REF:	2006-1-INF-311 v1	Creado:	TECNICO
Difusión:	Expediente	Revisado:	TECNICO
Fecha:	28.10.2008	Aprobado:	JEFEAREA

INFORME DE CERTIFICACION

Expediente: 2006-1
Datos del solicitante: A28704542 SERMEPA

Referencias:

EXT-150	Solicitud de Certificación Tarjeta Advantis Crypto, 09/05/06.
EXT-656	Informe Técnico de Evaluación del Producto Advantis Crypto v3.1, ETRSERM001 M2, LGAI-APPLUS, 04/08/08.
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).

Informe de Certificación del producto tarjeta Advantis Crypto v3.1 de la empresa Servicios para Medios de Pago S.A. (SERMEPA), compuesto sobre el Circuito Integrado para tarjeta inteligente SLE66CX80PE de Infineon AG Technologies, según la solicitud de referencia [EXT-150], de fecha 09/05/06, y evaluado por el laboratorio LGAI-APPLUS, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-656] de acuerdo a [CCRA], emitido el pasado 04/08/08.

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 producto tarjeta Advantis Crypto v3.1 de la empresa Servicios para Medios de Pago S.A. (SERMEPA), una tarjeta inteligente con capacidad criptográfica. Es una tarjeta multi-aplicación capaz de definir diferentes entornos de operación con su propio servicio de sistema de seguridad.

Fabricante: Servicios para Medios de Pago S.A. (SERMEPA).
C/ López Hoyos, 151. 28002 Madrid. España.

Patrocinador: Servicios para Medios de Pago S.A. (SERMEPA).

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

Laboratorio de Evaluación: LGAI-APPLUS.

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

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

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

Fecha de término de la evaluación: 04-08-2008.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4+ (aumentado con AVA_VLA.4, AVA_MSU.3, SOF high) 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 a nivel EAL4, definidas por los Criterios Comunes v2.3 [CC-P3] y la Metodología de Evaluación v2.3 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Advantis Crypto v3.1 sobre el Circuito Integrado para tarjeta inteligente SLE66CX80PE de Infineon AG Technologies, 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 la tarjeta Advantis Crypto v3.1 de la empresa Servicios para Medios de Pago S.A. (SERMEPA), una tarjeta inteligente con capacidad criptográfica. Es una tarjeta multi-aplicación capaz de definir diferentes entornos de operación con su propio servicio de sistema de seguridad. Dispone de una estructura jerárquica de ficheros y datos tipo árbol. Las distintas aplicaciones que implementa son:

a) Aplicación VISA/EMV

b) Aplicación propietaria monedero Advantis

c) Aplicación monedero CEPS

d) Aplicación WIM

e) Aplicación propietaria Firma Digital

f) Aplicación Firma Digital CWA14196

La tarjeta Advantis Crypto es por tanto un dispositivo seguro de creación de firma electrónica, y como tal cumple con los requisitos de seguridad aplicables, recogidos en el PP “CWA 14169:2004. Protection Profile – Secure Signature-Creation Device, Type 3, version 1.05”. El alcance de la certificación de esta Declaración de Seguridad se centra en las exigencias de seguridad necesarias para la firma electrónica como dispositivo seguro de creación de firma CWA14196 (a partir de ahora firma digital o firma electrónica), y no abarca otras aplicaciones o configuraciones de la tarjeta, que no forman parte del TOE. Éste se limita a la aplicación de firma digital.

El TOE es un producto compuesto del Sistema Operativo y aplicaciones de de Advantis Crypto sobre el circuito integrado SLE66CX80PE de Infineon AG Technologies. Este circuito dispone de la certificación CC con nivel de garantía EAL5+, satisfaciendo los requisitos expresados en el Perfil de Protección BSI-PP-0002-2001.

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, así como utiliza los objetivos, políticas, entorno, etc. definido por este documento.

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

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL4, 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.

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 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.

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)

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

- 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)
- 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)

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

Identificación

Producto: tarjeta inteligente (smartcard) “Advantis Crypto” versión 3.1.

Declaración de Seguridad: “TI345 ADVANTIS CRYPTO 3.1 – DECLARACIÓN DE SEGURIDAD”, versión 3.6 y revisión 1 del 01/07/08.

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

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

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

Política de seguridad

El uso del TOE 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

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

datos a ser firmados (DTBS) al firmante. La firma electrónica reconocida se basa en 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.

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

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

Las siguientes amenazas no suponen un riesgo explotable para el TOE, 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)

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

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

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.

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)

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

- 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.

