REF:	2008-17-INF-333 v1	Creado:	CERT2
Difusión:	Expediente	Revisado:	TECNICO
Fecha:	23.02.2009	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2008-17
Datos del solicitante: A24530735 INTECO

Referencias: EXT-622 Solicitud de Certificación del PP4 SCVA DNIE.
EXT-698 Informe de Evaluación, ETRINTE004 M1, 11/11/2008.
CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.

Informe de certificación del perfil de protección “PPSCVA-T2, EAL3. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL3”, según la solicitud de referencia [EXT-622], de fecha 04/07/2008, y evaluado por el laboratorio LGAI-APPLUS, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-698] de acuerdo a [CCRA], recibido el pasado 11/11/2008.

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 perfil de protección PPSCVA-T2-EAL3 v2.0 para aplicaciones del DNIe.

Este Perfil de Protección (PP) especifica los requisitos de seguridad para las aplicaciones de creación y verificación de firma electrónica (SCVA), que se deben usar con el DNI-e como dispositivo seguro de creación de firma (SSCD).

La SCVA y el SSCD son los "medios que el firmante debe mantener bajo su control exclusivo", tal como requieren la Directiva y la Ley 59/2003 para la consideración de la firma electrónica como avanzada. Utilizando un SSCD, las aplicaciones que cumplan con este Perfil de Protección permiten crear y verificar firmas electrónicas reconocidas.

Este PP corresponde a implementaciones de la SCVA, donde el fabricante opta por utilizar una plataforma de propósito general (por ejemplo, un ordenador personal con un sistema operativo de propósito general), y este tipo de implementación se denomina "SCVA - Tipo 2".

Otros PPs, el PPSCVA-T1-EAL1 y EAL3, suponen que la SCVA incluye todo el hardware, firmware y software necesarios para facilitar la funcionalidad requerida, incluyendo el interfaz con el firmante. Este modelo de aplicación se denomina "SCVA - Tipo 1".

Fabricante: INTECO.

Patrocinador: INTECO.

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

Laboratorio de Evaluación: LGAI-APPLUS.

Perfil de Protección: PPSCVA-T2-EAL3 v2.0.

Nivel de Evaluación declarado por el PP: CC v3.1 EAL3.

Fecha de término de la evaluación: 11-11-2008.

Todos los componentes de garantía requeridos por la actividad de evaluación APE (Evaluación de Perfiles de Protección) presentan el veredicto de "PASA". Por consiguiente, el laboratorio LGAI-APPLUS asigna el VEREDICTO de "PASA" a toda

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

la evaluación por satisfacer todas las acciones del evaluador para APE, 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 perfil de protección PPSCVA-T2-EAL3 v2.0, se propone la resolución estimatoria de la misma.

Resumen del TOE

El Objeto a Evaluar (OE), es un perfil de protección (PPSCVA-T2-EAL3) que especifica los requisitos de seguridad para las aplicaciones de creación y verificación de firma electrónica (SCVA) de Tipo 2, que se deben usar con el DNI-e como dispositivo seguro de creación de firma (SSCD), hasta nivel EAL3.

Este PP no supone que la SCVA incluye todo el hardware, firmware y software necesarios para facilitar la funcionalidad requerida, incluyendo el interfaz con el firmante. Este modelo de aplicación se denomina “SCVA - Tipo 2”.

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

• la capacidad de seleccionar un documento para firmar (SD);

• la capacidad de seleccionar la política de firma a aplicar, los atributos de la firma, y el certificado a utilizar para la firma, y componer los DTBS;

• la capacidad de 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;

• la capacidad de 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;

• la capacidad de asociar la firma electrónica creada por el SSCD al propio documento firmado, o de facilitar la firma realizada como datos separados;

• la capacidad de 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);

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

• 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 firmas válidas e inválidas, cuando el proceso de verificación ha podido realizarse, e identificará las firmas que no han podido verificarse.

Las comunicaciones entre la “SCVA - Tipo 1” y el DNI-e se suponen securizadas por la propia “SCVA - Tipo 1”, cumpliendo además con los requisitos exigibles por el Perfil de Protección CWA 14169 que se aplica al DNI-e .

Las comunicaciones entre una “SCVA - Tipo 2” y el DNI-e requieren de la colaboración del entorno. En esta configuración, es importante la securización de las comunicaciones entre el DNI-e y la SCVA, tal como requiere de nuevo el Perfil de Protección CWA 14169.

