REF: 2014-39-INF-1766 v2	Creado: CERT11
Difusión: Expediente	Revisado: CALIDAD
Fecha: 03.05.2017	Aprobado: TECNICO

INFORME DE CERTIFICACIÓN

Expediente: 2014-39 DNIe -DSCF v3.0

Datos del solicitante: ESQ2826004 Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda

Referencias:

[EXT-2582] Solicitud de Certificación de DNIe -DSCF v3.0

[EXT-3175] Informe Técnico de Evaluación de DNIe -DSCF v3.0

La documentación del producto referenciada en los documentos anteriores.

Informe de Certificación del producto DNIe-DSCF (dispositivo seguro de creación de firma) versión 3.0, según la solicitud de referencia [EXT-2582], de fecha 29/08/2014, evaluado por el laboratorio Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI), conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-3175], recibido el pasado 12/12/2016.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

ÍNDICE

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

RESUMEN

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

El TOE es una tarjeta inteligente con capacidad criptográfica configurada como dispositivo seguro de creación de firma. 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) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: CESTI-INTA.

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: 12/12/2016.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 aumentado con AVA_VAN.5 (*Advanced methodical vulnerability analysis*) 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 + AVA_VAN.5, definidas por los criterios de evaluación Common Criteria versión 3.1, revisión 4 y la metodología de evaluación 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-DSCF (dispositivo seguro de creación de firma) versión 3.0, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

La tarjeta inteligente DNIe-DSCF (Dispositivo seguro de creación de firma) versión 3.0 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-DCSF v3.0 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:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- 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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

	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

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

IDENTIFICACIÓN

Producto: DNIe-DSCF (dispositivo seguro de creación de firma) versión 3.0.

Declaración de Seguridad: Declaración de Seguridad de la tarjeta DNIe-DSCF 3.0, versión 1.1 Revisión 1 (13 de septiembre de 2016).

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. Nivel EAL4 + AVA_VAN.5.

POLÍTICA DE SEGURIDAD

El uso del producto DNIe-DSCF (Dispositivo seguro 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 Declaración de Seguridad. En síntesis, se establece la necesidad de implementar políticas organizativas relativas a los siguientes aspectos.

Nota: Las políticas organizativas de seguridad se reproducen como copia exacta de los perfiles de protección declarados y declaración de seguridad, por lo que se reproducen en el idioma original.

Política 01: P.CSP_Qcert: Qualified certificate.

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the directive [DIR], article 2, clause 9, and Annex I of [DIR]) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

Política 02: P.Qsign: Qualified electronic signatures.

The signatory uses a signature creation system to sign data with an advanced electronic signature (article 1, clause 2 of [DIR]), which is a qualified electronic signature if it is based on a valid qualified certificate (according to Annex I of [DIR]). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

Política 03: P.Sigy_SSCD: TOE as secure signature creation device.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

The TOE meets the requirements for an SSCD laid down in Annex III of the [DIR]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

Política 04: P.Sig_Non-Repud: Non-repudiation of signatures

The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

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. Por tanto, para garantizar el uso seguro del TOE, se parte de las siguientes 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.

Nota: Las hipótesis se reproducen como copia exacta de los perfiles de protección declarados y declaración de seguridad, por lo que se reproducen en el idioma original.

Hipótesis 01: A.CGA: Trustworthy certificate-generation application.

The CGA protects the authenticity of the signatory's name or pseudonym and theSVD in the (qualified) certificate by an advanced electronic signature of the CSP.

Hipótesis 02: A.SCA: Trustworthy signature-creation application.

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the signatory wishes to sign in a form appropriate for signing by the TOE.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto DNIe-DSCF (Dispositivo seguro de creación de firma) versión 3.0, aunque los agentes que realicen ataques tengan potencial de ataque Alto correspondiente a 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 esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Las amenazas cubiertas por las propiedades de seguridad del TOE se relacionan a continuación.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Nota: Las amenazas se reproducen como copia exacta de los perfiles de protección declarados y declaración de seguridad, por lo que se reproducen en el idioma original.

Amenaza 01: T.SCD_Divulg: Storing, copying and releasing of the signature creation data.

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

Amenaza 02: T.SCD_Derive: Derive the signature creation data.

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

Amenaza 03: T.Hack_Phys: Physical attacks through the TOE interfaces.

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

Amenaza 04: T.SVD_Forgery: Forgery of the signature verification data.

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

Amenaza 05: T.SigF_Misuse: Misuse of the signature creation function of the TOE.

An attacker misuses the signature creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

Amenaza 06: T.DTBS_Forgery: Forgery of the DTBS/R.

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

Amenaza 07: T.Sig_Forgery: Forgery of the electronic signature.

An attacker forges a signed data object, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

FUNCIONALIDAD DEL ENTORNO

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

Se relacionan, a continuación, los objetivos que se deben cubrir por el entorno de uso del TOE.

Nota: Los objetivos de seguridad para el entorno se reproducen como copia exacta de los perfiles de protección declarados y declaración de seguridad, por lo que se reproducen en el idioma original.

