Referencia: 2017-26-INF-2389-v1
Difusión: Público
Fecha: 15.06.2018

Creado por: CERT11
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2017-26**
TOE	**DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0**
Solicitante	**Q2826004J - Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda**

Referencias

[EXT-3475] 2017-26 Solicitud de Certificación

[EXT-4006] Informe Técnico de Evaluación de DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0

Informe de Certificación del producto DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0, según la solicitud de referencia [EXT-3475], de fecha 14/07/2017, evaluado por el laboratorio Applus Laboratories, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-4006], recibido el pasado 18/05/2018.

Este expediente es un expediente de re-certificación sobre el expediente 2014-39 según lo definido en el documento de apoyo [AC] y teniendo en cuenta el informe [IAR] en [EXT-3475].

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0.

El TOE es una tarjeta inteligente con capacidad criptográfica configurada como dispositivo cualificado de creación de firma (QSCD) según lo establecido en el reglamento [eIDAS].

Sus especificaciones técnicas están basadas en normas internacionales sobre tarjetas inteligentes, así como en las recomendaciones del grupo de trabajo [PC/SC]. Es una tarjeta con interfaz dual, lo que permite su uso tanto en modo con contactos como sin contactos, conforme a [ISO7816-3] e [ISO14443] respectivamente.

Fabricante: Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda.

Patrocinador: Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda.

Organismo de Certificación: Centro Criptológico Nacional (CCN).

Laboratorio de Evaluación: Applus Laboratories.

Perfiles de Protección: “Protection profiles for Secure signature creation device - Part 2: Device with key generation”, versión 2.0.1 (EN 419211-2:2013) y “Protection profiles for Secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application”, versión 1.0.1 (EN 419211-5:2013).

Nivel de Evaluación: Common Criteria versión 3.1, revisión 4 - EAL4 + AVA_VAN.5.

Fecha de término de la evaluación: 18/05/2018.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 aumentado con el componente AVA_VAN.5 (*Advanced methodical vulnerability analysis*) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Applus Laboratories asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4 + AVA_VAN.5, definidas por los criterios de evaluación Common Criteria versión 3.1, revisión 4 y Common Methodology for Information Technology Security Evaluation versión 3.1, revisión 4.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

La tarjeta inteligente DNIe-DCCF es una tarjeta multiaplicación capaz de definir diferentes entornos de operación con su propio servicio de sistema de seguridad. Además de la funcionalidad de firma electrónica, el DNIe-DCCF implementa otras funcionalidades que no forman parte del TOE, por ejemplo la función de autenticación del ciudadano.

El TOE proporciona las siguientes funcionalidades de seguridad:

- Generación de datos de creación de firma (SCD) y sus correspondientes datos de validación de firma (SVD).
- Exportación del SVD para su posterior certificación.
- Recibir y almacenar información del certificado.
- Gestionar el ciclo de vida.
- En caso de estar en fase operacional, crear firmas digitales, siguiendo los siguientes pasos:
    - Seleccionar un único SCD en caso de tener múltiples instancias.
    - Recibir los datos a ser firmados (DTBS).
    - Autenticar al firmante.
    - Aplicar la función criptográfica adecuada en el proceso de generación de firma digital.

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 AVA_VAN.5 (Advanced methodical vulnerability analysis), según Common Criteria versión 3.1, revisión 4.

Assurance Class	**Assurance components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model

	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.5 Advanced methodical vulnerability analysis**

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según Common Criteria versión 3.1, revisión 4.

TOE Security Functional Requirements	**Description**
FCS_CKM.1/RSA	Cryptographic key generation - RSA
FCS_CKM.1/DES	Cryptographic key generation - DES
FCS_CKM.1/AES	Cryptographic key generation - AES
FCS_CKM.1/EC	Cryptographic key generation - EC
FCS_CKM.4/RSA	Cryptographic key destruction – RSA
FCS_CKM.4/DES	Cryptographic key destruction – DES
FCS_CKM.4/AES	Cryptographic key destruction – AES
FCS_CKM.4/EC	Cryptographic key destruction – EC

