REF: 2011-1-INF-653 v1
Difusión: Público
Fecha: 21.06.2011

Creado: CERT6
Revisado: TECNICO
Aprobado: JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2011-1
Datos del solicitante: B83158386 REALIA TECHNOLOGIES

Referencias: EXT-1120 Solicitud de Certificación del Perfil de Protección HSM Realia Technologies v2.0
EXT-1227 ETR de REAL-PP-HSM-ETR v2.0.
CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.

Informe de certificación del perfil de protección HSM de Realia Technologies, versión 2.0, según la solicitud de referencia [EXT-1120], de fecha 13-12-2011, y evaluado por el laboratorio Epoche & Espri, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-1227] de acuerdo a [CCRA], recibido el pasado 12-04-2011.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

INDICE

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen

Este documento constituye el Informe de Certificación para el expediente del perfil de protección HSM de Realia Technologies, versión 2.0.

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

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

Patrocinador: Realia Technologies.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: Epoche & Espri.

Nivel de Evaluación: EAL4.

Fortaleza de las Funciones: no aplica en CC v3.1

Fecha de término de la evaluación: 11-04-2011.

Todos los componentes de garantía requeridos por el nivel de evaluación APE (Evaluación de Perfiles de Protección) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Epoche & Espri asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador para APE, definidas por los Criterios Comunes v3.1 [CC-P3] y la Metodología de Evaluación v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del perfil de protección HSM de Realia Technologies, versión 2.0, se propone la resolución estimatoria de la misma.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen del OE

El objeto a Evaluar (OE), es un perfil de protección HSM de Realia Technologies, versión 2.0 que especifica los requisitos de seguridad para un modulo criptográfico del tipo HSM que implementa funciones criptográficas cuyo objetivo es la protección de la confidencialidad, integridad de la información procesada, almacenada y trasmitida (datos de usuario) de acuerdo con una política de seguridad.

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

Características de seguridad físicas

El OE se define desde el punto de vista físico, como un conjunto de HW con su correspondiente SW y/o FW, que implementa funciones criptográficas y está contenido dentro de unos límites criptográficos definidos. El OE es un HSM en cualquier forma o configuración, formado un por único chip o por múltiples chips ensamblados en una placa.

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

Características de seguridad lógicas

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

1. Creación de firma digital, para dar soporte a servicios de autenticación en origen, integridad de datos y no repudio;

2. Verificación de firma digital, para detectar modificaciones de en datos firmados, como prueba de origen;

3. Cifrado, para proteger la confidencialidad de la información;

4. Descifrado, para dar soporte a la protección de la confidencialidad de la información;

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

5. Generación de resúmenes para su uso como algoritmo subyacente en otros procesos, o para control de integridad.

6. Generación de números aleatorios necesarios en otros procesos criptográficos (RNG).

7. Generación de claves usadas en las funciones criptográficas usando un RNG aprobado según [FIPS-ANEXOS].

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

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

Protección del material criptográfico

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

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación APE (Evaluación de Perfiles de Protección), según la parte 3 de CC v3.1 R3.

APE_INT.1 PP Introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

Los productos para los que es aplicable este perfil de protección se espera que cumplan con los requisitos de garantía de seguridad correspondientes al nivel EAL4 de CC v3.1 R3.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los requisitos funcionales, según la parte 2 de CC v3.1 R3, siguientes:

FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_CKM.5	Cryptographic key entry
FCS_COP.1	Cryptographic operation
FCS_RNG.1	Random Number Generation
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication
FIA_UAU.6	Re-authenticating
FIA_UAU.7	Protected authentication feedback
FIA_AFL.1	Authentication failure handling
FIA_USB.1	User-subject binding
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_ITC.2	Import of user data with security attributes
FDP_ETC.1	Export of user data without security attributes
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_PHP.3	Resistance to physical attack
FPT_FLS.1	Failure with preservation of secure state
FPT_TST.2	TST Self Testing
FPT_STM.1	Reliable time stamps
FPT_SEP.1	Interfaces Separation
FPT_FSM.1	Finite State Model

Donde son componentes extendidos a la parte 3 de CC v3.1 R3 los siguientes:

FCS_RNG.1	Random Number Generation

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

FCS_CKM.5	Cryptographic key entry
FPT_TST.2	TSF self test
FPT_SEP.1	Interfaces Separation
FPT_FSM.1	Finite State Model

Identificación

Perfil de Protección: Perfil de Protección HSM Realia Technologies S.L. v2.0.

