en claro, datos cifrados, material criptográfico y CSPs, datos de autenticación e información de estado de otra entidad);

(B) I/P de salida de datos: para todos los datos (excepto los datos de estado que salen por el I/P de estado) que salen del TOE (incluyendo datos en claro, datos cifrados, material criptográfico y CSPs, datos de autenticación e información de control para otra entidad);

(C) I/P de entrada de control: para todos comandos de entrada, señales y datos de control (incluyendo llamadas a funciones, controles manuales, botones, teclado) usados para el control de la operación del TOE;

(D) I/P de salida de estado: para la salida de señales, indicadores y datos de estado (incluyendo códigos de retorno de las funciones, indicadores físicos como LEDs o pantallas) que se usan para indicar el estado del TOE;

(E) I/P de alimentación: fuentes de alimentación externas.

**Nota de aplicación (2):**

Los interfaces físicos usados para la entrada y salida de material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar físicamente separados de otros interfaces, o bien los interfaces lógicos usados para la entrada y salida de material criptográfico y CSPs en claro (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar lógicamente separados utilizando un “trusted path”.

El material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales) debe entrar/salir directamente al módulo (TOE) mediante, por ejemplo, un “trusted path” o un cable directamente conectado.

144 **ADV_TDS.3 Basic modular design**

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:
ADV_TDS.3.1D The developer shall provide the design of the TOE.
ADV_TDS.3.2D 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.3.1C The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.3.2C The design shall describe the TSF in terms of modules.
ADV_TDS.3.3C The design shall identify all subsystems of the TSF.
ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.
ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.
ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.
ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.
ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.
ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.
ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

**Nota de aplicación**

El diseño deberá incluir:

(A) Un diagrama de bloques en el que se muestren los componentes HW más importantes y sus interconexiones incluyendo los microprocesadores, buffers de entrada/salida, buffers de datos en claro y cifrados, buffers de control, almacenes de claves, memoria.

(B) Subsistemas y módulos encargados de la gestión de claves. Interfaces físicos y lógicos por subsistema y módulos (SFR-enforcing) a través de los cuales se realiza entrada y salida de claves y demás CSPs.

(C) Se describirán

a. los roles soportados,

b. los servicios (aprobados y no aprobados), especificando para cada uno, las entradas y salidas, quién puede acceder a los mismos (conforme a los requisitos del PP), con que permisos, que funciones los implementan y qué algoritmos y material criptográfico usan;

c. mecanismos de autenticación, los métodos usados para el control de acceso al módulo por primera vez e inicializar los mecanismos de autenticación y la justificación de la fortaleza de los mismos.

(D) Características físicas y mecanismos HW de protección contra manipulaciones físicas y sondado de canales, proporcionando evidencia de la manipulación ("*tamper evidence*") y respondiendo automáticamente de forma que no se comprometan los activos que se protegen: mecanismos "*tamper response*" que deberán destruir inmediatamente el material criptográfico y demás CSPs en cuanto que se detecte la manipulación física ("*zeroization*"). Dependiendo del tipo de módulo, se documentará el tipo y características del encapsulado y epoxy y justificando su resistencia a los ataques especificados en este PP. En el caso de existir ranuras de ventilación, se justificará que su construcción evita que se pueda sondar o explorar internamente el TOE sin ser detectado y que están bloqueadas mecánicamente o mediante claves lógicas o protegidas mediante etiquetas tamper-evident.

(E) Gestión de claves. Se especificará todo el material criptográfico, datos de autenticación y demás CSPs: almacenamiento, entrada/salida, generación, establecimiento y métodos de zeroización.

(F) Respecto la RNG se describirá la métrica de calidad del mismo,

(G) Self-tests. Se detallarán los self-tests que realiza el TOE (power-up, demanda, condicionales), los estados de error en los que el TOE entra en caso de fallo y las acciones y condiciones necesarias para salir del estado de error y continuar con la operación normal. Se puede especificar como parte del modelo de estados finitos (ADV_ARC.1).

