REF:	2011-3-INF-664 v1	Creado:	CERT6
Difusión:	Público	Revisado:	TECNICO
Fecha:	21.06.2011	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2011-3
Datos del solicitante: B83158386 REALIA TECHNOLOGIES

Referencias:	EXT-1124	Solicitud de Certificación del perfil de protección Servicios en Red de Realia Technologies.
	EXT-1231	ETR del perfil de protección Servicios en Red de Realia Technologies. 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 Servicios en Red de Realia Technologies, versión 2.0, según la solicitud de referencia [EXT-1124], de fecha 13-12-2011, y evaluado por el laboratorio Epoche & Espri, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-1231] 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 Servicios en Red de Realia Technologies, versión 2.0.

El OE descrito en el PP 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.

Patrocinador: Realia Technologies.

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

Laboratorio de Evaluación: Epoche & Espri.

Nivel de Evaluación: EAL2.

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 Servicios en Red 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 Servicios en Red de Realia Technologies, versión 2.0 que especifica los requisitos de seguridad de 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.

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.

Características de seguridad lógicas

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].

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.

Uso del TOE

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

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

driver que de acceso a un dispositivo HSM y que proporcione al TOE los servicios criptográficos a bajo nivel.

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

Hardware y software no incluido en el OE

El Hardware no estará incluido en el OE.

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.

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

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 EAL2 de CC v3.1 R3.

Requisitos funcionales de seguridad

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

FTP_ITC.1	Inter-TSF trusted channel
FCS_COP.2	Delegated cryptographic operation
FAU_GEN.1	Audit data generation

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

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

FCS_COP.2 Delegated cryptographic operation

Identificación

Perfil de Protección: Perfil de protección Servicios en Red Realia Technologies S.L. v2.0.

Nivel de Evaluación: CC v3.1 R3 EAL2

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.HSM

El HSM utilizado deberá cumplir con [FIPS1402]. Además deberá de ser invocado a través de un driver de acceso a dispositivos HSM.

Política 02: P.AUDIT

Se registrarán los eventos de seguridad del sistema.

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.

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

Hipótesis 01: H.ACCESO_FISICO

Nadie tiene acceso al hardware sobre el que se ejecuta el TOE salvo los administradores del mismo.

Hipótesis 02: H. ADMINISTRADORES

Los administradores del TOE serán confiables y no negligentes, y cuidarán de la seguridad y correcto funcionamiento del TOE.

Hipótesis 03: 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.

Hipótesis 04: H.STM

El entorno proporciona una medida fiable de tiempo.

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 EAL2, 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.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”.

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

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.ACCESO_FISICO

Nadie tiene acceso al hardware sobre el que se ejecuta el TOE salvo los administradores del mismo.

Objetivo entorno 02: OE. ADMINISTRADORES

Los administradores del TOE serán confiables y no negligentes, y cuidarán de la seguridad y correcto funcionamiento del TOE.

Objetivo entorno 03: OE. HSM

El HSM utilizado deberá cumplir con [FIPS1402].

Objetivo entorno 04: 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.

Objetivo entorno 05: OE.STM

El entorno proporcionará una medida de tiempo fiable que se utilizará en la generación de la información de 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 TOE proporcionará un interfaz de comunicación con un driver que permita el acceso al HSM para solicitar operaciones criptográficas.

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

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

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

Arquitectura Física:

No Aplica

Documentos

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

Perfil de protección Servicios en Red 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 Servicios en Red 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.

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

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 Servicios en Red 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.

Glosario de términos

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
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 Servicios en Red 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