Perfil de Protección Servicios en Red Realia Technologies S.L.

24-12-2010

Versión 2.0

Hoja de Información General

CONTROL DOCUMENTAL

PROYECTO:	
TÍTULO:	Perfil de Protección Servicios en Red Realia Technologies S.L.
VERSIÓN	2.0
FECHA DE EDICIÓN:	24-12-2010
FICHERO:	Perfil de Protección Servicios en Red REALSEC
HERRAMIENTAS DE EDICIÓN:	MICROSOFT WORD 2003
AUTORES:	REALSEC
COMPAÑÍA:	REALSEC

Control de Versiones

Versión	Fecha	Afecta	Breve descripción del cambio
1.0	10/12/2010	Todo	Versión inicial
2.0	24/12/2010	Todo	Modificaciones para resolver los problemas encontrados en los informes de observación y cambios menores para mejorar la claridad del perfil.

Índice

1 Introducción

1 Este documento es el Perfil de Protección que describe los requisitos de seguridad de una aplicación que proporciona servicios de carácter criptográfico a través de la red a un usuario final, utilizando para ello un HSM (Hardware Security Module).

2 El TOE que declare cumplimiento con este PP deberá ejecutarse sobre un sistema operativo apropiadamente securizado.

3 El HSM utilizado deberá ser conforme a [FIPS1402] y a [FIPS-ANEXOS].

1.1 Identificación del PP

Título	Perfil de Protección Servicios en Red Realia Technologies S.L.
Versión	Versión 2.0
Autor	Realia Technologies S.L.
Fecha de publicación	24-12-2010

1.2 Resumen del TOE

1.2.1 Tipo de TOE

4 El TOE es una aplicación que se ejecuta sobre un sistema operativo securizado y que accede a los servicios criptográficos de un HSM, proporcionando servicios de carácter criptográfico a través de la red a los usuarios finales del mismo.

5 El objetivo del TOE es proporcionar servicios criptográficos de alto nivel a los usuarios finales, así como proteger y servir de interfaz para la configuración del HSM y del sistema operativo subyacente.

1.2.1.1 Características de seguridad lógicas

1.2.1.1.1 Invocación de servicios criptográficos

6 El TOE implementará funcionalidad de seguridad para la invocación de los servicios criptográficos de un HSM que cumpla con [FIPS1402] y

[FIPS-ANEXOS], y que proporcione 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].

7 Los algoritmos criptográficos que implementan las funciones de seguridad en el HSM 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 HSM deberá implementar al menos una función criptográfica aprobada usada en un modo de operación aprobado.

1.2.1.1.2 Interfaces del TOE

8 El TOE proporcionará un interfaz de comunicación con un driver que permita el acceso al HSM para solicitar operaciones criptográficas.

9 Además, el TOE proporciona un interfaz para realizar la configuración del propio TOE. Para este propósito es posible que se pueda utilizar el interfaz del TOE con el driver del HSM. Este interfaz deberá implementarse mediante un canal confiable

10 Por otro lado, existe otro interfaz de las aplicaciones con el sistema operativo subyacente que le proporciona los recursos necesarios a las aplicaciones.

1.2.1.1.3 Auditoría

11 El TOE proporciona la capacidad de detectar y registrar los eventos relevantes a la seguridad.

12 El entorno IT en el que opera el TOE deberá proporcionar una fuente de tiempo fiable.

1.2.2 Uso del TOE

13 El TOE se usa como una aplicación que proporciona servicios criptográficos de alto nivel a través de la red a otros usuarios o aplicaciones finales, utilizando además un driver que de acceso a un dispositivo HSM y que proporcione al TOE los servicios criptográficos a bajo nivel.

14 El TOE además proporciona interfaces de configuración a través de canales seguros, protegiendo la configuración del mismo y del HSM subyacente.

15 Algunos ejemplos de posibles TOEs serían:

(A) Autoridades de Certificación

(B) Autoridades de Registro

(C) Proxys de correo seguro

(D) Autoridades de Sellado Tiempo

(E) Servidores de firma

(F) Aplicaciones para la banca

(G) …

1.2.3 Hardware y software no incluido en el TOE

16 El hardware no estará incluido en el TOE.

17 El software correspondiente al sistema operativo sobre el que se ejecuta el TOE, no será considerado TOE. Tampoco se considera TOE el driver utilizado para la comunicación con el HSM.

18 El HSM con el que se comunica el TOE tampoco está incluido en el TOE.

2 Declaración de conformidad

2.1 Conformidad con respecto a la norma CC

19 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 EAL2 según [CC31p3].