Nivel de Evaluación: CC v3.1 R3 EAL4

Fortaleza de las Funciones: no aplica en CC v3.1.

Política de seguridad

El uso del perfil de protección, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de las políticas se encuentra en la declaración de seguridad. En síntesis, se establece la necesidad de implementar políticas organizativas relativas a:

Política 01: P.FUN_APROBADAS

Las funciones de seguridad del módulo (OE) deberán estar aprobadas en FIPS o recomendadas por el NIST, por lo que deberán estar incluidas en los anexos correspondientes [FIPS-ANEXOS] de [FIPS1402]. El módulo criptográfico (OE) deberá implementar al menos una función de seguridad aprobada usada en un modo de operación aprobado.

Política 02: P.IA

Todos los usuarios deberán identificarse y autenticarse frente al OE antes de permitirse cualquier acción (excepto self-tests) presentando sus credenciales que serán de tipo individual y no por grupos de usuarios.

Política 03: P.ROLES

Se separará y se distinguirá al menos entre los siguientes roles: usuarios y crypto-officer. En el caso de que se permita que operadores realicen labores de mantenimiento del módulo (OE), se deberá incluir un rol a tal efecto. Antes de identificarse, los usuarios tendrán el rol de usuario no identificado. Los roles deberán ser asignados a personas diferentes de la organización.

Política 04: P.INTERFACES

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Se proporcionarán los siguientes tipos de interfaces o puertos (I/P):

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

Política 05: P.SERVICIOS

Se proporcionarán al menos los siguientes servicios: mostrar el estado del OE, realizar auto-testing y ejecutar las funciones de seguridad (aprobadas por FIPS o recomendadas por NIST según [FIPS-ANEXOS]).

Política 06: P.AUDIT

Se registrarán los eventos de seguridad del sistema de forma que se pueda asociar a los usuarios del OE con sus acciones.

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

Hipótesis y entorno de uso

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la declaración de seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas.

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

Hipótesis 01: H.GENERACIÓN_CLAVES

Las claves generadas por el entorno e importadas dentro del OE deberán cumplir los mismos requisitos que se exigen al material criptográfico generado internamente por el OE.

Hipótesis 02: H.DISPONIBILIDAD

El entorno (el sistema que usa el OE), asegura la disponibilidad del material criptográfico necesario que depende de él.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para los productos que sean conformes con este perfil de protección, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a “Basic” de EAL4, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Amenazas cubiertas:

Amenaza 01: T.CSP_CONF

Comprometer confidencialidad de parámetros críticos de seguridad (CSP). El atacante puede tener acceso físico al OE o bien realizar el ataque en remoto tomando el control del sistema que interacciona con el OE.

El agente es un atacante no autorizado a la organización con recursos y experiencia limitada. El potencial de ataque asociado al atacante es “Enhanced basic”.

Este ataque permitiría en segundo orden comprometer los datos de usuarios protegidos.

Amenaza 02: T.CSP_INTEG

Comprometer integridad o autenticidad de parámetros críticos de seguridad (CSP) o funciones de seguridad. El atacante puede tener acceso físico al OE o bien realizar el ataque en remoto tomando el control del sistema que interacciona con el OE.

El agente es un atacante no autorizado a la organización con recursos y experiencia. El potencial de ataque asociado al atacante es “Enhanced basic”.

Este ataque permitiría en segundo orden comprometer los datos de usuarios protegidos.

Amenaza 03: T.ABUSO

Abuso de las funciones de instalación, configuración o mantenimiento del OE. El atacante podría usar estas funciones para revelar o manipular CSPs operacionales o datos de usuario o para posibilitar ataques sobre la integridad o confidencialidad de CSPs operacionales o datos de usuario mediante la manipulación (exploración,

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

bypass, cambio o desactivación) de mecanismos de seguridad o revelando o manipulando datos de la TSF.

El agente es un atacante interno a la organización con recursos y experiencia limitada. El potencial de ataque asociado al atacante es “Enhanced basic”.

Amenaza 04: T.PHY_TAMPER

Modificación de las medidas de seguridad físicas de forma que el atacante pueda acceder a los CSPs y/o datos de usuarios almacenados y comprometer su confidencialidad o integridad.

El agente es un atacante no autorizado con acceso físico al OE con recursos y experiencia limitada. El potencial de ataque asociado al atacante es “Enhanced basic”.

