REF: 2011-31-INF-1016 v1	Creado: CERT8
Difusión: Público	Revisado: CALIDAD
Fecha: 07.08.2012	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2011-31 ESIGNACRYPTO

Datos del solicitante: B97458996 Indenova, S.L.

Referencias:

[EXT-1380] Solicitud de Certificación de ESIGNACRYPTO

[EXT-1632] Informe Técnico de Evaluación de ESIGNACRYPTO

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto **eSigna Crypto** versión **2.1.1**, según la solicitud de referencia [EXT-1380], de fecha 24/08/2011, evaluado por el laboratorio EPOCHE&ESPRI, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-1632], 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

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 **eSigna Crypto** versión **2.1.1.**

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 que emplea el DNIe como dispositivo seguro de creación de firma (SSCD).

Fabricante: INDENOVA S.L.

Patrocinador: INDENOVA 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 **eSigna Crypto** versión **2.1.1**, 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 que emplea el DNIe como dispositivo seguro de creación de firma (SSCD).

La funcionalidad del TOE, para la creación de firma electrónica, incluye:

- Seleccionar un documento o texto para firmar (SD)
- Seleccionar la política de firma a aplicar, los atributos de la firma, y el certificado a utilizar para la firma, y componer los DTBS
- Mostrar de manera no ambigua los DTBS al firmante, para un número determinado de formatos de documento electrónico, y de detectar formatos o

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

construcciones problemáticas, en cuyo caso rechaza la operación de creación de firma de estos documentos

- Requerir el VAD del firmante de manera explícita en cada operación de firma, y de autenticarlo frente al SSCD, y de mandar los DTBSR al mismo SSCD, si el firmante expresa su voluntad inequívoca de firmar el documento
- Asociar la firma electrónica creada por el SSCD al propio documento firmado, o de facilitar la firma realizada como datos separados
- Eliminar del ámbito de control de la SCVA el VAD y los demás datos de usuario asociados a una firma tan pronto como dejan de ser necesarios para la realización de la misma

La funcionalidad del TOE, para la verificación de firma electrónica, incluye:

- La capacidad de seleccionar un documento firmado (SDO)
- La capacidad de seleccionar una política de certificación a aplicar
- La capacidad de mostrar al usuario que solicita su verificación, de manera no ambigua, el SDO y los correspondientes atributos de la firma, para un número determinado de formatos de documento electrónico, y de detectar formatos o construcciones problemáticas, en cuyo caso rechaza la operación de verificación de firma de estos documentos
- La capacidad de verificar la firma electrónica, conforme a la política de certificación seleccionada, y la capacidad de mostrar el resultado de la verificación al usuario que la ha solicitado. Este resultado deberá discriminar entre formas válidas e inválidas, cuando el proceso de verificación haya podido realizarse, e identificará las firmas que no han podido verificarse.

Las comunicaciones entre la SCVA y el DNIe se suponen securizadas por la propia SCVA, cumpliendo además con los requisitos exigibles por el perfil de protección CWA 14169 que se aplica al DNIe.

El TOE recibe el SD a través de uno de sus interfaces. El TOE dispone de interfaces de comunicaciones a redes confiables, vía HTTPS, y a interfaces a dispositivos locales, tales como discos o lectores de tarjetas de memoria como lectores de DNIe compatibles con CWA 14169. Un interfaz que siempre implementará el TOE es el interfaz propio al DNIe.

El TOE muestra el DTBS al firmante, de tal manera que su contenido no pueda ser malinterpretado, y que no tenga contenido oculto o ambiguo en su representación. En la declaración de seguridad se especifican los tipos de formato de documento electrónico que son capaces de presentar de manera fiable al firmante, y se detallan ciertos requisitos adicionales a esta presentación.

De igual manera, se requiere la voluntad expresa del firmante para que el TOE solicite una firma al DNIe. Se incluye requisitos para el proceso y secuencia de mostrar el DTBS al firmante, y de solicitar y confirmar la voluntad expresa del

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

mismo. Además, el TOE solicita el VAD al firmante, e inicia y ordena la operación de firma, que realiza en todo caso el DNIe.

El TOE también es capaz de verificar una firma electrónica. Para ello, permite la selección de documentos firmados desde el sistema de ficheros local. El TOE mostrará al usuario si el documento seleccionado corresponde a un formato de firma válido para la verificación o no. En el caso que el formato de firma a verificar sea válido, se mostrará al usuario el resultado de la firma.