(H) Descripción del entorno operacional en el que el TOE opera, incluyendo (si aplica), las medidas de seguridad del sistema operativo empleado por el TOE.

145 **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.

**Nota de aplicación**

(A) Separación de dominios

a. describirá la separación de interfaces según los requisitos de este PP.

b. describirá los casos en los que se la inhibe el interface de salida: generación de claves, entrada manual, self-test, carga de sofware, estado error, destrucción de claves.

c. Descripción de los dominios en términos de un modelo de estados finitos (semi formal), incluyendo al menos los siguientes estados operacionales y de error (según FPT_FSM.1):

i. Power on/off. Estados que definen el arranque y la parada del TOE. Estos estados pueden distinguir entre distintas fuentes de alimentación que se apliquen al TOE.

ii. Crypto officer. Refleja los estados en los que se ejecutan los servicios del crypto officer (por ejemplo., inicialización y gestión de claves).

iii. Entrada de claves/CSP. Refleja estados en los que se puede importar claves y CSPs al TOE.

iv. Usuarios. Estados en los que los usuarios autorizados acceden a los servicios, realizan operaciones criptográficas u otras funciones aprobadas o no aprobadas.

v. Self-test. Reflejan los estados en los que el modulo está realizando self-tests.

vi. Error. Estados en los que se ha producido un error (por ejemplo por fallo en self-test o intento de cifrado sin encontrar la clave o CSP adecuado). Pueden ser errores importante que indican que el TOE no está funcionando correctamente y pueden necesitar mantenimiento o reparación, o pueden ser errores del los que el TOE se puede recuperar mediante algún tipo de inicialización o reset. Deberá ser posible la recuperación en estado de error excepto en el caso de que el error requiera entrar en estado de mantenimiento o reparación del módulo.

Opcionales:

vii. Bypass. Reflejan estados en los que se active la capacidad de bypass y se proporcionan servicios sin procesamiento criptográfico (por ejemplo transferencia del datos en claro a través del TOE);

viii. Mantenimiento. Estados para el mantenimiento del TOE incluyendo pruebas locales físicas y lógicas. En el caso de existir el rol de mantenimiento, deberá existir un estado de mantenimiento.

El modelo deberá describir las transiciones entre estados teniendo en cuenta las entradas, los eventos internos y condiciones internas que causan las transiciones, los eventos de salida generados en cada transición. El modelo no debe permitir que el TOE se encuentre operativo en dos estados a la

vez. Si existe estado de bypass, se deberá demostrar que para entrar en ese estado deberán existir dos eventos independientes. El modelo de estados deberá ser consistente con la especificación funcional, el diseño, la representación de la implementación, las guías de usuario y la operativa del TOE.

(B) Anti-tamper y non- bypassability: se deberán describir teniendo en cuenta, entre otros, las capacidades físicas del TOE (FPT_PHP.3).

146 **ADV_IMP.1 Implementation representation of the TSF**

Dependencies:
ADV_TDS.3 Basic modular design
ALC_TAT.1 Well-defined development tools

Developer action elements:
ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.
ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements:
ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.
ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

**Nota de aplicación**

El código fuente deberá presentar anotaciones a la entrada de cada componente.

### 6.2.3 Guías de usuario (AGD)

147 **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.

148 **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.

### 6.2.4 Soporte al ciclo de vida (ALC)

**149** **ALC_CMC.4 Production support, acceptance procedures and automation**

Dependencies:

ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model

Developer action elements:
ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.4.2D The developer shall provide the CM documentation.
ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements:
ALC_CMC.4.1C The TOE shall be labelled with its unique reference.
ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.
ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.
ALC_CMC.4.6C The CM documentation shall include a CM plan.
ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

**150** **ALC_CMS.4 Problem tracking CM coverage**

Dependencies: No dependencies.

