REF: 2012-11-INF-1062 v1	Creado: CERT8
Difusión: Interno esquema (inc. laboratorios)	Revisado: CALIDAD
Fecha: 11.10.2012	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2012-11 CONTROLADOR JAVA DNIe

Datos del solicitante: S2833002E MINISTERIO DE ADMONES PUBLICAS

Referencias:

[EXT-1704] Solicitud Certificación CONTROLADOR JAVA DNIe

[EXT-1863] Informe Final CONTROLADOR JAVA DNIe v2.

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe, según la solicitud de referencia [EXT-1704], de fecha 01/06/2012, evaluado por el laboratorio Epoche & Espri, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-1863], recibido el pasado 01/08/2012.

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 certificación del producto CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe.

El TOE es un "driver", que permite exportar servicios de acceso a los mecanismos y funcionalidad del DNI electrónico, normalizados conforme a la arquitectura de seguridad Java. Se puede considerar que es como una librería java que facilita el acceso al DNIe.

Fabricante: Desarrollo realizado por la empresa Atos. Integración en INTECO (Instituto Nacional de Tecnologías de la Comunicación).

Patrocinador: Ministerio de Hacienda y Administraciones Públicas.

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

Laboratorio de Evaluación: Epoche & Espri.

Perfil de Protección: No aplica.

Nivel de Evaluación: Common Criteria versión 3.1. EAL 1.

Fecha de término de la evaluación: 01/08/2012.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 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 Common Criteria v 3.1 (CC_P1, CC_P2, CC_p3) y la Metodología de Evaluación [CEM]

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe, se propone la resolución estimatoria de la misma.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

RESUMEN DEL TOE

El TOE es un "driver", que permite exportar servicios de acceso a los mecanismos y funcionalidad del DNI electrónico, normalizados conforme a la arquitectura de seguridad Java. Se puede considerar que es como una librería java que facilita el acceso al DNIe.

La solución construida se integra en la Arquitectura Java de Criptografía (JCA, Java Cryptography Architecture).

Dicha arquitectura permite que todas aquellas aplicaciones que invocan los servicios de acceso a tarjeta inteligente sobre la arquitectura JAVA puedan trabajar contra los DNI electrónicos de una manera transparente, siendo necesario únicamente que la aplicación se ajuste al estándar definido por el fabricante de la arquitectura JAVA.

La librería criptográfica para el DNIe permite llamadas relacionadas con la lectura de objetos del DNI electrónico (Acceso a Almacén de Claves) y firma. No están soportadas las funciones definidas de generación de claves, creación, modificación o borrado de ningún tipo de objetos del DNI electrónico.

Además se permite validar firmas RSA realizadas externa e internamente.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, según [CC_P3].

Clase	Familia/Componente
ASE	INT.1 CCL.1 OBJ.1 ECD.1 REQ.1 TSS.1
AGD	OPE.1 PRE.1
ALC	CMC.1 CMS.1
ADV	FSP.1
ATE	IND.1
AVA	VAN.1

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 siguientes requisitos funcionales, según [CC_P2].

Clase	Familia/Componente	
FTP	ITC.1	Inter-TSF trusted channel
FDP	OAK.1	Operation Acknowledge
FDP	RIP.1	Subset residual information protection
FCS	COP.1	Cryptographic operation
FCS	COP.2	Delegated cryptographic operation
FDP	ITC.1	Import of user data without security attributes

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

IDENTIFICACIÓN

Producto: CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe.

Declaración de Seguridad: Declaración de Seguridad para el Controlador JAVA de la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (DGMAPIAE) para el DNIe, versión 1.14 de 18 de julio de 2012.

Perfil de Protección: No aplica.

Nivel de Evaluación: Common criteria v 3.1 R3, EAL1.