Objetivo entorno 01: OE.SVD_Auth: Authenticity of the SVD.

The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

Objetivo entorno 02: OE.CGA_QCert: Generation of qualified certificates

The CGA generates a qualified certificate that includes, inter alias

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and controlled by the signatory,
- the advanced signature of the CSP.

The CGA confirms with the generated certificate that the SCD corresponding to the SVD is stored in a SSCD.

Objetivo entorno 03: OE.SSCD_Prov_Service: Authentic SSCD provided by SSCD Provisioning Service

The SSCD Provisioning Service handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalises and delivers the TOE as SSCD to the signatory.

Objetivo entorno 04: OE.HID_TC_VAD_Exp: Trusted channel of HID for VAD export.

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

Objetivo entorno 05: OE.DTBS_Intend: SCA sends data intended to be signed

The Signatory uses trustworthy SCA that

- generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- attaches the signature produced by the TOE to the data or provides it separately.

OE.SCA_TC_DTBS_Exp: Trusted channel of SCA for DTBS export.

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Objetivo entorno 07: OE.Signatory: Security obligation of the Signatory

The Signatory checks that the SCD stored in the SSCD received from SSCD provisioning service is in non-operational state. The Signatory keeps his or her SVAD confidential.

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

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 seguro de creación de firma (SSCD) 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

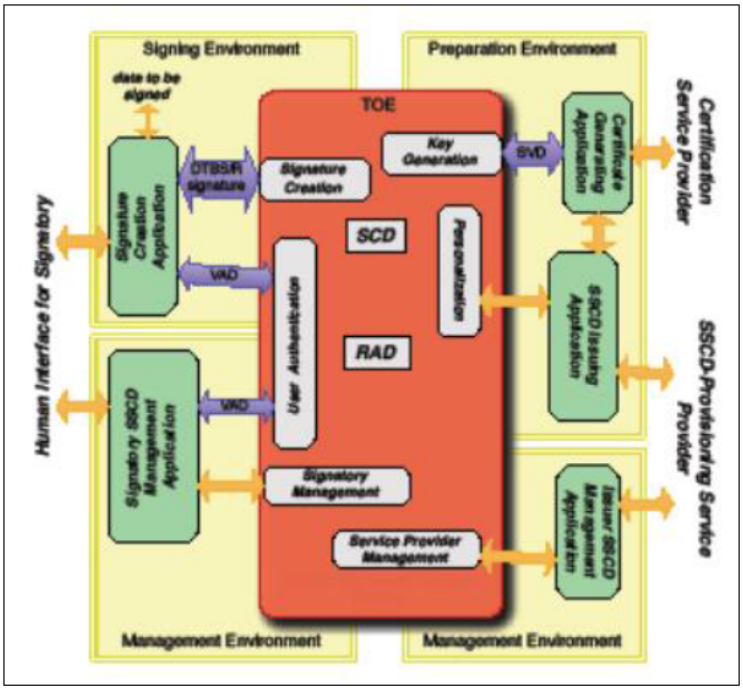
ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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 la directiva [DIR] si el certificado para el SVD es un certificado cualificado (Anexo I de [DIR]).

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.



ARQUITECTURA FÍSICA

El TOE es un elemento compuesto de:

- Plataforma IC subyacente.
- Sistema Operativo DNIe.

El TOE soporta dos configuraciones certificadas:

- DNIe-DSCF 04.10 A31 H 0155 EXP 3-4.6.2
- DNIe-DSCF 04.10 B31 H 0155 EXP 3-4.6.2

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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
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.

- Guía Preparativa Tarjeta DNIe-DSCF 3.0, versión 1.1, revisión 1 (13 septiembre 2016).
- Guía Operacional para Usuarios Tarjeta DNIe-DSCF 3.0, versión 1.1, revisión 1 (13 septiembre 2016).
- Guía Operativa para Administrador Tarjeta DNIe-DSCF 3.0, versión 1.1, revisión 1 (13 septiembre 2016).
- DNI electrónico - Guía de Referencia Básica v1.3, 26 Octubre 2010.
- Especificación Funcional de la tarjeta DNIe-DSCF 3.0 – Manual de comandos, versión 1.1, revisión 1 (14 septiembre 2016).

PRUEBAS DEL PRODUCTO

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante, en sus instalaciones, con resultado satisfactorio.

Durante el proceso de evaluación se han 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 las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido el 100% 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.

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 representa un problema para la seguridad, ni supone una merma en la capacidad funcional del producto.

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 un análisis de vulnerabilidades 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, junto con los requisitos específicos del TOE y su entorno operacional declarados en su 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-DSCF (dispositivo seguro de creación de firma) Versión: 3.0 presenta dos posibles configuraciones:

- DNIe-DSCF 04.10 A31 H 0155 EXP 3-4.6.2
- DNIe-DSCF 04.10 B31 H 0155 EXP 3-4.6.2

Ambas 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-DSCF 3.0", versión 1.1, Revisión 1 (13 septiembre 2016).

