REF:	2010-4-INF-508 v1	Creado:	CERT8
Difusión:	Público	Revisado:	TECNICO
Fecha:	24.08.2010	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente:2010-4 SIAVAL Módulo Crypto
Datos del solicitante: A82733262 Sistemas Informáticos Abiertos

Referencias: EXT-997 Solicitud de Certificación
EXT-1026 ETR Final
CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.

Informe de certificación del producto eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1, según la solicitud de referencia [EXT-997], de fecha 11 de mayo de 2010, y evaluado por el laboratorio Epoche & Espri, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-1026] de acuerdo a [CCRA], recibido el pasado 16 de julio 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

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 de la certificación del producto eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1.

El TOE es parte del producto eAS/Trusted Signatura Platform v6.2.1. El TOE está compuesto por el módulo Crypto, que ofrece las operaciones funcionales de firma electrónica, cifrado/descifrado de datos y validación de certificados, el API de integración que facilita las llamadas a los servicios web que ofrece el módulo Crypto y los ficheros de configuración que previamente deberán haber sido establecidos por un módulo de administración externo al TOE.

Fabricante: Sistemas Informáticos Abiertos, S.A.

Patrocinador: Sistemas Informáticos Abiertos, S.A.

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

Laboratorio de Evaluación: Epoche & Espri.

Perfil de Protección: Ninguno.

Nivel de Evaluación: EAL1+ALC_FLR.1

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

Fecha de término de la evaluación: 16 de julio de 2010.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 (aumentado con ALC_FLR.1) 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, a nivel EAL1, 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 producto eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto, 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 subconjunto de elementos que forman parte del producto **eAS/Trusted Signature Platform v6.2.1**, también conocido como **SIAVAL**. El producto completo es una Plataforma de Firma y Custodia que permite tanto la generación como la validación de firma electrónica, utilizando diferentes formatos como XMLDSig, XAdES 1.2.2, CAdES 1.7.3, PKCS#7 y PDF, así como la Custodia de Documentos (firmados o no), custodia de firmas y almacenamiento simple.

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, más las requeridas para el componente adicional, ALC_FLR.1, según la parte 3 de CC v3.1 r3.

ASE_INT.1	ST Introduction
ASE_CCL.1	Conformance claims
ASE_OBJ.1	Security objectives for the operational environment
ASE_ECD.1	Extended components definition
ASE_REQ.1	Stated security requirements
ASE_TSS.1	TOE summary specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labelling of the TOE
ALC_CMS.1	Parts of the TOE CM coverage
ALC_FLR.1	Basic Flaw Remediation
ADV_FSP.1	Basic functional specification
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los requisitos funcionales, según la parte 2 de CC v3.1 r3, siguientes:

FCS_COP.1	Cryptographic Operation
FCS_CKM.1	Cryptographic Key Generation

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

FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security Attribute Based Access Control
FIA_UID.2	User Identification Before Any Action
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.5	Multiple Authentication Mechanisms
FAU_GEN.1	Audit Data Generation
FPT_CII.1	Basic Confidentiality and Integrity of Imported Data (extendido)

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

Identificación

Producto: eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1

Declaración de Seguridad: eAS/Trusted Signatura Platform (SIAVAL): Módulo Crypto v6.2.1 - Declaración de Seguridad v1.6, junio 2010

Perfil de Protección: Ninguno.

Nivel de Evaluación: CC v3.1 r3 EAL1+ (ALC_FLR.1).

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

Problema de seguridad

Al tratarse de una Declaración de Seguridad de baja garantía (Low Assurance Security Target) no es necesario describir la definición del problema de seguridad. Únicamente se mantiene la descripción de los objetivos del entorno operacional.

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:

Objetivo entorno 01: Acceso restringido

El TOE estará instalado en un servidor físico y en un servidor de aplicaciones ubicados en un entorno seguro y controlado por administradores de confianza los cuales serán los encargados de gestionar el acceso físico al TOE, tanto a sus ficheros de configuración como a los ficheros ejecutables del TOE.

