Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Declaración de Seguridad

reducida de la

TARJETA DNIE-DCCF 3.0

28 de noviembre de 2017

Versión 1.1 Revisión 6

	NOMBRE	FECHA
Elaborado por:	Área de Desarrollo – Documentos de Identificación / Tarjetas	28/11/2017
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO				
Versión	**Revisión**	**Fecha**	**Descripción**	**Autor**
1.1	6	28/11/2017	Versión reducida	FNMT-RCM

Documento clasificado como: *Público*

Destinatarios: Departamento de Documentos de Identificación/Tarjetas de la FNMT-RCM, Instituto Nacional de Técnicas Aeroespaciales, Applus Laboratories, Centro Criptológico Nacional

Índice

1 Introducción

1.1 Identificación

1.1.1 Identificación de la declaración de seguridad

Título: Declaración de Seguridad de la tarjeta DNIe-DCCF 3.0

Nombre del fichero: Declaración de Seguridad DNIe-DCCF 3.0 reducida

Versión: 1.1.

Revisión: 6.

Autor: FNMT - Departamento de Documentos de Identificación – Tarjetas

Fecha: 28 de noviembre de 2017

1.1.2 Identificación del objeto a evaluar (TOE)

TOE: DNIe-DCCF (dispositivo cualificado de creación de firma)

Versión: 3.0

Compuesto de:

IC plataforma subyacente

Sistema Operativo DNIe

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

1.2 Resumen

Esta declaración de seguridad establece las bases para la evaluación Common Criteria [CC] de la tarjeta “Documento Nacional de Identidad Electrónico como dispositivo cualificado de creación de firma” en su versión y configuración identificadas anteriormente.

De aquí en adelante, al TOE se le denominará indistintamente “DNIe-DCCF”, “DNIe”, “tarjeta DNIe”, “tarjeta DNIe-DCCF” o simplemente “tarjeta”.

El TOE es una tarjeta inteligente con capacidad criptográfica configurada como dispositivo cualificado 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.

La figura 1 presenta funcionalmente el TOE en su entorno de uso:

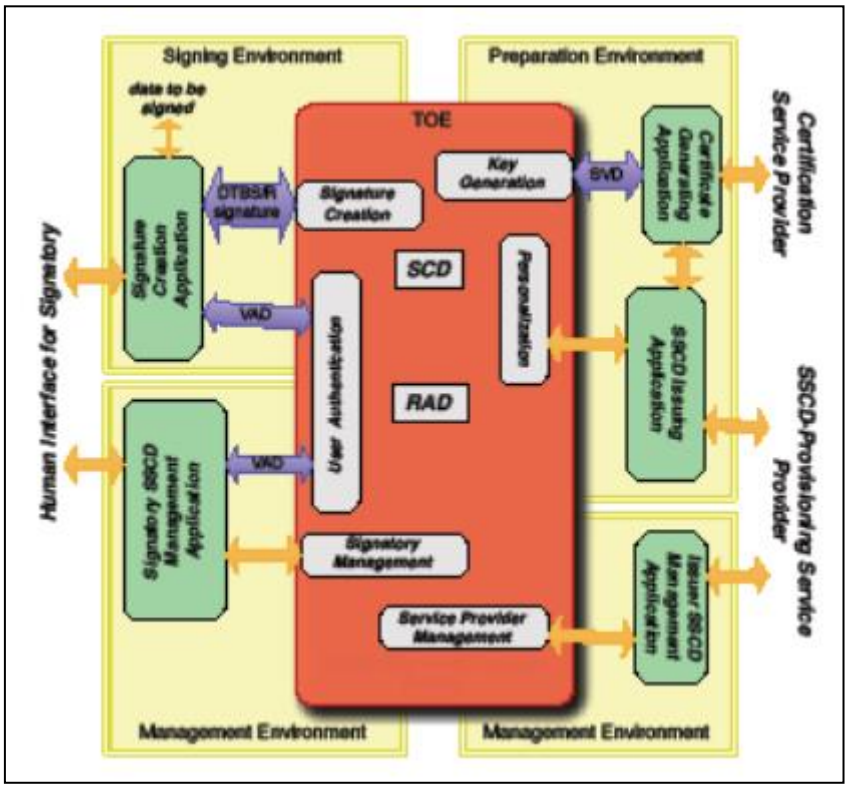


Figura 1.- Funciones Principales del TOE y entorno operacional

El entorno de uso del TOE 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.

1.3 Descripción del TOE

Como se ha indicado en el apartado 1.1.2 Identificación del objeto a evaluar (TOE), el TOE está compuesto de cinco elementos: un controlador de seguridad (chip) y un sistema operativo (DNIe, versión 4.21 ó 4.22). También se incluyen los manuales que contienen los procedimientos de operación e instalación:

Documento	**Referencia**
Guía preparativa. Tarjeta DNIe-DCCF 3.0. v1.1 r4. 28/11/17.	[GP]
Guía operativa para usuario final. Tarjeta DNIe-DCCF 3.0. v1.1 r4. 28/11/17.	[GOU]
Guía operativa para administrador. Tarjeta DNIe-DCCF 3.0. v1.1 r4. 28/11/17.	[GOA]
DNI electrónico. Guía de Referencia Básica. v1.3. 26/10/10.	[GRB]
Especificación funcional de la Tarjeta DNIe-DCCF 3.0. - Manual de comandos. v1.1 r4. 28/11/17.	[CMD]

El conjunto de todos ellos conforma un dispositivo criptográfico seguro de creación de firma con las funciones de seguridad que a lo largo de este apartado se detallan.

Los dos primeros elementos, el controlador de seguridad (HW) y librería criptográfica (FW), ya han sido evaluados y certificados por su fabricante. Los resultados de estas certificaciones se emplean para realizar la evaluación compuesta del TOE, conforme a los requisitos del documento [ASE_COMP].

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.

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.

1.4 Ciclo de vida

El ciclo de vida de la tarjeta inteligente DNIe-DCCF está definido en la figura 2, la cual distingue entre las etapas de desarrollo, producción, preparación y operativo. Las etapas de desarrollo y producción forman conjuntamente la fase de desarrollo del TOE. La fase de desarrollo está sujeta a la evaluación CC de acuerdo lo establecido a la clase ALC. La fase de desarrollo acaba con la entrega del TOE al proveedor de servicios del QSCD.