Requisitos de garantía de seguridad

El perfil de protección se evaluó con todas las evidencias necesarias para la satisfacción de la actividad de evaluación APE (Evaluación de Perfiles de Protección), según la parte 3 de CC v3.1 R2.

APE_INT.1 PP Introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

Los productos para los que es aplicable este perfil de protección se espera que cumplan con los requisitos de garantía de seguridad correspondientes al nivel **EAL3** de CC v3.1 R2.

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto objeto de este perfil de protección propone la satisfacción de los requisitos funcionales, según la parte 2 de CC v3.1 R2, siguientes:

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

FDP_SDI.2	Stored data integrity monitoring and action
FTP_ITC.1.UD	Inter-TSF trusted channel
FTP_ITC.1.VAD	Inter-TSF trusted channel/VAD
FPT_TST.1	TSF testing
FDP_RIP.1	Subset residual information protection
FDP_SVR.1	Secure viewer and SCVA interface
FDP_ISD.1	Import of Signer's Document
FDP_ITC.1	Import of user data without security attributes
FCS_COP.1_SIGNATURE_CREATION_PROCESS	Cryptographic operation
FCS_COP.1_SIGNATURE_VERIFICATION	Cryptographic operation

Donde son componentes extendidos a la P2 de CC v3.1 R2 los siguientes:

FDP_SVR.1	Secure viewer and SCVA interface
FDP_ISD.1	Import of Signer's Document

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

Identificación

Perfil de Protección: PPSCVA-T2-EAL3 v2.0. “PPSCVA-T2, EAL3. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL3”.

Nivel de Evaluación declarado por el PP: Es conforme al nivel de evaluación EAL3, tal como define CC en su parte 3.

Conformidad respecto a otros PP: Este PP no declara el cumplimiento de ningún otro PP.

Declaraciones de conformidad con respecto a este PP: Este PP requiere que la conformidad al mismo se declare de manera demostrable, tal como se define en la norma CC.

Política de seguridad

El uso del perfil de protección, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

En síntesis, se establece la necesidad de implementar políticas organizativas relativas a:

Dispositivo Seguro de Creación de Firma - P.SSCD;

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

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 DNI-e.

Protección de Datos de Carácter Personal - P.LOPD;

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

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

AS.ITENV; Entorno de computación.

La plataforma de propósito general que la "SCVA - Tipo 2" necesite para operar y para facilitar los interfaces de firmante y con el **¡Error! No se encuentra el origen de la referencia.**, facilita las protecciones y mecanismos de seguridad adecuados para proteger los activos de la SCVA.

Esto implica que las vulnerabilidades que sean eficaces a través del entorno de uso de la SCVA, pero que no explotan una vulnerabilidad propia de la construcción u operación de la SCVA, no se consideran que afecten a la certificación de la misma, sino que deben resolverse mediante la configuración y uso de un entorno adecuado para la misma. Cómo configurar una plataforma de propósito general de manera que no presente formas de ataque a los activos de la SCVA es una tarea ardua, fuera del alcance de este PP.

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para los productos que sean conformes con este perfil de protección, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a "Basic" de EAL3 (AVA_VAN.2), y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el certificado y el resultado de la evaluación de las propiedades de un producto conforme sólo a este perfil de protección, no garantizan resistencia alguna.

Amenazas cubiertas por el perfil de protección:

• **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, se firma de manera inadvertida.

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.

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

• **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.

• **T.VAD**;

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

• **T.ARC**;

Dado que el TOE no identifica ni autentica usuarios, un atacante puede violar los mecanismos implementados de autoprotección, separación de dominios y defensa frente a las amenazas definidas para el mantenimiento del la integridad y confidencialidad de los activos a proteger por la SCVA

Funcionalidad del entorno.

El perfil de protección 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:

• **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, mediante una combinación eficaz de medidas de índole técnico, de procedimientos y de securización de su entorno.

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

Arquitectura

Este Perfil de Protección (PP) especifica requisitos de seguridad para productos tipo aplicaciones de creación y verificación de firma electrónica (SCVA), que se deben usar con el DNI-e como dispositivo seguro de creación de firma (SSCD).

La SCVA y el SSCD son los "medios que el firmante debe mantener bajo su control exclusivo", tal como requieren la Directiva y la Ley 59/2003 para la consideración de la firma electrónica como avanzada. Utilizando un SSCD, las aplicaciones que cumplan con este Perfil de Protección permiten crear y verificar firmas electrónicas reconocidas.