Objetivo entorno 02: Comunicaciones seguras

Las comunicaciones que se establecen a los servicios del TOE deben siempre realizarse a través de mecanismos seguros. La conexión desde los clientes al TOE deberá realizarse a través de una conexión http sobre SSL; de esta manera las aplicaciones clientes se aseguran que se conectan a un servidor seguro, puesto que deberán confiar en el certificado correspondiente del servidor.

Objetivo entorno 03: Datos de autenticación

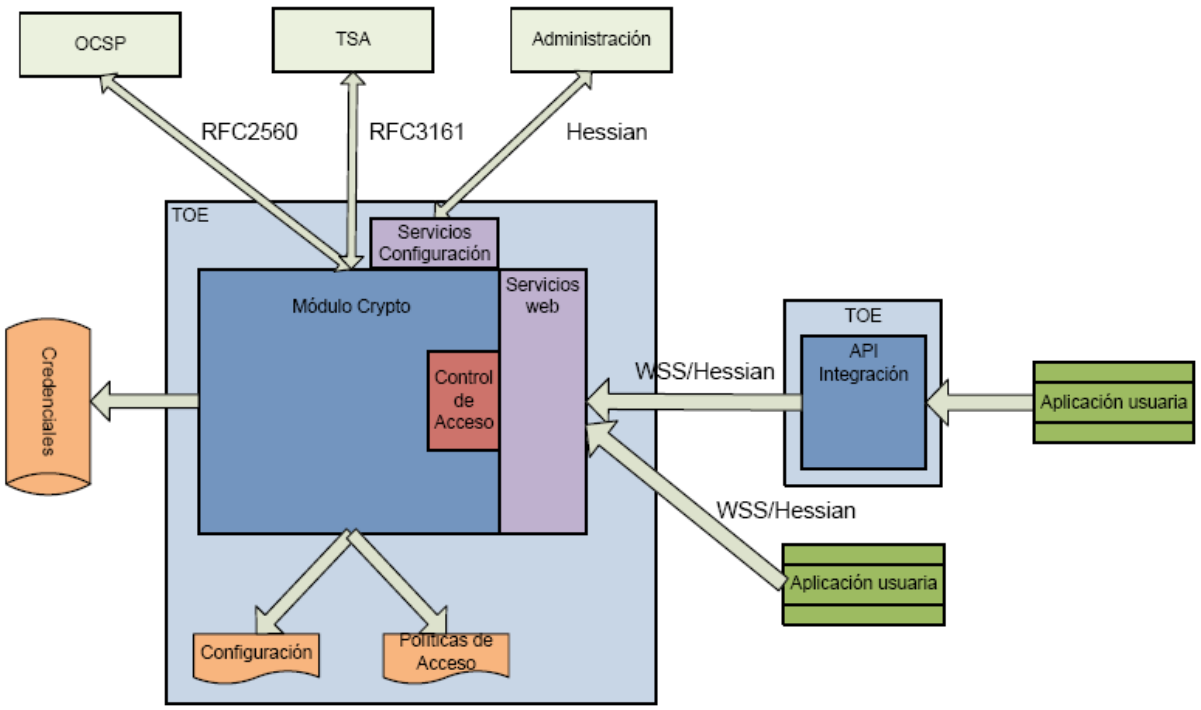
ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

El entorno debe asegurar los distintos datos de autenticación de los usuarios y, en el caso de autenticación mediante certificados, éstos deberán ser emitidos por una fuente fiable y disponer de los procesos pertinentes para la renovación y verificación de los mismos.

Arquitectura

Arquitectura Lógica:

- **Módulo Crypto**: Proporciona todos los servicios de firma electrónica, cifrado/descifrado de información y validación de certificados. Estos servicios se ofrecen a través de servicios web WSS o mediante servicios web mediante protocolo binario Hessian.
- **API de Integración Crypto**: Este API realiza las llamadas a los servicios que proporciona el módulo Crypto de manera transparente al usuario abstrayendo la complejidad de la construcción de los WSDL o llamadas binarias Hessian, de manera que el usuario realiza las llamadas a través de un API Java.



Arquitectura Física:

Se trata de un producto software.

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

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.

