Declaración de Seguridad de Cryptosec+Firmware PKCS#11 Versión 1.0

Realia Technologies, S.L.

21 de Junio de 2010

Índice general

Capítulo 1

Introducción

1.1. Identificación de la ST

Título: Declaración de Seguridad de Cryptosec+Firmware PKCS#11

Versión 1.0

Autor: Realia Technologies, S.L.

Fecha de publicación: 21 de Junio de 2010

1.2. Identificación del TOE

Nombre: Cryptosec+Firmware PKCS#11

Versión 1.0

Desarrollador: Realia Technologies, S.L.

1.3. Resumen del TOE

Cryptosec+Firmware PKCS#11 es un producto del tipo HSM genérico. Su funcionalidad es proporcionar servicios criptográficos y de protección de claves al host. Los servicios proporcionados por el host son suficientes para implementar de forma segura la API [18, PKCS#11]. El TOE proporciona mecanismos de gestión de claves y del propio TOE.

Las operaciones criptográficas que proporciona el TOE son: MD5, SHA-1, RSA y T-DES.

Existen tres tipos de usuarios que permiten la gestión del TOE, la gestión de las claves y el transporte de claves.

- Superusuario: encargado de la gestión del TOE.
- Usuario de operación: encargado de la gestión de las claves.
- Custodio: encargado del transporte de claves mediante partición de las claves.

Para poder exportar claves entre diferentes custodios mediante impresión el TOE necesita una impresora.

El TOE dispone de dos interfaces:

- Un conector contra bus PCI 2.2 para la comunicación con el host.
- El TOE dispone de una interfaz [7, RS-232] para su gestión y para la impresión de claves de custodio.

El TOE está compuesto por hardware y firmware, cuyas versiones son:

- Hardware: Cryptosec versión 1.0
- Firmware: Firmware PKCS#11 versión 01.00.0308

Capítulo 2

Descripción del TOE

El TOE es un módulo de seguridad por hardware (HSM), actualmente certificado bajo la norma [15, FIPS 140-2].

El TOE proporciona los servicios criptográficos para la implementación de un subconjunto de la API [18, PKCS#11].

El TOE se utiliza como módulo de seguridad para un host que requiera realizar operaciones criptográficas, protegiendo la confidencialidad de las claves. El host generalmente es un ordenador tipo PC con un sistema operativo de propósito general y una aplicación de control del TOE. La gestión de claves la realiza el TOE en nombre de los usuarios.

Ejemplos de uso del TOE son:

- Acelerador SSL
- Elemento de seguridad que forma parte de una TSA.
- Parte de un sistema perteneciente a una CA.
- Cifrado de flujos de datos, como por ejemplo televisión por pago.
- Cifrado de bloques de datos, como por ejemplo operaciones de backup y acceso transparente a datos.
- En sistemas bancarios, como parte del sistema de verificación de transacciones.
- Sistemas de prepersonalización y personalización de tarjetas de banda magnética y EMV.
- Sistemas de telepeaje.
- Sistemas de carga de claves en PIN pads.

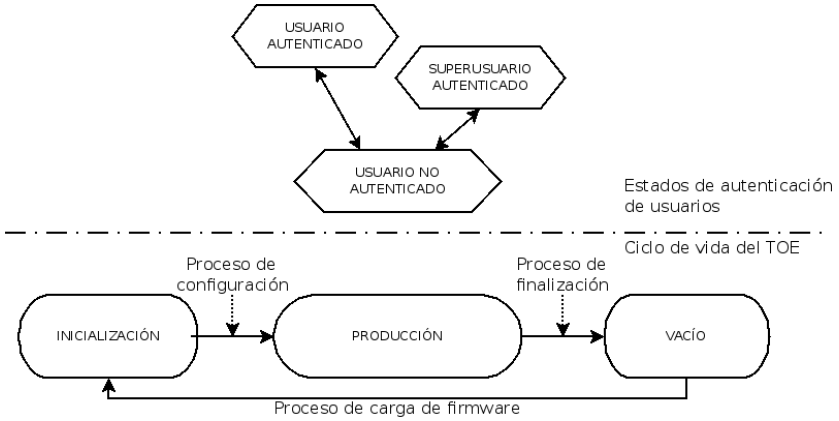

Figura 2.1: Ciclo de vida y estados de autenticación del TOE

El ciclo de vida del TOE es simple. Existen tres estados que son:

- Vacío: El TOE no contiene firmware ni datos confidenciales.
- Inicialización: El TOE dispone de firmware pero no se ha configurado ni inicializado.
- Producción: Estado de operación habitual.

El firmware es un elemento software que define buena parte del comportamiento del TOE. Una vez cargado sobre el hardware es cuando se considera TOE. La carga se debe realizar en un entorno seguro. A partir del momento en que se ha creado una clave RSA para autenticar la identidad del TOE se puede verificar que el software cargado no ha sido modificado.

El TOE está compuesto de elementos software y hardware.

(tal como se presenta en la figura 2.2). Los límites físicos del TOE son la superficie de la tarjeta PCI , protegida por una carcasa metálica (anti-tampering) que protege su interior. Su interior contiene un procesador que realiza las operaciones criptográficas, una controladora para el bus PCI, un RTC, una memoria para almacenar datos/claves/configuración y una controladora para el puerto serie.

El TOE proporciona dos interfaces de comunicación con el entorno:

- Puerto [7, RS-232], para la comunicación en fases de personalización, configuración e impresiones de sobres ciegos. El protocolo de comunicación a usar es [6].

Figura 2.2: Aspecto físico del TOE

- Interfaz PCI 2.2 con velocidad de bus a 50-60 MHz, para la comunicación con la aplicación de control en fase de producción.

El TOE cuenta con mecanismos de auto-protección frente a ataques físicos:

- Tampering
- Inyección de fallos
- Análisis de sus emanaciones

El TOE dispone de tres tipos de usuarios: el superusuario, usuario de operación y custodios. El superusuario tiene capacidades de administración sobre el TOE. El usuario de operación tiene capacidades de realizar operaciones criptográficas y de gestión de claves. Los custodios sólo están autorizados para importar y exportar claves bajo la supervisión del usuario de operación. Todos los usuarios disponen de una contraseña de autenticación.

El TOE usará una impresora conectada al puerto serie para imprimir los sobres ciegos.

El TOE dispone de dos configuraciones de seguridad básicas:

- Modo FIPS

- Modo no-FIPS

El modo FIPS fuerza el cumplimiento del estándar [15, FIPS 140-2], y básicamente consiste en permitir la autenticación y la gestión del TOE y las claves mediante una interfaz segura, que en el caso del TOE es la interfaz RS-232. Sólo se evaluará el TOE en modo FIPS.