FCS_COP.1/RSA	Cryptographic operation - RSA
FCS_COP.1/DES	Cryptographic operation - DES
FCS_COP.1/AES	Cryptographic operation - AES
FCS_COP.1/SHA	Cryptographic operation - SHA
FCS_COP.1/ECDH	Cryptographic operation - ECDH
FDP_ACC.1/SCD/SVD_Generation	Subset access control -SCD/SVD_Generation
FDP_ACC.1/SVD_Transfer	SCD/SVD_Generation - SVD_Transfer
FDP_ACC.1/Signature_Creation	Subset access control- Signature_Creation
FDP_ACF.1/SCD/SVD_Generation	Security attribute based access control - SCD/SVD_Generation
FDP_ACF.1/SVD_Transfer	Security attribute based access control – SVD Transfer
FDP_ACF.1/Signature_Creation	Security attribute based access control - Signature_Creation
FDP_RIP.1	Subset residual information protection
FDP_SDI.2/Persistent	Stored data integrity monitoring and action - Persistent
FDP_SDI.2/DTBS	Stored data integrity monitoring and action - DBTS
FIA_AFL.1	Authentication failure handling
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1/Admin	Management of security attributes - Admin
FMT_MSA.1/Signatory	Management of security attributes - Signatory
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MSA.4	Security attribute value inheritance
FMT_MTD.1/Admin	Management of TSF data - Admin
FMT_MTD.1/Signatory	Management of TSF data – Signatory

FMT_SMR.1	Security roles
FMT_SMF.1	Specification of Management Functions
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack
FPT_TST.1	TSF testing
FDP_UIT.1/DTBS	Data exchange integrity - DTBS
FTP_ITC.1/VAD	Inter-TSF trusted channel - VAD
FTP_ITC.1/DTBS	Inter-TSF trusted channel - DTBS

IDENTIFICACIÓN

Producto: DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0.

Declaración de Seguridad: Declaración de Seguridad de la tarjeta DNIe-DCCF 3.0, Versión: 1.1 Revisión: 5, de 28 de noviembre de 2017.

Perfiles de Protección: "Protection profiles for Secure signature creation device - Part 2: Device with key generation", versión 2.0.1 (EN 419211-2:2013) y "Protection profiles for Secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application", versión 1.0.1 (EN 419211-5:2013).

Nivel de Evaluación: Common Criteria versión 3.1, revisión 4 - EAL4 + AVA_VAN.5

POLÍTICA DE SEGURIDAD

El uso del producto DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de estas políticas se encuentra en la sección 3.5 de la Declaración de Seguridad [ST].

HIPÓTESIS Y ENTORNO DE USO

Las hipótesis definidas en la declaración de seguridad 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. Por tanto, para garantizar el uso seguro del TOE, se parte de las hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

El detalle de las hipótesis sobre el entorno de uso se encuentra en la sección 3.6 de la Declaración de Seguridad [ST].

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las amenazas definidas en la declaración de seguridad no suponen un riesgo explotable para el producto DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0, aunque los agentes que realicen ataques tengan potencial de ataque Alto correspondiente al nivel de evaluación EAL4 + AVA_VAN.5, 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 la declaración de seguridad, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

El detalle de las amenazas definidas se encuentra en la sección 3.4 de la Declaración de Seguridad [ST].

FUNCIONALIDAD DEL ENTORNO

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

El detalle de los objetivos de seguridad del entorno se encuentra en la sección 4.2 de la Declaración de Seguridad [ST].

Los detalles de la definición de los objetivos de seguridad y de los requisitos de seguridad del TOE se encuentran respectivamente en las secciones 4.1 y 6 de la correspondiente Declaración de Seguridad [ST].

ARQUITECTURA

ARQUITECTURA LÓGICA

La figura de la página siguiente muestra el TOE en su entorno de uso. Este entorno de uso se puede dividir en:

- Entorno de firma, usado por el firmante a través de la aplicación de creación de firma (SCA) para firmar datos previa autenticación del firmante mediante PIN. La SCA proporciona los datos a ser firmados (DTBS) o su representación unívoca (DTBS/R) al TOE para su posterior firma digital. El TOE también provee la funcionalidad para comunicarse con la aplicación de creación de firma (SCA) mediante un canal seguro (con o sin contactos) para asegurar la integridad de los datos a ser firmados (DTBS).
- Entorno preparativo, usado por el proveedor de servicios de certificación, a través de la aplicación de generación de certificados (CGA) para obtener el certificado generado a partir de los datos de validación de firma (SVD) e intrínsecamente correlacionados con los datos de creación de firma (SCD) generados por el TOE.
- Entorno de gestión, dónde el usuario o el proveedor de servicios del dispositivo cualificado de creación de firma (QSCD) puede realizar las operaciones de gestión, ej: resetear el PIN bloqueado, cambiar el código PIN.

