REF:	2009-2-INF-541 v1	Creado:	CERT3
Difusión:	Expediente	Revisado:	TECNICO
Fecha:	25.08.2010	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2009-2 CRYPTOSEC + FIRMWARE PKCS#11-v1.0
Datos del solicitante: B83158286 REALIA TECHNOLOGIES

Referencias:
- [EXT-709]. Solicitud de Certificación de CRYPTOSEC + FIRMWARE PKCS#11 V1.0.
- [EXT-1090]. Informe Técnico de Evaluación, M3.
- [CCRA]. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.

Informe de certificación del producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0, según la solicitud de referencia [EXT-709], de fecha 11 de febrero de 2009, y evaluado por el laboratorio LGAI Technological Center S.A-APPLUS., conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-1090] de acuerdo a [CCRA], recibido el pasado 4 de agosto de 2010.

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

ÍNDICE

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 de la certificación del producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0.

El TOE es un HSM genérico que proporciona los servicios criptográficos para la implementación de un subconjunto de la API PKCS#11.

El uso esperado del TOE es como módulo de seguridad para un sistema que requiera realizar operaciones criptográficas. El TOE se usará como módulo del sistema que necesite realizar operaciones criptográficas sin que las claves criptográficas sean transferidas sin proteger desde el TOE a este sistema.

Este sistema generalmente será un ordenador tipo PC con un sistema operativo de propósito general con una aplicación de control del TOE.

Fabricante: Realia Technologies S.L.

Patrocinador: Realia Technologies S.L.

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

Laboratorio de Evaluación: LGAI Technological Center S.A-APPLUS.

Perfil de Protección: Ninguno.

Nivel de Evaluación: EAL4+ (ALC_FLR.1).

Fecha de término de la evaluación: 21.06.2010.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4+ (aumentado con ALC_FLR.1) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio LGAI-APPLUS asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4+(ALC_FLR.1), definidas por los Criterios Comunes, v3.1 [CC-P3], y por la Metodología de Evaluación, v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0, 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 TOE

El TOE es un módulo de seguridad por hardware HSM, actualmente certificado bajo la norma FIPS-140-2. Proporciona los servicios criptográficos para la implementación de un subconjunto de la API 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.

El TOE está compuesto de elementos software y hardware.

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 RS-232, para la comunicación en fases de personalización, configuración e impresiones de sobres ciegos. El protocolo de comunicación a usar es ECMA-48.
- Interfaz PCI 2.2 con velocidad de bus a 50-60 MHz, para la comunicación con la aplicación de control en fase de producción.

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 numeros aleatorios que será usada en la generación de claves DES y RSA.

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL4, más las requeridas para el componente adicional, ALC_FLR.1, según la parte 3 de CC v3.1, r2.

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

Se enumeran, a continuación, los componentes de garantía satisfechos en esta evaluación:

ASE_CCL.1	ADV_TDS.3
ASE_ECD.1	AGD_OPE.1
ASE_INT.1	AGD_PRE.1
ASE_OBJ.2	ALC_DVS.1
ASE_REQ.2	ALC_LCD.1
ASE_SPD.1	ALC_TAT.1
ALC_CMC.4	ATE_COV.2
ALC_CMS.4	ATE_DPT.2
ALC_DEL.1	ATE_FUN.1
ADV_ARC.1	ATE_IND.2
ADV_FSP.4	AVA_VAN.3
ADV_IMP.1	ALC_FLR

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los requisitos funcionales, según la Parte 2 de CC v3.1 r2 [CC-P2], siguientes:

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

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

Asimismo, la funcionalidad de seguridad del producto también satisface los siguientes componentes funcionales extendidos, definidos expresamente en la Declaración de Seguridad:

FCS_RND.1 FPT_EMSEC.1

Identificación

Producto: CRYPTOSEC + FIRMWARE PKCS#11-v1.0.

Declaración de Seguridad: Declaración de Seguridad de CRYPTOSEC + FIRMWARE PKCS#11-v1.0; versión 1.0, de 21 de junio de 2010.

Perfil de Protección: ninguno.

Nivel de Evaluación: CC v3.1 r2 – EAL4+ (ALC_FLR.1).

Política de seguridad

Para el uso seguro del producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0, se deben aplicar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de estas políticas se encuentra en la Declaración de Seguridad. En síntesis, se establece la necesidad de implementar políticas organizativas relativas a los siguientes aspectos:

Operaciones criptográficas (P.CRYPTOOPERATIONS)

El TOE debe realizar correctamente las siguientes operaciones criptográficas:

- Cifrado y descifrado DES con longitudes de clave doble y triple.

- Cifrado, descifrado, _rma y veri_cación de _rma RSA en formato PKCS.

- Cálculo del resultado de las funciones de hash SHA-1 y MD5.

- Generación de números aleatorios RNG.

Gestión de claves (P.KEYMANAGEMENT)

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.

Administración del TOE (P.MANAGEMENT)

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.

