REF: 2011-43-INF-974 v1	Creado: CERT8
Difusión: Interno OC	Revisado: CALIDAD
Fecha: 14.06.2012	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2011-43 Driver DNIe PKCS'11

Datos del solicitante: Q2826004J FABRICA NACIONAL DE MONEDA Y TIMBRE

Referencias:

[EXT-1494] Solicitud de Certificación de Driver DNIe PKCS'11

[EXT-1728] Informe Técnico de Evaluación de Driver DNIe PKCS'11.

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto Driver DNIe PKCS'11, según la solicitud de referencia [EXT-1494], de fecha 24/10/2011, evaluado por el laboratorio Epoche & Espri, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-1728], recibido el pasado 26/12/2011.

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 certificación del producto **Driver DNI electrónico PKCS#11 v 1.0**.

El TOE es un "driver", que permite exportar servicios de acceso a los mecanismos y funcionalidad del DNI electrónico, normalizados conforme a la especificación de interfaz de nivel de aplicación PKCS #11. Dicho interfaz permite que todas aquellas aplicaciones que soporten PKCS#11 puedan trabajar contra los DNI electrónicos de una manera transparente, siendo necesario únicamente que la aplicación se ajuste al estándar.

Fabricante: Fábrica Nacional de Moneda y Timbre

Patrocinador: Fábrica Nacional de Moneda y Timbre

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. EAL1.

Fecha de término de la evaluación: 26/12/2011

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 **Driver DNI electrónico PKCS#11 v 1.0**, se propone la resolución estimatoria de la misma.

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 especificación de interfaz de nivel de aplicación PKCS #11. Dicho interfaz permite que todas aquellas aplicaciones que soporten PKCS#11 puedan trabajar contra los DNI electrónicos de una manera transparente, siendo necesario únicamente que la aplicación se ajuste al estándar.

Conforme a la definición del PKCS#11, la librería criptográfica desarrollada por la FNMT-RCM para el DNIe soporta todas las llamadas del estándar, si bien sólo están

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

permitidas aquellas relacionadas con la lectura de objetos del DNI electrónico, firma y verificación. No están soportadas las funciones definidas en el PKCS#11 de generación de claves, creación, modificación o borrado de ningún tipo de objetos del DNI electrónico.

El TOE requiere de su instalación en el sistema de firma electrónica, según las restricciones que cada sistema operativo establece. El TOE es invocado y utilizado por aplicaciones confiables de generación o verificación de firma, o de autenticación, que son las que interactúan con el firmante, y que utilizan los servicios del DNI electrónico a través del TOE.

El TOE establece un diálogo con el firmante para la captura de su consentimiento en el momento de realizar una firma electrónica, y es capaz de notificar diferentes estados y resultados de error en la ejecución de sus operaciones.

El DNI electrónico requiere que las comunicaciones entre la aplicación y la tarjeta se realicen con un canal securizado. Este canal cifrado lo establece y lo gestiona el propio TOE de manera transparente para la aplicación, encargándose de su establecimiento, cifrado/descifrado de mensajes y, en su caso, destrucción de dicho canal.

Adicionalmente, el TOE recibe el PIN del usuario del DNI electrónico, necesario tanto para la realización de operaciones de firma como para la lectura de certificados públicos. La adquisición de este PIN corresponde a las aplicaciones que invocan el TOE, y el TOE lo destruye de su ámbito de control cuando deja de ser necesario.

El TOE no entiende de tipos de documentos a firmar, ni incorpora visor de los datos a firmar o de su representación ("hash"), cuestiones que pertenecen al ámbito de las aplicaciones o el sistema de firma que utiliza este TOE.

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

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

ATE	IND.1
AVA	VAN.1

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

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: Driver DNI electrónico PKCS#11 v 1.0.