El objeto de evaluación almacena los datos de creación de firma (SCD) y los datos de referencia de autenticidad (RAD). El TOE puede contener múltiples instancias del SCD. En este caso el TOE debe proporcionar una función que permita identificar cada SCD y la SCA debe proporcionar una interfaz al firmante para seleccionar el SCD a ser usada en la función de creación de firma.

También protege la confidencialidad del SCD y restringe su uso en la creación de firma al firmante. La firma digital creada con el TOE es una firma electrónica cualificada tal y como define el reglamento [eIDAS] si el certificado para el SVD es un certificado cualificado.

El TOE almacena los datos de referencia de autenticidad (RAD) para autenticar al usuario como firmante. El RAD es una contraseña, ej: PIN y/o BIO.

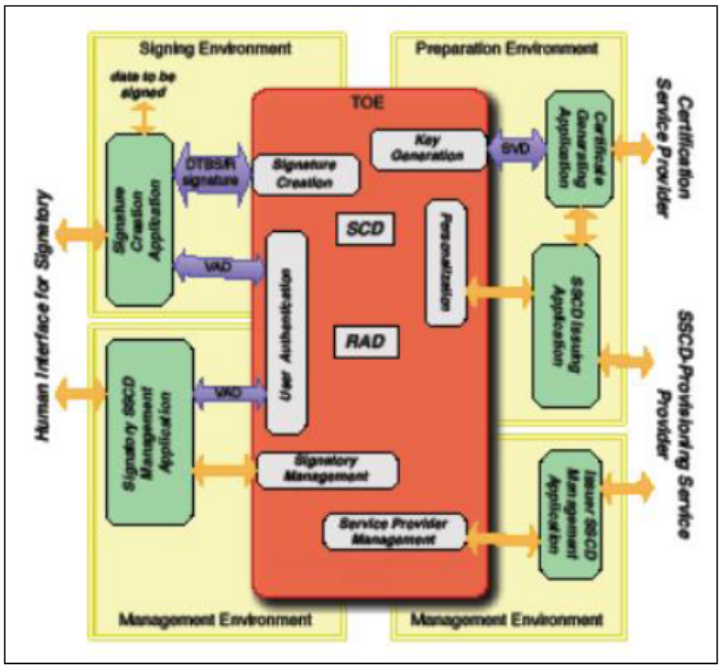

Figura 1 - Funciones Principales del TOE y entorno operacional

ARQUITECTURA FÍSICA

El TOE es un elemento compuesto de:

- Plataforma IC subyacente.
- Sistema Operativo DNIe.

El TOE soporta cuatro configuraciones certificadas:

- DNIe-DCCF 04.21 A31 H 0155 EXP 3-4.6.2
- DNIe-DCCF 04.21 B31 H 0155 EXP 3-4.6.2
- DNIe-DCCF 04.22 A31 H 0155 EXP 3-4.6.2
- DNIe-DCCF 04.22 B31 H 0155 EXP 3-4.6.2

El TOE incluye, además, los documentos que se detallan en la sección siguiente.

DOCUMENTOS

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los consumidores de la versión evaluada.

- Guía Preparativa Tarjeta DNIe-DCCF 3.0, versión 1.1, revisión 4, 28 de noviembre de 2017.
- Guía operativa para usuario final. Tarjeta DNIe-DCCF 3.0, versión 1.1, revisión 4, 28 de noviembre de 2017.
- Guía Operativa para Administrador. Tarjeta DNIe-DCCF 3.0, versión 1.1, revisión 4, 28 de noviembre de 2017.
- DNI electrónico - Guía de Referencia Básica v1.3, 26 Octubre 2010.
- Especificación Funcional de la tarjeta DNIe-DCCF 3.0 – Manual de comandos, versión 1.1, revisión 4, 28 de noviembre de 2017.

PRUEBAS DEL PRODUCTO

Este expediente es un expediente de re-certificación según lo definido en el documento de apoyo [AC]. Teniendo en cuenta los cambios declarados por el fabricante en [IAR] y las evidencias proporcionadas por el fabricante, parte de las pruebas del producto han sido re-utilizadas de las realizadas en el expediente 2014-39. Teniendo en cuenta esto, el fabricante ha realizado pruebas para todas las funciones de seguridad declaradas. Todas las pruebas han sido realizadas por el fabricante, en sus instalaciones, con resultado satisfactorio.

Durante el proceso de evaluación se ha verificado que los resultados obtenidos siguen siendo aplicables para 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, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no representa un problema para la seguridad, ni supone una merma en la capacidad funcional del producto conforme a lo declarado en su declaración de seguridad.

ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

Teniendo en cuenta la lista de vulnerabilidades aplicables al TOE por su naturaleza y su entorno operacional, el equipo de evaluación desarrolló nuevo un análisis de vulnerabilidades teniendo en cuenta el estado del arte en el momento de la evaluación de este expediente y preparó un entorno

de pruebas para realización de pruebas de penetración de acuerdo a los documentos de apoyo de JIL (*Joint Interpretation Library*) aplicables al dominio técnico de "*Smartcards and Similar devices*" [JILAAPS] y [JILADVARC].

El equipo de evaluación analizó también la lista de requisitos de seguridad de la plataforma certificada subyacente basándose en el informe técnico de evaluación compuesto y teniendo en cuenta el estado del arte en el momento de emisión del nuevo informe de análisis de vulnerabilidades, junto con los requisitos específicos del TOE y su entorno operacional declarados en la declaración de seguridad aplicable.

Teniendo en cuenta lo anterior, se diseñaron y ejecutaron una serie de pruebas de penetración. Como resultado final de las pruebas realizadas, el equipo evaluador concluye que, teniendo en cuenta el estado del arte a la fecha de emisión de su informe, no existe ninguna vulnerabilidad explotable en el entorno operacional declarado, por lo tanto el TOE es resistente a atacantes con potencial de ataque alto según se define en Common Criteria versión 3.1 revisión 4.

CONFIGURACIÓN EVALUADA

El producto DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0 presenta cuatro posibles configuraciones:

- DNIe-DCCF 04.21 A31 H 0155 EXP 3-4.6.2
- DNIe-DCCF 04.21 B31 H 0155 EXP 3-4.6.2
- DNIe-DCCF 04.22 A31 H 0155 EXP 3-4.6.2
- DNIe-DCCF 04.22 B31 H 0155 EXP 3-4.6.2

Todas las configuraciones han sido sometidas al proceso de evaluación.

El consumidor del TOE puede verificar la configuración incluida en el TOE siguiendo el procedimiento de recepción definido en el apartado 3.4.2 "Entrega segura y recepción segura" del documento "Guía preparativa tarjeta DNIe-DCCF 3.0", versión 1.1, Revisión 4, de 28 de noviembre de 2017.

RESULTADOS DE LA EVALUACIÓN

El producto DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0, ha sido evaluado en base a la Declaración de Seguridad: "Declaración de Seguridad de la tarjeta DNIe-DCCF 3.0, Versión: 1.1 Revisión: 5", de 28 de noviembre de 2017.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 + AVA_VAN.5 presentan el veredicto de "PASA". Por consiguiente, el laboratorio Applus Laboratories asigna el **VEREDICTO de "PASA"** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel

EAL4 + AVA_VAN.5, definidas por los Common Criteria versión 3.1, revisión 4 y la Common Methodology for Information Technology Security Evaluation versión 3.1, revisión 4.

Los resultados de la evaluación, recogidos en el Informe Técnico de Evaluación, son válidos sólo para la versión evaluada del producto: DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0, cuya identificación aparece en el apartado "1.1.2 Identificación del objeto a evaluar (TOE)" de la “Declaración de Seguridad de la tarjeta DNIe-DCCF 3.0, Versión: 1.1 Revisión: 5”, de 28 de noviembre de 2017.

El OE ha sido probado con estas configuraciones. Todos los resultados de la evaluación son válidos únicamente para esta versión del OE. Cualquier modificación sobre esta configuración (producto, declaración de seguridad y guías) realizada por el desarrollador debe ser comunicada al Organismo de Certificación. Cualquier modificación queda fuera del alcance de esta evaluación. Los resultados de la evaluación de la nueva configuración pueden ser diferentes a los presentes.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

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.

El laboratorio realiza las siguientes recomendaciones de seguridad:

- Utilizar el dispositivo según las guías de seguridad proporcionadas por el fabricante.
- Mantener el dispositivo en el lector únicamente cuando sea necesaria su utilización y el resto del tiempo bajo control del usuario.
- Mantener el PIN bajo condiciones de seguridad equivalentes a las del propio producto.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto DNIe-DCCF (dispositivo cualificado de creación de firma), versión 3.0, se propone la resolución estimatoria de la misma.

La lista de recomendaciones técnicas del certificador se encuentra en el Anexo [INF-1773] que se encuentra custodiado en el Organismo de Certificación.