Developer action elements:
ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.
ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.
ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

151 **ALC_DEL.1 Delivery procedures**

Dependencies: No dependencies.

Developer action elements:
ALC_DEL.1.1D The developer shall document and provide 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.

152 **ALC_DVS.1 Identification of security measures**

Dependencies: No dependencies.

Developer action elements:
ALC_DVS.1.1D The developer shall produce and provide 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.

153 **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.

154 **ALC_TAT.1 Well-defined development tools**

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:
ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.
ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

Content and presentation elements:
ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.
ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.
ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

### 6.2.5 Pruebas (ATE)

155 **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.

156 **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.

157 **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.

158 **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.

**Nota de aplicación metodológica**

Respecto a la acción del evaluador:

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified

El evaluador deberá probar que el modelo de estados definido es consistente con la operativa del TOE.

### 6.2.6 Análisis de vulnerabilidades (AVA)

**159 AVA_VAN.3 Focused vulnerability analysis**

Dependencies:
ADV_ARC.1 Security architecture description
ADV_FSP.4 Complete functional specification
ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_DPT.1 Testing: basic design

Developer action elements:
AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements:
AVA_VAN.3.1C The TOE shall be suitable for testing.

## 6.3 Justificación de los requisitos de seguridad

### 6.3.1 Justificación de los requisitos de funcionalidad de seguridad

160 A continuación se incluye una tabla en la que se muestran los requisitos funcionales que dan cumplimiento a los objetivos de seguridad definidos.

| | O.FUN_APROBADAS | O.IA | O.ROLES | O.INTERFACES | O.SEP_INTERFACES | O.STATUS_FUN_APR | O.SELF_TEST | O.CONTROL_ACCESO_SERVICIOS | O.GESTIÓN_CLAVES | O.CONTROL_ACCESO_CLAVES | O.IO_CLAVES | O.GENERACIÓN_CLAVES | O.DESTRUCCIÓN_CLAVES | O.PHYSICAL_PROTECCIÓN | O.AUDITORÍA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FCS_CKM.1 | X | | | | | | | | X | | | X | | | |
| FCS_CKM.5 | X | | | | X | | | | X | | X | | | | |
| FCS_CKM.2 | X | | | | X | | | | X | | X | | | | |
| FCS_CKM.4 | X | | | | | | | | X | | | | X | | |
| FCS_COP.1 | X | | | | | X | | | | | | | | | |
| FCS_RNG.1 | X | | | | | | | | | | | X | | | |
| FPT_SEP.1 | | | | X | X | | | | | | | | | | |
| FIA_ATD.1 | | X | | | | | | | | | | | | | |
| FIA_UID.1 | | X | | | | | | | | | | | | | |
| FIA_UAU.1 | | X | | | | | | | | | | | | | |
| FIA_UAU.6 | | X | | | | | | | | | | | | | |
| FIA_UAU.7 | | X | | | | | | | | | | | | | |
| FIA_AFL.1 | | X | | | | | | | | | | | | | |
| FIA_USB.1 | | X | | | | | | | | | | | | | |
| FDP_ACC.2/ CLAVES | | | | | | | | | X | X | | | | | |
| FDP_ACF.1 / CLAVES | | | | | | | | | X | X | | | X | | |
| FMT_MSA.1 / CLAVES | | | | | | | | | X | X | | | | | |
| FMT_MSA.3 / CLAVES | | | | | | | | | X | X | | X | | | |
| FDP_ACC.2 / SERVICIOS | | | | | | X | | X | | | | | | | |
| FDP_ACF.1 / SERVICIOS | | | | | | X | | X | | | | | | | |
| FMT_MSA.1 / SERVICIOS | | | | | | X | | X | | | | | | | |
| FMT_MSA.3 / SERVICIOS | | | | | | X | | X | | | | | | | |
| FPT_ FSM.1 | | | | | | X | | X | | | | | | | |
| FDP_ITC.2 | X | | | | | | | | X | | X | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FDP_TDC.1 | X | | | | | | | | X | | X | | | | |
| FDP_ETC.1 | X | | | | | | | | X | | X | | | | |
| FMT_SMF.1 | | | | | | | | | X | | | | X | | |
| FMT_SMR.2 | | | X | | | | | | X | | | | | | |
| FPT_PHP.3 | | | | | | | | | | | | | | X | |
| FPT_FLS.1 | | | | | | X | X | | | | | | | | |
| FPT_TST.2 | | | | | | X | X | | | | | | | | |
| FAU_GEN.1 | | | | | | | | | | | | | | | X |
| FAU_GEN.2 | | | | | | | | | | | | | | | X |
| FPT_STM.1 | | | | | | | | | | X (*) | | | | | X |