- eAS/Trusted Signatura Platform v6.2.1 Manual de Administración v1.0, Julio 2010.
- eAS/Trusted Signatura Platform v6.2.1 Manual del Asistente de Instalación v1.0, julio 2010.
- eAS/Trusted Signatura Platform v6.2.1 Manual de Control de Acceso v1.0, Julio 2010.
- eAS/Trusted Signatura Platform v6.2.1 Manual de Despliegue v1.0, Julio 2010.
- eAS/Trusted Signatura Platform v6.2.1 Manual de Integración Crypto v1.0, julio 2010.
- eAS/Trusted Signatura Platform v6.2.1 Interfaces Modo Seguro v1.0, Julio 2010.
- eAS/Trusted Signatura Platform v6.2.1 Manual de Instalación Modo Seguro v1.0, Julio 2010.
- eAS/Trusted Signatura Platform v6.2.1 Manual de Auditoría v1.0, Julio 2010.
- eAS/Trusted Signatura Platform (SIAVAL): Módulo Crypto v6.2.1 Declaración de Seguridad v1.6, Junio 2010.

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 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 cubrir.

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 los las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido entorno a un 25 % de las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más relevantes.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados así obtenidos son consistentes con los resultados obtenidos por el fabricante.

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

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.

Configuración evaluada

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento del producto eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1 es necesario disponer de los siguientes componentes software:

- **Sistema Operativo en servidor del TOE:** Microsoft Windows 2003 Server
- **Sistema Operativo en servidor de servicios externos:** Microsoft Windows 2003 Server
- **Sistema Operativo en cliente:** Microsoft Windows XP SP3
- **Servidor de Aplicaciones:** JBOSS 4.0.4 GA
- **Java Runtime Enviroment en servidor:** JDK 1.5.0.15 con JCE Unlimited Strength
- **Java Runtime Enviroment en cliente:** JDK 1.5.0.15 con JCE Unlimited Strength
- **Módulo de administración:** Módulo que establece la configuración al TOE eAS/TSP tspAdmin v6.2
- **TSA:** Módulo para el sellado de tiempo eAS/TSP TSA v6.2 que cumple con la RFC3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”
- **OCSP:** OCSP que cumple con la RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”

En cuanto a los componentes hardware, el único requisito es que soporten los elementos software detallados previamente.

Dentro de todas las posibilidades que ofrecen estos requisitos software, la configuración que se ha elegido para su evaluación es la siguiente:

- **Máquina Servidor:** PC Intel 32 bits.
- **Máquina Cliente:** PC Intel 32 bits.
- **Módulo Criptográfico:** Luna SA v 4.4 de SafeNet mediante acceso de API cliente propio de SafeNet.

Resultados de la Evaluación

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

El producto eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1 ha sido evaluado frente a la declaración de seguridad "eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1 Declaración de Seguridad", v1.6 de junio de 2010.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL1+** (aumentado con **ALC_FLR.1**) 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 a nivel EAL1+ALC_FLR.1, 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

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.

- El producto esta compuesto de diversos módulos, uno de los cuales es el objeto de evaluación (TOE). Se recomienda que la conexión entre estos módulos se limite a un entorno seguro donde ningún atacante pueda observar ni interferir la comunicación.
- Configurar el firewall del sistema operativo del TOE para denegar el acceso a los puertos que permiten el acceso no cifrado.
- Configurar el firewall del sistema operativo del TOE para denegar el acceso al puerto RMI levantado por el TOE.
- Evitar el acceso a la consola de JBoss a través de puertos en claro, y utilizar una password fuerte para protegerla.
- Permitir el acceso a los servicios del TOE únicamente a clientes confiables.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1, se propone la resolución estimatoria de la misma.

Glosario de términos

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ETR	Evaluation Technical Report (Informe Técnico de Evaluación)
OC	Organismo de Certificación
TOE	Target Of Evaluation (Objeto de Evaluación)

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, Julio 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r3, Julio 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r3, Julio 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, Julio 2009.

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: **eAS/Trusted Signature Platform (SIAVAL): Módulo Crypto v6.2.1 Declaración de Seguridad v 1.6, junio 2010**.

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