Amenaza 05: T.SUPLANTAR

El atacante se hace pasar por una fuente de datos autorizada o receptor autorizado para realizar operaciones de usuarios autorizado o acceder al OE sin ser detectado comprometiendo la integridad y confidencialidad de los activos.

El agente es un atacante no autorizado con recursos y experiencia limitada. El potencial de ataque asociado al atacante es “Enhanced basic”.

Funcionalidad del entorno.

El producto que cumpla con el perfil de protección requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del producto son los siguientes:

Objetivo entorno 01: OE.GENERACIÓN_CLAVES

Las claves generadas por el entorno e importadas dentro del OE deberán cumplir los mismos requisitos que se exigen al material criptográfico generado internamente por el OE.

Objetivo entorno 02: OE.DISPONIBILIDAD

El entorno (el sistema que usa el OE), deberá asegurar la disponibilidad del material criptográfico necesario que depende de él.

Objetivo entorno 03: OE.PERSONAL

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

El entorno del OE deberá asegurar que el rol de administrador (Crypto-officer), el rol de usuario y, en caso de existir, el rol de mantenimiento, deberán ser asignados a personas diferentes de la organización.

El entorno del OE deberá asegurar que los administradores del OE (Crypto-officer, rol de mantenimiento) son confiables y cuidan de la seguridad y correcto funcionamiento del OE.

Objetivo entorno 04: OE.AUDITORÍA

El entorno del OE deberá revisar los registros de auditoría generados por el OE para detectar posibles violaciones, pudiéndose asociar las acciones a los usuarios del OE.

El administrador (crypto-officer) es responsable de configurar la auditoría.

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad), o de los requisitos de seguridad del OE se encuentran en la correspondiente Declaración de Seguridad.

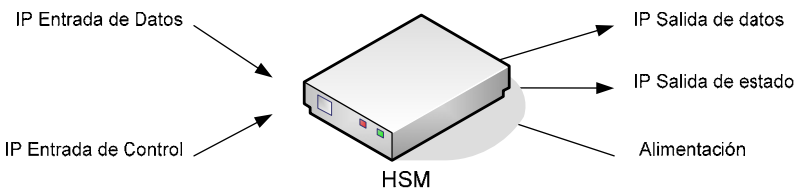
Arquitectura

Arquitectura Lógica:

El objeto de evaluación que cumpla con el perfil de protección, podría contener los siguientes módulos:

- Auditoría
- Identificación
- Criptografía
- Generación de Números Aleatorios
- Auto test
- Verificación de ataques

Arquitectura Física:



Documentos

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

El perfil de protección sólo consta de un documento que se indica a continuación.

Perfil de Protección HSM Realia Technologies S.L. Versión 2.0.

Pruebas del producto

No aplica

Configuración evaluada

No aplica

Resultados de la Evaluación

El perfil de protección ha sido evaluado frente al "Perfil de Protección HSM Realia Technologies S.L.", v2.0 de 11 de abril de 2011.

Todos los componentes de garantía requeridos por el nivel de evaluación APE (Evaluación de Perfiles de Protección) presentan el veredicto de "PASA". Por consiguiente, el laboratorio Epoch & Espri asigna el VEREDICTO de "PASA" a toda la evaluación por satisfacer todas las acciones del evaluador definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 R3.

Recomendaciones y comentarios de los evaluadores

No hay recomendaciones adicionales por parte de los evaluadores.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del perfil de protección "Perfil de Protección HSM Realia Technologies S.L.", versión 2.0, se propone la resolución estimatoria de la misma.

El perfil certificado ha sido desarrollado por la empresa Realia Technologies S.L. para ser utilizado en futuras certificaciones de sus productos. Este perfil de protección no se puede considerar una recomendación o exigencia del Centro Criptológico Nacional para los productos del tipo HSM.

Glosario de términos

CCN Centro Criptológico Nacional

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

CNI	Centro Nacional de Inteligencia
CSP	Parámetros Críticos de Seguridad
ETR	Evaluation Technical Report
OC	Organismo de Certificación
OE	Objeto de Evaluación
PP	Perfil de Protección

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Bibliografía

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, R3, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, R3, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, R3, July 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, R3, July 2009.

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

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

ANEXO A: Approved Security Functions
ANEXO C: Approved Random Number Generators
ANEXO D: Approved Key Establishment Techniques

Perfil de Protección

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación del perfil de protección completo de "Perfil de Protección HSM Realia Technologies S.L.", versión 2.0 de 11 de abril de 2011.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es