RESULTADOS DE LA EVALUACIÓN

El producto DNIe-DSCF (dispositivo seguro de creación de firma) Versión: 3.0 ha sido evaluado en base a la Declaración de Seguridad de la tarjeta DNIe-DSCF 3.0, versión 1.1 Revisión 1 (13 de septiembre de 2016).

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 + AVA_VAN.5 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 + AVA_VAN.5, definidas por los criterios de evaluación Common Criteria versión 3.1, revisión 4 y la metodología de

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

evaluación 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-DSCF versión v3.0, cuya identificación aparece en el apartado "1.1.2 Identificación del objeto a evaluar (TOE)" de la "Declaración de Seguridad de la Tarjeta DNIe-DSCF 3.0 v1.1 Rev1 13 Septiembre 2016".

El usuario puede verificar que la tarjeta es la versión evaluada, comprobando el ATR que devuelve después de conectarla al lector de tarjetas o después de realizar un reset de la misma. El ATR devuelto será diferente en función de la configuración biométrica.

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) realizada por el desarrollador debe ser comunicada a la autoridad 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.

1. 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.
2. Para un uso seguro del OE, debe tenerse en cuenta el cumplimiento de las políticas de seguridad recogidas en la declaración de seguridad apartado 3.5 a través de los objetivos del entorno definidos en el apartado 4.2.
3. 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 y contenga caracteres alfanuméricos. (letras, números, signos de puntuación, etc).

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

4. El usuario firmante debe seguir las recomendaciones de seguridad del apartado 3.3 del documento "Guia Operacional para Usuarios , Tarjeta DNIe-DSCF 3.0", que son las siguientes:

   - Protección de los datos de verificación de autenticación (PIN, Huella dactilar). El dispositivo externo donde se autentique el ciudadano debe garantizar la confidencialidad y la integridad de los datos de verificación de autenticación (PIN, Huella dactilar) según lo necesite el método de autenticación empleado.
   - La aplicación de creación de firma envía los datos que se pretenden firmar. El ciudadano usando la aplicación de creación de firma confiable, la cual genera el “hash” que representa los datos a ser firmados que pretenden ser firmados por el ciudadano en una forma apropiada para la firma por el DNIe-DSCF, envía el “hash” al DNIe-DSCF habilitando la verificación de la integridad del “hash” por el DNIe-DSCF. La firma producida por el DNIe-DSCF se adjunta a los datos a ser firmados o se proporciona de manera separada.
   - La aplicación de creación de firma debe proteger los datos a ser firmados. El entorno operacional debe asegurar que el “hash” no puede ser alterado en el tránsito entre la aplicación de creación de firma y el DNIe-DSCF.
   - Obligación de seguridad del ciudadano. El ciudadano debe revisar que las claves privadas almacenadas en el DNIe-DSCF proporcionado por la DGP están en estado no operacional. El ciudadano debe mantener la confidencialidad de su PIN.
   - La longitud del PIN debe ser mayor de 12 bytes.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto DNIe-DSCF (dispositivo seguro 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] adjunto a este informe de certificación 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) debe ser comunicada al Organismo de Certificación y queda fuera del alcance de esta certificación.

ENAC
CERTIFICACIÓN
Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

GLOSARIO DE TÉRMINOS

ATR	Answer To Reset
CC	Common Criteria
CCN	Centro Criptológico Nacional
CEM	Common Evaluation Methodology
CESTI	Centro de Evaluación de la Seguridad de las Tecnologías de la Información
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
DSCF	Dispositivo Seguro 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
INTA	Instituto de Técnica Aeroespacial
OC	Organismo de Certificación
PP	Perfil de Protección
RAD	Reference Authentication Data
SCA	Signature Creation Application
SCD	Signature Creation Data
SPA	Simple Power Analysis
SSCD	Secure Signature Creation Device
SVD	Signature Verification Data
SW	Software
TI	Tecnologías de la Información

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TOE Objeto a Evaluar

BIBLIOGRAFÍA

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

[CC_P1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1. Revision 4. Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. Version 3.1. Revision 4. Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. Version 3.1. Revision 4. Sept. 2012

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4. Sept. 2012.

[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.

[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.

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

[DIR] 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.

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

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

DECLARACIÓN DE SEGURIDAD

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

- Declaración de Seguridad de la tarjeta DNIe-DSCF 3.0, versión 1.1 Revisión 1 (13 de septiembre de 2016).

Basándose en el documento anterior, el patrocinador ha generado una versión pública de la declaración de seguridad para preservar su información propietaria. Esta versión ha sido revisada conforme al documento de apoyo [CCDB-2006-04-004] y se publica junto con este informe de certificación en los sitios web del Organismo de Certificación y del CCRA. El identificador de la versión pública de la declaración de seguridad es:

- Declaración de seguridad reducida de la TARJETA DNIE-DSCF 3.0. 15 de diciembre de 2016. Versión 1.1 Revisión 2.

ENAC
CERTIFICACIÓN
Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es