REF: 2011-34-INF-1022 v1	Creado: CERT8
Difusión: Público	Revisado: CALIDAD
Fecha: 07.08.2012	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2011-34 CRYPTOX

Datos del solicitante: B74074824 INIXA DEL PRINCIPADO

Referencias:

[EXT-1383] Solicitud de Certificación de CRYPTOX

[EXT-1633] Informe Técnico de Evaluación de CRYPTOX

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto **Crypto.X** versión **2.3.6.1**, según la solicitud de referencia [EXT-1383], de fecha 30/082012, evaluado por el laboratorio EPOCHE&ESPRI, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-1633], recibido el pasado 16/02/2012.

ENAC CERTIFICACIÓN Nº 45/C-PR110

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

ÍNDICE

RESUMEN **3**
RESUMEN DEL TOE 3
REQUISITOS DE GARANTÍA DE SEGURIDAD 4
REQUISITOS FUNCIONALES DE SEGURIDAD 5
IDENTIFICACIÓN **5**
POLÍTICA DE SEGURIDAD **5**
HIPÓTESIS Y ENTORNO DE USO **7**
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS 7
FUNCIONALIDAD DEL ENTORNO 8
ARQUITECTURA **8**
ARQUITECTURA LÓGICA 8
ARQUITECTURA FÍSICA 9
DOCUMENTOS **9**
PRUEBAS DEL PRODUCTO **9**
CONFIGURACIÓN EVALUADA **10**
RESULTADOS DE LA EVALUACIÓN **11**
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES **11**
RECOMENDACIONES DEL CERTIFICADOR **11**
GLOSARIO DE TÉRMINOS **12**
BIBLIOGRAFÍA **12**
DECLARACIÓN DE SEGURIDAD **13**

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 **Crypto.X** versión **2.3.6.1.**

El TOE es una SCVA de Tipo 2 conforme al Perfil de protección PPSCVA-T2, EAL1, v 2.0; es una aplicación de creación y verificación de firma electrónica, e incluye la funcionalidad necesaria para verificar y crear una firma electrónica, utilizando el propio DNI-e, que es un elemento de uso obligado.

Fabricante: INIXA S.L.

Patrocinador: INIXA S.L.

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: 16/02/2012

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, conforme al perfil de protección [PPSCVA-T2] y 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 **Crypto.X** version **2.3.6.1**, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El TOE es una SCVA de Tipo 2 conforme al Perfil de protección PPSCVA-T2, EAL1, v 2.0; una “SCVA - Tipo 2” es una aplicación de creación y verificación de firma electrónica, e incluye la funcionalidad necesaria para verificar y crear una firma electrónica, utilizando el propio DNI-e, que es un elemento de uso obligado.

La “SCVA - Tipo 2” requiere de una plataforma de computación, fuera del ámbito del TOE, para el interfaz con el firmante, las comunicaciones con el DNI-e, y para acceder y utilizar recursos generales de computación, tales como CPU o memoria.

Esta plataforma de propósito general debe ser confiable, y será configurada y gestionada de tal manera.

La “SCVA - Tipo 2” requiere de un DNI-e como dispositivo seguro de creación de firma.

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

Los siguientes datos se reciben a través de uno de los interfaces de la SCVA. No se supone si estos interfaces lo son para entidades locales o remotas:

- el Documento del Firmante (SD), y
- los Datos de verificación de firma (SVD).

El Objeto de datos firmados (SDO) es un resultado de la funcionalidad de creación de firma del TOE, y se exporta a través de uno de los interfaces de la SCVA, sin que se suponga si es una exportación local o remota. El SDO se recibe como entrada para realizar la funcionalidad de verificación de firma, también a través de uno de sus interfaces, y de nuevo sin distinguir sobre si es una importación local o remota.

El TOE descansa en su entorno para comunicarse con el firmante, así como con el DNI-e.

Mientras que los SD, SDO y SVD se reciben probablemente de una entidad externa, nada impide que el propio firmante los introduzca directamente a través del interfaz que posee la SCVA, ni que los lea a través del mismo interfaz. En todo caso, no hay hipótesis de seguridad relativas a estas entidades externas que facilitan o reciben el SD, SDO y SVD.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, conforme al perfil de protección [PPSCVA-T2] 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
FDP	SDI.2 Stored data integrity monitoring and action
	ITC.1 Import of user data without security attributes
	RIP.1 Subset residual information protection
	SVR.1 (extendido) Secure viewer and SCVA interface
	ISD.1 (extendido) Import of Signer's Document
FPT	TST.1 TSF testing
FTP	ITC.1.UD Inter-TSF trusted channel
	ITC.1.VAD Inter-TSF trusted channel
FCS	COP.1 _SIGNATURE_CEATION_PROCESS Cryptographic operation
FCS	COP.1 _SIGNATURE_VERIFICATION Cryptographic operation

IDENTIFICACIÓN

Producto: **Crypto.X** versión **2.3.6.1.**

Declaración de Seguridad: Declaración de Seguridad para el producto Crypto.X. v RC5 Febrero 2012

Perfil de Protección: Perfil de protección PPSCVA-T2, EAL1, v 2.0

Nivel de Evaluación: Common criteria v 3.1 R3, EAL1

POLÍTICA DE SEGURIDAD

En la evaluación del producto **Crypto.X** versión **2.3.6.1,** el fabricante declara conformidad con el siguiente perfil de protección [PPSCVA-T2]:

- PPSCVA-T2, EAL1. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL1.

