Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DECLARACIÓN DE SEGURIDAD

TARJETA DNIE

8 de mayo de 2007

Common Criteria Versión 2.2

Common Criteria Revisión 326

Índice

Índice de figuras

Índice de tablas

1 Introducción

1.1 Identificación

1.1.1 Identificación de la Declaración de Seguridad

1 **Título:** Declaración de seguridad DNIe

2 **Versión:** 1.0

3 **Revisión:** 7 (Revisión pública)

4 **Autor:** FNMT - RCM

5 **Fecha de publicación:** 8 de mayo de 2007

1.1.2 Identificación del Objeto a Evaluar

6 **Fabricante:** FNMT - RCM

7 **Nombre del producto:** Tarjeta "DNIe"

8 **Versión:** 1.13

9 **Configuraciones (2)**:

- A11 H 4C34 EXP 1-1
- B11 H 4C34 EXP 1-1

1.2 Resumen

10 Esta declaración de seguridad establece las bases para la evaluación Common Criteria de la tarjeta "DNIe" en su versión y configuración identificadas anteriormente y de aquí en adelante tarjeta "DNIe".

11 La tarjeta DNIe es una tarjeta inteligente con capacidad criptográfica. Sus especificaciones técnicas están basadas en normas internacionales sobre tarjetas inteligentes, así como en las recomendaciones del grupo de trabajo PC/SC "Interoperatibility Specification for ICCs and Personal Computer System" versión 1.0 Diciembre 1997.

1.3 Ajuste a la norma "Common Criteria" ISO/IEC 15408

12 Esta declaración de seguridad cumple con los requisitos de la norma CC v 2.2, rev 326, partes 2 y 3, y define un nivel de garantía de evaluación EAL4, aumentado por los componentes AVA_VLA.4 Highly resistant,

AVA_MSU.3 Analysis and testing for insecure states y ALC_FLR.1 Basic flaw remediation, fortaleza de función alta.

13 La selección del nivel de evaluación se justifica por la necesidad de garantía de las propiedades de seguridad del producto, que vienen fijadas por el Perfil de Protección CWA14169, y que determina un producto altamente resistente a diferentes ataques, así como de mantener el producto libre de vulnerabilidades una vez certificado, (ALC_FLR.1 Basic flaw remediation).

2 Descripción del producto a evaluar.

14 La tarjeta DNIe es una tarjeta inteligente con capacidad criptográfica. Sus especificaciones técnicas están basadas en normas internacionales sobre tarjetas inteligentes, así como en las recomendaciones del grupo de trabajo PC/SC “Interoperatibility Specification for ICCs and Personal Computer System” versión 1.0 Diciembre 1997.

15 Es una tarjeta multiaplicación capaz de definir diferentes entornos de operación con su propio servicio de sistema de seguridad. Dispone de una estructura jerárquica de ficheros y datos tipo árbol.

16 La tarjeta DNIe está especialmente diseñada para infraestructuras de clave pública en las que se requiere autenticación de una entidad, integridad, confidencialidad de datos y el no repudio en origen. Mantiene el material sensible criptográfico siempre interno a la tarjeta y, protege su uso mediante control de acceso. De esta forma, se obtiene una considerable ventaja en términos de seguridad y portabilidad sobre las soluciones software.

17 La tarjeta DNIe 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.

18 Las características del procesador de ST 19WL34, en conjunción con el escrupuloso diseño del sistema operativo, consigue una herramienta eficaz que dificulta ataques basados en fuerza bruta y análisis diferencial.

19 Un rasgo diferenciado es la posibilidad de que las claves RSA sean generadas por el emisor y almacenadas en un estado inactivo. Así, se asegura que las claves no son operativas hasta que un usuario en conocimiento de una clave de activación desencadene el proceso interno de descifrado.

20 El Sistema Operativo proporciona 32 Kbytes de EEPROM. Este espacio de memoria puede ser utilizado para extender la funcionalidad de la tarjeta por el emisor de una forma segura y, se convierte en un amplio soporte de información de usuario protegido y portable.

21 El SO prevé la posibilidad de definir una estructura de ficheros acorde a la recomendación PKCS#15 de RSA con el fin de facilitar la interoperabilidad con aplicaciones basadas en tarjeta inteligente.

