REF:	2004-4-INF-148 v2	Creado:	CERT2
Difusión:	Público	Revisado:	TECNICO
Fecha:	30.07.2007	Aprobado:	JEFEAREA

INFORME DE CERTIFICACION

Expediente: 2004-4 DNIe v1.13

Referencias:

EXT-30	Solicitud de Certificación Tarjeta CERES (DNIe).
EXT-343	Informe Técnico de Evaluación del Producto Tarjeta “DNIe” v1.13 , TFC/TRE/2042/001/INTA/07, CESTI-INTA, ed.1.0, 29/03/2007.
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.
DIRF	Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
CWA14169	"Dispositivos seguros de creación de firma (EAL4+)" v1.05 Tipo 3 - Marzo 2002.

Informe de certificación del producto DNIe (Documento Nacional de Identidad electrónico), versión 1.13, configuraciones DNIe 1.13 A11 H4C34 EXP 1-1 y DNIe 1.13 B11 H4C34 EXP 1-1, según la solicitud de referencia [EXT-30], de fecha 28/07/2004, y evaluado por el laboratorio CESTI-INTA, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-343] de acuerdo a [CCRA], recibido el pasado 04/04/2007.

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

INDICE

RESUMEN **3**
RESUMEN DEL TOE 4
REQUISITOS DE GARANTÍA DE SEGURIDAD 4
REQUISITOS FUNCIONALES DE SEGURIDAD 5
Requisitos expresados conforme a [CWA14169]: *5*
Requisitos adicionales definidos en [CWA14169]: *6*
IDENTIFICACIÓN **7**
POLÍTICA DE SEGURIDAD **7**
HIPÓTESIS Y ENTORNO DE USO **9**
HIPÓTESIS DE USO 9
HIPÓTESIS RELATIVAS AL ENTORNO 9
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS 9
FUNCIONALIDAD DEL ENTORNO 11
ARQUITECTURA **12**
DOCUMENTOS **13**
PRUEBAS DEL PRODUCTO **13**
CONFIGURACIÓN EVALUADA **15**
RESULTADOS DE LA EVALUACIÓN **15**
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES **15**
RECOMENDACIONES DEL CERTIFICADOR **18**
GLOSARIO DE TÉRMINOS **18**
BIBLIOGRAFÍA **19**
DECLARACIÓN DE SEGURIDAD **19**

 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 producto DNIe (Documento Nacional de Identidad electrónico) versión 1.13, configuraciones DNIe 1.13 A11 H4C34 EXP 1-1 y DNIe 1.13 B11 H4C34 EXP 1-1. El producto ha sido desarrollado sobre un circuito integrado para tarjetas inteligentes ST19WL34A, fabricado por ST-Microelectronics y con un Sistema Operativo desarrollado por FNMT-RCM para ser utilizado como soporte del Documento Nacional de Identidad.

Fabricante: FNMT-RCM (Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda).

Patrocinador: FNMT-RCM (Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda).

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

Laboratorio de Evaluación: Centro de Evaluación de la Seguridad de las TI (CESTI), del Instituto Nacional de Técnica Aeroespacial “Esteban Terradas” (INTA).

Perfil de Protección: CWA 14169 "Dispositivos seguros de creación de firma (EAL4+)" v1.05 Tipo 3 - Marzo 2002.

Nivel de Evaluación: EAL4+ (ALC-FLR.1, AVA-MSU.3, AVA-VLA.4).

Fortaleza de las Funciones: nivel Alto (SOF high).

Fecha de término de la evaluación: 29-03-2007.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4+ (aumentado con ALC_FLR.1, AVA_VLA.4, AVA_MSU.3, SOF high) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio CESTI-INTA asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4, definidas por los Criterios Comunes v2.2 [CC-P3] y la Metodología de Evaluación v2.2 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto DNIe versión 1.13 sobre el Circuito Integrado para tarjeta inteligente ST19WL34A, 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 Objeto de Evaluación (OE) es el DNIe (Documento Nacional de Identidad electrónico), versión 1.13, configuraciones DNIe 1.13 A11 H4C34 EXP 1-1 y DNIe 1.13 B11 H4C34 EXP 1-1, desarrollado sobre un circuito integrado para tarjetas inteligentes ST19WL34A, fabricado por ST-Microelectronics y con un Sistema Operativo desarrollado por FNMT-RCM para ser utilizado como soporte del Documento Nacional de Identidad.