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

Dicho PP fue certificado por el CCN con fecha 14 de abril de 2009, tal y como se especifica en el BOE Número 91 del Martes 14 de abril de 2009, sección III, página 34864 y el correspondiente informe de certificación 2008-15-INF-331 V1 del 23 de febrero de 2009.

El Perfil de protección [PPSCVA-T2] especifica que los TOEs que declaren cumplimiento con él, deberán ser evaluados con un nivel de garantía EAL1.

El nivel de garantía EAL1 requiere que el fabricante desarrolle una declaración de seguridad de baja garantía o "low assurance" en la que no se especifican, ni el problema de seguridad, ni los objetivos de seguridad del TOE. Únicamente se declaran objetivos de seguridad para el entorno y se listan los requisitos funcionales que el TOE deberá cumplir.

Sin embargo, el perfil de protección [PPSCVA-T2], aunque declara un nivel EAL1 (incluyendo los SARs correspondientes a una declaración de seguridad de baja garantía), sí define un problema de seguridad, unos objetivos de seguridad completos (para el TOE y el entorno) que resuelven el problema de seguridad y un conjunto de requisitos funcionales de seguridad que hacen cumplir dichos objetivos de seguridad.

A continuación se exponen las políticas de seguridad organizativas, que son las declaradas en el perfil de protección.

Dispositivo Seguro de Creación de Firma

- **P.SSCD;**

  El dispositivo seguro de creación de firma que usa la SCVA será el DNIe.

Algoritmos criptográficos

- **P.CRYPTO;**

  Los algoritmos criptográficos que realice la SCVA, así como el certificado seleccionado para crear o verificar una firma deberán ser tales que se verifiquen y produzcan firmas reconocidas con el DNIe.

Protección de Datos de Carácter Personal

- **P.LOPD;**

  La SCVA avisará al firmante sobre el hecho de que datos suyos de carácter personal que se incluyen en la firma, tal como la realiza el DNIe.

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

HIPÓTESIS Y ENTORNO DE USO

Al igual que se expone en la sección anterior, a continuación se listan las hipótesis de entorno del perfil de protección aplicado en la evaluación del producto **Crypto.X** versión **2.3.6.1.**

Entorno de computación

- **AS.ITENV;**

  La plataforma de propósito general que la "SCVA - Tipo 2" necesite para operar y para facilitar los interfaces de firmante y con el DNI-e, facilita las protecciones y mecanismos de seguridad adecuados para proteger los activos de la SCVA (A.DSCVA, A.VAD y A.SCVA).

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Al igual que se expone en la sección anterior, a continuación se listan las amenazas especificadas en el perfil de protección aplicado en la evaluación del producto **Crypto.X** versión **2.3.6.1.**

- **T.DSCVA;**

  Un atacante modifica cualquiera de los datos de usuario que intervienen en la creación o verificación de firma, mientras están en posesión de la SCVA, o durante el proceso de remisión al DNI-e para la realización de la firma.

  Un atacante es capaz de incluir información en el SD, que no se muestra por la SCVA al firmante, y que aún siendo conforme con el formato de documento electrónico del SD, que se firma de manera inadvertida. Esta amenaza compromete el activo A.DSCVA

  Un atacante es capaz de incluir información en el SDO, que no se muestra por la SCVA al firmante, y que aún siendo conforme con el formato de documento electrónico del SDO, se verifica de manera inadvertida. Esta amenaza compromete el activo A.DSCVA.

- **T.SCVA;**

  Un atacante es capaz de tomar el control del proceso de firma, engañando al firmante, o abusando de los medios de firma, de manera que puede obtener firmas electrónicas sin el consentimiento del titular legítimo del DNI-e.

  Lo mismo aplica al proceso de verificación de firmas, forzando falsos positivos o negativos. Esta amenaza incluye una posible modificación del propio TOE, de manera que se altere su funcionalidad. Esta amenaza compromete el activo A.SCVA.

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

- **T.VAD;**

  Un atacante compromete la confidencialidad del VAD, perdiendo su titular el control del exclusivo del DNI-e. Esta amenaza compromete el activo A.VAD.

FUNCIONALIDAD DEL ENTORNO

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

- **O.SSCD;**

  El dispositivo seguro de creación de firma que usa la SCVA será el DNI-e.

- **O.ITENV;**

  La plataforma de propósito general que la "SCVA - Tipo 2" necesita para operar y para facilitar los interfaces de firmante y con el DNI-e, facilita las protecciones y mecanismos de seguridad adecuados para proteger los activos de la SCVA (A.DSCVA, A.VAD y A.SCVA), mediante una combinación eficaz de medidas de índole técnico, de procedimientos y de securización de su entorno.