POLÍTICA DE SEGURIDAD

En la evaluación del producto **CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe** CC v 3.1 R3 EAL1, se ha utilizado una declaración de seguridad de baja garantía que no requiere la definición del problema de seguridad, por lo que no se dan políticas organizativas.

HIPÓTESIS Y ENTORNO DE USO

En la evaluación del producto **CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe** CC v 3.1 R3 EAL1, se ha utilizado una declaración de seguridad de baja garantía que no requiere la definición del problema de seguridad, por lo que no se dan hipótesis de entorno.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

En la evaluación del producto **CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe** CC v 3.1 R3 EAL1, se ha utilizado una declaración de seguridad de baja garantía que no requiere la definición del problema de seguridad, por lo que no se dan amenazas.

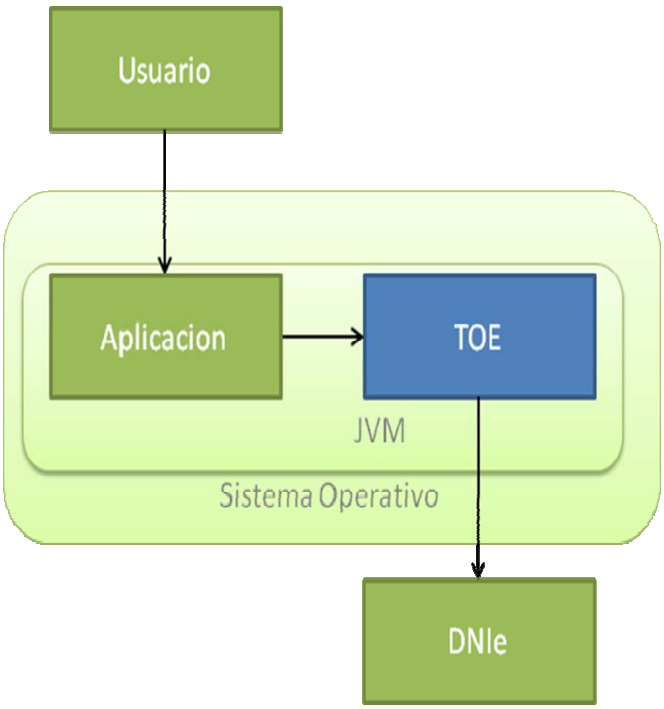
FUNCIONALIDAD DEL ENTORNO

No se ha definido ningún objetivo de seguridad para el entorno operacional.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

ARQUITECTURA

ARQUITECTURA LÓGICA



El TOE se ejecuta y usa como un driver en la máquina virtual de java que se esté ejecutando en el sistema operativo y es invocado por las aplicaciones java siguiendo los mecanismos que la máquina virtual de java provee. Las comunicaciones con el DNI electrónico se realizan igualmente a través del mismo sistema operativo, en particular mediando el uso de los correspondientes drivers del lector de tarjetas. Los diálogos con el usuario y la captura de sus entradas a través del teclado se realizan a través de las capacidades del interfaz de usuario del sistema operativo.

Todas las comunicaciones del TOE están, por tanto, mediadas por el sistema operativo y la máquina virtual de java en el que se instala y/o utiliza el driver.

ARQUITECTURA FÍSICA

El TOE, una vez instalado, se compone de la siguiente librería:

DNIeJCAProvider.jar

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:

- Declaración de Seguridad para el Controlador JAVA de la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (DGMAPIAE) para el DNIe, versión 1.14 de 18 de julio de 2012.

PRUEBAS DEL PRODUCTO

El evaluador ha seleccionado un subconjunto de pruebas y una estrategia apropiada para el TOE entregado por el fabricante. La documentación describe el comportamiento de las TSFIs y el evaluador ha aplicado esa información a la hora de desarrollar sus pruebas.