**(*) en el caso de que el TOE implemente un control de caducidad de las claves mediante el atributo "periodo de validez", tal y como se indica en la definición de la política de control de acceso a CLAVES (FDP_ACF.1)**

161 A continuación se incluye la justificación de necesidad y suficiencia de cada uno de los requisitos funcionales de forma que se garantice el cumplimiento de los objetivos de seguridad.

162 El objetivo de seguridad O.FUN_APROBADAS requiere que el TOE implemente funciones de seguridad que estén aprobadas en FIPS o recomendadas por el NIST, por lo que deberán estar incluidas en los anexos correspondientes [FIPS-ANEXOS] de [FIPS1402]. Este objetivo de seguridad se cumple mediante los requisitos FCS_CKM.1, FCS_CKM.5, FCS_CKM.2, FCS_CKM.4, FCS_COP.1, FCS_RNG.1 que requieren el uso de funciones aprobadas. Los requisitos FDP_ITC.2 (con su dependencia FPT_TDC.1) y FDP_ETC.1 obligan al uso de funciones criptográficas aprobadas para la importación e importación del material criptográfico.

163 El objetivo de seguridad O.IA requiere que el TOE verifique y autentique a todos los usuarios antes de permitirse cualquier acción (excepto self-tests). Los credenciales que verifica y autentica el TOE deberán ser de tipo individual y no por grupos de usuarios. Este objetivo de seguridad se cumple mediante los requisitos:

- FIA_ATD.1: requiere el mantenimiento de los atributos individuales de los usuarios (Identidad, Rol), requisitos para la I&A.
- FIA_UID.1: requiere la identificación del usuario antes de realizarse cualquier acción (excepto self-test).
- FIA_UAU.1: requiere la autenticación del usuario antes de realizarse cualquier acción (excepto self-test).
- FIA_UAU.6: define los casos en los que el usuario debe re-autenticarse.

- FIA_UAU.7: requiere la limitación del feedback que se proporciona al usuário.
- FIA_AFL.1: requiere la detección y reacción ante un número concreto de fallos de autenticación;
- FIA_USB.1: requiere que se asocie la identidad del usuario y el rol a los sujetos que actúan en nombre del usuario autenticado.

164 El objetivo de seguridad O.ROLES requiere que el TOE soporte los siguientes roles: usuarios y crypto-officer. En el caso de que se permita que operadores realicen labores de mantenimiento del TOE, se deberá incluir un rol a tal efecto. Este objetivo de seguridad se cumple mediante el requisito FMT_SMR.2 que proporciona al menos el rol de Usuario no identificado, de Crypto-officer, de Usuario y de Mantenimiento (si el TOE proporciona dicha funcionalidad). Se incluyen las condiciones para la asignación de usuarios a roles.

165 El objetivo de seguridad O.INTERFACES requiere que el TOE proporcione los siguientes tipos de interfaces o *puertos* (I/P): I/P de entrada de datos, I/P de salida de datos, I/P de entrada de control, I/P de salida de estado, I/P de alimentación. Este objetivo de seguridad se cumple mediante el requisito FPT_SEP.1 que requiere que se implementen dichos interfaces o puertos.