El termino Circuito integrado (CI) se utiliza en este documento para referenciar todo el hardware y el firmware sobre el que se apoya el Sistema Operativo. El Circuito Integrado ya se ha evaluado y certificado EAL5+ de acuerdo a los Criterios Comunes, como se demuestra en el documento del IC Çertification Report 2005/40 ST19WL34A microcontroler" y de acuerdo a su Declaración de seguridad "ST19WL34 Security Target", disponibles en el Esquema de Francia.

La tarjeta DNIe es una tarjeta inteligente con capacidades criptográficas. Esta diseñada para ser utilizada dentro de una infraestructura de clave pública en las que se requiera autenticación de una entidad, integridad, confidencialidad de los datos y el no repudio en origen. Manteniendo la información criptográfica sensible interna a la tarjeta y protegiendo su uso mediante control de acceso.

La tarjeta DNIe tiene soporte para biometría mediante algoritmos Match on Card, es decir, la verificación de los datos biométricos frente a los datos de referencia se realiza dentro de la tarjeta. Por tanto, se mantienen los datos biométricos sensibles siempre internos a la tarjeta y su utilización está controlada mediante control de acceso.

Asimismo la tarjeta DNIe proporciona mecanismos fiables para el establecimiento y la gestión de un canal seguro de comunicación entre la tarjeta y el mundo exterior, conforme a la norma CWA 14890-1:2004, que incluye el uso de certificados verificables por la tarjeta, para la autenticación de la entidad externa.

El producto protege frente a las amenazas definidas en el perfil de protección CWA 14169 "Dispositivos seguros de creación de firma (EAL4+)" v1.05 Tipo 3 - Marzo 2002, así como utiliza los objetivos, políticas, entorno, etc. definido por este documento.

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL4, más las requeridas para el componente adicional, ALC_FLR.1, y los aumentos relativos a la ausencia de vulnerabilidades explotables requeridas por el perfil de protección CWA 14169, AVA_MSU.3 y AVA_VLA.4.

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

Clase de requisitos	Componente
Gestión de configuración	ACM AUT.1, ACM CAP.4, ACM SCP.2
Distribución y operación	ADO DEL.2, ADO IGS.1
Desarrollo	ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1
Manuales	AGD ADM.1, AGD USR.1
Ciclo de vida	ALC DVS.1, ALC LCD.1, ALC FLR.1, ALC TAT.1
Pruebas	ATE COV.2, ATE FUN.1, ATE IND.2, ATE DPT.1
Análisis de vulnerabilidades	AVA SOF.1, AVA VLA.4, AVA MSU.3

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface, con la colaboración del entorno, el perfil de protección CWA 14169 "Dispositivos seguros de creación de firma (EAL4+)" v1.05 Tipo 3 - Marzo 2002.

Los requisitos funcionales que satisface el producto son los siguientes:

Requisitos expresados conforme a [CWA14169]:

- Generación de claves criptográficas (FCS_CKM.1
- Destrucción de claves criptográficas (FCS_CKM.4)
- Operación criptográfica (FCS_COP.1)
- Subconjunto de control de acceso (FDP_ACC.1)
- Control de acceso basado en atributos de seguridad (FDP_ACF.1)
- Exportación de datos de usuario sin atributos de seguridad (FDP_ETC.1)
- Importación de datos de usuario sin atributos de seguridad (FDP_ITC.1)
- Protección de la información residual (FDP_RIP.1)
- Acción y supervisión de la integridad de los datos almacenados (FDP_SDI.2)
- Integridad en el intercambio de datos (FDP_UIT.1)
- Manejo de fallos de autenticación (FIA_AFL.1)
- Definición del atributo de usuario (FIA_ATD.1)
- Secuencia de autenticación (FIA_UAU.1)
- Secuencia de identificación (FIA_UID.1)
- Gestión del comportamiento de las funciones de seguridad (FMT_MOF.1)
- Gestión de los atributos de seguridad (FMT_MSA.1)