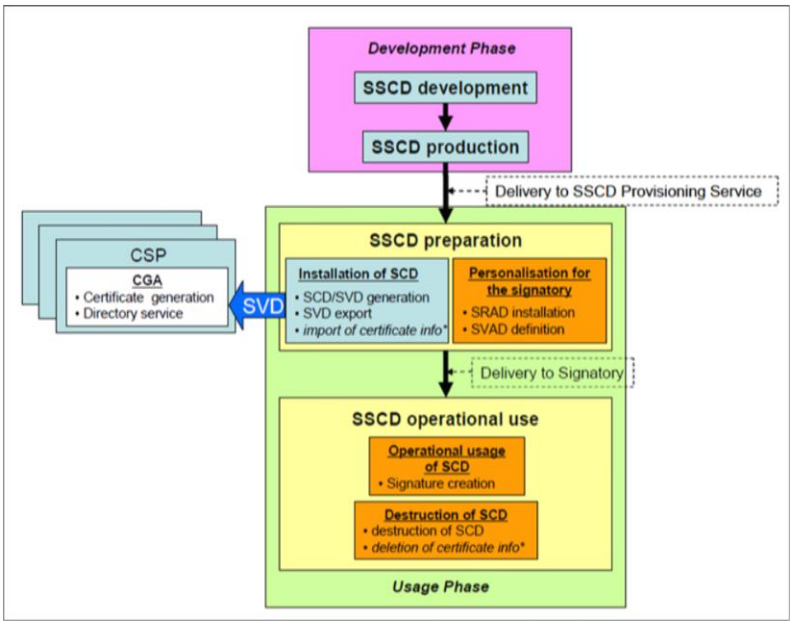


Figura 2.- Ciclo de Vida del Objeto a Evaluar (TOE)

1.4.1 Etapa preparativa

Un proveedor de servicios del QSCD aceptado por el fabricante, prepara el TOE para su uso y entrega al usuario legítimo del TOE. La fase de preparación acaba cuando el usuario legítimo ha recibido su TOE y habilita el SCD para su uso. Habilitar el TOE para la firma requiere al menos de una clave almacenada en memoria. Durante la preparación del TOE, el proveedor de servicios del TOE realiza las siguientes tareas:

- Obtener la información del usuario legítimo para su posterior proceso de preparación.

- Generación del PIN y obtención de las minucias del usuario legítimo, almacenamiento de estos datos como RAD en el TOE y preparación de la información del VAD para entregar al usuario legítimo.
- El TOE genera el par de claves SCD/SVD y obtiene un certificado de la SVD exportada desde el TOE. Este proceso se repite por cada par de claves SCD/SVD generadas.
- Presentar información del certificado en el QSCD.
- Entrega del TOE y su información de VAD al usuario legítimo.

Los datos requeridos en el certificado del SVD son entre otros (Anexo I de [eIDAS]):

- SVD
- Nombre del firmante siendo éste:
  - Nombre legal o,
  - Un seudónimo junto a una indicación de tal acto.

Los datos incluidos en el certificado son almacenados en el TOE en un fichero elemental durante la fase de personalización.

Antes de inicializar la firma del certificado en curso, la aplicación de generación de certificados debe verificar el SVD recibido del TOE por:

- establecer el remitente como el objeto a evaluar (TOE) genuino,
- establecer la integridad del SVD enviada por el objeto a evaluar (TOE) genuina,
- establecer que el objeto a evaluar (TOE) ha sido personalizado por un usuario legítimo
- establecer la correspondencia entre el SCD y el SVD y
- verificar que el algoritmo de firma con su correspondiente longitud de clave es apropiado y aprobado para el tipo de certificado.

El objeto a evaluar (TOE) proporciona una función de verificación de correspondencia entre el SVD y el SCD en tiempo de creación y por tanto cuando se exporta, la correspondencia es implícita.

1.4.2 Etapa uso operativo

La etapa de uso operativo del TOE comienza cuando el firmante ha obtenido tanto el VAD como el TOE. La habilitación del TOE para firma requiere que al menos un conjunto de SCD esté almacenado en memoria.

En esta etapa del ciclo de vida el firmante puede utilizar el TOE para crear firmas electrónicas avanzadas.

El firmante puede también interactuar con el TOE para realizar las operaciones de gestión, como modificar o desbloquear el valor de un PIN, etc. Tales operaciones requieren de un entorno seguro.

El usuario también puede renovar los certificados para lo que también requiere de un entorno seguro.

En el caso de que se deje el último SCD del TOE permanentemente inutilizable, la vida del TOE como QSCD acaba. También finaliza cuando se destruyen todos los SCD almacenados en el TOE. Esto puede incluir el borrado de los correspondientes certificados.

2 Ajuste a la norma

Esta declaración de seguridad cumple con los requisitos de la norma [CC]:

- Conforme con Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012.
- Conforme con Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012. Conformidad extendida con FPT_EMS.1 (definida en el apartado 5 Extended components definition).
- Conforme con Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 4, September 2012.

Esta declaración de seguridad cumple **estrictamente** los siguientes perfiles de protección [PP] y [PP5]:

- Título: Protection profiles for Secure signature creation device — Part 2: Device with key generation
- Versión: 2.0.1
- Autor: CEN / CENELEC (TC224/WG17)

- Título: 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
- Autor: CEN / CENELEC (TC224/WG17)

Esta declaración de seguridad cumple **estrictamente** el paquete de garantía EAL4 aumentado con AVA_VAN.5 definido en:

- Título: Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components.
- Versión: Version 3.1. Revision 4. September 2012.

2.1 Justificación del ajuste a la norma

El TOE presentado en la ST se ajusta al tipo de objeto definido en [PP] y [PP5], como dispositivo cualificado de creación de firma.

Se deduce del análisis del contenido y de la presentación de las evidencias, que se satisfacen los requisitos del nivel de evaluación exigido, esto es, EAL4+ aumentado con AVA_VAN.5.

La definición del problema de seguridad, los objetivos y requisitos de seguridad son consistentes con los presentados en el [PP] y [PP5] cumpliendo la conformidad estricta.

3 Security problem definition

3.1 Assets and objects

SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.

SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.

DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

3.2 Users and subjects acting for users

User: End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

Administrator: User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

Signatory: User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

3.3 Threat agents

Attacker: Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret.

3.4 Threats

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.

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.

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.

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.

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.

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.

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.

3.5 Organisational security policies.

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.

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][2]), 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.

