REF:	2011-2-INF-663 v1	Creado:	CERT6
Difusión:	Público	Revisado:	TECNICO
Fecha:	21.06.2011	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2011-2
Datos del solicitante: B83158386 REALIA TECHNOLOGIES

Referencias:	EXT-1122	Solicitud de Certificación del perfil de protección Appliance de Realia Technologies, versión 2.1
	EXT-1230	ETR del perfil de protección Appliance 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 Appliance de Realia Technologies, versión 2.1, según la solicitud de referencia [EXT-1122], de fecha 13-12-2011, y evaluado por el laboratorio Epoche & Espri, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-1230] 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 Appliance de Realia Technologies, versión 2.1.

El OE descrito en el PP es un sistema operativo personalizado y configurado de manera segura; de modo que las aplicaciones que son ejecutadas en el appliance pueden confiar en él.

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 Appliance de Realia Technologies, versión 2.1, 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 Appliance de Realia Technologies, versión 2.1 que especifica los requisitos de seguridad de un sistema operativo personalizado y configurado de manera segura; de modo que las aplicaciones que son ejecutadas en el appliance pueden confiar en él.

El OE es un sistema operativo multiusuario y multitarea basado en Linux. El OE puede proveer servicios a varios usuarios a la vez. Después de realizar la autenticación, los usuarios tienen acceso a un entorno que permite arrancar aplicaciones, ejecutar comandos o crear y acceder a ficheros.

El OE proporciona mecanismos adecuados para separar a los usuarios y proteger sus datos.

Los comandos con privilegios están restringidos a los usuarios con rol superusuario.

El acceso al OE se realizará de manera local, puesto que la personalización y configuración del OE cierra los accesos remotos al mismo.

El OE está compuesto únicamente por software, por lo tanto sólo se tendrá en cuenta el OE desde el punto de vista lógico.

Características de seguridad lógicas

El OE permite la configuración de los parámetros de seguridad. Mediante este mecanismo, se obtiene un sistema operativo personalizado y configurado de manera segura que se puede considerar una plataforma segura para que se ejecuten diferentes aplicaciones.

El OE proporciona un interfaz a través de la consola local, que permite la configuración y personalización del sistema operativo. Existe otro interfaz entre el sistema operativo y el HSM, a través de un driver que se encarga de abstraer el hardware del HSM a las aplicaciones que harán uso de él.

El OE soportará los siguientes roles: usuario y superusuario. Los usuarios tendrán acceso a la información almacenada en el OE dependiendo del rol que posean. El OE implementará un mecanismo de autenticación basado en la identidad de los usuarios que garantizará la confidencialidad e integridad de la información almacenada en el OE.

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

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

Hardware y software no incluido en el OE

El Hardware no estará incluido en el OE.

El software correspondiente a las aplicaciones que se ejecutan en el OE, no será considerado OE. Por tanto, todas las aplicaciones que no formen parte del CORE del OE, no estarán incluidas en el OE.

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:

FAU_GEN.1	Audit data generation
FMT_SMR.1	Security roles
FMT_SMF.1	Specification of Management Functions
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FDP_ACF.1	Security attribute based access control
FDP_ACC.2	Complete access control
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action

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

Identificación

Perfil de Protección: Perfil de Protección Appliance Realia Technologies S.L. v2.1.

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.ROLES

Se separará y se distinguirá entre los siguientes roles: usuario y superusuario.

Política 02: P.AUDIT

Se registrarán los eventos de seguridad del sistema.

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.

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.ACCESO_FISICO

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

Los atacantes no disponen de acceso físico al OE, es decir el entorno operacional será lo suficientemente seguro para que el atacante no pueda realizar ataques al hardware donde se está ejecutando el OE.

Hipótesis 02: H.APLICACIONES_SEGURAS

Las aplicaciones que se ejecutarán en el appliance serán seguras y no comprometerán la seguridad del OE.

Hipótesis 03: 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. ACCESS

Un atacante (no usuario del OE) puede ganar acceso a recursos o realizar operaciones para las cuales no tiene los permisos necesarios.

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

Amenaza 02: T.PERMISOS

Un usuario del OE puede ganar acceso a recursos o realizar operaciones para las cuales no tiene los permisos necesarios.

El agente es un usuario autorizado en el OE con el rol de usuario. El potencial de ataque asociado al atacante es “Basic”.

Amenaza 03: T. BAD_ADMIN

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

Los activos del OE pueden comprometerse debido a una administración incorrecta del OE.

El agente es un usuario autorizado en el OE con el rol de superusuario. El potencial de ataque asociado al atacante es “Basic”.

Amenaza 04: T. ASSIGN_ROLES

La asignación no coherente de los roles a los usuarios puede provocar un acceso incorrecto a los recursos del OE.

El agente es un usuario autorizado en el OE con el rol de superusuario que actúa de manera negligente en la asignación de los roles. El potencial de ataque asociado al atacante es “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.ACCESO_FISICO

Los atacantes no disponen de acceso físico al OE, es decir el entorno operacional será lo suficientemente seguro para que el atacante no pueda realizar ataques al hardware donde se está ejecutando el OE.

Objetivo entorno 02: OE.ASSIGN_ROLES

Los administradores del OE asignarán los roles a los usuarios de manera coherente permitiéndole realizar únicamente las operaciones para las que fueron autorizado.

Objetivo entorno 03: OE.ADMINISTRADORES

Los administradores del OE recibirán la formación necesaria para evitar que los activos del OE se puedan ver comprometidos. Además, los administradores del OE serán confiables y cuidarán de la seguridad y correcto funcionamiento del OE.

Objetivo entorno 04: OE.APLICACIONES_SEGURAS

Los administradores del OE recibirán la formación necesaria para evitar que los activos del OE se puedan ver comprometidos. Además, los administradores del OE serán confiables y cuidarán de la seguridad y correcto funcionamiento 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

Objetivo entorno 05: OE.AUDITORÍA

El entorno del OE deberá revisar los registros de auditoría generados por el OE para detectar posibles violaciones.

Objetivo entorno 06: OE.STM

El entorno proporcionará una medida de tiempo 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 objeto de evaluación que cumpla con el perfil de protección, podría contener los siguientes módulos:

Auditoría
Identificación
Control de Acceso

Arquitectura Física:

No Aplica

Documentos

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

Perfil de Protección Appliance Realia Technologies S.L. Versión 2.1.

Pruebas del producto

No aplica

Configuración evaluada

No aplica

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

Resultados de la Evaluación

El perfil de protección ha sido evaluado frente al "Perfil de Protección Appliance Realia Technologies S.L.", v2.1 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 Appliance Realia Technologies S.L.", versión 2.1, 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 sistemas operativos personalizados.

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 Appliance Realia Technologies S.L.", versión 2.1 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