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

- Atributos de seguridad seguros (FMT_MSA.2)
- Inicialización de atributos (FMT_MSA.3)
- Gestión de datos de TSF (FMT_MTD.1)
- Especificación de funciones administrativas (FMT_SMF.1)
- Roles de seguridad (FMT_SMR.1)
- Pruebas de la máquina abstracta (FPT_AMT.1)
- Emisiones del OE (FPT_EMSEC.1)
- Fallo con preservación del estado seguro (FPT_FLS.1)
- Detección pasiva de ataque físico (FPT_PHP.1)
- Resistencia al ataque físico (FPT_PHP.3)
- Pruebas de TSF (FPT_TST.1)
- Canal confiable inter – TSF (FTP_ITC.1)
- Ruta confiable (FTP_TRP.1)

Requisitos extendidos definidos en [CWA14169]:

- Emisiones del OE (FPT_EMSEC.1)

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

Identificación

Producto: DNIe (Documento Nacional de Identidad electrónico) versión 1.13, configuraciones DNIe 1.13 A11 H4C34 EXP 1-1 y DNIe 1.13 B11 H4C34 EXP 1-1.

Declaración de Seguridad: "Declaración de Seguridad Tarjeta DNIe", versión 1.0 y revisión 6. 22 de marzo de 2007.

Perfil de Protección: CWA 14169 "Dispositivos seguros de creación de firma (EAL4+)" v1.05 Tipo 3 - Marzo 2002.

Nivel de Evaluación: EAL4+ (ALC-FLR.1, AVA-MSU.3, AVA-VLA.4). CC/CEM v2.2.

Fortaleza de las Funciones: nivel Alto (SOF high).

Política de seguridad

El uso del producto DNIe 1.13 como tarjeta inteligente criptográfica a modo de dispositivo seguro de creación de firma electrónica, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de las políticas como dispositivo de firma se encuentra en la declaración de seguridad, y se basan en el perfil de protección antes citado CWA 14169. En síntesis, se establece la necesidad de implementar políticas organizativas relativas a:

P.CSP_Qcert Certificado reconocido

El proveedor de servicios de certificación (CSP) usa una aplicación de generación de certificados (CGA) de confianza para generar el certificado reconocido para los datos de verificación de firma (SVD) generados por el dispositivo seguro de creación de firma (SSCD). Los certificados reconocidos contienen, al menos, los elementos definidos en el anexo I de la Directiva [DIRF], es decir, el nombre del firmante y los SVD que se corresponden con los datos de creación de firma (SCD) implementados en el objeto de evaluación (OE) bajo el único control del firmante. El CSP garantiza que el uso del OE es evidente mediante firmas en el certificado o en otra información públicamente disponible.

P.Qsign Firmas electrónicas reconocidas

El firmante usa un sistema de creación de firma para firmar los datos con firmas electrónicas reconocidas. La aplicación de creación de firma (SCA) presenta los datos a ser firmados (DTBS) al firmante. La firma electrónica reconocida se basa en

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

un certificado reconocido y la crea un dispositivo seguro de creación de firma (SSCD).

P.Sigy_SSCD El objeto de evaluación (OE) como Dispositivo seguro de creación de firma

El objeto de evaluación (OE) almacena los datos de creación de firma (SCD) utilizados para la creación de firma bajo el único control del firmante. Los SCD utilizados para la generación de firma sólo pueden ocurrir prácticamente una vez.

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

Hipótesis y entorno de uso

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la declaración de seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas.

Hipótesis de uso

No se han declarado hipótesis de uso específicas.

Hipótesis relativas al entorno

Ver perfil de protección CWA 14169:

A.CGA Aplicación de generación de certificados de confianza

La aplicación de generación de certificados (CGA) protege la autenticidad del nombre del firmante y de los datos de verificación de firma (SVD) en el certificado reconocido mediante una firma electrónica avanzada del proveedor de servicios de certificación (CSP).

A.SCA Aplicación de creación de firma de confianza

El firmante utiliza sólo una aplicación de creación de firma (SCA) de confianza. La SCA genera y envía la representación de datos a ser firmados (DTBS) de los datos que el firmante quiere firmar con un formato apropiado para que el objeto de evaluación (OE) los firme.

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para el producto DNIe 1.13, aunque los agentes que realicen ataques tengan alto potencial de ataque, 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 resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Amenazas cubiertas: (ver perfil de protección CWA 14169)

T.Hack_Phys Ataques físicos a través de los interfaces del objeto de evaluación (OE)

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

Un atacante interactúa con los interfaces del objeto de evaluación (OE) para explotar vulnerabilidades, dando lugar a compromisos arbitrarios de seguridad. Esta amenaza se dirige a todos los activos.