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

[2] Se mantienen las referencias a [DIR] por respetar los perfiles de protección originales [PP] y [PP5], pero estas referencias se deben entender realizadas a [eIDAS] toda vez que en el Anexo de la [DE] se referencian los mismos perfiles de protección [EN419211-2] y [EN419211-5] para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas según se indica en los informes de mantenimiento [MR2] y [MR5].

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.

3.6 Assumptions

A.CGA: Trustworthy certificate generation application.
The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

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.

4 Security objectives

A continuación se detallan los objetivos de seguridad aplicables a la tarjeta inteligente DNIe-DCCF y el entorno en el que opera, clasificados por su aplicabilidad.

4.1 Security objectives for the TOE

OT.Lifecycle_Security: Lifecycle security.
The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

Application note 1: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

OT.SCD/SVD_Auth_Gen: Authorized SCD/SVD generation.
The TOE shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD.

OT.SCD_Unique: Uniqueness of the signature creation data.

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

OT.SCD_SVD_Corresp: Correspondence between SVD and SCD.

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

OT.SCD_Secrecy: Secrecy of the signature creation data.

The secrecy of the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

Application note 2: The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.

OT.Sig_Secure: Cryptographic security of the electronic signature.
The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.Sigy_SigF: Signature creation function for the legitimate signatory only.

The TOE shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

OT.DTBS_Integrity_TOE: DTBS/R integrity inside the TOE.
The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

OT.EMSEC_Design: Provide physical emanations security.
The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

OT.Tamper_ID: Tamper detection.
The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches.

OT.Tamper_Resistance: Tamper resistance.
The TOE shall prevent or resist physical tampering with specified system devices and components.

OT.TOE_TC_VAD_Imp: Trusted channel of TOE for VAD import
The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

OT.TOE_TC_DTBS_Imp: Trusted channel of TOE for DTBS import
The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS.

4.2 Security objectives for the operational environment

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.

OE.CGA_Qcert: Generation of qualified certificates.
The CGA shall generate a qualified certificate that includes (amongst others)
a) the name of the signatory controlling the TOE,
b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
c) the advanced signature of the CSP.

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

OE.SSCD_Prov_Service: Authentic SSCD provided by SSCD-provisioning service.
The SSCD-provisioning service shall initialise and personalise for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

OE.HID_TC_VAD_Exp[3]: 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.

OE.DTBS_Intend: SCA sends data intended to be signed.
The signatory shall use a 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,
- 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[4]: 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.

OE.Signatory: Security obligation of the signatory.
The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

4.3 Security objectives rationale

4.3.1 Security objectives backtracking

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_TC_VAD_Exp	OE.DTBS_Intend	OE.SCA_TC_DTBS_Exp	OE.Signatory
T.SCD_Divulg					X															
T.SCD_Derive		X				X														

[3] Dado que el DNIe-DCCF incluye la funcionalidad del canal seguro, este OE es el resultado de adaptar el OE.HI_VAD de [PP] tal y como se indica en [PP5].
[4] Dado que el DNIe-DCCF incluye la funcionalidad del canal seguro, este OE es el resultado de adaptar el OE.DTBS_Protect de [PP] tal y como se indica en [PP5].

T.Hack_Phys					X				X	X	X									
T.SVD_Forgery				X											X					
T.SigF_Misuse	X						X	X				X	X				X	X	X	X
T.DTBS_Forgery								X					X					X	X	
T.Sig_Forgery			X			X								X						
P.CSP_Qcert	X			X										X						
P.Qsign						X	X							X				X		
P.Sigy_SSCD	X	X	X		X	X	X	X	X		X					X				
P.Sig_Non-Repud	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A.CGA														X	X					
A.SCA																		X		

Tabla 1.- Mapping of security problem definition to security objectives

4.3.2 Security objectives sufficiency

Countering of threats by security objectives:

T.SCD_Divulg (Storing, copying and releasing of the signature creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of [DIR]. This threat is countered by OT.SCD_Secrecy, which assures the secrecy of the SCD used for signature creation.

T.SCD_Derive (Derive the signature creation data) deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OT.SCD/SVD_Auth_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures.

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

T.SVD_Forgery (Forgery of the signature verification data) deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA.

T.SigF_Misuse (Misuse of the signature creation function of the TOE) addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create an electronic signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of Annex III of [DIR]. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation and

operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign. The combination of OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission form the SCA to the TOE. OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) requires the HID to protect the confidentiality and the integrity of the VAD as needed by the authentication method employed. The HID and the TOE will protect the VAD by a trusted channel between HID and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). OE.Signatory (Security obligation of the signatory) ensures that the signatory checks that an SCD stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory (Security obligation of the signatory) ensures also that the signatory keeps their VAD confidential.

T.DTBS_Forgery (Forgery of the DTBS/R) addresses the threat arising from modifications of the DTBS/R sent to the TOE for signing which than does not correspond to the DTBS/R corresponding to the DTBS the signatory intends to sign. The threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE. The TOE counters internally this threat by the means of OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensuring the integrity of the DTBS/R inside the TOE. The TOE IT environment also addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE.

T.Sig_Forgery (Forgery of the electronic signature) deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (Cryptographic security of the electronic signature) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD_Unique and ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

Enforcement of OSPs by security objectives:

P.CSP_QCert (CSP generates qualified certificates) establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalization and operational usage,
- OT.SCD_SVD_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation,
- OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD (TOE as secure signature creation device) requires the TOE to meet Annex III of [DIR]. This is ensured as follows:

- OT.SCD_Unique meets the paragraph 1(a) of Annex III of [DIR], by the requirements that the SCD used for signature creation can practically occur only once;
- OT.SCD_Unique, OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(a) of Annex III of [DIR] by the requirements to ensure secrecy of the SCD. OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III of [DIR] by the requirements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;
- OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III of [DIR] by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;
- OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III of [DIR] as the TOE must not alter the DTBS/R.

Paragraph 2 of Annex III of [DIR], requires that an SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send it to the SSCD for signing.

The usage of SCD under sole control of the signatory is ensured by

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- OT.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialised and personalised SSCD from an SSCD-provisioning service.

P.Sig_Non-Repud (Non-repudiation of signatures) deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures generated with the TOE. OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service) ensures that the signatory uses an authentic TOE, initialised and personalised for the signatory. OE.CGA_QCert (Generation of qualified certificates) ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth (Authenticity of the SVD) and OE.CGA_QCert (Generation of qualified certificates) require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) ensures that the SVD exported by the TOE corresponds to the SCD that is stored in the TOE. OT.SCD_Unique (Uniqueness of the signature creation data) provides that the signatory's SCD can practically occur just once.