Arquitectura

El TOE presenta una arquitectura tradicional de tarjeta inteligente con capacidades criptográficas y multi-aplicación, capaz de definir diferentes entornos de operación con su propio servicio de sistema de seguridad. Dispone de una estructura jerárquica de ficheros y datos tipo árbol. Las distintas aplicaciones que implementa son:

a) Aplicación VISA/EMV

b) Aplicación propietaria monedero Advantis

c) Aplicación monedero CEPS

d) Aplicación WIM

e) Aplicación propietaria Firma Digital

f) Aplicación Firma Digital CWA14196

La tarjeta Advantis Crypto es por tanto un dispositivo seguro de creación de firma electrónica, y como tal cumple con los requisitos de seguridad aplicables, recogidos en el PP “CWA 14169:2004. Protection Profile – Secure Signature-Creation Device, Type 3, version 1.05”. El alcance de la certificación de esta Declaración de Seguridad se centra en las exigencias de seguridad necesarias para la firma electrónica como dispositivo seguro de creación de firma CWA14196 (a partir de ahora firma digital o firma electrónica), y no abarca otras aplicaciones o configuraciones de la tarjeta, que no forman parte del TOE. Éste se limita a la aplicación de firma digital.

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

El sistema operativo o máscara Advantis Crypto constituye el código que el fabricante del componente incluye en el mismo. El sistema operativo define el funcionamiento de la tarjeta en los siguientes ámbitos:

1. Gestión de memoria: el sistema operativo predetermina y gestiona la disposición lógica y física de memoria EEPROM. Con ello, ofrece a los emisores de aplicaciones estructuras definidas de memoria a las que se pueden añadir las condiciones de acceso necesarias en función de la política de seguridad de sus aplicaciones. El sistema operativo gestiona la memoria a través de estructuras TLV, que deben codificarse de acuerdo con las reglas de codificación de estructuras BER-TLV, con etiquetas y longitudes de 1 ó 2 bytes únicamente.

2. Seguridad: el sistema operativo incluye diversos procedimientos criptográficos y las claves secretas asociadas. De esta forma, es posible realizar operaciones protegidas de lectura, escritura y actualización en la memoria de la tarjeta, así como autenticaciones tanto externas como internas. Además, gestiona la verificación de los códigos secretos y certificados utilizados por la aplicación exterior para obtener acceso a la tarjeta.

3. Interfaz de comunicaciones: el sistema operativo dispone de un conjunto definido de comandos y gestiona un protocolo de comunicación estándar, T = 0 (ISO 7816-3)

4. Ciclo de vida de la tarjeta: el sistema operativo gestiona totalmente las diferentes fases en el ciclo de vida de la tarjeta.

El circuito integrado de Infineon AG Technologies sobre el que se implementa el sistema operativo Advantis Crypto es el SLE66CX80PE. Ha superado la evaluación CC alcanzando el nivel de garantía EAL5 +, satisfaciendo los requisitos expresados en el Perfil de Protección BSI-PP-0002-2001. Consta, entre otros, de los siguientes componentes:

- Microprocesador (CPU)
- Unidad de Gestión de la Memoria (MMU)
- Diferentes clases de memoria
- Seguridad lógica
- Timer
- Interfaz de entrada/salida controlado por interrupciones
- Generador de número aleatorio (RNG)

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

- Módulo CRC (checksum)
- Unidad criptográfica (ACE)

Incluye también la criptolibrería RSA2048 cryptolibrary y los componentes firmware RMS y STS.

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, así como utiliza los objetivos, políticas, entorno, etc. definido por este documento.

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.

- **Infineon AG Technologies**:

- BSI-DSZ-CC-0344-2005 – Infineon Smartcard IC (Security Controller) SLE66CX162PE/m1531-a24 and SLE66CX80PE/m1533-a24 both with RSA2048 v1.4 and specific IC dedicated Software.
- BSI-DSZ-CC-0344-2005-MA-01-Mantenance report– Infineon Smartcard IC (Security Controller) SLE66CX162PE/m1531-a24 and SLE66CX80PE/m1533-a24 both with RSA2048 v1.4 and specific IC dedicated Software.
- BSI-DSZ-CC-0344-2005-MA-02-Mantenance report– Infineon Smartcard IC (Security Controller) SLE66CX162PE/m1531-a24 and SLE66CX80PE/m1533-a24 both with RSA2048 v1.4 and specific IC dedicated Software

- **SERMEPA**:

- “TI345 Advantis Crypto 3.1 - Declaración de Seguridad”, versión 3.6 y revisión 1, 01/07/08.
- “TI317 Manual de usuario Advantis Crypto”, v3.3, 23/04/08.
- “TI421 Manual de mantenimiento de tarjetas”, v1.0, 26/03/08.
- “TI431 Manual de usuario final del dispositivo de firma electrónica Advantis Crypto”, v1.0, 04/02/08.
- “TI348 Aplicación de firma digital CWA 14169”, v2.4, 30/05/08
- “TI407 Medidas generales de seguridad para el usuario de tarjeta advantis crypto como dispositivo de firma electrónica”, v1.1, 04/07/07.
- “TI200Manual de prepersonalización: Advantis y Advantis Crypto”, v3.2, 29/01/08.