T.SCD_Divulg Almacenamiento, copia y divulgación de los datos de creación de firma

Un atacante puede almacenar o copiar los datos de creación de firma (SCD) fuera del objeto de evaluación (OE). Un atacante puede divulgar los SCD durante su generación, almacenamiento y uso para la creación de firma en el OE.

T.SCD_Derive Deducción de los datos de creación de firma

Un atacante deduce los datos de creación de firma (SCD) de los datos conocidos públicamente, como los datos de verificación de firma (SVD) que corresponden a los SCD o las firmas creadas por medio de los SCD o cualquier otro dato comunicado fuera del objeto de evaluación (OE), que constituye una amenaza contra la confidencialidad de los SCD.

T.Sig_Forgery Falsificación de la firma electrónica

Un atacante falsifica el objeto de datos firmados, quizás junto con su firma electrónica, creados por el objeto de evaluación (OE) y la violación de la integridad del objeto de datos firmados no es detectable por el firmante o por terceras partes. La firma generada por el OE está sujeta a ataques deliberados realizados por expertos que tienen una capacidad de ataque alta con un conocimiento avanzado de los principios y conceptos de seguridad empleados por el OE.

T.Sig_Repud Repudio de firmas

Si un atacante puede atacar cualquier activo con éxito, entonces el no repudio de la firma electrónica está comprometido. El firmante puede negar haber firmado datos usando los datos de creación de firma (SCD) del objeto de evaluación (OE) bajo su control aun cuando la firma se verifica con éxito con los datos de verificación de firma (SVD) contenidos en su certificado no revocado.

T.SVD_Forgery Falsificación de los datos de verificación de firma

Un atacante falsifica los datos de verificación de firma (SVD) presentados por el objeto de evaluación (OE) a la aplicación de generación de certificados (CGA). Esto da lugar a la pérdida de la integridad de los SVD en el certificado del firmante.

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

T.DTBS_Forgery Falsificación de la representación de datos a ser firmados (DTBS)

Un atacante modifica la representación de datos a ser firmados (DTBS) enviada por la aplicación de creación de firma (SCA). Por consiguiente, la representación de DTBS utilizada por el objeto de evaluación (OE) para firmar no corresponde con los DTBS que el firmante pretende firmar.

T.SigF_Misuse Mal uso de la función de creación de firma del objeto de evaluación (OE)

Un atacante hace mal uso de la función de creación de firma del objeto de evaluación (OE) para crear objeto de datos firmado (SDO) con datos que el firmante no ha decidido firmar. El OE es objeto de ataques deliberados realizados por expertos que tienen una capacidad de ataque alta, con un conocimiento avanzado de los principios y conceptos de seguridad empleados por el OE.

Funcionalidad del entorno.

El producto requiere de la colaboración del entorno para la satisfacción de los requisitos del perfil de protección [CWA14169].

Los requisitos funcionales que se deben satisfacer por el entorno de uso del producto son los siguientes:

Aplicación de generación de certificación (CGA)

- Distribución de claves criptográficas (FCS_CKM.2)
- Acceso a claves criptográficas (FCS_CKM.3)
- Integridad del intercambio de datos (FDP_UIT.1)
- Canal confiable inter – TSF (FTP_ITC.1)

Aplicación de creación de firma (SCA)

- Funcionamiento criptográfico (FCS_COP.1)
- Integridad del intercambio de datos (FDP_UIT.1)
- Canal confiable inter – TSF (FTP_ITC.1)
- Ruta confiable (FTP_TRP.1)

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad), o de los requisitos de seguridad del OE se encuentran en la correspondiente Declaración de Seguridad.

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

Arquitectura

El TOE presenta una arquitectura tradicional de tarjeta inteligente con capacidades criptográficas y multiaplicación, capaz de definir diferentes entornos de operación con su propio servicio de sistema de seguridad.

La arquitectura técnica presenta unas especificaciones estándar basadas en las recomendaciones del grupo de trabajo PC/SC “Interoperability Specification for ICCs and Personal Computer System” versión 1.0 diciembre 1997.