OE.Signatory (Security obligation of the signatory) ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy_SigF (Signature creation function for the legitimate signatory only) provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory (Security obligation of the signatory) ensures that the signatory keeps their VAD confidential. The confidentiality of VAD is protected during the transmission between the HI device and TOE according to OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD) and OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD). OE.DTBS_Intend (SCA sends data intended to be signed), OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE), OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) and OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure (Cryptographic security of the electronic signature) ensure that only this SCD may generate a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

Upkeep of assumptions by security objectives:

A.SCA (Trustworthy signature creation application) establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS/R of the data that have been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

A.CGA (Trustworthy certificate generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates), which ensures the generation of qualified certificates, and by OE.SVD_Auth (Authenticity of the SVD), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

5 Extended components definition

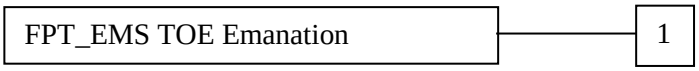
The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMS is taken from the Protection Profile Secure Signature Creation Device [BSI].

FPT_EMS TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if **FAU_GEN** (Security audit data generation) is included in a PP or ST using FPT_EMS.1.

FPT_EMS TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMS.1.2	The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

6 Requisitos de seguridad

6.1 Requisitos funcionales de seguridad del objeto a evaluar (TOE)

Las operaciones sobre los requisitos de seguridad se agrupan en asignación, selección, iteración y refinamiento marcadas como:

- Asignación: texto subrayado, ej.: ejemplo.
- Selección: Texto en itálico y color negro, ej.: *ejemplo*.
- Iteración: con una barra / y un identificador unívoco.
- Refinamiento: texto en negrita, ej.: **ejemplo**.

FCS_CKM.1/RSA Cryptographic key generation - RSA

Hierarchical to: No other components.

Dependencies: FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation.
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/RSA The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm [PKCS#1] with Miller-Rabin primality test and specified cryptographic key size 2048 bits that meet the following: [PKCS#1] v2.1 RFC 3447.

FCS_CKM.1/DES Cryptographic key generation - DES

Hierarchical to: No other components.

Dependencies: FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation.
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/DES The TSF shall generate **a session key** in accordance with a specified cryptographic key generation algorithm Section 8.10.4.1 of [EN419212-1] or Section 8.9.1 of [EN14890-1] and specified cryptographic key sizes of 2 x 56 bits that meet the following: [EN419212-1] or [EN14890-1].

FCS_CKM.1/AES Cryptographic key generation - AES

Hierarchical to: No other components.

Dependencies: FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/AES The TSF shall generate **a session key** in accordance with a specified cryptographic key generation algorithm Section 8.9.3 of [EN419212-1] or Section 8.9.3 of [EN14890-1] and specified cryptographic key sizes 128 bits that meet the following: [EN419212-1] or [EN14890-1].

FCS_CKM.1/EC Cryptographic key generation - EC

Hierarchical to: No other components.

Dependencies: FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation.
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/EC The TSF shall generate **cryptographic keys** in accordance with a specified cryptographic key generation algorithm Appendix A.4.3 in [ANSI X9.62] and section 6.1 in [ISO15946-1] and specified cryptographic key sizes 256 bits that meet the following: [ANSI X9.62].

FCS_CKM.4/RSA Cryptographic key destruction - RSA

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.

FCS_CKM.4.1/RSA The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroes writing in the zone memory in where SCD/SVD is stored that meets the following: none.

FCS_CKM.4/DES Cryptographic key destruction - DES

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.

FCS_CKM.4.1/DES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroes writing in the zone memory in where (DES) session key is stored that meets the following: none.

FCS_CKM.4/AES Cryptographic key destruction - AES

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.

FCS_CKM.4.1/AES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroes writing in the zone memory in where (AES) session key is stored that meets the following: none.

FCS_CKM.4/EC Cryptographic key destruction - EC

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.

FCS_CKM.4.1/EC The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroes writing in the zone memory in where SCD/SVD is stored that meets the following: none.

FCS_COP.1/RSA[5] Cryptographic operation - RSA

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.
FCS_CKM.4 Cryptographic key destruction.

FCS_COP.1.1/RSA The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA and cryptographic key size 2048 bits that meet the following: [PKCS#1] v2.1 RFC 3447.

FCS_COP.1/DES Cryptographic operation - DES

Hierarchical to: No other components.

[5] El esquema de firma empleado es PKCS#1 v2.1: RSASSA-PKCS1-v1.5

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.
FCS_CKM.4 Cryptographic key destruction.

FCS_COP.1.1/DES The TSF shall perform ciphered APDUs generation and verification in accordance with a specified cryptographic algorithm 3DES and cryptographic key sizes 2 x 56 bits that meet the following: NIST Special Publication 800-67, Version 1.1 [3DES] and [EN419212-1] or [EN14890-1].

FCS_COP.1/AES Cryptographic operation - AES

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.
FCS_CKM.4 Cryptographic key destruction.

FCS_COP.1.1/AES The TSF shall perform ciphered APDUs generation and verification in accordance with a specified cryptographic algorithm AES and cryptographic key sizes 128 bits that meet the following: Federal Information Processing Standards (FIPS) Publication 197 [AES] and [EN419212-1] or [EN14890-1].

FCS_COP.1/SHA Cryptographic operation - SHA

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.
FCS_CKM.4 Cryptographic key destruction.

FCS_COP.1.1/SHA The TSF shall perform hash-value calculation of user chosen data in accordance with a specified cryptographic algorithm SHA-256 and cryptographic key sizes of none that meet the following: Federal Information Processing Standards (FIPS) Publication 180-4 [SHS].

FCS_COP.1/ECDH Cryptographic operation - ECDH

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation.
FCS_CKM.4 Cryptographic key destruction.

FCS_COP.1.1/ECDH The TSF shall perform elliptic curve Diffie-Hellman key agreement in accordance with a specified cryptographic algorithm ECDH and cryptographic key sizes 256 bits that meet the following standard:

1. According to section 5.4.1 in ANSI X9.63 -2001 Unlike section 5.4.1.3 our, implementation not only returns the x-coordinate of the shared secret, but rather the x-coordinate and y-coordinate.

2. According to sections 8.4.2.1, 8.4.2.2, 8.4.2.3, and 8.4.2.4 in ISO/IEC 15946-3:2002: The function enables the operations described in the four sections.