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

Desde un punto de vista lógico, el producto proporciona la siguiente funcionalidad:

- Implementa medidas de seguridad para comprobar el formato del texto que se desea firmar, detectando cualquier modificación o error de integridad en el mismo antes de realizar la firma.
- Provee un canal de comunicación seguro entre sí mismo y el DNI-e para la creación de firma.
- Permite la autenticación del firmante utilizando el DNI-e.
- Implementa medidas de seguridad para liberar los recursos utilizados tras la creación/verificación de firma.
- Implementa medidas de seguridad de auto comprobación para garantizar el correcto funcionamiento y la no alteración. Estas medidas se realizan durante el arranque inicial, periódicamente durante su operación normal, y bajo petición del usuario.

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

- Implementa un visor seguro el cual permite visualizar el texto a firmar previamente.
- Provee un sistema de seguridad que evita la impersonación del firmante y que permite al usuario expresar su voluntad para llevar a cabo la operación.
- Únicamente acepta para la firma documentos de texto almacenados en ficheros con extensión .txt y de no más de 5000 caracteres en formato ASCII restringido a los caracteres con códigos desde 0x30 a 0x7E ambos excluidos.
- Importa firmas en formato PKCS7 en un fichero situado en el mismo directorio y con el mismo nombre (extensión .p7s) que el archivo firmado.
- Crea firmas en formato PKCS7 utilizando el hash SHA-1 del documento a firmar utilizando certificados de firma del DNI-e con longitud mínima de 2048 bits.
- Verifica tanto la firma del documento como el certificado que firma.

ARQUITECTURA FÍSICA

El TOE es una aplicación puramente software que incluye los siguientes componentes:

- Binarios Crypto·X (CryptoX.exe , CryptoXH.dll)
- Binarios del driver del DNIe: UsrDNIeCertStore.dll y dniecsp.dll

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 producto Crypto.X. v RC5. Febrero 2012
- MANUAL INSTALACIÓN de Crypto.X versión 1.4 Febrero 2012

PRUEBAS DEL PRODUCTO

El evaluador ha definido una estrategia de pruebas apropiada para el TOE entregado por el fabricante que posteriormente ha ejecutado. 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:

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

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

Para el diseño 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 SFRs y 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 **Crypto.X** versión **2.3.6.1** es necesario disponer de los siguientes componentes.

La “SCVA - Tipo 2” requiere de una plataforma de computación, fuera del ámbito del TOE, para el interfaz con el firmante, las comunicaciones con el DNI-e, y para acceder y utilizar recursos generales de computación, tales como CPU o memoria.

Esta plataforma de propósito general debe ser confiable, y será configurada y gestionada de tal manera. El sistema operativo sobre el que corre el TOE es un Windows XP Bastionado.

La citada plataforma deberá cumplir unos requisitos mínimos de capacidad de computación y contener el hardware necesario para el funcionamiento del TOE. Estos elementos se enumeran a continuación:

- Procesador Intel Pentium 1 GHz o CPU con velocidad de procesado equivalente.
- Memoria RAM de al menos 256 Megabytes.

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

- Disco duro de al menos 3 Gigabytes.
- Monitor con una resolución mínima de 800x600.
- Un puerto USB como mínimo.
- Lector y grabador de CDs.
- Lector de tarjetas inteligentes USB que cumpla con el estándar USB CCID compatible con el DNI-e:
    - Debe cumplir el estándar ISO-7816 (1, 2 y 3).
    - Debe soportar tarjetas asíncronas en protocolos T=0 y T=1.
    - Debe soportar velocidades de comunicación mínimas de 9.600 bps.
    - Debe soportar los estándares API PC/SC, CSP, API PKCS#11.

La "SCVA - Tipo 2" requiere de un DNI-e como dispositivo seguro de creación de firma.

RESULTADOS DE LA EVALUACIÓN

El producto **Crypto.X** versión **2.3.6.1** ha sido evaluado en base a la **Declaración de Seguridad para el producto Crypto.X. v RC5 Febrero 2012.**

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 (especificados en el [PPSCVA-T2]), 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

A continuación se indican las recomendaciones de uso seguro que se estiman conveniente tener en cuenta:

- Durante la instalación del producto, es necesario prestar especial atención a la preparación del entorno del TOE, tal y como se indica en el manual de instalación. El sistema Windows XP bastionado, en conjunción con el cifrado del disco, y la preparación del entorno sobre una máquina física (no virtualizada) mitigan los riesgos que supone ejecutar el TOE en un sistema operativo comercial. Con esta configuración, fugas como pudiera ser la captura del PIN del DNIe por otros procesos del sistema operativo quedan solventadas.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto **Crypto.X** versión **2.3.6.1**, 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

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
SCVA	Signature Creation and Verification Application
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.

[PPSCVA-T2] PPSCVA-T2, EAL1. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL1.

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

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 el producto Crypto.X. v RC5 Febrero 2012

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