20 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].

21 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

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

2.3 Declaraciones de conformidad con respecto a este PP

23 Este PP requiere que la conformidad al mismo se declare de manera estricta, tal como se define en la norma CC**¡Error! No se encuentra el origen de la referencia.**

3 Definición del problema de seguridad (SPD)

24 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

25 Se tienen en cuenta los siguientes activos:

Id	Descripción del Activo	Valor del activo
A.CONF_HSM	Datos de configuración del HSM. A través de las aplicaciones se pueden configurar parámetros del HSM. Estos parámetro serán protegidos por el TOE.	Confidencialidad Integridad
A.CONF_TOE	Datos de configuración del TOE.	Confidencialidad Integridad

3.2 Amenazas

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

Id	Descripción	Activos afectados
T.ACCESO_CONF_INTERFAZ_CONF	Comprometer confidencialidad o integridad de la configuración del TOE o del HSM subyacente mediante la rotura del canal de confianza entre el TOE y otras entidades externas que usan un interfaz de configuración. El agente es un **atacante no autorizado** a la organización con recursos y experiencia limitada. El potencial de ataque asociado al atacante es "**Basic**".	A.CONF_HSM (C) A.CONF_HSM (I) A.CONF_TOE (C) A.CONF_TOE (I)

3.3 Políticas de seguridad organizativas (OSPs)

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

Id	Descripción
P.HSM	El HSM utilizado deberá cumplir con [FIPS1402]. Además deberá de ser invocado a través de un driver de acceso a dispositivos HSM.
P.AUDIT	Se registrarán los eventos de seguridad del sistema.

3.4 Hipótesis

28 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.ACCESO_FISICO	Nadie tiene acceso al hardware sobre el que se ejecuta el TOE salvo los administradores del mismo.
H.ADMINISTRADORES	Los administradores del TOE serán confiables y no negligentes, y cuidarán de la seguridad y correcto funcionamiento del TOE
H.SISTEMA_OPERATIVO	El Sistema Operativo sobre el que se instala el TOE estará correctamente configurado, carecerá de vulnerabilidades explotables y sus usuarios serán confiables.
H.STM	El entorno proporciona una medida de tiempo fiable.

4 Objetivos de seguridad

29 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.CANAL_CONFIABLE_CONF	El TOE implementará un canal confiable para la configuración del mismo y del HSM.
O.DRIVER_HSM	Para proporcionar sus servicios, el TOE invocará a un driver del sistema operativo que se comunique con un HSM que cumpla con [FIPS1402] y que realice las operaciones criptográficas.
O.AUDITORIA	El TOE debe proporcionar la capacidad de detectar y registrar los eventos relevantes a la seguridad.

4.2 Objetivos de seguridad para el entorno operacional

Id	Descripción
OE.ACCESO_FISICO	Nadie tiene acceso al hardware sobre el que se ejecuta el TOE salvo los administradores del mismo.
OE.ADMINISTRADORES	Los administradores del TOE serán confiables y no negligentes, y cuidarán de la seguridad y correcto funcionamiento del TOE.
OE.HSM	El HSM utilizado deberá cumplir con [FIPS1402].
OE.SISTEMA_OPERATIVO	El Sistema Operativo sobre el que se instala el TOE estará correctamente configurado, carecerá de vulnerabilidades explotables y sus usuarios serán confiables.
OE.STM	El entorno proporcionará una medida de tiempo fiable que se utilizará en la generación de la información de la auditoría.

4.3 Justificación de los objetivos de seguridad

	T.ACCESO_CONF_INTERFAZ_CONF	P.HSM	P.AUDITORIA	H.ACCESO_FISICO	H.ADMINISTRADORES	H.SISTEMA_OPERATIVO	H.STM
O.CANAL_CONFIABLE_CONF	X						
O.DRIVER_HSM		X					
O.AUDITORIA			X				
OE.ACCESO_FISICO	X			X			
OE.ADMINISTRADORES					X		
OE.SISTEMA_OPERATIVO						X	
OE.STM							X
OE.HSM		X					

Correspondencia de los objetivos de seguridad

30 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.