Nota de aplicación: Estas claves se utilizan para el establecimiento del canal seguro en el modo sin contactos. Concretamente en el protocolo PACE.

User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

FDP_ACC.1/ SCD/SVD_Generation **Subset access control**

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/ SCD/SVD_Generation	The TSF shall enforce the SCD/SVD Generation SFP on: (1) subjects: S.User, (2) objects: SCD, SVD, (3) operations: generation of SCD/SVD pair.
FDP_ACF.1/SCD/SVD_Generation	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/SCD/SVD_Generation	The TSF shall enforce the SCD/SVD Generation SFP to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management".
FDP_ACF.1.2/SCD/SVD_Generation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to generate SCD/SVD pair.
FDP_ACF.1.3/SCD/SVD_Generation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/SCD/SVD_Generation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.

FDP_ACC.1/SVD_Transfer	**Subset access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control.
FDP_ACC.1.1/SVD_Transfer	The TSF shall enforce the SVD Transfer SFP on: (1) subjects: S.User, (2) objects: SVD, (3) operations: export.
FDP_ACF.1/SVD_Transfer	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/SVD_Transfer	The TSF shall enforce the SVD Transfer SFP to objects based on the following: (1) the S.User is associated with the security attribute Role, (2) the SVD.
FDP_ACF.1.2/SVD_Transfer	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *R.Admin*, *R.Sigy* is allowed to export SVD.
FDP_ACF.1.3/SVD_Transfer	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.
FDP_ACC.1/Signature_Creation	**Subset access control**
Hierarchical to:	No other components.

Dependencies:	FDP_ACF.1 Security attribute based access control.
FDP_ACC.1.1/Signature_Creation	The TSF shall enforce the Signature Creation SFP on (1) subjects: S.User, (2) objects: DTBS/R, SCD, (3) operations: signature creation.
FDP_ACF.1/ Signature_Creation	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ Signature_Creation	The TSF shall enforce the Signature Creation SFP to objects based on the following: (1) the user S.User is associated with the security attribute "Role" and (2) the SCD with the security attribute "SCD Operational".
FDP_ACF.1.2/ Signature_Creation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes".
FDP_ACF.1.3/ Signature_Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4/ Signature_Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD which

	security attribute “SCD operational” is set to “no”.
FDP_RIP.1	**Subset residual information protection**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource from* the following objects: SCD.

The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data":

1. SCD
2. SVD (if persistently stored by the TOE).

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data":

FDP_SDI.2/Persistent	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.
FDP_SDI.2.1 / Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored data.
FDP_SDI.2.2 / Persistent	Upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data (2) inform the S.Sigy about integrity error.
FDP_SDI.2/DTBS	**Stored data integrity monitoring and action**

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.
FDP_SDI.2.1 / DTBS	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes: integrity checked stored DTBS.
FDP_SDI.2.2 / DTBS	Upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data (2) inform the S.Sigy about integrity error.

FIA_UID.1	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow (1) Self-test according to FPT_TST.1, (2) To establish a trusted channel between the user and the TOE and to establish a trusted channel between the SCA and the TOE, on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.

FIA_UAU.1.1	The TSF shall allow (1) Self-test according to FPT_TST.1, (2) Identification of the user by means of TSF required by FIA_UID.1. (3) establishing a trusted channel between the HID and the TOE by means of TSF required by FTP_ITC.1/VAD, (4) none. on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_AFL.1	**Authentication failure handling**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication.
FIA_AFL.1.1	The TSF shall detect when *3* unsuccessful authentication attempts occur related to consecutive failed authentication attempts.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall block RAD.
FMT_SMR.1	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FMT_SMR.1.1	The TSF shall maintain the roles R.Admin and R.Sigy.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

FMT_SMF.1	**Security management functions**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: (1) Creation and modification of RAD, (2) Enabling the signature creation function, (3) Modification of the security attribute SCD/SVD management, SCD operational, (4) Change the default value of the security attribute SCD Identifier, (5) None.
FMT_MOF.1	**Management of security functions behaviour**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions.
FMT_MOF.1.1	The TSF shall restrict the ability to *enable* the functions signature creation function to R.Sigy.
FMT_MSA.1/Admin	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1 / Admin	The TSF shall enforce the SCD/SVD Generation SFP to restrict the ability to

	modify the security attributes SCD/SVD management to R.Admin.
FMT_MSA.1/ Signatory	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1 / Signatory	The TSF shall enforce the Signature Creation SFP to restrict the ability to *modify* the security attributes SCD operational to R.Sigy.
FMT_MSA.2	**Secure security attributes**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control. FMT_MSA.1 Management of security attributes. FMT_SMR.1 Security roles.
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for *SCD/SVD Management and SCD operational*.
FMT_MSA.3	**Static attribute initialisation**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles.
FMT_MSA.3.1	The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP to provide

	restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the R.Admin to specify alternative initial values to override the default values when an object or information is created.
FMT_MSA.4	**Security attribute value inheritance**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
FMT_MSA.4.1	The TSF shall use the following rules to set the value of security attributes: (1) If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation. (2) If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation.
FMT_MTD.1/Admin	**Management of TSF data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/Admin	The TSF shall restrict the ability to *create* the RAD to R.Admin.
FMT_MTD.1/ Signatory	**Management of TSF data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Signatory	The TSF shall restrict the ability to *modify and unblock* the RAD to R.Sigy.
FPT_EMS.1	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1	The TOE shall not emit information about chip power consumption or command execution time in excess of useless information enabling access to RAD and SCD.
FPT_EMS.1.2	The TSF shall ensure attackers are unable to use the following interface VCC, GND and IO pads to gain access to RAD and SCD.
FPT_FLS.1	**Failure with preservation of secure state**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: (1) self-test according to FPT_TST fails, (2) any communication protocol attack or sensor detection of not detected parameters.
FPT_PHP.1	**Passive detection of physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has

	occurred.
FPT_PHP.3	**Resistance to physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical tampering and physical probing to the clock frecuency, power supply, data integrity in RAM, EEPROM and ROM memories and active shield by responding automatically such that the SFRs are always enforced.
FPT_TST.1	**TSF testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up* to demonstrate the correct operation of *the TSF*.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of *TSF*.
FDP_UIT.1/DTBS	**Data exchange integrity**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control. FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path.
FDP_UIT.1.1/DTBS	The TSF shall enforce the Signature

	Creation SFP to *receive* user data in a manner protected from *modification and insertion* errors.
FDP_UIT.1.2/DTBS	The TSF shall be able to determine on receipt of user data, whether *modification and insertion* has occurred.