Las funcionalidades de administración permiten al superusuario cambiar la configuración de habilitación de la impresora, reiniciar el TOE, añadir y quitar custodios y modificar las contraseñas de todos los usuarios del sistema. Antes de cambiar cualquier contraseña se requiere que el usuario al que pertenece la contraseña se autentique.

Para poder realizar las operaciones anteriormente descritas, el TOE proporciona la capacidad de crear, importar, exportar, cargar y extraer claves mediante custodios y revocar claves.

El usuario de operación del TOE es el rol autorizado para realizar estas operaciones y debe estar autenticado para elegir los roles de las claves, aunque en determinadas operaciones puede requerir de la colaboración del superusuario y/o de los custodios.

Las funcionalidades criptográficas del TOE son:

- RSA: firma, verificación, cifrado y descifrado
- DES, T-DESede, T-DESeee: cifrado y descifrado
- MD5: hash
- SHA-1: hash
- RNG: Generación de números aleatorios

El TOE utiliza su propia implementación de números aleatorios que será usada en la generación de claves T-DES y RSA.

Existen dos tipos de claves de producción:

- Claves de producción: Son aquellas usadas en producción para realizar operaciones de cifrado, descifrado y firma de datos. Estas clases se pueden subdividir en:
  - Claves de cifrado: Pueden ser claves DES (ya sea en longitud doble o triple) o RSA (privadas para descifrar y públicas para cifrar)
  - Claves de firma: Son exclusivamente claves RSA (públicas y privadas tanto para la realización como para la verificación de firma)

- Claves de wrapping: Podemos considerarlas claves de transporte de claves, ya que se usan para cifrar y descifrar las claves que se importarán y exportarán del TOE.

Capítulo 3

Conformidad respecto a la norma

Esta ST se ha escrito conforme a la norma Common Criteria en su versión 3.1.

> [2, CCMB-2006-09-001] Common Criteria for Information Technology Security Evaluation, part 1: Introduction and general model, version 3.1 release 1 September 2006
>
> [3, CCMB-2007-09-002] Common Criteria for Information Technology Security Evaluation, part 2: Security functional components, version 3.1 release 2 September 2007
>
> [4, CCMB-2007-09-003] Common Criteria for Information Technology Security Evaluation, part 3: Security assurance components, version 3.1 release 2 September 2007

La conformidad respecto a la segunda parte de CC es extendida; en cambio para la parte tres la conformidad es estricta. El nivel de garantía para esta evaluación es EAL4 con la aumentación ALC_FLR.1.

Capítulo 4

Definición del problema de seguridad

4.1. Activos

O.MasterFWKey - Clave maestra de firmware
Es una clave T-DESeee que sirve para cifrar las claves de CMM (cifrado y autenticación). Es generada por el propio TOE y reside en la NSRAM del chip que implementa las operaciones de seguridad. No existe ningún comando que permita la extracción de la clave.

O.CMM - Claves Maestras de Módulo
Estas claves sirven para cifrar las claves usadas en producción. Son del tipo T-DESeee y su misión es cifrar y autenticar las claves que se almacenan fuera del TOE (*O.PrivateKey* y *O.SecretKey*). Se almacenan en NSRAM cifradas mediante la clave *O.MasterFWKey*.

O.PublicKey - Claves públicas RSA
Las claves públicas son claves RSA de entre 1024 y 4096 bits. Sus usos son el cifrado y verificación de firma y también la exportación de claves. Se almacenan en el host, autentificadas mediante *CMM*.

O.PrivateKey - Claves privadas RSA
Las claves privadas son claves RSA de entre 1024 y 4096 bits. Sus usos son el descifrado y generación de firma y también la importación de claves. Se almacenan en el host, cifradas y autenticadas mediante *CMM*.

O.SecretKey - Claves simétricas
Las claves T-DES son usadas para la importación de claves en producción. Se almacenan en el host, cifradas y autentificadas mediante *CMM*.

O.VAD - Credencial de usuario
Contraseña de acceso al TOE. Ésta puede ser la contraseña de un superusuario, usuario de operación o custodio (contraseña más identificador).

4.2. Amenazas

T.KEYLEAK - Revelación de clave criptográfica
Un atacante recupera una clave criptográfica protegida por los mecanismos de seguridad del TOE. Los activos afectados por esta amenaza son *O.MasterFWKey*, *O.CMM*, *O.PublicKey*, *O.PrivateKey*, *O.SecretKey*. y/o una clave de autenticación *O.VAD*.

4.3. Hipótesis

A.HUMAN - Usuarios competentes
Los usuarios del TOE que realizan operaciones de administración y los custodios serán confiables.

A.PHYSPROT - Ubicación segura en estado de producción
El TOE se conectará a un host mediante la interfaz PCI y en su uso en estado de producción se ubicara en un entorno físico protegido y además que ofrezca protección frente a emanación tipo TEMPEST.

4.4. Políticas de seguridad organizativas

P.CRYPTOOPERATIONS - Operaciones criptográficas
El TOE debe realizar correctamente las siguientes operaciones criptográficas:

- Cifrado y descifrado DES con longitudes de clave doble y triple.
- Cifrado, descifrado, firma y verificación de firma RSA en formato PKCS.
- Cálculo del resultado de las funciones de hash SHA-1 y MD5
- Generación de números aleatorios RNG

P.KEYMANAGEMENT - Gestión de claves

El TOE proporciona mecanismos de gestión de claves, permitiendo la creación (mediante el uso del generador de números aleatorios), importación, exportación, extracción y revocación de claves.

P.MANAGEMENT - Administración del TOE

El TOE proporciona mecanismos para su administración. Los mecanismos de administración serán:

- Elección del modo FIPS.
- Auto-comprobación del TOE.
- Reset del módulo, eliminando el firmware.
- Instalación y desinstalación de impresora, y lectura de su dato de configuración.
- Carga de las cadenas de formato y de impresión para la impresora.