Este PP no supone que la SCVA incluye todo el hardware, firmware y software necesarios para facilitar la funcionalidad requerida, incluyendo el interfaz con el firmante. Este modelo de aplicación se denomina "SCVA - Tipo 2". Si hiciera esta hipótesis e incluyera todo lo demás estaríamos en una "SCVA - Tipo 1".

En la implementación de la SCVA, algunos fabricantes pueden optar por utilizar una plataforma de propósito general (por ejemplo, un ordenador personal con un sistema operativo de propósito general), y este tipo de implementación se denomina "SCVA - Tipo 2".

La arquitectura básica de este tipo de productos se muestra en las siguientes figuras.

Figura 1 - SCVA - Tipo 1

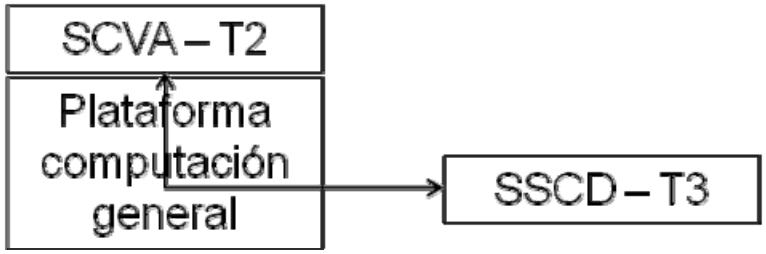

Figura 2 - SCVA - Tipo 2

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 perfil de protección sólo consta de un documento que se indica a continuación.

PPSCVA-T2-EAL3 v2.0. " PPSCVA-T2, EAL3. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL3".

Pruebas del producto

No aplica.

Configuración evaluada

En la evaluación del perfil de protección PPSCVA-T2-EAL3 se utilizaron diversas configuraciones, siendo la única que finalmente obtuvo el veredicto PASA en todas la actividad APE la PPSCVA-T2-EAL3 v2.0. "PPSCVA-T2, EAL3. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL3".

Cabe destacar que aunque el Informe Técnico de Evaluación final hace referencia a la v1.4 del PP, posteriormente a este informe se generó por el desarrollador una versión 2.0 que corregía aspectos menores ortográficos. Esta nueva versión fue también remitida al laboratorio y estas diferencias fueron corroboradas positivamente por lo que se consideran aplicables todas las conclusiones del informe de evaluación a esta última versión.

Resultados de la Evaluación

El objeto de esta evaluación ha sido el PPSCVA-T2-EAL3 v2.0. "PPSCVA-T2, EAL3. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL3".

Todos los componentes de garantía requeridos por la actividad de evaluación **APE** (Evaluación de Perfiles de Protección) presentan el veredicto de "PASA". Por consiguiente, el laboratorio LGAI-APPLUS asigna el **VEREDICTO de "PASA"** a toda la evaluación por satisfacer todas las acciones del evaluador definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 R2.

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

Recomendaciones y comentarios de los evaluadores

No hay recomendaciones adicionales por parte de los evaluadores.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del perfil de protección PPSCVA-T2-EAL3 v2.0. “PPSCVA-T2, EAL3. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, con nivel de evaluación de los requisitos de seguridad EAL3”, se propone la resolución estimatoria de la misma.

Glosario de términos

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ETR	Evaluation Technical Report
OC	Organismo de Certificación
DTBS	Datos a ser firmados
SCD	Datos de creación de firma
VAD	Datos de verificación de autenticación
SVD	Datos de verificación de firma
SSCD	Dispositivo seguro de creación de firma
SD	Documento del Firmante
SDO	Objeto de datos firmados
SCVA	Aplicaciones de creación y verificación de firma electrónica

Bibliografía

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC31p1] Common Criteria for Information Technology Security Evaluation.
Part 1: Introduction and general model. Version 3.1 R1. September 2006.

[CC31p2] Common Criteria for Information Technology Security Evaluation.
Part 2: Security Functional Components Version 3.1 R2. September 2007.

[CC31p3] Common Criteria for Information Technology Security Evaluation.
Part 3: Security Assurance Components Version 3.1 R2. September 2007.

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

[CEM31] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology Version 3.1 R2. September 2007.

Declaración de seguridad

No aplica.

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