FTP_ITC.1/VAD	**Inter-TSF trusted channel – TC Human Interface Device**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/VAD	The TSF shall provide a communication channel between itself and another trusted IT product **HID** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/VAD	The TSF shall permit *the remote trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3/VAD	The TSF **or the HID** shall initiate communication via the trusted channel for (1) User authentication according to FIA_UAU.1, (2) signature verification and SVD export.

FTP_ITC.1/DTBS	**Inter-TSF trusted channel – Signature creation Application**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/DTBS	The TSF shall provide a communication channel between itself and another trusted IT product **SCA** that is logically distinct from other communication channels and provides assured identification of its end

	points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/DTBS	The TSF shall permit *the remote trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3/DTBS	The TSF **or the SCA** shall initiate communication via the trusted channel for (1) signature creation (2) signature verification and SVD export.

6.2 Requisitos de Garantía de Seguridad del objeto a evaluar (TOE)

La evaluación se realizará conforme al nivel de garantía definido, según la versión Common Criteria [CC] de aplicación, por:

- EAL4
- Aumentado con el componente AVA_VAN.5

Los requisitos de garantía de seguridad se justifican mediante la presentación a la evaluación de los distintos documentos que acreditan el cumplimiento de los correspondientes requisitos.

Componente	Documentos
ADV_ARC.1 Security architecture description	Descripción de la arquitectura de seguridad
ADV_FSP.4 Complete functional specification	Especificación funcional - Manual de comandos
ADV_IMP.1 Implementation representation of the TSF	Código fuente y mapas de ficheros DNIe-DCCF
ADV_TDS.3 Basic modular design	Diseño DNIe-DCCF
AGD_OPE.1 Operational user guidance	Guía operativa para administrador y para usuario final
AGD_PRE.1 Preparative procedures	Guía preparativa
ALC_CMC.4 Production support, acceptance procedures and automation	Plan de gestión de la configuración
ALC_CMS.4 Problem tracking CM coverage	Listado de configuración
ALC_DEL.1 Delivery procedures	Procedimientos de entrega
ALC_DVS.1 Identification of security measures	Medidas de seguridad para de desarrollo
ALC_LCD.1 Developer defined life-cycle model	Ciclo de vida de la tarjeta DNIe-DCCF

ALC_TAT.1 Well-defined development tools	Herramientas y técnicas para el desarrollo del Sistema Operativo de la tarjeta DNIe-DCCF
ASE_CCL.1 Conformance claims	Declaración de seguridad de la tarjeta DNIe-DCCF
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_COV.2 Analysis of coverage	Análisis de la cobertura de las pruebas para la especificación funcional
ATE_DPT.1 Testing: basic design	Definición de las pruebas de los subsistemas
ATE_FUN.1 Functional testing	Plan de pruebas
ATE_IND.2 Independent testing – sample	Documentación de pruebas
AVA_VAN.5 Advanced methodical vulnerability analysis	Documentación de análisis de vulnerabilidades

Tabla 2.- Documentación y requisitos de garantía de seguridad.

6.3 Justificación de los Requisitos de Seguridad del objeto a evaluar (TOE)

6.3.1 Cobertura de los requisitos funcionales de seguridad

TOE security objectives / Functional requirements	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp
FCS_CKM.1\RSA	X		X	X	X								
FCS_CKM.1\DES	X		X	X	X								
FCS_CKM.1\AES	X		X	X	X								
FCS_CKM.1\EC	X		X	X	X								
FCS_CKM.4\RSA	X				X								
FCS_CKM.4\DES	X				X								
FCS_CKM.4\AES	X				X								
FCS_CKM.4\EC	X				X								
FCS_COP.1\RSA	X					X							
FCS_COP.1\DES	X					X							
FCS_COP.1\AES	X					X							
FCS_COP.1\SHA	X					X							
FCS_COP.1\ECDH	X					X							
FDP_ACC.1/SCD/SVD_Generation	X	X											
FDP_ACC.1/SVD_Transfer	X												
FDP_ACC.1/Signature_Creation	X						X						
FDP_ACF.1/SCD/SVD_Generation	X	X											
FDP_ACF.1/SVD_Transfer	X												
FDP_ACF.1/Signature_Creation	X						X						
FDP_RIP.1					X		X						
FDP_SDI.2/Persistent				X	X	X							
FDP_SDI.2/DTBS							X	X					
FIA_AFL.1							X						
FIA_UAU.1		X					X						
FIA_UID.1		X					X						
FMT_MOF.1	X						X						
FMT_MSA.1/Admin	X	X											
FMT_MSA.1/Signatory	X						X						
FMT_MSA.2	X	X					X						
FMT_MSA.3	X	X					X						

FMT_MSA.4	X	X		X			X						
FMT_MTD.1/Admin	X						X						
FMT_MTD.1/Signatory	X						X						
FMT_SMR.1	X						X						
FMT_SMF.1	X			X			X						
FPT_EMS.1					X				X				
FPT_FLS.1					X								
FPT_PHP.1										X			
FPT_PHP.3					X						X		
FPT_TST.1	X				X	X							
FDP_UIT.1/DTBS													X
FTP_ITC.1/VAD												X	
FTP_ITC.1/DTBS													X

6.3.2 TOE Security Requirements Sufficiency

OT.Lifecycle_Security (Lifecycle security) is provided by the SFR for SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.4 which ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer. The SCD usage is ensured by access control FDP_ACC.1/Signature_Creation, FDP_AFC.1/Signature_Creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle.

OT.SCD/SVD_Auth_Gen (Authorized SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The SFR FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

OT.SCD_Unique (Uniqueness of the signature creation data) implements the requirement of practically unique SCD as laid down in Annex III of [DIR], paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD

and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

OT.SCD_Secrecy (Secrecy of signature creation data) is provided by the security functions specified by the following SFR. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA).

SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensures the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

OT.Sigy_SigF (Signature creation function for the legitimate signatory only) is provided by an SFR for identification authentication and access control.

FIA_UAU.1 and FIA_UID.1 ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1 restricts the ability to enable the signature creation function to the signatory.

FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP_SDI.2/DTBS require that the DTBS/R has not been altered by the TOE.

OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMS.1.1.

OT.Tamper_ID (Tamper detection) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

OT.TOE_TC_VAD_Imp (Trusted channel of TOE for VAD import) is provided by FTP_ITC.1/VAD to provide a trusted channel to protect the VAD provided by the HID to the TOE.

OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

6.3.3 Satisfaction of dependencies of security requirements

Functional requirement	Dependencies	Satisfied by
FCS_CKM.1/RSA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/RSA, FCS_CKM.4/RSA
FCS_CKM.1/DES	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/DES, FCS_CKM.4/DES
FCS_CKM.1/AES	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/AES, FCS_CKM.4/AES
FCS_CKM.1/EC	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/ECDH, FCS_CKM.4/EC
FCS_CKM.4/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/RSA
FCS_CKM.4/DES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/DES
FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/AES
FCS_CKM.4/EC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/EC
FCS_COP.1/RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/RSA, FCS_CKM.4/RSA
FCS_COP.1/DES	[FDP_ITC.1 or	FCS_CKM.1/DES,

	FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.4/DES
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/AES, FCS_CKM.4/AES
FCS_COP.1/ECDH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/EC, FCS_CKM.4/EC
FCS_COP.1/SHA	The dependency FCS_CKM.1 is not required for the SHA-256 algorithm, because the SHA-256 algorithm is a keyless operation. The dependency FCS_CKM.4 is not required for the SHA-256 algorithm, because the SHA-256 algorithm is a keyless operation.	
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3
FDR_RIP.1	No dependencies	n/a
FDP_SDI.2/Persistent	No dependencies	n/a
FDP_SDI.2/DTBS	No dependencies	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1,	FMT_SMR.1, FMT_SMF.1

	FMT_SMF.1	
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_FLS.1	No dependencies	n/a
FPT_PHP.1	No dependencies	n/a
FPT_PHP.3	No dependencies	n/a
FPT_TST.1	No dependencies	n/a
FDP_UIT.1/DTBS	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FTP_ITC.1/VAD	No dependencies	n/a
FTP_ITC.1/DTBS	No dependencies	n/a

Tabla 3.- Satisfaction of dependencies of security functional requirements

Assurance requirement(s)	**Dependencies**	**Satisfied by**
EAL4 package	(dependencies of EAL4 package are not reproduced here)	By construction, all dependencies are satisfied in a CC EAL package
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1 (all are included in EAL4 package)

Tabla 4.- Satisfaction of dependencies of security assurance requirements

6.3.4 Rationale for chosen security assurance requirements

The assurance level for this protection profile is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this protection profile is just such a product. Augmentation results from the selection of:

AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be

shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

7 Resumen de la especificación funcional del producto

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.

La tarjeta DNIe-DCCF provee las siguientes capacidades relacionadas con la funcionalidad de firma electrónica:

1. Establecimiento del canal seguro (con o sin contactos)

   Para el establecimiento del canal seguro, en primer lugar, se realiza un intercambio de las claves públicas de la tarjeta y el terminal mediante certificados que serán verificados por ambas partes. A continuación se realiza un protocolo de autenticación mutua, con intercambio de semillas para la derivación de una semilla común que dé lugar a las claves de sesión de cifrado y autenticado.

   Una vez concluido el protocolo para el establecimiento de la semilla común todos los mensajes deben transmitirse securizados.

   Si se rompe el canal seguro establecido debido a que se haya recibido un comando APDU que no respete el formato de mensaje securizado o a que la información de autenticación o MAC sea errónea, el canal queda deshabilitado y el estado de seguridad de la tarjeta es reseteado (se borran las claves de sesión y los secretos presentados quedan invalidados).

   El canal seguro se puede establecer empleando tanto el interfaz con contactos como el sin contactos.

   Este procedimiento permite que cada una de las partes (tarjeta y aplicación externa) confíe en la otra, mediante la presentación mutua de certificados, y su verificación. En el proceso, también se incluye el intercambio seguro de unas claves de sesión, que deberán ser utilizadas para securizar (encriptar) todos los mensajes intercambiados posteriormente.

   Cuando se completa con éxito el establecimiento de un canal seguro, se adquiere un nuevo estado de seguridad en el diálogo con la tarjeta, que en función del certificado utilizado por el terminal.

2. Securización de mensajes

   La tarjeta DNIe-DCCF puede, previo establecimiento de un canal seguro, securizar los mensajes transmitidos. Para el establecimiento es necesaria la autenticación previa del terminal y la tarjeta, mediante el uso de certificados electrónicos.

   Cuando el canal está establecido, los mensajes intercambiados entre la tarjeta y terminal se cifran y autentican, de tal forma que se asegura una comunicación una-a-uno entre los dos puntos originarios de canal. El canal seguro puede ser requerido por la aplicación o puede ser una restricción de acceso impuesta a algún recurso de la tarjeta.

3. Identificación y Autenticación

   La tarjeta dispone de distintos métodos de autenticación, mediante los que una entidad externa demuestra su identidad, o el conocimiento de algún dato secreto almacenado en la tarjeta.

   La correcta realización de cada uno de estos métodos, permite obtener unas condiciones de seguridad, que podrán ser requeridas para el acceso a los distintos recursos de la tarjeta.

   - Autenticación de usuario mediante PIN

     La tarjeta soporta verificación de usuario (CHV- Card Holder verification) para el acceso a determinados ficheros. La verificación es realizada, a través del canal seguro de PIN, comprobando el código facilitado por la entidad externa a través del comando diseñado para tal fin. El dato es comparado con la información de referencia almacenada en el fichero CHV. Cada código CHV tiene su propio contador de intentos. El contador de intentos es decrementado cada vez que se realiza una presentación errónea, pudiendo llegar a bloquearlo si el contador llega a cero. Es posible desbloquear un código CHV tras una correcta presentación del código de desbloqueo.

   - Desbloqueo de PIN

     La tarjeta DNIe-DCCF tiene soporte para biometría con algoritmo “Match on Card”, es decir, la verificación de los datos biométricos frente a los datos de referencia se realiza dentro de la propia tarjeta. Por tanto, se mantienen los datos sensibles de biometría siempre internos a la tarjeta, y su utilización está controlada mediante control de acceso. Esta característica de “Match on Card” confiere una importante diferencia frente a algoritmos “Match off Card”, donde la tarjeta sólo es utilizada como soporte de los datos para la verificación externa.