166 El objetivo de seguridad O.SEP_INTERFACES requiere que los interfaces físicos usados para la entrada y salida de material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar físicamente separados de otros interfaces, o bien los interfaces lógicos usados para la entrada y salida de material criptográfico y CSPs en claro (incluyendo interfaces para la entrada de datos de autenticación confidenciales), deberán estar lógicamente separados utilizando un "*trusted path*". El material criptográfico y CSPs (incluyendo interfaces para la entrada de datos de autenticación confidenciales) debe entrar/salir directamente al módulo (TOE) mediante, por ejemplo, un "*trusted path*" o un cable directamente conectado. Se considera el "*trusted path*"como un canal que proporciona la confianza necesaria para cumplir la política de seguridad del módulo y su operación, que considera que los requisitos de entrada/salida de material criptográfico y demás CSPs (cifrado y split knowledge) indicados, establecen la política de seguridad necesaria para confiar en el canal. Este objetivo de seguridad se cumple mediante los siguientes requisitos:

- FPT_SEP.1 que requiere que define las reglas que regulan dicha separación entre los interfaces implementados para entrada y salida del material criptográfico y demás CSPs;

- FCS_CKM.5, FCS_CKM.2 para realizar entrada y salida de claves por métodos automáticos o manuales conforme a funciones criptográficas aprobadas o de split knowledge.

167 El objetivo de seguridad O.STATUS_FUN_APR requiere que el TOE proporcione los servicios de mostrado de su estado del TOE a través del interface de salida de estado y ejecute las funciones de seguridad (aprobadas por FIPS o recomendadas por NIST según [FIPS-ANEXOS]). Este objetivo de seguridad se cumple mediante los siguientes requisitos:

- FCS_COP.1: que requiere que se ejecuten funciones criptográficas aprobadas;
- FDP_ACC.2 / SERVICIOS, FDP_ACF.1 / SERVICIOS, FMT_MSA.1 / SERVICIOS, FMT_MSA.3 / SERVICIOS: que define los servicios identificados y establece una política de control de acceso sobre los mismos;
- FPT_FLS.1, FPT_TST.2 que establece que se muestra el estado del TOE por la salida de estado cuando se produce un error.
- FPT_ FSM.1 que establece el modelo de estados que definen la operativa del TOE. Los modos operacionales limitan los servicios disponibles en cada estado.

168 El objetivo de seguridad O.SELF_TEST requiere que el TOE proporcione el servicio de auto-test durante el proceso de arranque (power-up), bajo demanda y realización de pruebas condicionales. Este objetivo de seguridad se cumple mediante los siguientes requisitos:

- FPT_TST.2 que requiere la realización de self-tests.
- FPT_FLS.1 que requiere que el TOE quede en estado seguro cuando falla un self-test.

169 El objetivo de seguridad O.CONTROL_ACCESO_SERVICIOS requiere que el TOE restrinja el acceso a sus servicios dependiendo el rol del usuario. La asignación de los servicios a los roles deberá hacerse por defecto a bien por una acción explícita del administrador (crypto-officer). Este objetivo de seguridad se cumple mediante los siguientes requisitos:

- FDP_ACC.2 / SERVICIOS, FDP_ACF.1 / SERVICIOS, FMT_MSA.1 / SERVICIOS, FMT_MSA.3 / SERVICIOS: que define los servicios identificados y establece una política de control de acceso sobre los mismos;
- FPT_ FSM.1 que establece el modelo de estados que definen la operativa del TOE. Los modos operacionales limitan los servicios disponibles en cada estado.