Declaración de Seguridad: Declaración de Seguridad para "Driver DNI electrónico PKCS#11" versión 1.0 Diciembre 2011

Perfil de Protección: no aplica

Nivel de Evaluación: Common criteria v 3.1 R3, EAL1

POLÍTICA DE SEGURIDAD

En la evaluación del producto **Driver DNI electrónico PKCS#11 v 1.0** 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 **Driver DNI electrónico PKCS#11 v 1.0 v 1.0** 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 **Driver DNI electrónico PKCS#11 v 1.0 v 1.0** 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

Se relacionan, a continuación, los objetivos que se deben cubrir por el entorno de uso del TOE.

OE.ENTORNO SEGURO;

La plataforma de propósito general sobre la que se instala y opera el TOE es confiable y no es fuente de ataques, incluyendo las aplicaciones que invocan y usan el TOE.

No requiere confianza y puede ser objeto de ataques, el canal de comunicaciones con la tarjeta, esto es, el lector de tarjetas y sus comunicaciones con el ordenador de propósito general, ya sea por cable, wireless o por red.

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

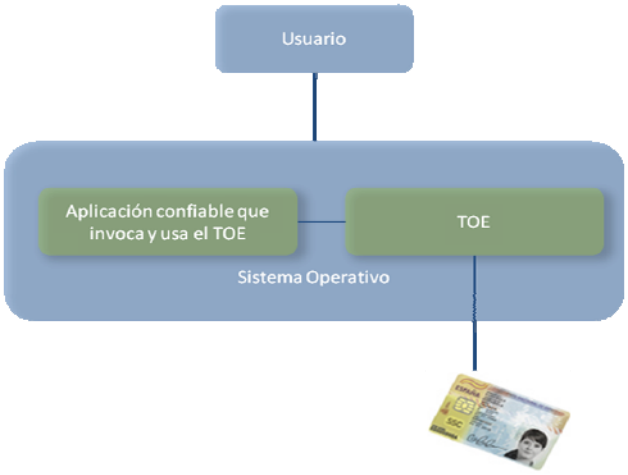
Los detalles de la definición del entorno del producto o de los requisitos de seguridad del TOE se encuentran en la correspondiente Declaración de Seguridad.

ARQUITECTURA

ARQUITECTURA LÓGICA

El TOE se instala e integra como un driver PKCS#11 en el sistema operativo, y es invocado por las aplicaciones siguiendo los mecanismos que el propio sistema operativo establece. 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 en el que se instala y utiliza.



ARQUITECTURA FÍSICA

El TOE, una vez instalado, se compone de los siguientes ficheros o librerías dinámicas y versiones:

- DNIeP11.dll versión 1.0.0.1

Es un "driver" que se instala e integra en las siguientes versiones del sistema operativo "Microsoft Windows":

- Microsoft Windows 7 32 bits
- Microsoft Windows 7 64 bits

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

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, y velocidad de comunicación mínima de 9.600 bps.

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 – Driver DNI Electrónico PKCS#11 Versión 1.0, Diciembre 2011
- PKCS#11 Specification. RSA Laboratories. Version 2.30

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.

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

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

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 **Driver DNI electrónico PKCS#11 v1.0** es necesario disponer de los siguientes componentes software:

- Sistema operativo "Microsoft Windows":
  a. Microsoft Windows 7 32 bits
  b. Microsoft Windows 7 64 bits

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, y velocidad de comunicación mínima de 9.600 bps.

RESULTADOS DE LA EVALUACIÓN

El producto **Driver DNI electrónico PKCS#11 v1.0** ha sido evaluado en base a la **Declaración de Seguridad para "Driver DNI electrónico PKCS#11" versión 1.0 Diciembre 2011.**

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].

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

No se describen recomendaciones de uso seguro derivados del análisis realizado.

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

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto **Driver DNI electrónico PKCS#11 v1.0**, 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

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:

Declaración de Seguridad para "Driver DNI electrónico PKCS#11" versión 1.0 Diciembre 2011

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