2.1 Características principales del chip ST 19WL34

a) CPU de 8 bits avanzado con modos extendidos de direccionamiento.

b) 224 Kbytes de ROM para código organizable en particiones.

c) 6 Kbytes de RAM organizable en particiones.

d) 34 Kbytes de EEPROM

   1) Zona de seguridad de tipo PROM

   2) Borrado/escritura hasta 64 bytes de EEPROM en 1.5ms.

   3) Retención de datos en EEPROM de un mínimo de 10 años.

   4) 500.000 ciclos de borrado/escritura garantizados.

   5) Organización basada en particiones.

e) Cripto-procesador hardware avanzado de 1088 bits.

   1) Exponenciaciones y multiplicaciones modulares basadas en el método Montgomery.

   2) Librería criptográfica implementada en firmware.

   3) Operadores de hasta 2176 bits.

f) Acelerador hardware con medidas de seguridad avanzadas para el cálculo de Triple Des.

g) Firewalls de seguridad entre particiones de memoria; permite especificar restricciones de acceso entre las diferentes áreas.

h) Reloj interno asíncrono de hasta 10Mhz.

i) 2 generadores internos de números impredecibles.

j) 3 timers de 8 bits.

k) Módulo para la transferencia asíncrona de datos.

l) Tensión de alimentación de 3 y 5 voltios.

m) Módulo para el cálculo de CRC ISO 3309.

n) Características de seguridad

   1) Identificación única para cada chip

2) Características adicionales de seguridad de última generación.

o) Funciones adicionales

1) Modo Standby de ahorro de energía

2) Rango de frecuencia externa 1-10Mhz.

3) Tensión de trabajo entre 2.7 y 5.5 voltios.

p) Certificación de seguridad Common Criteria EAL 5 +.

1) Certificación a fecha de 18-11-2005 del componente ST 19WL34A.

2) La certificación incluye tanto el hardware como las librerías criptográficas RSA y DES.

22 Tiempos de ejecución de diferentes funciones del cripto-procesador estimados por ST:

Tabla 1 Rendimiento del cripto-procesador

Operación	Tiempo
Firma RSA 1024 bits con CRT	85ms
Firma RSA 1024 bits sin CRT	282ms
Verificación RSA 1024 (e=0x10001)	5.5ms
Generación de claves RSA 1024 bits	2.5s
Firma RSA 2048 bits con CRT	570ms
Verificación RSA 2048 (e=0x10001)	91ms
Triple DES con mecanismos de seguridad avanzados	58us
DES con mecanismos de seguridad avanzados	43us

2.2 Ciclo de vida del TOE

23 Esta declaración de seguridad define como TOE una tarjeta inteligente apta para su uso por usuarios finales, lo que en terminología CC-JIL incluye desde las fases 1 - desarrollo del software embebido - hasta la fase 7 - uso final.

24 La correspondencia de estas fases con lo indicado en el Perfil de Protección CWA14169 se muestra en la tabla siguiente:

Tabla 2 Ciclo de vida del TOE

CC-JIL	Perfil de Protección CWA14169
Fase 1: desarrollo de software embebido.	Design
Fase 2: desarrollo del circuito integrado	
Fase 3: fabricación del circuito integrado y pruebas	Fabrication
Fase 4: empaquetado y pruebas del circuito integrado	
Fase 5: finalización del producto	
Fase 6: personalización	Personalisation
Fase 7: uso del producto	Usage
	Destruction