170 El objetivo de seguridad O.GESTIÓN_CLAVES requiere que el TOE gestione de manera eficiente y segura el material criptográfico necesario en los algoritmos y protocolos implementados y sus atributos de seguridad. El TOE asociará atributos de seguridad de la entidad a la que es asignada la clave (secreta, privada o pública), de forma que las claves se puedan asociar con la entidad correcta (persona, grupo o proceso). Este objetivo de seguridad se cumple mediante los siguientes requisitos:

- FCS_CKM.1, FCS_CKM.5, FCS_CKM.2, FCS_CKM.4: definen funciones aprobadas para la gestión de claves;
- FDP_ACC.2/ CLAVES, FDP_ACF.1 / CLAVES, FMT_MSA.1 / CLAVES, FMT_MSA.3 / CLAVES que establece una política de control de acceso sobre las claves;
- FDP_ITC.2 (con su dependencia FPT_TDC.1) y FDP_ETC.1 definen requisitos para la exportación e importación del material criptográfico y demás CSPs. En el caso de exportación se especifican los casos en los que se debe inhibir el interface de salida para evitar la fuga de claves.
- FMT_SMF.1: definen las funciones de gestión de administración de claves en base a los roles de FMT_SMR.2.

171 El objetivo de seguridad O.CONTROL_ACCESO_CLAVES requiere que el TOE restrinja el acceso al material criptográfico y otros CSPs en base a sus atributos de seguridad. Este objetivo de seguridad se cumple mediante los siguientes requisitos:

- FDP_ACC.2/ CLAVES, FDP_ACF.1 / CLAVES, FMT_MSA.1 / CLAVES, FMT_MSA.3 / CLAVES que establece una política de control de acceso sobre las claves;
- En el caso de que el TOE implemente control de caducidad de las claves, sería necesario el requisito FPT_STM.1 requiere que el TOE proporcione una fuente de tiempos que se usa para el control de caducidad de las claves (atributo de seguridad “periodo de validez”).

172 El objetivo de seguridad O.IO_CLAVES requiere que el TOE, para entrada y salida de claves:

(A) Si se usan métodos automáticos, las claves privadas y secretas entrarán y saldrán del TOE cifradas.
(B) Si se usan métodos manuales, las claves privadas y secretas entrarán y saldrán del módulo (TOE) cifradas o mediante la implementación de algún procedimiento de conocimiento dividido (split-knowledge).
(C) Las claves públicas pueden entrar y salir del módulo (TOE) en claro.

La salida de datos se inhibe durante el proceso de generación de claves, entrada manual de claves a través de este puerto, Self-test, estado de error, destrucción de claves y carga de software. La exportación e importación de claves se realiza con sus atributos de seguridad. Se protege la integridad de las claves y sus atributos.

Este objetivo de seguridad se cumple mediante los siguientes requisitos:

- FCS_CKM.5, FCS_CKM.2, requieren que el TOE realice la entrada/salida de claves utilizando funciones de seguridad aprobadas. El refinamiento incluido especifica las reglas definidas en el objetivo para la entrada/salida usando medios manuales o automáticos.
- FDP_ITC.2 (con su dependencia FPT_TDC.1) , FDP_ETC.1 definen requisitos para la exportación e importación del material criptográfico y demás CSPs. En el caso de importación, se asocian sus atributos de seguridad de manera no ambigua. En exportación, la salida de datos se inhibe durante el proceso de generación de claves, entrada manual de claves a través de este puerto, Self-test, estado de error, destrucción de claves y carga de software.

173 El objetivo de seguridad O.GENERACIÓN_CLAVES requiere que el TOE genere claves utilizando algoritmos criptográficos de generación de claves y RNGs aprobados, según [FIPS-ANEXOS]. Este objetivo de seguridad se cumple mediante los requisitos:

- FCS_CKM.1, que requiere el uso de funciones de seguridad aprobadas para la generación de claves;
- FCS_RNG.1 que define las características de de los RNGs necesarios para la generación de las claves;
- FMT_MSA.3 / CLAVES que requiere valores restrictivos por defecto para los atributos de las claves y limita al crypto-officer la capacidad de especificar valores iniciales alternativos.