El principal objetivo de las pruebas realizadas por el evaluador es comprobar el cumplimiento de los requisitos especificados en la declaración de seguridad a través de los interfaces TSFIs. Para ello se ha tenido en cuenta:

- Trascendencia de los interfaces (si se ejercita algún requisito a través del interfaz).
- Tipos de interfaces (enforcing, supporting, non interfering)
- Número de interfaces

Para la selección de las pruebas se han utilizado como criterios: la búsqueda de parámetros críticos en la interacción con las TSFIs, los requisitos que ejercita el interfaz, realización de pruebas exhaustivas en las TSFIs de mayor importancia y sospechas de mal comportamiento de las TSFIs ante determinados parámetros de entrada.

También se han realizado pruebas con parámetros de las TSFIs que pudieran tener especial relevancia en el mantenimiento de la seguridad del TOE.

En el plan independiente se han definido casos de prueba para los requisitos definidos en la declaración de seguridad, sobre los que hubiera mayores sospechas sobre su cumplimiento.

El plan de pruebas del evaluador está orientado hacia la funcionalidad de los requisitos incluidos en la declaración de seguridad.

La totalidad de los TSFIs accesibles del TOE han sido ejercitados como resultado de las pruebas realizadas.

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. No se ha presentado ninguna desviación.

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 CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe es necesario disponer de los siguientes componentes software:

- Sistema operativo Microsoft Windows 7
- Java Virtual Machine 6u32

El TOE se integra con el cliente de @firma, utilizando el MiniApplet @firma y una página HTML simple de pruebas. El MiniApplet deberá ser publicado en un servidor Web.

En cuanto a los componentes hardware (al margen del hardware del ordenador de propósito general que se requiera para el correcto funcionamiento del Sistema Operativo que conforma el entorno del TOE), éste requiere de un lector de tarjetas inteligentes y del propio DNI electrónico. No hay más requisitos para el lector que su compatibilidad con el estándar ISO 7816 (1, 2 y 3), soporte para tarjetas asíncronas basadas en protocolos T=0 y T=1, velocidad de comunicación mínima de 9.600 bps y compatibilidad con JSE SmartCardIO (JSR-268).

RESULTADOS DE LA EVALUACIÓN

El producto CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe ha sido evaluado en base a la Declaración de Seguridad para el Controlador JAVA de la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (DGMAPIAE) para el DNIe, versión 1.14 de 18 de julio de 2012.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 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 de evaluación Common Criteria [CC_P3] y la Metodología de Evaluación [CEM].

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

En esta sección, se describen algunos aspectos importantes que podrían condicionar el uso del producto, teniendo en cuenta el alcance de los problemas encontrados durante la evaluación y su declaración de seguridad [ST114].

La última versión del TOE [TOE14] ha corregido algunas de las vulnerabilidades explotadas en su entorno de operación. No obstante existen vulnerabilidades que no han sido cerradas mediante la funcionalidad de seguridad implementada por el TOE. Para estas vulnerabilidades, el fabricante ha optado por la inclusión de un objetivo de seguridad para el entorno operacional en [ST114] que evita que, en el entorno operacional definido, éstas no sean explotables. Se considera que son vulnerabilidades residuales, en tanto en cuanto siguen presentes en el TOE, pero si se configura un entorno operacional conforme al definido en la ST, no serán explotables.

Este objetivo indica que la instalación y operación con el producto requiere la configuración previa de un entorno operacional con una plataforma en la que ejecuta el TOE que esté libre de malware. Se define como único path de ataque, el canal de comunicaciones con el DNIe (incluyendo el lector del DNIe y sus comunicaciones con el ordenador), siendo la protección de dicho canal (establecmiento de “trusted channel”), la funcionalidad de seguridad que mitiga estos ataques.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe, se propone la resolución estimatoria de la misma.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

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 Final, July 2009.

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

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

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R3 Final, July 2009.

DECLARACIÓN DE SEGURIDAD

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

Título: DECLARACIÓN DE SEGURIDAD – CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe

Versión: 1.14

Fecha de publicación: 18 de Julio de 2012

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es