8 Acrónimos

ALC	Clase Life-Cycle Support
CA	Autoridad de Certificación
CC	Common Criteria
CGA	Certificate-generation application, Aplicación de Generación de Certificados
CPU	Central Processing Unit, Unidad Central de Proceso
CRT	Chinese Remainder Theorem, Teorema del Residuo Chino
CSP	Certification Service Provider, Proveedor de Servicios de Certificación
DES	Data Encryption Standard
DNIe	Documento Nacional de Identidad Electrónico
DCCF	Dispositivo Cualificado de Creación de Firma
DTBS	Data to be signed, Datos a ser firmados
DTBS/R	Data to be signed or its unique representation, Representación unívoca de los datos a ser firmados
EAL	Evaluation Assurance Level, Nivel de garantía de evaluación
ECC	Elliptic curve cryptography, Criptografía de curvas elípticas
EEPROM	Electrically Erasable Programable Read Only Memory, Memoria ROM programable eléctricamente
FDP	User Data Protection, Protección de datos de usuario
FIPS	Federal Information Processing Standard
GND	Ground, Tierra
HI	Human Interface, Interfaz humana
IC	Integrated Circuit, Circuito Integrado
IO	Input/Output, Entrada/Salida
ISO	International Organization for Standardization
PKCS	Public Key Cryptography Standards, Normas de Criptografía de Clave Pública
PIN	Personal Identification Number, Número de Identificación Personal
PP	Protection Profile, Perfil de Protección
RAD	Reference authentication data, Datos de referencia de autenticidad
RAM	Random Access Memory, Memoria de acceso aleatorio
ROM	Read Only Memory, Memoria de solo lectura
RSA	Rivest, Shamir & Adleman
SCA	Signature Creation Application, Aplicación de creación de firma
SCD	Signature Creation Data, Datos de creación de firma

SDO	Signed Data Object, Objeto de datos firmado
SFP	Security Function Policy, Política de función de seguridad
SFR	Security Functional Requirement, Requisito funcional de seguridad
SHA	Secure Hashing Algorithm
QSCD	Qualified signature-creation device, Dispositivo cualificado de creación de firma
ST	Security Target, Declaración de Conformidad
SVD	Signature Verification Data, Datos de verificación de firma
TOE	Target of Evaluation, Objeto a evaluar
TSF	TOE Security Functionality, Funciones de seguridad del TOE
TSFI	TSF Interface, Interfaz de las funciones de seguridad del TOE
VAD	Verification Authentication Data, Datos de verificación de identidad
VCC	Supply Voltage, Tensión de Alimentación

9 Bibliografía

[AES] Federal Information Processing Standards Publication 197 Advanced Encryption Standard. U.S. Department of Commerce/National Institute of Standards and Technology, 2001 November 26.

[ANSI X9.62] Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA). American National Standards Institute, ANSI, 2005.

[ANSI X9.63] Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography. American National Standards Institute, ANSI, 2001.

[ASE_COMP] Composite product evaluation for smart card and similar devices, v1.2, Jan. 2012.

[BSI] BSI-PP-0006-2002 for Protection Profile – Secure Signature-Creation Device Type 3, Version 1.05 developed by CEN/ISSS – Information Society Standardization System, Workshop on Electronic Signatures.

[CC] Common Criteria for Information Technology Security Evaluation September 2012. Version 3.1. Revision 4.

[CMD] Especificación funcional de la Tarjeta DNIe-DCCF 3.0. Manual de comandos. V1.1 r4. 28/11/17.

[CVTDNIe] Ciclo de vida de la tarjeta DNIe-DCCF 3.0. v1.0 r10. 28/11/17.

[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.

[EN14890-1] Interfaz de aplicación para tarjetas inteligentes utilizadas como dispositivos seguros de creación de firma. Parte 1: Servicios básicos. Diciembre 2008.

[EN419211-2] EN 419211-2 Protection profiles for secure signature creation device — Part 2: Device with key generation (Perfil de protección para los dispositivos seguros de creación de firma. Parte 2: Dispositivo con generación de claves). 2013.

[EN419211-5] EN 419211-5 Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application (Perfil de protección para los dispositivos seguros de creación de firma. Parte 5: Dispositivo con generación de claves y comunicación confiada con aplicación de creación de firma). 2013.

[EN419212-1] Interfaz de aplicación para tarjetas inteligentes utilizadas como dispositivos seguros de creación de firma. Parte 1: Servicios básicos. Febrero 2015.

[3DES] National Institute of Standards and Technology. NIST Special Publication 800-67, Version 1.1.

[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.

[DE] Decisión de ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

[GOA] Guía operativa para administrador. Tarjeta DNIe-DCCF 3.0. v1.1 r4. 28/11/17.

[GOU] Guía Operativa para usuario final. Tarjeta DNIe-DCCF 3.0. v1.1 r4. 28/11/17.

[GP] Guía preparativa. Tarjeta DNIe-DCCF 3.0. v1.1 r4. 28/11/17.

[GRB] DNI electrónico. Guía de Referencia Básica. v1.3. 26/10/10.

[ISO7816-1] ISO/IEC 7816 Identification cards -- Integrated circuit cards -- Part 1: Cards with contacts -- Physical characteristics. 2011.

[ISO7816-2] ISO/IEC 7816 Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts. 2007.

[ISO7816-3] ISO/IEC 7816 Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols. 2006.

[ISO7816-4] Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange. 2005.

[ISO9796] Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms. 2002.

[ISO9797] Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher. 1999.

[ISO9798] ISO/IEC 9798-3 Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques. 1998.

[ISO14443-1] ISO/IEC 14443-1 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics. 2013.

[ISO14443-2] Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface. 2010.

[ISO14443-3] Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision. 2011.

[ISO14443-4] Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol. 2008.

[ISO15946-1] ISO/IEC 15946-1 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General. 2002.

[MR2] Assurance Continuity Maintenance Report. BSI-CC-PP-0059-2009-MA-02. 30/06/2016.

[MR5] Assurance Continuity Maintenance Report. BSI-CC-PP-0072-2012-MA-01. 30/06/2016.

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

[PKCS#1] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1: RSASSA-PKCS1-v1.5.

[PKCS#15] Cryptographic Token Information Format Standard. Version 1.1.

[PP] Protection profiles for secure signature creation device — Part 2: Device with key generation. Version: 2.0.1. January 2012.

[PP5] Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application. Version: 1.0.1. November 2012.

[SHS] Federal Information Processing Standards Publication 180-4 Secure Hash Standard, U.S. Department of Commerce/National Institute of Standards and Technology, March 2012.

[STIC] Declaración de seguridad: Security Target Lite. M7892 B11 Recertification. Common Criteria CC v3.1 EAL6 augmented (EAL6+). Infineon Technologies AG. Version 3.0. 10 November 2017.