Los privilegios, interfaces y estados del TOE para realizar las diferentes acciones son:

- La elección del modo FIPS sólo se puede realizar en fase de inicialización del TOE desde la interfaz PCI.
- La auto-comprobación del TOE se debe realizar en fase de inicialización o de producción desde cualquiera de las dos interfaces, y no requiere autenticación.
- El reset del módulo debe ser permitido libremente en fase de inicialización o desde la interfaz PCI, y se debe requerir autenticación del administrador para acceder desde RS-232.
- La gestión de habilitación y la carga de cadenas de formato de la impresora sólo se permite al administrador del TOE. La lectura de la configuración de habilitación debe ser permitida desde cualquier estado de autenticación. Ambas operaciones deben ser accesibles sólo desde la interfaz PCI.
- La carga de cadenas de impresión sólo debe estar permitida en fase de producción sin usuario autenticado o con usuario de operación autenticado. Esta operación sólo será accesible a través de la interfaz PCI

P.GOODHASHES - Usos correctos de los hashes

Las operaciones de hash que se ordenen al TOE se usarán de manera que las operaciones criptográficas de más alto nivel (como sería la generación de un certificado) no se vean afectadas por vulnerabilidades detectadas en los algoritmos.

La vulnerabilidad más común es que el algoritmo sea vulnerable a ataques de colisión, que permiten a un atacante crear dos documentos diferentes (preimagenes) que generen el mismo resultado (la imagen).

En el momento de la redacción de la ST, MD5 se considera inseguro frente a ataques de colisión, pero sigue siendo válido para ciertas aplicaciones como HMAC-MD5 o firmas con relleno aleatorio.

P.STRONGCRYPTO - Uso correcto de operaciones criptográficos

Aunque el TOE permite la realización de operaciones criptográficas con distintas longitudes de clave, por motivos de fortaleza del algoritmo criptográfico, el usuario del TOE debe evitar usar los algoritmos RSA y DES con las siguientes propiedades:

- RSA con longitudes de clave inferior a 1024 bits
- DES con clave simple

Capítulo 5

Objetivos de seguridad

5.1. Objetivos de seguridad para el TOE

OT.KEYLEAK - Impedir la revelación de claves a entidades no autorizadas

El TOE impedirá que las claves cargadas en él sean reveladas. La protección será de forma reactiva destruyendo las claves en los casos detectables (tampering y ataques de perturbación, software y/o protocolo). En los casos que no se puedan detectar los ataques, como serían ataques laterales o desactivación del mecanismo de anti-tampering, se implementaran técnicas para reducir la explotabilidad vía firmware.

OT.CRYPTOOPERATIONS - Operaciones criptográficas

El TOE realizará las operaciones criptográficas especificadas por el firmware cargado, cumpliendo con los estándares públicos. La petición de realización de estas operaciones se realizará mediante la interfaz PCI.

Estas operaciones serán la generación de claves T-DES, generación de claves RSA, hashes MD5 y SHA-1, cifrado y descifrado T-DES y cifrado, descifrado, firma y verificación de firma RSA.

Las funciones que puede realizar una clave son:

- Cifrado: Permite realizar operaciones de cifrado y descifrado.
- Firma: Permite realizar operaciones de firma y verificación.
- Wrapping: Permite su uso para el cifrado al exportar una clave.
- Externas: el host usa estas claves para implementar ciertas partes de PKCS#11

OT.KEYMANAGEMENT - Gestión de claves

El TOE proporcionará la capacidad de gestión de claves al usuario de operación cuando éste esté autenticado. Esta gestión se realizará a través de la interfaz RS-232 y consistirá en la creación, importación, exportación, carga, extracción, revocación de claves DES y RSA y en la asignación de funciones a cada una de las claves.

OT.MANAGEMENT - Administración del TOE

El TOE proporcionará mecanismos para su administración, siendo éstos:

- Elección del modo FIPS.
- Auto-comprobación del TOE.
- Reseteo del módulo, eliminando el firmware.
- Instalación y desinstalación de impresora, y lectura de su dato de configuración.
- Carga de las cadenas de formato y de impresión para la impresora.

Los privilegios, interfaces y estados del TOE para realizar las diferentes acciones son:

- La elección del modo FIPS sólo se podrá realizar en fase de inicialización del TOE desde la interfaz PCI.
- La auto comprobación del TOE se podrá realizar en fase de inicialización o de producción, desde cualquiera de las dos interfaces y no se requerirá autenticación.
- El reset del módulo será permitido libremente en fase de inicialización y se requerirá autenticación del administrador para acceder desde RS-232.
- La gestión de habilitación y la carga de cadenas de formato de la impresora sólo estará permitida al administrador del TOE. Ambas operaciones serán accesibles sólo desde la interfaz PCI.
- La carga de cadenas de impresión sólo estará permitida en fase de producción sin usuario autenticado o con usuario de operación autenticado. Esta operación sólo será accesible a través de la interfaz PCI.

5.2. Objetivos de seguridad para el entorno

OE.HUMAN - Personal confiable

Los usuarios que realicen operaciones administrativas y los custodios seguirán las guías y procedimientos.

OE.PHYSPROT - Ubicación segura en estado de producción

El TOE debe estar ubicado en un entorno protegido cuando se use en su estado de producción.

OE.GOODHASHES - Usos seguros de las funciones de hash

El administrador y los desarrolladores de aplicaciones se asegurarán que los usos que hagan las aplicaciones de las funcionalidades de hash del TOE no se vean afectados por vulnerabilidades conocidas.

OE.STRONGCRYPTO - Uso correcto de operaciones criptográficos

Los usuarios del TOE se asegurarán que las longitudes de claves para las distintas aplicaciones cumplan con los requisitos mínimos, siendo los aplicables:

- RSA con longitudes de clave de cómo mínimo de 1024 bits
- T-DES con claves de 128 o 192 bits

Capítulo 6

Definición de requisitos extendidos

6.1. Requisitos funcionales de seguridad

6.1.1. FPT_EMSEC - TOE Emanation

Family Behaviour

This family defines requirements to mitigate intelligible emanations.

FPT_EMSEC.1 - TOE Emanation

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no auditable events foreseen.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall not emit *[assignment: types of emissions]* in excess of *[assignment: specified limits]* enabling access to *[assignment: assets requiring confidentiality protection]*.
FPT_EMSEC.1.2	The TSF shall ensure *[assignment: type of users]* are unable to use the following interface *[assignment: type of connection]* to gain access to *[assignment: assets requiring confidentiality protection]*.

Justificación de creación de requisitos extendidos

Se ha creado esta familia porque el catálogo de requisitos funcionales de Common Criteria no contiene ningún requisito que pueda cubrir los ataques

basados en análisis de emanaciones. El autor de la ST se ha basado en el requisito FPT_EMSEC.1 del documento [9, CWA14169].