Dentro de la arquitectura se ha incluido también los módulos necesarios para el soporte de funciones biométricas de tipo Match On Card i.e. que los algoritmos de comparación de minucias y las funciones de decisión se ejecutan dentro de la propia arquitectura, y no fuera como ocurre en las arquitecturas llamadas Template On Card.

El sistema operativo del OE tiene una estructura jerárquica y modular, cuyas funciones se agrupan en:

(1) **Inicialización**: mecanismos encargados del arranque e inicialización del sistema operativo, así como de la gestión de las distintas llamadas a comandos y las comprobaciones de arranque necesarias.

(2) **Comandos**: incluye la comprobación, gestión y ejecución de los distintos comandos que se soliciten al sistema operativo, ya sean administrativos, de seguridad o criptográficos. Se cubren las funciones de:

- gestión del sistema de ficheros.
- fases de vida de la tarjeta.
- operaciones criptográficas.
- seguridad del sistema operativo.
- gestión de escritura y lectura binaria de ficheros elementales.
- verificación en la tarjeta de datos biométricos.

(3) **Funciones Auxiliares**: contiene funcionalidad común, requerida por los otros partes del OE para realizar sus respectivas funciones.

(4) **Librerías**: contiene funcionalidad biométrica y funcionalidad para el acceso a los recursos del hardware subyacente.

- Librerías de algoritmos MoC para verificación biométrica.
- Librerías del chip para la interfaz de acceso a los recursos de componente electrónico sobre el que se ejecuta el Sistema Operativo.

 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.

- ST-Microelectronics:

  - Çertification Report 2005/40 ST19WL34A microcontroler. 18/11/2005. Secretaría General de la Defensa Nacional (República Francesa).
  - Declaración de seguridad "ST19WL34 Security Target" (SMD-ST19WL34-ST-05-001-v01.02). ST-Microelectronics.

- FNMT-RCM:

  - “Declaración de Seguridad Tarjeta DNIe” de versión 1.0 y revisión 6, 22/03/2007.
  - “Declaración de Seguridad Tarjeta DNIe” de versión 1.0 y revisión 7, 08/0/2007, correspondiente a la versión pública de la anterior.
  - “Manual de Comandos – Sistema operativo DNIe v1.1”, v1.07, 03/01/2007.
  - “DNI electrónico – Guía de Referencia Básica”, v1.21, 05/02/2007.
  - “Manual de Administrador de la Tarjeta DNIe”, v1.2 , 09/02/2007.
  - “Procedimiento de instalación, generación y puesta en marcha de la tarjeta DNIe”, v1.3, 29/11/2006.

Pruebas del producto

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todos las pruebas ha sido realizados por el fabricante en sus instalaciones con resultado satisfactorio.

El proceso ha verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas acorde a la arquitectura identificada en la declaración de seguridad.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Para verificar los resultados de los las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido entorno a un 25 % de las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más

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

relevantes: funciones de generación de auditoría, funciones criptográficas y funciones de protección de los datos de usuario.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados así obtenidos son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado el evaluador ha constatado que dicha variación no representaba un problema para la seguridad, ni suponía una merma en la capacidad funcional del producto.

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

Configuración evaluada

El producto DNIe puede ser utilizado en varias plataformas y lectores, siempre que satisfagan los requisitos e hipótesis de seguridad ya indicados.

En particular, durante la evaluación se han utilizado:

- Tarjetas DNIe (Muestras del OE en diferentes estados y fases).

- Lectores/grabadores de tarjetas inteligentes (tipo PC/SC - LTC31 de C3PO- y tipo Phoenix).

- Lector de Huellas biométricas CROSS MATCH Verifier 300, LCD 3.0, USB 2.0.

- Ordenadores tipo PC, para ejecutar el software de pruebas (con sistema operativoWindows 2000 Second Edition, Windows XP SP2, Linux Debian).

- Emulador de las tarjetas distribuido por ST-Microelectronics.

- Software de pruebas de ST-Microelectronics y de la FNMT-RCM.

- Diverso software y otros instrumentos de medida hardware auxiliares, y que no se corresponden con una aplicación de generación de certificados (CGA). No forma parte de esta evaluación la identificación de un entorno de uso de la tarjeta que pueda considerarse como una aplicación de generación de certificados (CGA) en el sentido del Perfil de Protección CWA 14169.