El usuario puede firmar una cadena de texto ASCII o un fichero en formato XML que cumpla un esquema propio denominado FormSchema. Los formatos de firma aceptados por el TOE son:

- XAdES-BES
- XAdES-T
- XAdES-XL

En el caso de formatos XAdES-T y XAdES-XL se aplica como autoridad de sellado de tiempo (TSA) la ACCV. La versión de XAdES generada es la 1.2.21 attached. En el caso de los documentos XML se aplicará una firma enveloped, incluyéndola en un nodo signatures. En caso de firmar un mensaje texto ASCII se empleará siempre una firma enveloping. En el caso de verificación de firma electrónica, se aceptarán los siguientes formatos de firma:

- XAdES-BES
- XAdES-T
- XAdES-XL

Se verificarán firmas attached tanto enveloping y enveloped, en formatos de XAdES 1.2.2. Se empleará el DNIe como dispositivo de verificación de la firma. Para ello, el usuario seleccionará un documento firmado de la carpeta de trabajo y procederá a su verificación.

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

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

	REQ.1 TSS.1
AGD	OPE.1 PRE.1
ALC	CMC.1 CMS.1
ADV	FSP.1
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**
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: **eSigna Crypto** versión **2.1.1.**

Declaración de Seguridad: eSigna Crypto 2.1.1 – Declaración de Seguridad. Versión 1.9 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

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 **eSigna Crypto** versión **2.1.1,** 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.

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.

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

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.

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 **eSigna Crypto** versión **2.1.1.**

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 **eSigna Crypto** versión **2.1.1.**

- **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;**

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

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.

- **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, la funcionalidad del TOE incluye la creación de firmas electrónicas empleando formatos XAdES-BES, XAdES-T y XAdES-XL y la verificación de las mismas mediante DNIe. En el caso de los formatos avanzados XAdES-T y XAdES-XL se le aplicarán de forma automática un sellado de tiempo utilizando el servicio de la ACCV (Autoridad Certificadora de la Comunidad Valenciana).

Los datos objeto a firmar pueden ser:

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

- Un documento XML que valide un formato determinado de Indenova S.L
- Una cadena de texto

La funcionalidad del TOE, para la creación de firma electrónica, incluye:

- Seleccionar un documento o texto para firmar (SD)
- Seleccionar la política de firma a aplicar, los atributos de la firma, y el certificado a utilizar para la firma, y componer los DTBS
- Mostrar de manera no ambigua los DTBS al firmante, para un número determinado de formatos de documento electrónico, y de detectar formatos o construcciones problemáticas, en cuyo caso rechaza la operación de creación de firma de estos documentos
- Requerir el VAD del firmante de manera explícita en cada operación de firma, y de autenticarlo frente al SSCD, y de mandar los DTBSR al mismo SSCD, si el firmante expresa su voluntad inequívoca de firmar el documento
- Asociar la firma electrónica creada por el SSCD al propio documento firmado, o de facilitar la firma realizada como datos separados
- Eliminar del ámbito de control de la SCVA el VAD y los demás datos de usuario asociados a una firma tan pronto como dejan de ser necesarios para la realización de la misma