6.1.2. FCS_RND - Generation of random number

Family Behaviour

This family defines quality metrics for generating random numbers intended for cryptographic purposes

FCS_RND.1 - Generation of random numbers

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no auditable events foreseen.

Hierarchical to:	No other components.
Dependencies:	FPT_TST.1
FCS_RND.1.1	The TSFs shall provide a mechanism for generating random numbers that meet *[assignment: a defined quality metric]*.
FCS_RND.1.2	The TSFs shall be able to enforce the use of TSF-generated random numbers for *[assignment: list of TSF functions]*.

Justificación de creación de requisitos extendidos

Se ha creado esta familia porque el catálogo de requisitos funcionales de Common Criteria no contiene ningún requisito que pueda cubrir los requisitos de generación de números aleatorios [8, CWA14167-4].

Capítulo 7

Requisitos funcionales de seguridad

FCS_COP.1/DES - Cryptographic operation

FCS_COP.1.1 The TSF shall perform *[assignment: cifrado y descifrado]* in accordance with a specified cryptographic algorithm *[assignment: T-DES]* and cryptographic key sizes *[assignment: 112 y 168 bits (sin contar los bits de paridad)]* that meet the following: *[assignment: [11, FIPS 46-3]]*.

FCS_COP.1/RSA - Cryptographic operation

FCS_COP.1.1 The TSF shall perform *[assignment: cifrado, descifrado, firma y verificación]* in accordance with a specified cryptographic algorithm *[assignment: RSA]* and cryptographic key sizes *[assignment: Entre 1024 y 4096]* that meet the following: *[assignment: [17, PKCS#1]]*.

FCS_COP.1/MD5 - Cryptographic operation

FCS_COP.1.1 The TSF shall perform *[assignment: operación de hash]* in accordance with a specified cryptographic algorithm *[assignment: MD5]* and cryptographic key sizes *[assignment: (no aplica)]* that meet the following: *[assignment: [16, RFC1321]]*.

FCS_COP.1/SHA-1 - Cryptographic operation

FCS_COP.1.1 The TSF shall perform *[assignment: operación de hash]* in accordance with a specified cryptographic algorithm *[assignment: SHA-1]* and cryptographic key sizes *[assignment: (no aplica)]* that meet the following: *[assignment: [14, FIPS 180-2]]*.

FCS_CKM.1/DES - Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[assignment: PRNG descrito en [12, FIPS 186-2]]* and specified cryptographic key sizes *[assignment: 112 y 168 bits (sin contar los bits de paridad)]* that meet the following: *[assignment: [12, FIPS 186-2]]*.

FCS_CKM.1/RSA - Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[assignment: RSAgen1]* and specified cryptographic key sizes *[assignment: entre 1024 y 4096 bits]* that meet the following: *[assignment: estándar Rigen1]*.

FASE_CKM.4/INTERNAL - Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[assignment: sobreescritura del valor de la clave con ceros]* that meets the following: *[assignment: [15, FIPS 140-2]]*.

FCS_CKM.4/REVOCATION - Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[assignment: mecanismo de revocación de claves]* that meets the following: *[assignment: ninguno]*.

FCS_RND.1 - Generation of random numbers

FCS_RND.1.1 The TSFs shall provide a mechanism for generating random numbers that meet *[assignment: AIS 20 version 1, functional class and evaluation methodology for deterministic RNG, 2-dec-1999, class K4 (see [1, AIS 20])]*.

FCS_RND.1.2 The TSFs shall be able to enforce the use of TSF-generated random numbers for *[assignment: FCS_CKM.1 and randomN command.]*.

FDP_ITC.2/KEYUNWRAP - Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the *[assignment: política de control de importación de 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: *[assignment: sólo se permitirá la importación de una clave dentro del dominio de protección del TOE si el usuario lo autoriza explícitamente.]*.

FDP_ITC.2/KEYLOAD - Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the *[assignment: política de control de carga de 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: *[assignment: sólo se permitirá la carga de claves que estén bajo el dominio de protección del TOE si su MAC es válido]*.

FDP_ETC.1/KEYWRAP - Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the *[assignment: política de control de exportación de 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

FDP_ETC.2/KEYUNWRAP - Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the *[assignment: política de control de importación de claves]* when exporting user data, controlled under the SFP(s), outside of the TOE.

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

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

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

FDP_ACC.1/KEYWRAP - Subset access control

FDP_ACC.1.1 The TSF shall enforce the *[assignment: política de control de exportación de claves]* on *[assignment: exportación de claves]*.

FDP_ACC.1/KEYUNWRAP - Subset access control

FDP_ACC.1.1 The TSF shall enforce the *[assignment: política de control de importación de claves]* on *[assignment: importacion de claves]*.

FDP_IFC.1/KEYLOAD - Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the *[assignment: política de control de carga de claves]* on *[assignment: carga de claves protegidas por el dominio de protección del TOE]*.

FTP_ITC.1/KEYUNWRAP - Inter-TSF trusted channel

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

FTP_ITC.1.2 The TSF shall permit *[selection: another trusted IT product]*

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *[assignment: importación y exportación de claves mediante claves de transporte]*.

FTP_ITC.1/KEYLOAD - Inter-TSF trusted channel

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

FTP_ITC.1.2 The TSF shall permit *[selection: another trusted IT product]*

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *[assignment: importación y exportación de claves mediante CMMs]*.

FPT_TDC.1 - Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *[assignment: claves DES (longitud doble o triple) y claves RSA (publicas y privadas)]* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *[assignment: reglas de interpretación definidas en el documento de especificación del TOE]* when interpreting the TSF data from another trusted IT product.

FDP_ACF.1/KEYUNWRAP - Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the *[assignment: política de control de importación de claves]* to objects based on the following: *[assignment: claves a importar (T-DES y RSA -publica y privada-)]*.

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: sólo se permitirá la importación de una clave si el usuario lo permite explicitamente a través del canal seguro (puerto serie)]*.

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

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

FDP_ACF.1/KEYWRAP - Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the *[assignment: política de control de exportación de claves]* to objects based on the following: *[assignment: claves a exportar (T-DES y RSA -publica y privada-)]*.

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: sólo se permitirá la exportación de una clave si el usuario lo permite explicitamente a través del canal seguro (puerto serie)]*.

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

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

FDP_IFF.1/KEYLOAD - Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the *[assignment: política de control carga de claves]* based on the following types of subject and information security attributes: *[assignment: valor MAC]*.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *[assignment: valor MAC válido]*.

FDP_IFF.1.3 The TSF shall enforce the *[assignment: ninguna]*.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: *[assignment: ninguna]*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *[assignment: ninguna]*.