31 La amenaza T.ACCESO_CONF_INTERFAZ_CONF, compromete la confidencialidad o integridad de la configuración del TOE y del HSM subyacente mediante la rotura del canal de confianza establecido entre el TOE y otras entidades externas que utilizan los interfaces de configuración del TOE. El objetivo de seguridad del TOE O.CANAL_CONFIABLE_CONF, requiere que el TOE establezca un canal de comunicación seguro entre el TOE y otras entidades externas que utilicen los interfaces de configuración del TOE. Además, el objetivo de seguridad del entorno OE.ACCESO_FISICO mitiga los ataques que se puedan realizar accediendo físicamente al TOE, por lo que ambos objetivos conjuntamente contrarrestan las amenazas

32 La política P.HSM especifica que el HSM utilizado deberá cumplir con [FIPS1402]. Esto se asegura directamente mediante el objetivo de

seguridad del entorno OE.HSM y el objetivo de seguridad del TOE O.DRIVER_HSM.

33 La política P.AUDITORIA especifica que el TOE generará auditoría con los eventos relativos a la seguridad. Esto se asegura directamente mediante el objetivo de seguridad del TOE O.AUDITORIA.

34 La hipótesis H.ACCESO_FISICO supone que sólo los administradores tendrán acceso físico al TOE. Esta suposición es directamente cubierta por el objetivo del entorno OE.ACCESO_FISICO

35 La hipótesis H.ADMINISTRADORES supone que los administradores del TOE son confiables y no negligentes. Esta suposición es directamente cubierta por el objetivo del entorno OE.ADMINISTRADORES.

36 La hipótesis H.SISTEMA_OPERATIVO supone que el sistema operativo está bien configurado y carece de vulnerabilidades explotables. Esta suposición es directamente cubierta por el objetivo del entorno OE.SISTEMA_OPERATIVO.

37 La hipótesis H.STM supone que el entorno proporciona una fuente de tiempo confiable. Esta suposición es directamente cubierta por el objetivo del entorno OE.STM.

5 Definición de componentes extendidos

5.1 Definición del componente funcional FCS_COP.2

38 Se define el componente extendido FCS_COP.2 con el objeto de especificar los requisitos de invocación a las operaciones criptográficas que permitan definir el objetivo de seguridad del TOE O.DRIVER_HSM.

O.DRIVER_HSM	Para proporcionar sus servicios, el TOE invocará a un HSM que cumpla con [FIPS1402] y que realice las operaciones criptográficas.

39 Se utiliza la familia FCS_COP definida en [CC31p2] que proporciona el componente FCS_COP.1. El nuevo componente contempla la invocación a una entidad externa para la realización de operaciones criptográficas. Esta funcionalidad no se contempla con el requisito FCS_COP.1.

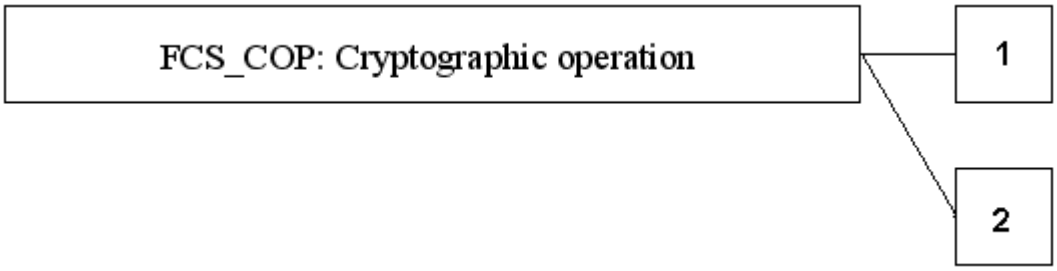
40 Family behaviour

41 In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. This family should be included whenever there are requirements for cryptographic operations to be performed.

42 Typical cryptographic operations include data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement.

43 Component 2 has been added as an extended component to fulfil the aforementioned TOE requirement.

44 Component Levelling



45 FCS_COP.1 Cryptographic operation, as specified in CC Part 2.

46 FCS_COP.2 Delegated cryptographic operation, requires a cryptographic operation to be performed by an entity external to the TOE, in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

47 Management: FCS_COP.1, FCS_COP.2

48 There are no management activities foreseen.

49 Audit: FCS_COP.1, FCS_COP.2

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

51 a) Minimal: Success and failure, and the type of cryptographic operation.

52 b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

FCS_COP.2 Delegated cryptographic operation

Dependencies: No dependencies

FCS_COP.2.1 The TSF shall invoke an external entity to 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: *list of standards*].

6 Requisitos de seguridad del TOE

6.1 Requisitos funcionales de seguridad

6.1.1 Operaciones criptográficas

53 FCS_COP.2 Delegated cryptographic operation

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

FCS_COP.2.1 The TSF shall invoke an external entity to 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: *[FIPS1402] y [FIPS1402-ANEXOS]*].

6.1.2 Canales confiables

54 FTP_ITC.1/INTERFAZ_CONF Inter-TSF trusted channel

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

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*assignment: list of functions for which a trusted channel is required*].