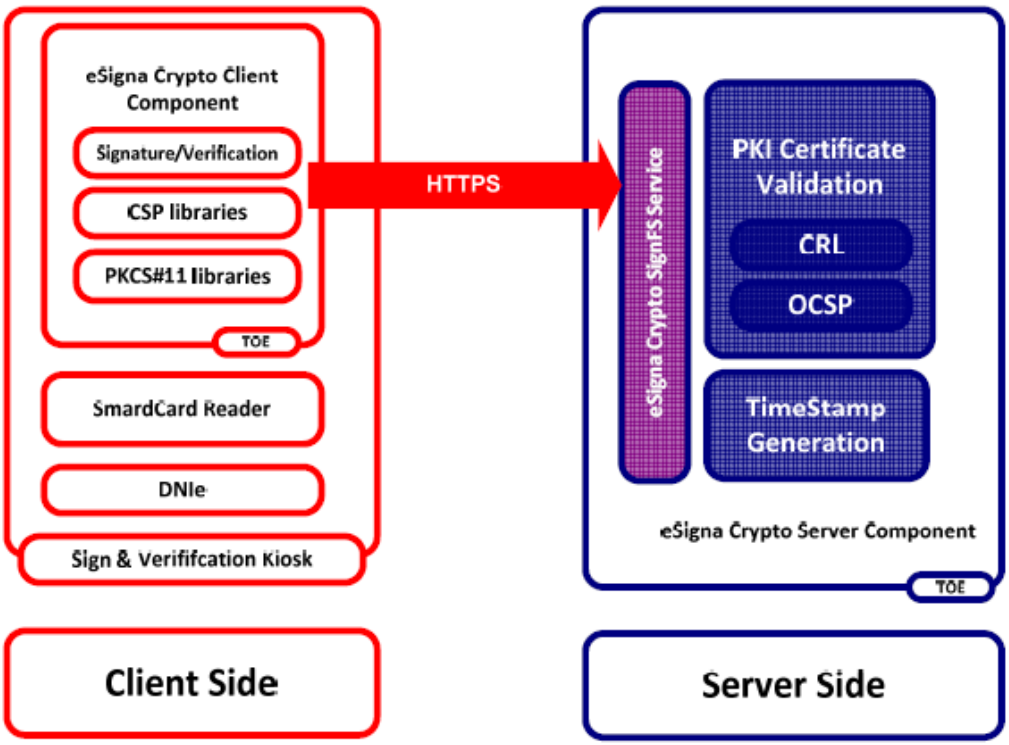
La funcionalidad del TOE, para la verificación de firma electrónica, incluye:

- La capacidad de seleccionar un documento firmado (SDO)
- La capacidad de seleccionar una política de certificación a aplicar
- La capacidad de mostrar al usuario que solicita su verificación, de manera no ambigua, el SDO y los correspondientes atributos de la firma, para un número determinado de formatos de documento electrónico, y de detectar formatos o construcciones problemáticas, en cuyo caso rechaza la operación de verificación de firma de estos documentos
- La capacidad de verificar la firma electrónica, conforme a la política de certificación seleccionada, y la capacidad de mostrar el resultado de la verificación al usuario que la ha solicitado. Este resultado deberá discriminar entre formas válidas e inválidas, cuando el proceso de verificación haya podido realizarse, e identificará las firmas que no han podido verificarse.

El TOE es definido como una aplicación compuesta de un componente cliente y un componente servidor. El componente cliente funciona a modo de Java Applet, ejecutando en el navegador del usuario. El componente servidor lleva a cabo la composición del objeto XAdES y ejecuta en una máquina a la que se accede mediante un interfaz web:

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

En la siguiente figura se puede ver un resumen de los elementos que forman parte del TOE así como otros que son parte del entorno operacional (arquitecturas lógica y física):



ARQUITECTURA FÍSICA

Como se explica en la sección anterior, el TOE está compuesto por los componentes

- eSigna Crypto Client Component: se trata de un componente que se ejecuta en el navegador web del cliente. Este componente es el punto de entrada que incorpora la lógica de comunicación con el componente servidor eSigna Crypto Server Component.
- eSigna Crypto Server Component: este componente reside en servidor y se encarga básicamente de la composición del objeto XAdES. Este componente ofrece al eSigna Crypto Cliente Component, una interfaz web service a través la cual se comunica.

Conforme a esta arquitectura, desde el punto de vista físico está formado por los siguientes elementos:

- SeSignaCryptoClientComponent.jar es un archivo JAR que contiene el componente Java Applet que se ejecuta en el navegador y que interactúa con la

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

parte servidora. Las dependencias de esta librería como son Sjce.jar y Sylib.jar no forman parte del TOE.

- eSignaCryptoServerComponent.war es un archivo WAR que contiene la implementación web service de los servicios de criptografía relacionados con la firma electrónica. Este WAR dispone de dependencias de librería de terceros y de Indenova SL que no forman parte de la evaluación del TOE.

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.

- eSigna Crypto 2.1.1 – Declaración de Seguridad. Versión 1.9, Febrero 2012
- eSigna Crypto 2.1.1 – Guía preparativa. Versión 1.8, Febrero 2012
- eSigna Crypto 2.1.1 – Manual de usuario. Versión 1.5, Enero 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:

- 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.

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

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.