FIA_UAU.1 - Timing of authentication

FIA_UAU.1.1 The TSF shall allow *[assignment: powerTest, firmwareVersion, getHSMIdentification, getServerConf, putServerConf, resetModule, getConfigurationData, loadSwVersion, saveSwVersion]* 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.

FIA_UID.1 - Timing of identification

FIA_UID.1.1 The TSF shall allow *[assignment: powerTest, firmwareVersion, getHSMIdentification, getServerConf, putServerConf, resetModule, getConfigurationData, loadSwVersion, saveSwVersion]* 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.

FDP_RIP.1 - Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *[selection: deallocation of the resource from]* the following objects: *[assignment: toda información bajo el control de las TSFs que deba ser considerada como confidencial y que no sea una clave]*.

FMT_MTD.1 - Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to *[selection: modify]* the *[assignment: habilitación de la impresora]* to *[assignment: administrador del TOE]*.

FMT_SMR.1 - Security roles

FMT_SMR.1.1 The TSF shall maintain the roles *[assignment: Superusuario, usuario de operación y custodios]*.

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

FMT_SMF.1 - Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: *[assignment: putUpDateConf, resetModule, loadConfigurationData, loadPFString]*.

FPT_PHP.3 - Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist *[assignment: intentos de tamper]* to the *[assignment: el TOE en su integridad]* by responding automatically such that the SFRs are always enforced.

FPT_EMSEC.1 - TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit *[assignment: cualquier tipo de emanación]* in excess of *[assignment: calidad]* enabling access to *[assignment: O.MasterFWKey, O.CMM, O.PrivateKey, O.SecretKey or O.VAD]*.

FPT_EMSEC.1.2 The TSF shall ensure *[assignment: atacantes]* are unable to use the following interface *[assignment: PCI, RS-232 y la superficie física del TOE]* to gain access to *[assignment: O.MasterFWKey, O.CMM, O.PrivateKey, O.SecretKey or O.VAD]*.

FPT_TST.1 - TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests *[selection: durante el arranque inicial y bajo demanda de un usuario autorizado]* to demonstrate the correct operation of *[selection:* [assignment: RNG, T-DES y RSA] *]*.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *[selection:* [assignment: RNG, T-DES y RSA] *]*.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Capítulo 8

Requisitos de garantía de seguridad

El nivel de garantía elegido es EAL4+ALC_FLR.1, ya que cubre las necesidades de garantía del producto en el entorno de producción especificado en esta ST.

Componente	Titulo
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.2	Security objectives
ASE_REQ.2	Derived security requirements
ASE_SPD.1	Security problem definition
ASE_TSS.1	TOE summary specification
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.2	Testing: security enforcing modules
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.3	Focused vulnerability analysis
ALC_FLR.1	Basic flaw remediation

Capítulo 9

Resumen de la especificación del TOE

TSF.MANAGEMENT

FIA_UAU.1 El TOE implementa un control de flujo de operación, el cual permite la ejecución de las siguientes operaciones powerTest, firmwareVersion, getHSMIdentification, getServerConf, putServerConf, resetModule, getConfigurationData, loadSwVersion, saveSwVersion sin estar autenticado. Para el resto de operaciones el usuario debe estar autenticado.

FIA_UID.1 El TOE implementa un control de flujo de operación, el cual permite la ejecución de las siguientes operaciones powerTest, firmwareVersion, getHSMIdentification, getServerConf, putServerConf, resetModule, getConfigurationData, loadSwVersion, saveSwVersion sin estar autenticado. Para el resto de operaciones el usuario debe estar identificado.

FMT_MTD.1 La gestión de habilitación y la carga de cadenas de formato de la impresora sólo esta permitida al administrador del TOE, la lectura de la configuración de habilitación está permitida desde cualquier estado de autenticación. Ambas operaciones sólo son accesibles desde la interfaz PCI.

FMT_SMF.1 Cubre la especificación de las funciones de gestión de la configuración.

TSF.USERS

FDP_RIP.1 El TOE implementa la destrucción de objetos liberados "deallocated" mediante una sobre-escritura con zeros.

FMT_SMR.1 El TOE soporta tres tipos de usuarios: superusuario, usuario de operación y custodios. Existe una sola cuenta de superusuario, que debe ser controlada por el administrador de seguridad del TOE. También existe una sola cuenta de usuario de operación, que no es usada de forma directa por el TOE, sino que el host usa el estado de autenticación para la implementación de la librería PKCS#11.

Una vez en producción, el TOE es capaz de mantener el estado de autenticación de los usuarios, uno de forma concurrente. Dependiendo del estado de autenticación se permitirá realizar distintas operaciones. También permite que el superusuario permita a los usuarios el cambio de passwords.

TSF.CRYPTOOPS

FCS_COP.1/DES El TOE implementa el algoritmo T-DES con una longitud de clave de 112 bits y 168 bits conforme con FIPS 46-3. Estas operaciones deben ser accesibles libremente desde la interfaz PCI. Los modos de cifrado son ECB, CBC, OFB-64 y CFB-64.

FCS_COP.1/RSA El TOE implementa las operaciones de cifrado, descifrado, firma y verificación con el algoritmo RSA con formato PKCS, mediante las operaciones $m^e(modn)$ y $m^d(modn)$ con claves RSA. Estas operaciones deben ser accesibles libremente desde la interfaz PCI.

FCS_COP.1/MD5 El TOE implementa el algoritmo MD5 conforme al estándar [16, RFC1321]. Estas operaciones deben ser accesibles libremente desde la interfaz PCI.

FCS_COP.1/SHA-1 El TOE implementa el algoritmo SHA-1 conforme al estándar [14, FIPS 180-2]. Estas operaciones deben ser accesibles libremente desde la interfaz PCI.

FCS_CKM.4/INTERNAL El TOE implementa la destrucción de las claves criptográficas mediante la sobre-escritura del valor de la clave con zeros.

FCS_RND.1 El TOE implementa la generación de números aleatorios mediante una semilla TRNG y un post-procesado, generando un DRNG.

FDP_ITC.2/KEYLOAD El TOE implementa la validación de la operación de importación de claves de operación mediante la validación del MAC con la CMM correspondiente.

FDP_IFC.1/KEYLOAD El TOE no guardará las claves de operaciones, sino que guardará un juego de claves en su interior (las CMM). Se usarán las CMM para descifrar y comprobar la autenticidad y función de las claves. El TOE dispondrá de diferentes CMM, una para cada una de las operaciones. Cada vez que se requiera realizar una operación criptográfica con clave, la clave se cargará al TOE al realizar la propia operación.