6.1.3 Auditoría de seguridad

55 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. [*assignment: other specifically defined auditable events*].

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*].

6.2 Requisitos de garantía de seguridad

56 Los requisitos de garantía que se incluyen a continuación se corresponden con el nivel de garantía definido EAL2, conforme a [CC31p3].

6.2.1 Declaración de seguridad (ASE)

57 **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.

58 **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.

59 **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.

60 **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.

61 **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.

62 **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.

63 **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)

64 **ADV_FSP.2 Security-enforcing functional specification**

Dependencies: ADV_TDS.1 Basic design

Developer action elements:
ADV_FSP.2.1D The developer shall provide a functional specification.
ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:
ADV_FSP.2.1C The functional specification shall completely represent the TSF.
ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.
ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

65 **ADV_TDS.1 Basic design**

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:
ADV_TDS.1.1D The developer shall provide the design of the TOE.
ADV_TDS.1.2D 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.1.1C The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2C The design shall identify all subsystems of the TSF.
ADV_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.
ADV_TDS.1.4C The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

66 **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.

6.2.3 Guías de usuario (AGD)

67 **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.

68 **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)

69 ALC_CMC.2 Use of a CM system

Dependencies:

ALC_CMS.1 TOE CM coverage

Developer action elements:
ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2D The developer shall provide the CM documentation.
ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:
ALC_CMC.2.1C The TOE shall be labelled with its unique reference.
ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

70 **ALC_CMS.2 Parts of the TOE CM coverage**

Dependencies: No dependencies.

Developer action elements:
ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:
ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

71 **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.

6.2.5 Pruebas (ATE)

72 **ATE_COV.1 Evidence of coverage**

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

Developer action elements:
ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:
ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

73 **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.

74 **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.

6.2.6 Análisis de vulnerabilidades (AVA)

75 **AVA_VAN.2 Vulnerability analysis**

Dependencies:

ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.1 Basic design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:
AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:
AVA_VAN.2.1C The TOE shall be suitable for testing.

6.3 Justificación de los requisitos de garantía de seguridad

6.3.1 Justificación de los requisitos de funcionalidad de seguridad

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

77 Así mismo 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

	O.CANAL_CONFIABLE_CONF	O.DRIVER_HSM	O.AUDITORIA
FTP_ITC.1/INTERFAZ_CONF	X		
FCS_COP.2		X	
FAU_GEN.1			X

78 El objetivo de seguridad del TOE O.CANAL_CONFIABLE_CONF, requiere que el TOE establezca un canal de comunicación seguro entre el TOE y otras entidades externas que utilicen los interfaces de configuración del

TOE. Este objetivo de seguridad se cumple mediante el requisito FTP_ITC.1/INTERFAZ_CONF que requiere que se establezca un canal seguro con otras entidades externas que utilicen los interfaces de configuración del TOE.

79 El objetivo de seguridad del TOE O.DRIVER_HSM, requiere que el TOE invoque a un driver del sistema operativo que se comunique con un HSM que cumpla con [FIPS1402] y que realice las operaciones criptográficas. Este objetivo de seguridad se cumple mediante el requisito FTP_COP.2 que requiere que el TOE invoque a un driver del sistema operativo que se comunique con un HSM que cumpla con [FIPS1402] y que realice las operaciones criptográficas.

80 El objetivo de seguridad del TOE O.AUDITORIA, requiere que el TOE sea capaz de detectar y registrar los eventos relevantes a la seguridad. Este objetivo de seguridad se cumple mediante el requisito FAU_GEN.1 que requiere que el TOE detecte y registre los eventos relativos a la seguridad.

6.3.2 Dependencias de los requisitos funcionales de seguridad

81 Este perfil de protección satisface todos los requisitos de dependencias de [CC31p2] excepto FPT_STM.1 que se deriva al entorno.

6.3.3 Justificación de los requisitos de garantía de seguridad

82 La garantía de seguridad deseada para este tipo de TOE es la proporcionada por el nivel de evaluación EAL2.

7 Acrónimos y definiciones

7.1 Acrónimos

83 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
OSPs	Organisational Security Policies
SPD	Security Problem Definition
SW	Software
PC	Personal Computer
TOE	Target of Evaluation
TSF	TOE Security Functionality

7.2 Definiciones

84 Ninguna.

8 Referencias

85 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

86 FIPS 140-2

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

[FIPS-ANEXOS] ANEXO Sec. A: Approved Security Functions
ANEXO Sec. C: Approved Random Number Generators
ANEXO Sec. D: Approved Key Establishment Techniques