Resultados de la Evaluación

El producto DNIe 1.13 sobre el Circuito Integrado para tarjeta inteligente ST19WL34A ha sido evaluado frente a la declaración de seguridad “Declaración de Seguridad Tarjeta DNIe - Version 1 - Revision 6”, de fecha 22/03/07.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL4+** (aumentado con ALC_FLR.1, AVA_VLA.4, AVA_MSU.3, SOF high) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio CESTI-INTA asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 2.2.

Recomendaciones y comentarios de los evaluadores

Para llevar a cabo el análisis independiente de vulnerabilidades y otros aspectos básicos de la evaluación se han utilizado los documentos de referencia para este

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

tipo de tecnología proporcionados por los grupos de trabajo asociados de la ISCI (International Security Certification Initiative) y JIL (Joint Interpretation Library):

- ISCI/WG2 Attack Methods Description.
- Introduction to Differential Power Analysis and Related Attacks. P. Kocher, J. Jaffe, B. Jun, Cryptographic Research, Inc.,San Francisco 1998.
- Requirements to perform Integrated Circuit Evaluations, Annex A: Examples for Smartcard Specific Attacks. Version 1.1, July 2003. Joint Interpretation Library.
- Application of attack potential to smart-cards, v2.2, January 2007. CC Supporting document.
- Attack Methods for Smartcard and similar devices, v 1.2. January 2007. CC Supporting document.

A continuación se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

1. **Identificación del OE evaluado**.

Para identificar que una tarjeta Tarjeta "DNIe"v 1.13 es la versión evaluada se debe ejecutar los dos procedimientos que a continuación se detalla. La tarjeta devolverá una respuesta en función de la configuración biométrica que tenga configurada DNIe 1.13 A11 H4C34 EXP 1-1 y DNIe 1.13 B11 H4C34 EXP 1-1.

A continuación se detallan los dos pasos a realizar:

a) Hacer un reset de la tarjeta para solicitar el ATR Enviar comando: ATR
respuesta tarjeta biometría de SAGEM:
3B 7F 38 00 00 00 6A 44 4E 49 65 10 02 4C 34 01 13 03 90 00
respuesta tarjeta biometría de SIEMENS:
3B 7F 38 00 00 00 6A 44 4E 49 65 20 02 4C 34 01 13 03 90 00

b) Leer el contenido del fichero ’2F03’ donde se guarda la identificación de la versión de la tarjeta que se corresponderá con una de las configuraciones evaluadas: DNIe 1.13 A11 H4C34 EXP 1-1 y DNIe 1.13 B11 H4C34 EXP 1-1. Para leer el contenido del fichero se deben realizar varios pasos, primero se selecciona el fichero y a continuación se lee su contenido. Los comandos a enviar a la tarjeta son los siguientes:

Enviar comando: 00 a4 00 00 02 2f 03
respuesta tarjeta: 61 0e
Enviar comando: 00 c0 00 00 0e
respuesta tarjeta: 6f 0c 85 0a 01 2f 03 00 28 00 80 ff ff ff 90 00
Enviar comando: 00 b0 00 00 28

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

respuesta tarjeta biometría de SAGEM:
44 4e 49 65 20 30 31 2e 31 33 20 41 31 31 20 48 20 34 43 33 34 20 45 58
50 20 31 2d 31 00 00 00 00 00 00 00 00 00 00 00 90 00
(La respuesta se corresponde con los caracteres en ASCII del id del SW:
"DNIe 01.13 A11 H 4C34 EXP 1-1")

respuesta tarjeta biometría de SIEMENS:
44 4e 49 65 20 30 31 2e 31 33 20 42 31 31 20 48 20 34 43 33 34 20 45 58
50 20 31 2d 31 00 00 00 00 00 00 00 00 00 00 00 90 00
(La respuesta se corresponde con los caracteres en ASCII del id del SW:
"DNIe 01.13 B11 H 4C34 EXP 1-1")

2. **Verificación de la fase de vida de la tarjeta**.

Para poder realizar las operaciones de firma se verificará que la tarjeta está en la fase de vida adecuada.

Fase de usuario, para realizar las funcionalidades de firma, o fase Final, si por errores internos la tarjeta no permite realizar la funcionalidades de firma asociadas.