FTP_ITC.1/KEYLOAD El TOE implementa la operación de importación y exportación de claves de operación mediante CMMs a través del canal confiable RS-232.

FPT_TDC.1 El TOE implementa reglas validación de los formatos de las claves T-DES (longitud doble 128 bits o triple 192 bits) y claves RSA (publicas y privadas) cuando se cargan en el TOE.

Además, permite validar para las claves RSA los roles disponibles:

- Cifrado: para claves públicas que sean autenticadas con la CMM de cifrado
- Descifrado: para claves privadas que sean autenticadas con la CMM de cifrado
- Firma: para claves privada que sean autenticadas con la CMM de firma
- Verificación de firma: para claves públicas que sean autenticadas con la CMM de firma
- Importación: para claves privadas que sean autenticadas con la CMM de wrapping
- Exportación: para claves públicas que sean autenticadas con la CMM de wrapping

Y para las claves DES los roles disponibles:

- Cifrado y descifrado: para claves públicas que sean autenticadas con la CMM de cifrado

- Importación y exportación: para claves privadas que sean autenticadas con la CMM de wrapping

FDP_IFF.1/KEYLOAD El TOE implementa la validación de la operación de carga de claves de operación mediante la validación del MAC con la CMM correspondiente.

FPT_TST.1 El TOE dispone de mecanismos de autotest para verificar el correcto funcionamiento de las TSFs y los algoritmos criptográficos implementados en el el firmware (T-DES y RSA). Además también permite verificar la integridad del mecanismo de generación de números aleatorios mediante el comando testModule, el cual valida las operación en ambos sentidos validando el resultado obtenido con el esperado. A partir del momento en que se ha creado una clave RSA para autenticar la identidad del TOE se puede verificar que el firmware cargado no ha sido modificado.

TSF.KEYMANAGEMENT

FCS_CKM.1/DES El TOE implementa la generación de claves DES mediante la ejecución del generador de números aleatorios y seleccionando el numero de bits dependiendo de la longitud de la clave doble o triple (128 y 192 bits).

FCS_CKM.1/RSA El TOE implementa la creación de claves RSA mediante la ejecución del generador de números aleatorios dependiendo de la longitud de la clave (1024 a 4096 bits) verificando la primalidad por medio del test de Fermat o el de Miller-Rabin.

FCS_CKM.4/INTERNAL El TOE implementa la destrucción de las claves criptográficas mediante la sobre-escritura del valor de la clave con zeros.

FCS_CKM.4/REVOCATION La revocación de claves requieren la intervención del administrador del TOE y del usuario de operación. Esta operación se implementa mediante la carga de nuevas CMMs que remplazan a las anteriores (sin borrado) y permiten la re-asignación de claves a éstas nuevas.

FCS_RND.1 El TOE implementa la generación de números aleatorios mediante una semilla TRNG y un post-procesado, generando un DRNG.

FDP_ITC.2/KEYUNWRAP El TOE implementa la exportación de claves T-DES y RSA por la interfaz PCI si hay una aceptación explícita por el puerto RS-232 del usuario de operación.

FDP_ETC.1/KEYWRAP El TOE implementa la exportación de claves T-DES y RSA por la interfaz PCI si hay una aceptación explícita por el puerto RS-232 del usuario de operación

FDP_ETC.2/KEYUNWRAP El TOE implementa la importación de una clave "wrappeada" con una clave de transporte (wrapping).

FDP_ACC.1/KEYWRAP El TOE implementa la exportación de claves T-DES y RSA por la interfaz PCI si hay una aceptación explícita por el puerto RS-232 del usuario de operación

FDP_ACC.1/KEYUNWRAP El TOE implementa la exportación de claves T-DES y RSA por la interfaz PCI si hay una aceptación explícita por el puerto RS-232 del usuario de operación.

FTP_ITC.1/KEYUNWRAP El TOE implementa la operación de importación y exportación de claves de operación mediante claves de transporte (wrapping) a través de la interfaz PCI.

FDP_ACF.1/KEYUNWRAP El TOE implementa la exportación de claves T-DES y RSA por la interfaz PCI si hay una aceptación explícita por el puerto RS-232 del usuario de operación.

FDP_ACF.1/KEYWRAP El TOE implementa la exportación de claves T-DES y RSA por la interfaz PCI si hay una aceptación explícita por el puerto RS-232 del usuario de operación

TSF.SELFPROTECTION

FDP_RIP.1 El TOE implementa la destrucción de datos confidenciales que no sean claves mediante una sobre-escritura con zeros en el momento que estos dejan de ser usados.

FPT_PHP.3 El TOE es capaz de detectar intentos de tampering por parte de un atacante externo con acceso físico al TOE. Esta protección está implementada mediante un conjunto de sensores que detectan cuando se está intentando acceder físicamente en las partes internas del TOE, y un mecanismo de alarma que borra toda la memoria interna.

FPT_EMSEC.1 El TOE está diseñado para impedir la liberación de emanaciones por encima de un nivel que permita a un atacante recuperar información confidencial.

FPT_TST.1 El TOE dispone de mecanismos de autotest para verificar el correcto funcionamiento de las TSFs y los algoritmos criptográficos implementados en el el firmware (T-DES y RSA). Además también permite verificar la integridad del mecanismo de generación de números aleatorios mediante el comando testModule, el cual valida las operación en ambos sentidos validando el resultado obtenido con el esperado. A partir del momento en que se ha creado una clave RSA para autenticar la identidad del TOE se puede verificar que el firmware cargado no ha sido modificado.

Capítulo 10

Justificaciones

10.1. Objetivos de seguridad

	A.HUMAN	A.PHYSPROT	T.KEYLEAK	P.CRYPTOOPERATIONS	P.KEYMANAGEMENT	P.MANAGEMENT	P.GOODHASHES	P.STRONGCRYPTO
OT.KEYLEAK			✓					
OT.CRYPTOOPERATIONS				✓				
OT.KEYMANAGEMENT					✓			
OT.MANAGEMENT						✓		
OE.HUMAN	✓							
OE.PHYSPROT		✓	✓	✓	✓	✓		
OE.GOODHASHES							✓	
OE.STRONGCRYPTO								✓

OT.KEYLEAK-T.KEYLEAK

Impide la revelación de clave (ataques de perturbación, ataques software o protocolo y reducción de las emanaciones).

OT.CRYPTOOPERATIONS-P.CRYPTOOPERATIONS

Mapeo directo.