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

- "TI201 Manual de prepersonalización: Advantis y Advantis Crypto", v2.2, 05/01/08.

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 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.

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

Configuración evaluada

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

La versión que finalmente ha superado la evaluación y que se propone para su certificación es la **Advantis Crypto v3.1**.

El alcance de la certificación de la Declaración de Seguridad se centra en las exigencias de seguridad necesarias para la firma electrónica como dispositivo seguro de creación de firma CWA14196 (a partir de ahora firma digital o firma electrónica), y no abarca otras aplicaciones o configuraciones de la tarjeta, que no forman parte del TOE. Éste se limita a la aplicación de firma digital.

En particular, durante la evaluación se han utilizado:

- Tarjetas Advantis Crypto (Muestras del TOE en diferentes estados y fases).

- Lectores/grabadores de tarjetas inteligentes (tipo PC/SC).

- Ordenadores tipo PC, para ejecutar el software de pruebas.

- Emuladores y software de pruebas del fabricante de Infineon y SERMEPA.

- Diverso software y otros instrumentos de medida hardware auxiliares para la generación de certificados digitales de prueba.

- Equipos hardware y software especializados para pruebas de penetración a circuitos integrados y tarjetas inteligentes.

Resultados de la Evaluación

El producto Advantis Crypto v3.1 de la empresa Servicios para Medios de Pago S.A. (SERMEPA) sobre el Circuito Integrado para tarjeta inteligente SLE66CX80PE de Infineon AG Technologies ha sido evaluado frente a la declaración de seguridad “TI345 ADVANTIS CRYPTO 3.1 – DECLARACIÓN DE SEGURIDAD”, versión 3.6 y revisión 1 del 01/07/08.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL4+** (aumentado con AVA_VLA.4, AVA_MSU.3, SOF high) 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 a nivel

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

EAL4, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 2.3.

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

- Application of attack potential to smart-cards, v2.3, April 2007. CC Supporting document. CCDB-2007-04-001.
- Smartcard Evaluation Guidance, v1.3, March 2006. CC Supporting document. CCDB-2006-04-001.
- Attack Methods for Smartcard and similar devices, v1.2. January 2007. CC Supporting document.
- ETR-lite for Composition, v1.3, April 2006. CCDB-2006-04-005.
- The Application of CC to Integrate Circuits, v2.0, April 2006, CCDB-2006-04-003.

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. La configuración del Tarjeta inteligente Advantis Crypto Versión 3.1 es la definida en el TI348, en la cual se define un escenario con un sistema de fichero: MF (master file) → DFA (aplicación de firma electrónica CWA) -> Un EF [ID 01 01: Fichero de clave privada de Longitud BYTEs (300 a 700 dependiendo de la longitud de clave 768 a 1984) y un EF [ID 03 01: Fichero del Certificado]. Además se pueden crear distintos directorios DFA, todos ellos con la estructura de diferentes clave privada más certificado.

2. La guía de administración describen cómo configurar de manera segura el TOE en el entorno operacional de uso, teniendo en cuenta las hipótesis (aplicación de generación de certificados y creación de firma confiables). La guía de usuario describe cómo usar de manera segura el TOE en el entorno operacional.

3. Para un uso seguro del TOE, debe tenerse en cuenta el cumplimiento de las suposiciones de seguridad del entorno. Estas suposiciones se encuentran recogidas en la Declaración de Seguridad y corresponden a las del [CWA14169].

4. Para un uso seguro del TOE, debe tenerse en cuenta el cumplimiento de los objetivos de seguridad del entorno. Estos objetivos se encuentran recogidos en la Declaración de Seguridad y corresponden a las del [CWA14169].

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

5. Para un uso seguro del TOE, debe tenerse en cuenta el cumplimiento de los requisitos de seguridad del entorno TI. Estos requisitos se encuentran recogidos en la Declaración de Seguridad y corresponden a las del [CWA14169].

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Advantis Crypto versión 3.1, sobre el Circuito Integrado para tarjeta inteligente SLE66CX80PE de Infineon AG Technologies, 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

ENAC CERTIFICACIÓN Nº 45/C-PR110
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 2.3, August 2005.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.3, August 2005.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 2.3, August 2005.

[CWA14169] Anexo C de la CWA 14169 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: **"TI345 ADVANTIS CRYPTO 3.1 – DECLARACIÓN DE SEGURIDAD", versión 3.6 y revisión 1 del 01/07/08**.

La versión ***pública*** que se hace disponible por medio de la página web del OC http://www.oc.ccn.cni.es, es la **"TI345 ADVANTIS CRYPTO 3.1 – DECLARACIÓN DE SEGURIDAD", versión 1.2 del 18/08/08**. 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.

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