Para identificar la fase de la tarjeta, se realizará un análisis del ATR de la tarjeta, el antepenúltimo byte de la respuesta del ATR será: "03"Fase usuario o "04"Fase Final. A continuación se detalla los pasos a realizar y las respuestas en función de las diferentes biometrías:

Hacer un reset de la tarjeta para solicitar el ATR
Enviar comando: ATR

respuesta tarjeta biometría de SAGEM:
3B 7F 38 00 00 00 6A 44 4E 49 65 10 02 4C 34 01 13 XX 90 00

respuesta tarjeta biometría de SIEMENS:
3B 7F 38 00 00 00 6A 44 4E 49 65 20 02 4C 34 01 13 XX 90 00

Los bytes marcados con "XX"serán: "03"si la tarjeta se encuentra en Fase de Usuario o "04"si la tarjeta está en Fase Final.

3. Para un uso seguro del OE, debe tenerse en cuenta el cumplimiento de las **suposiciones de seguridad del entorno**. Estas suposiciones se encuentran recogidas en Declaración de Seguridad DNIe - versión 1 Revisión 6 sección 3.2 "Entorno de Seguridad del OE: Hipótesis 2 en CWA 14169: Secure Signature-Creation Devices "EAL4+"Level 3 14169:2002 E March 2002 sección 3.1 "TOE Security Environment: Assumptions".

4. Para un uso seguro del OE, debe tenerse en cuenta el cumplimiento de los **objetivos de seguridad del entorno**. Estos objetivos se encuentran recogidos en

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

Declaración de Seguridad DNIe - versión 1 Revisión 6 sección 4.2 .Objetivos de Seguridad aplicables al Entorno 2 en CWA 14169: Secure Signature-Creation Devices "EAL4+"Level 3 14169:2002 E March 2002 sección 4.2 "Security Objetives for the Environment".

5. Para un uso seguro del OE, debe tenerse en cuenta el cumplimiento de los **requisitos de seguridad del entorno TI**. Estos requisitos se encuentran recogidos en Declaración de Seguridad DNIe – versión 1 Revisión 6 sección 5.2 Requisitos de Seguridad aplicables al Entorno 2 en CWA 14169: Secure Signature-Creation Devices "EAL4+"Level 3 14169:2002 E March 2002 sección 5.3 "Security Requirements for the IT Environment".

6. Es recomendable que el usuario **modifique las claves de acceso** entregadas en el proceso de expedición, por unas claves personales sólo conocidas por él. Se recomienda que la clave sea del máximo número de caracteres posibles (16 bytes) y contenga caracteres alfanuméricos. (letras, números, signos de puntuación,... etc).

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto DNIe versión 1.13, configuraciones DNIe 1.13 A11 H4C34 EXP 1-1 y DNIe 1.13 B11 H4C34 EXP 1-1, sobre el Circuito Integrado para tarjeta inteligente ST19WL34A, se propone la resolución estimatoria de la misma.

Glosario de términos

APDU - Application Protocol Data Unit
CCA - Cipher Creation Application
CGA - Certificate Generation Application
CI - Circuito Integrado
DTBS - Data To Be Signed
EAL - Evaluation assurance level
SCA - Signature Creation Application
SCD - Signature Creation Device
SSCD - Secure Signature Creation Device
SVD - Signature Verification Data

 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 2.2, rev 326, December 2004.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, rev 326, December 2004.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2, rev 326, December 2004.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 2.2, rev 326, December 2004.

[AIS-34] AIS-34, Evaluation Methodology for CC Assurance classes for EAL5+ v1.0 1-june-2004 BSI.

[CWA14169] Anexo C de la CWA 14169:2002. Protection Profile – Secure Signature-Creation Device, Type 3, version 1.05 (Perfil de Protección – Dispositivo Seguro de Creación de Firma).

Declaración de seguridad

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación de la declaración de seguridad completa de la evaluación: **“Declaración de Seguridad Tarjeta DNIe - Version 1 - Revision 6”, de fecha 22/03/07**.

La versión ***pública*** que se hace disponible por medio de la página web del OC http://www.oc.ccn.cni.es, es la **“Declaración de Seguridad Tarjeta DNIe - Version 1 - Revision 7”, de fecha 08/05/07**. Esta declaración de seguridad corresponde a la versión completa de la evaluación, pero sin la información de diseño interno sensible para el fabricante, y sin perjuicio de permitir conocer las propiedades de seguridad del TOE o del alcance de la evaluación efectuada.

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