174 El objetivo de seguridad O.DESTRUCCIÓN_CLAVES requiere que el TOE destruya todo el material criptográfico y otros CSPs por demanda del crypto-officer o como caso de tamper-response en caso de que el TOE se vea comprometido físicamente. Este objetivo de seguridad se cumple mediante los requisitos:

- FCS_CKM.4, que requiere el uso de funciones de seguridad aprobadas para la destrucción de claves;
- FDP_ACF.1 / CLAVES limita la destrucción de claves al crypto-officer;

- FMT_SMF.1 especifica la destrucción del claves como función de administración del crypto-officer.

175 El objetivo de seguridad O.PHYSICAL_PROTECCIÓN requiere que el TOE resista ataques físicos de un atacante con potencial de ataque **Enhanced Basic.** El TOE debe implementar mecanismos HW de protección contra manipulaciones físicas y sondado de canales, proporcionando evidencia de la manipulación ("*tamper evidence*") y respondiendo automáticamente de forma que no se comprometan los activos que se protegen: mecanismos "*tamper response*" que deberán destruir inmediatamente el material criptográfico y demás CSPs en cuanto que se detecte la manipulación física ("*zeroization*"). Estos mecanismos se aplican especialmente cuando existen tapas que se puedan eliminar o interfaces para la realización de operaciones de mantenimiento del módulo (TOE). Esto se cumple mediante el requisito FPT_PHP.3.

176 El objetivo de seguridad O.AUDITORÍA requiere que el TOE proporcione la capacidad de detectar y registrar los eventos relevantes a la seguridad. La información registrada deberá permitir asociar los eventos con usuarios. Este objetivo de seguridad se cumple mediante los requisitos:

- FAU_GEN.1 que lista los eventos auditables que proporciona el TOE;
- FAU_GEN.2 requiere que se asocie a los eventos auditados, la identidad del usuario que ha causado el evento.
- FPT_STM.1 requiere que el TOE proporcione una fuente de tiempos que se usa para incluirlo en el registro de cada evento.

### 6.3.2 Dependencias de los requisitos de seguridad

177 En este perfil de protección se satisfacen todas las dependencias tanto de requisitos funcionales de seguridad (SFRs), excepto para el caso de importación de datos de usuario con atributos de seguridad (FDP_ITC.2) que exige la satisfacción de creación de una canal - "*trusted channel*" o camino confiable - "*trusted path*" (FTP_ITC.1 o FTP_TRP.1).

178 La definición de canal o camino confiable en CC y reflejada en los requisitos FTP_ITC.1 o FTP_TRP.1, exige la autenticación de ambas partes y la protección del canal contra modificaciones y contra revelaciones no autorizadas. La creación del canal o camino confiable garantiza la separación lógica del mismo de otros canales.

179 La definición del término "trusted path", según [FIPS1402] incluida en la sección 7.2 Definiciones, considera un canal que proporciona la confianza necesaria para cumplir la política de seguridad del módulo y su operación. En este perfil de protección, este "trusted path" es una de las opciones

permitidas para cumplir los requisitos de entrada/salida de material criptográfico y demás CSPs, al implementar mecanismos de cifrado o de split knowledge, estableciendo de esta manera la política de seguridad necesaria para confiar en el canal (tal y como se refleja en los requisitos FCS_CKM.2, FCS_CKM.5 y los de importación y exportación – FDP_ITC.2 y FDP_ETC.1).

180 La característica de separación de interfaces se cumple con el componente FPT_SEP.1, que permite también la realización de entrada/salida de material criptográfico y demás CSPs mediante un cable directamente conectado al módulo.

181 Por lo tanto, aunque no se satisfaga directamente la dependencia, los requisitos adicionales explicados, proporcionan las garantías necesarias para llevar a cabo la importación del material criptográfico con sus atributos de seguridad.