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

Uso correcto de las funciones HASH (P.GOODHASHES)

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.

Uso correcto de operaciones criptográficas (P.STRONGCRYPTO)

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.

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 TOE, 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 TOE.

Usuarios competentes (A.HUMAN)

Los usuarios del TOE que realizan operaciones de administración y los custodios serán confiables.

Ubicación segura en estado de producción (A.PHYSPROT)

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

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para el producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a “Enhanced-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.

Revelación de clave criptográfica (T.KEYLEAK)

Un atacante recupera una clave criptográfica protegida por los mecanismos de seguridad del TOE.

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 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:

Personal confiable (OE.HUMAN)

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

Ubicación segura en estado de producción (OE.PHYSPROT)

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

Usos seguros de las funciones de hash (OE.GOODHASHES)

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.

Uso correcto de operaciones criptográficas (OE.STRONGCRYPTO)

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.

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

Arquitectura

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

- Hardware: Cryptosec versión 1.0.

- Firmware: Firmware PKCS#11 versión 01.00.0308.

Arquitectura Lógica

El TOE cuenta con:

- un procesador, que realiza las operaciones criptográficas,

- una controladora para el bus PCI,

- un reloj (RTC),

- una memoria para almacenar datos/claves/configuración,

- y una controladora para el puerto serie.

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

Arquitectura Física

Los límites físicos del TOE son la superficie de la tarjeta PCI , protegida por una carcasa metálica (antitampering) que protege su interior.

Y dispone de dos interfaces:

- Un conector contra bus PCI 2.2 para la comunicación con el host.

- Una interfaz RS-232 para su gestión y para la impresión de claves de custodio.

Documentos

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- Declaración de Seguridad de CRYPTOSEC + FIRMWARE PKCS#11-v1.0; versión 1.0, de 21 de junio de 2010.

- Guías de CRYPTOSEC + FIRMWARE PKCS#11-v1.0, versión 1.3 que, a su vez, incluye:

  1) Preparación segura de CRYPTOSEC + FIRMWARE PKCS#11-v1.0, versión 1.3.

  2) Manual de operación de CRYPTOSEC + FIRMWARE PKCS#11-v1.0, versión 1.3.

Pruebas del producto

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante en sus instalaciones con resultado satisfactorio. El proceso de evaluación ha verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea verificar. Todas las pruebas se han realizado sobre un mismo escenario de pruebas acorde a la arquitectura identificada en la Declaración de Seguridad. Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Para verificar los resultados de las pruebas del fabricante, el laboratorio ha repetido todas las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación.

Adicionalmente, el laboratorio ha desarrollado su propia batería de pruebas, verificando que los resultados así obtenidos son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados y, en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no representaba un problema para la seguridad, ni suponía una merma en la capacidad funcional del producto.

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

Configuración evaluada

El producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0 ha sido evaluado en base a la siguiente configuración:

- Hardware: Cryptosec versión 1.0.

- Firmware: Firmware PKCS#11, versión 01.00.0308.

Entre las posibles opciones de configuración de seguridad que ofrece el firmware (Modo FIPS, Modo NO-FIPS), la única configuración evaluada es:

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

Resultados de la Evaluación

El producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0 ha sido evaluado frente a la declaración de seguridad “Declaración de Seguridad de CRYPTOSEC + FIRMWARE PKCS#11-v1.0; versión 1.0”, de 21 de junio de 2010.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4+ (aumentado con ALC_FLR.1) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio LGAI-APPLUS asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4+ (ALC_FLR.1), definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 r2.

Recomendaciones y comentarios de los evaluadores

A continuación se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

Para un uso seguro del producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0 habrá que aplicar las políticas organizativas y satisfacer las hipótesis incluidas en la Declaración de Seguridad, con especial atención a las siguientes:

- P.STRONGCRYPTO, que establece una restricción en la longitud de las claves utilizadas en las operaciones criptográficas de RSA y DES.

- A.PHYSPROT, que proporciona la cobertura frente a ataques físicos en el entorno de uso del producto.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto CRYPTOSEC + FIRMWARE PKCS#11-v1.0, 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

Glosario de términos

CC	Common Criteria
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
RTC	Real Time Clock
TOE	Target Of Evaluation

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, r1.

- [CC-P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, r2.

- [CC-P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, r2.

- [CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1, r2.

- [Attack Potential] Application of Attack Potential to Smartcards and similar devices.

- [AIS20] Functionality classes and evaluation methodology for deterministic random number generators.

- [Security Boxes] Análisis de Vulnerabilidades de TOEs Hardware con ``Caja de Seguridad´´.

Declaración de seguridad

Conjuntamente con este Informe de Certificación, se dispone en el Organismo de Certificación de la declaración de seguridad completa de la evaluación: Declaración de Seguridad de CRYPTOSEC + FIRMWARE PKCS#11-v1.0; versión 1.0, de 21 de junio de 2010.

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