Cabe señalar adicionalmente que el TOE ha sido certificado teniendo en cuenta las configuraciones especificadas en el apartado CONFIGURACIÓN EVALUADA e identificadas en la declaración de seguridad aplicable. Todos los resultados de la evaluación son válidos únicamente para esta versión y configuración del TOE. Cualquier modificación sobre esta configuración (producto, declaración de seguridad y guías) debe ser comunicada al Organismo de Certificación y queda fuera del alcance de esta certificación. Para que el TOE se encuentre en la configuración evaluada el administrador debe

seguir todas las recomendaciones proporcionadas en la sección 3.3 del documento "Guía operativa para administrador de la tarjeta DNIe-DCCF 3.0, versión 1.1 revisión 4", de 28 de noviembre de 2017.

Se recomienda que la validez de los certificados generados con las claves generadas por el TOE tengan un período de validez máximo de 24 meses.

Se recomienda que la longitud del PIN que desbloquea el certificado de firma tenga una longitud mínima de 12 bytes.

Se recomienda que los consumidores de la firma electrónica del TOE verifiquen que el certificado de firma se encontraba vigente en el momento de la emisión de la firma consultando los servicios y listas de revocación de certificados aplicables al TOE.

Finalmente, se debe señalar que la norma Common Criteria no cubre la evaluación de la fortaleza de los algoritmos criptográficos declarados. A este respecto, desde el Organismo de Certificación se aconseja seguir las recomendaciones de algoritmos y longitudes de clave especificados en la guía *"CCN-STIC-807 Criptología de empleo en el ENS"*.

GLOSARIO DE TÉRMINOS

ATR	Answer To Reset
CC	Common Criteria
CCN	Centro Criptológico Nacional
CEM	Common Evaluation Methodology
CGA	Certificate Generation Application
CNI	Centro Nacional de Inteligencia
CSP	Certificate Service Provider
DNIe	Documento Nacional de Identidad electrónico
DPA	Differential Power Analysis
DS	Declaración de Seguridad
DCCF	Dispositivo Cualificado de Creación de Firma
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
ENS	Esquema Nacional de Seguridad
ETR	Evaluation Technical Report
FW	Firmware

HID	Human Interface Device
HW	Hardware
OC	Organismo de Certificación
PP	Perfil de Protección
RAD	Reference Authentication Data
SCA	Signature Creation Application
SCD	Signature Creation Data
SPA	Simple Power Analysis
QSCD	Qualified Signature Creation Device
SVD	Signature Verification Data
SW	Software
TI	Tecnologías de la Información
TOE	Objeto a Evaluar

BIBLIOGRAFÍA

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

[AC] Assurance Continuity: CCRA requirements. v2.1. CCMC. June 2012.

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CCDB-2006-04-004] ST sanitising for publication. CCMC. April 2006.

[CCN10] Resolución Interpretación: Evaluación de ASE en Common Criteria versión 6. 18 de diciembre 2014. CNI-CCN.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.

[eIDAS] Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

[IAR] Informe De Análisis De Impacto (IAR) DNI-DSCF 3.0. Cambios en el Sistema Operativo, versión 1.0. 26/06/2017. Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda.

[JILAAPS] Application of Attack Potential to Smartcards, version 2.9. Jan. 2013. Joint Interpretation Library.

[JILADVARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.0. Jan 2012. Joint Interpretation Library.

[JILCOMP] Composite product evaluation for Smart Cards and similar devices, version 1.2. Jan. 2012. Joint Interpretation Library.

[JILMSSR] Minimum site security requirements, version 1.1. July 2013. Joint Interpretation Library.

[PC/SC] Interoperatibility Specification for ICCs and Personal Computer System. Version 1.0. December 1997.

[PPSSCD-2] Protection Profiles for secure signature creation device - Part 2: Device with Key Generation , v 2.0.1 , January 2012.

[PPSSCD-5] Protection profiles for Secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application", versión 1.0.1.

[ST] Declaración de Seguridad de la tarjeta DNIe-DCCF 3.0, Versión: 1.1 Revisión: 5, de 28 de noviembre de 2017.

DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

- Declaración de Seguridad de la tarjeta DNIe-DCCF 3.0, Versión: 1.1 Revisión: 5, de 28 de noviembre de 2017.

La versión pública de este documento constituye la "Declaración de Seguridad LITE" que ha sido revisada siguiendo el documento con código [CCDB-2006-04-004], y se publica con el informe de certificación en las webs del CCRA y del OC. El identificador de la "Declaración de Seguridad LITE" es:

- Declaración de Seguridad reducida de la tarjeta DNIE-DCCF 3.0, Versión 1.1 Revisión 6, de 28 de noviembre de 2017.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for assurance components up to EAL4.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.