OT.KEYMANAGEMENT-P.KEYMANAGEMENT

Mapeo directo.

OT.MANAGEMENT-P.MANAGEMENT
Mapeo directo.

OE.HUMAN-A.HUMAN
Mapeo directo.

OE.PHYSPROT-A.PHYSPROT-P.CRYPTOOPERATIONS-P.KEYMANAGEMENT-P.MANAGEMENT
Cubre la ubicación física protegida en el uso del producto y sus funcionalidades en estado de producción

OE.GOODHASHES-P.GOODHASHES
Mapeo directo.

OE.STRONGCRYPTO-P.STRONGCRYPTO
Mapeo directo.

10.2. Requisitos funcionales de seguridad

	OT.KEYLEAK	OT.CRYPTOOPERATIONS	OT.KEYMANAGEMENT	OT.MANAGEMENT
FCS_COP.1/DES		✓	✓	
FCS_COP.1/RSA		✓	✓	
FCS_COP.1/MD5		✓		
FCS_COP.1/SHA-1		✓		
FCS_CKM.1/DES			✓	
FCS_CKM.1/RSA			✓	
FCS_CKM.4/INTERNAL			✓	
FCS_CKM.4/REVOCATION			✓	
FCS_RND.1			✓	
FDP_ITC.2/KEYUNWRAP			✓	
FDP_ITC.2/KEYLOAD		✓	✓	
FDP_ETC.1/KEYWRAP			✓	
FDP_ETC.2/KEYUNWRAP			✓	
FDP_ACC.1/KEYWRAP			✓	
FDP_ACC.1/KEYUNWRAP			✓	
FDP_IFC.1/KEYLOAD		✓		
FTP_ITC.1/KEYUNWRAP			✓	
FTP_ITC.1/KEYLOAD		✓	✓	
FPT_TDC.1		✓	✓	
FDP_ACF.1/KEYUNWRAP			✓	
FDP_ACF.1/KEYWRAP			✓	
FDP_IFF.1/KEYLOAD		✓	✓	
FIA_UAU.1				✓
FIA_UID.1				✓
FDP_RIP.1	✓			✓
FMT_MTD.1				✓
FMT_SMR.1				✓
FMT_SMF.1				✓
FPT_PHP.3	✓			
FPT_EMSEC.1	✓			
FPT_TST.1		✓	✓	

FCS_COP.1/DES-OT.CRYPTOOPERATIONS
Cubre la especificación de las operaciones con el cifrado T-DES.

FCS_COP.1/DES-OT.KEYMANAGEMENT
Cubre el wrapping y unwrapping de claves mediante claves T-DES.

FCS_COP.1/RSA-OT.CRYPTOOPERATIONS
Cubre la especificación de las operaciones con el algoritmo RSA para op-

eraciones de firma y cifrado.

FCS_COP.1/RSA-OT.KEYMANAGEMENT
Cubre el wrapping y unwrapping de claves mediante claves RSA.

FCS_COP.1/MD5-OT.CRYPTOOPERATIONS
Cubre la especificación de las operaciones con el algoritmo MD5 para operaciones de firma y cifrado.

FCS_COP.1/SHA-1-OT.CRYPTOOPERATIONS
Cubre la especificación de las operaciones con el algoritmo SHA-1 para operaciones de firma y cifrado.

FCS_CKM.1/DES-OT.KEYMANAGEMENT
Especifica los requisitos para la generación de claves DES.

FCS_CKM.1/RSA-OT.KEYMANAGEMENT
Especifica los requisitos para la creación de claves RSA.

FCS_CKM.4/INTERNAL-OT.KEYMANAGEMENT
Especifica la destrucción de claves criptográficas.
Especifica la destrucción de claves criptográficas.

FCS_CKM.4/REVOCATION-OT.KEYMANAGEMENT
Especifica la revocación de claves criptográficas.

FCS_RND.1-OT.KEYMANAGEMENT
Describe la generación de números aleatorios.

FDP_ITC.2/KEYUNWRAP-OT.KEYMANAGEMENT
Especifica la importación de claves criptográficas.

FDP_ITC.2/KEYLOAD-OT.CRYPTOOPERATIONS
Especifica la carga de claves criptográficas.

FDP_ITC.2/KEYLOAD-OT.KEYMANAGEMENT
Especifica la carga de claves criptográficas de soporte para la gestión de claves.

FDP_ETC.1/KEYWRAP-OT.KEYMANAGEMENT
Especifica la exportación de claves criptográficas.

FDP_ETC.2/KEYUNWRAP-OT.KEYMANAGEMENT
Especifica el almacenamiento fuera del TOE de claves criptográficas importadas en el dominio de protección del TOE.

FDP_ACC.1/KEYWRAP-OT.KEYMANAGEMENT
Especifica que para las operaciones exportación de claves se debe aplicar la política de exportación de claves.

FDP_ACC.1/KEYUNWRAP-OT.KEYMANAGEMENT
Especifica que para las operaciones importación de claves se debe aplicar la política de control de importación de claves.

FDP_IFC.1/KEYLOAD-OT.CRYPTOOPERATIONS
Especifica la carga de claves bajo el dominio de protección del TOE.

FTP_ITC.1/KEYUNWRAP-OT.KEYMANAGEMENT
Especifica los mecanismos de protección de las claves durante su importación.

FTP_ITC.1/KEYLOAD-OT.CRYPTOOPERATIONS
Especifica los mecanismos de protección de las claves durante su carga.

FTP_ITC.1/KEYLOAD-OT.KEYMANAGEMENT
Especifica los mecanismos de protección de las claves durante su carga.

FPT_TDC.1-OT.CRYPTOOPERATIONS
Especifica los formatos de las claves criptográficas.

FPT_TDC.1-OT.KEYMANAGEMENT
Especifica los formatos de las claves criptográficas.

FDP_ACF.1/KEYUNWRAP-OT.KEYMANAGEMENT
Describe las reglas en las que consiste la política de control de importación de claves.

FDP_ACF.1/KEYWRAP-OT.KEYMANAGEMENT
Describe las reglas en las que consiste la política de control de exportación de claves.

FDP_IFF.1/KEYLOAD-OT.CRYPTOOPERATIONS
Describe las reglas en las que consiste la política de control de carga de claves.

FDP_IFF.1/KEYLOAD-OT.KEYMANAGEMENT
Describe las reglas en las que consiste la política de control de carga de claves.

FIA_UAU.1-OT.MANAGEMENT
Especifica las operaciones que puede realizar el superusuario sin estar autenticado.