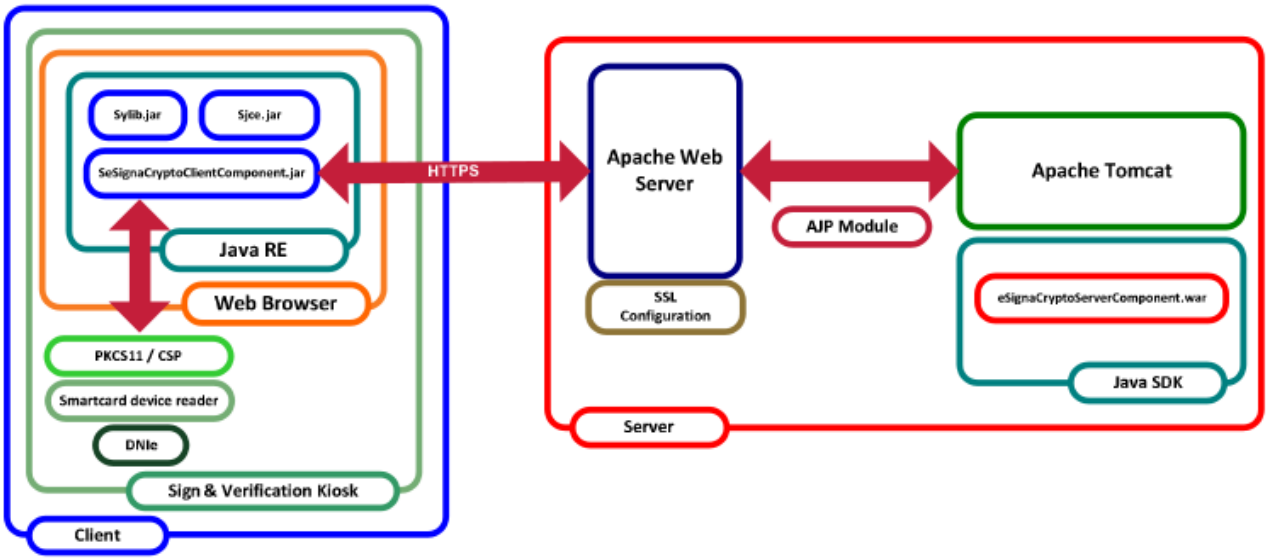
Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados. No se ha presentado ninguna desviación.

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 **eSigna Crypto** versión **2.1.1** 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. A continuación se presenta el diagrama que define la plataforma que conforma la configuración evaluada así como la información del versionado de sus componentes.



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

Parte cliente	
Sistema operativo	Microsoft Windows XP Professional
Plataforma hardware	Procesador: Doble núcleo 2GHz o superior Memoria: 2GB o superior Disco duro: 10GB o superior 3 Puertos USB 1.0 o superior disponibles
Navegador web	Internet Explorer 6
Máquina virtual de Java – plugin para navegador	Java Runtime Environment (JRE) versión 1.5 o superior
Dispositivo criptográfico – Lector de tarjetas inteligentes	Cumplimiento de los estándares ISO 7816 (1, 2 y 3) y los API PC/SC, CSP y PKCS#11
DNIe	DNIe del firmante/ verificador

Parte servidora	
Sistema operativo	Ubuntu 10.04 LTS
Plataforma hardware	Procesador: Doble núcleo 2GHz o superior
	Memoria: 2GB o superior Disco duro: 10GB o superior
Servidor web	Apache HTTP Server 2.0 o superior
Contenedor web JavaEE	Apache Tomcat 7.0
Máquina virtual Java	Java Development Kit (JDK) versión 6

RESULTADOS DE LA EVALUACIÓN

El producto **eSigna Crypto** versión **2.1.1** ha sido evaluado en base a la declaración de seguridad "**eSigna Crypto 2.1.1 – Declaración de Seguridad**", versión 1.9 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:

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

- Durante la instalación del producto, es necesario prestar especial atención a la preparación del entorno del TOE, tal y como se indica en la "guía preparativa". El sistema Windows XP con aplicación en Kiosko, en conjunción con el cifrado del disco, 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 **eSigna Crypto** versión **2.1.1**, 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
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:

“eSigna Crypto 2.1.1 – Declaración de Seguridad”, versión 1.9 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