182 En este perfil de protección se satisfacen todas las dependencias de requisitos de garantía de seguridad (SARs).

### 6.3.3 Justificación de los requisitos de garantía de seguridad

183 La garantía de seguridad deseada para este tipo de TOE es la proporcionada por el nivel de evaluación EAL4.

184 Se ha elegido EAL4 para que el usuario final obtenga la máxima confianza en el producto desarrollado en base métodos de ingeniería sistemáticos y buenas prácticas de desarrollo, siendo capaz el producto de resistir a ataques con potencial de ataque "**Enhanced Basic**".

# 7 Acrónimos y definiciones

## 7.1 Acrónimos

185 Son de aplicación todos los acrónimos y definiciones incluidos en [CC31p1] y [FIPS1402].

| | |
|---|---|
| CC | Common Criteria |
| CCN | Centro Criptológico Nacional |
| CSP | Critical Security Parameter |
| FW | FirmWare |
| HW | HardWare |
| HSM | Hardware Security Module |
| I&A | Identificación & Autenticación (también IA) |
| IV | Initialization Vector |
| KAT | Known Answer Tests |
| LED | Light Emitting Diode |
| OSPs | Organisational Security Policies |
| SPD | Security Problem Definition |
| SW | Software |
| PC | Personal Computer |
| RAD | Datos de autenticación de referencia |
| TOE | Target of Evaluation |
| TSA | Time-Stamp Authority |
| TSF | TOE Security Functionality |

## 7.2 Definiciones

186 ***Atributos de seguridad de las claves***:

- Identidad: identificador único de la clave;
- Entidad a la que está ligada: identificador de la entidad dueña de la clave;
- Permisos de control de acceso: información asociada a la clave que permite ejecutar las reglas de control de acceso;
- Otros atributos: USO (propósito de la clave), PERIODO DE VALIDEZ (permite decidir sobre la caducidad de la clave), EXPORTABLE (la clave puede salir del módulo), etc.

187 ***CSP***: Critical Security Parameters. La pérdida de C o I comprometen la seguridad del módulo.

188 ***KAT***: prueba de un algoritmo criptográfico que involucra datos para los que se conoce de antemano la salida que proporciona el algoritmo con esos datos. Si la salida calculada con esos datos no coincide con la conocida, el test falla.

189 ***Modelo de estados finitos***: modelo matemático que describe la operación del módulo

190 ***Puerto***: implementación física de un interface lógico que proporciona acceso al TOE para señales físicas representadas por flujos de información lógicos.

191 ***Tamper detection***: determinación automática de se ha intentado comprometer la seguridad física del módulo.

192 ***Tamper evidence***: señal externa observable por un operador que indica que ha habido un intento de comprometer la seguridad física del módulo.

193 ***Tamper response***: acción automática realizada por el módulo cuando se detecta intento de comprometer la seguridad física del módulo.

194 ***Trusted path***: medio por el que una entidad y el TOE se pueden comunicar con la confianza necesaria para dar soporte a una política de seguridad.

195 ***Zeroizacion***: método de borrado electrónico que evita la recuperación de los datos almacenados en el dispositivo

# 8 Referencias

**196** **Common Criteria**


[CC31p2] Common Criteria for Information Technology Security Evaluation.
Part 2: Security Functional Components
Version 3.1 R3

[CC31p3] Common Criteria for Information Technology Security Evaluation.
Part 3: Security Assurance Components
Version 3.1 R3

[CEM31] Common Criteria for Information Technology Security Evaluation.
Evaluation Methodology
Version 3.1 R3


**197** **FIPS 140-2**


[FIPS1402] FIPS140-2 PUB FIPS 140-2 Security Requirements for cryptographic modules

[FIPS-ANEXOS] FIPS140-2 PUB FIPS 140-2 Security Requirements for cryptographic modules.
ANEXO A: Approved Security Functions
ANEXO C: Approved Random Number Generators
ANEXO D: Approved Key Establishment Techniques