FIA_UID.1-OT.MANAGEMENT
Especifica las operaciones que puede realizar el superusuario sin estar identificado.

FDP_RIP.1-OT.KEYLEAK
Cubre la destrucción del VAD.

FDP_RIP.1-OT.MANAGEMENT
Cubre la destrucción de credenciales.

FMT_MTD.1-OT.MANAGEMENT
Especifica los roles que tienen capacidad de realizar operaciones de administración del TOE.

FMT_SMR.1-OT.MANAGEMENT
Especifica que el TOE debe ser capaz de distinguir entre superusuarios, usuarios de operación y custodios.

FMT_SMF.1-OT.MANAGEMENT
Especifica las funcionalidades de gestión del TOE.

FPT_PHP.3-OT.KEYLEAK
Impide la revelación de claves mediante tampering.

FPT_EMSEC.1-OT.KEYLEAK
Especifica que el TOE no debe permitir emanaciones que permitan recuperar una clave de forma no invasiva.

FPT_TST.1-OT.CRYPTOOPERATIONS
Especifica la correcta implantación de las operaciones criptográficas T-DES y RSA.

FPT_TST.1-OT.KEYMANAGEMENT
Especifica la integridad del generador de números aleatorios en su operación.

10.2.1. Justificación de dependencias

Se han incluido todas las dependencias de todos los requisitos funcionales por reproducción explícita, excepto el requisito funcional de seguridad FMT_MSA.3 de FDP_ACF.1 ya que no existen atributos por defecto. En todas las operaciones de importación, exportación y carga de claves se debe especificar todos los atributos de seguridad. En el caso de FCS_COP.1/SHA-1 y FCS_COP.1/MD5 no se han cubierto sus dependencias (FCS_CKM.1 y uno del conjunto FCS_CKM.1, FDP_ITC.1, FDP_ITC.2) ya que en las operaciones de hash no tienen claves asociadas.

Acrónimos

API Application Programming Interface

CA Certification Authority

CBC Cipher Block Chaining mode. ver [5]

CFB-64 Cipher feedback mode, ver [5]

CMM Clave Maestra de Módulo

DES Data Encryption Standard, ver [11]

DRNG Determinstc Random Number Generator

EAL Evaluation Assurance Level

ECB Electronic Code Book mode, ver [5]

EMV Europay, Mastercard and Visa

FIPS Federal Information Processing Standard

HMAC Keyed-Hash Message Authentication Code, ver [13]

HSM Hardware Security Module

MAC Message Authentication Code

MD5 Message-Digest Algorithm 5, ver [16]

NSRAM Non-volatile Secure RAM

OFB-64 Output feedback mode, ver [5]

PC Personal Computer

PCI Peripheral Component Interconnect

PIN Personal Identification Number

PRNG Pseudo Random Number Generator

RNG Random Number Generator

RSA Rivest, Shamir i Adleman, ver [17]

RTC Real Time Clock

SFP Security Function Policy

SHA-1 Secure Hash Algorithm, ver [14], [10]

SSL Secure Sockets Layer

ST Security Target

TOE Target Of Evaluation

TSA Time Stamping Authority

Glosario

Clave Maestra de Módulo Son claves que residen en el HSM y que sirven para cifrar y autenticar las claves de producción.

TEMPEST Es el nombre en código para referirse a emanaciones que comprometen la confidencialidad de la información, en el caso del TOE se refiere especialmente a emanaciones de tipo electromagnético generadas por la interfaz RS-232 y la interfaz de usuario asociada a ella.

aplicación de control Aplicación encargada de indicar que operaciones criptográficas debe realizar el TOE. Normalmente actúa cómo pasarela de un sistema mayor o ofreciendo servicio a sistemas finales.

custodio Persona que se encarga del transporte de una parte de una clave. Existen diferentes métodos de partición de claves, pero todos tienen en común que para recuperar una clave se requiere la partición de todos los custodios que disponen de un secreto.

dominio de protección Conjunto de activos protegidos por el TOE. Por ejemplo, cuando se importa una clave, esta se carga en el dominio de protección.

host Sistema externo, usualmente un PC, que usa los servicios proporcionados por el TOE. Entendemos el host cómo la máquina física que se conecta físicamente contra la interfaz PCI del TOE. El host y la aplicación de control están íntimamente enlazados ya que comparten el mismo dominio de protección.

sobres ciegos Sobre cerrado con mecanismos para preservar la confidencialidad cuya manipulación o intento de apertura no puede ocultarse. Generalmente es usado para entregar datos confidenciales -un PIN, una clave- a un usuario.

tampering Acción de manipular físicamente un elemento IT con el objetivo de afectar a las propiedades de seguridad.

Bibliografía

[1] Bundesamt fur Sicherheit in der Informationstechnik. *Functionality classes and evaluation methodology for deterministic random number generators.*

[2] Common Criteria Management Body. *Common Criteria for Information Technology Security Evaluation, part 1: Introduction and general model, version 3.1r1 September 2006.*

[3] Common Criteria Management Body. *Common Criteria for Information Technology Security Evaluation, part 2: Security functional components, version 3.1r2 September 2007.*

[4] Common Criteria Management Boody. *Common Criteria for Information Technology Security Evaluation, part 3: Security assurance components, version 3.1r2 September 2007.*

[5] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation - Methods and Techniques.* National Institute of Standards and Technology.

[6] Ecma International. *Control Functions for Coded Character Sets.*

[7] Electronics Industries Association. *Recommended Standard 232.*

[8] European Committee for Standarization. *Cryptographic Module for CSP Signing Operations Protection Profile, CMCSO-PP, Version: 0.28.*

[9] European Committee for Standarization. *CWA 14169:2004 Secure signature-creation devices EAL4+.*

[10] Internet Engineering Task Force. *US Secure Hash Algorithm 1 (SHA1).*

[11] National Institute of Standards and Technology. *DATA ENCRYPTION STANDARD (DES).*

[12] National Institute of Standards and Technology. *Digital Signature Standard (DSS).*

[13] National Institute of Standards and Technology. *The Keyed-Hash Message Authentication Code (HMAC).*

[14] National Institute of Standards and Technology. *Secure Hash Standard.*

[15] National Institute of Standards and Technology. *SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES.*

[16] R. Rivest. *The MD5 Message-Digest Algorithm.* Internet Engineering Task Force.

[17] RSA Laboratories. *PKCS #1 v2.1: RSA Cryptography Standard.*

[18] RSA Laboratories. *PKCS #11 v2.20: Cryptographic Token Interface Standard.*