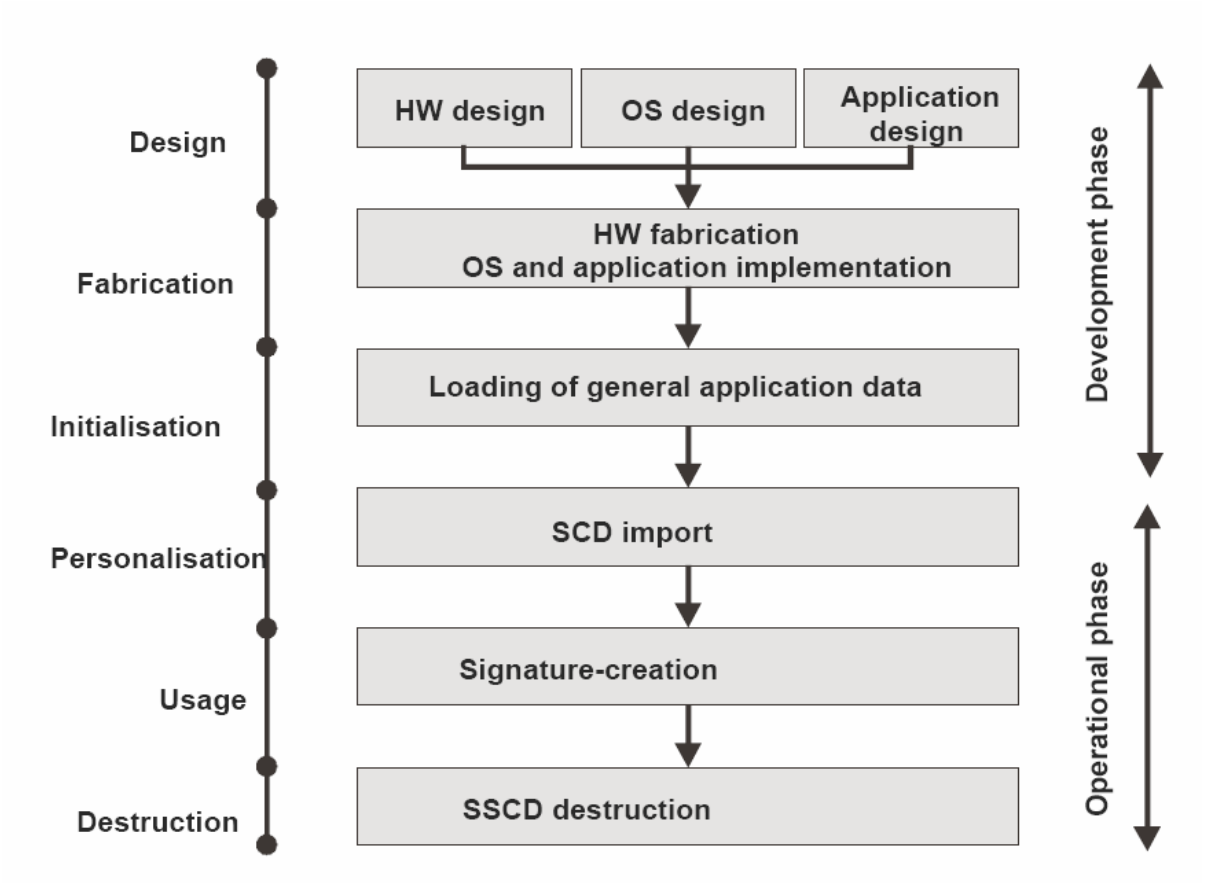

Figura 1 - Ciclo de vida conforme CWA14169

3 Entorno de seguridad.

3.1 Activos, usuarios y atacantes

Activos

1. Datos de creación de firma (SCD): clave privada utilizada para realizar una operación de firma electrónica (se debe mantener la confidencialidad de los SCD).

2. Datos de verificación de firma (SVD): clave pública asociada con los datos de creación de firma (SCD) y utilizada para realizar una verificación de firma electrónica (se debe mantener la integridad de los SVD cuando se exportan).

3. Datos a ser firmados (DTBS) y representación de DTBS: conjunto de datos o su representación que se quieren firmar (se debe mantener su integridad).

4. Datos de verificación de autenticación (VAD): Número de identificación personal (PIN) o datos biométricos introducidos por el usuario final para realizar una operación de firma (se debe mantener la confidencialidad y autenticidad de los VAD según lo requiera el método de autenticación utilizado).

5. Datos de autenticación de referencia (RAD). Referencia del número de identificación personal (PIN) o referencia de autenticación biométrica utilizadas para identificar y autenticar al usuario final (se debe mantener la integridad y confidencialidad de los RAD).

6. Función de creación de firma del dispositivo seguro de creación de firma (SSCD) que utiliza los datos de creación de firma (SCD): (se debe mantener la calidad de la función para que pueda participar de la validez legal de las firmas electrónicas).

7. Firma electrónica: (Se debe garantizar la imposibilidad de falsificación de las firmas electrónicas).

Sujetos

1. **S. User** Usuario final del objeto de evaluación (TOE) que puede ser identificado como Administrador o Firmante

2. **S. Admin** Usuario encargado de realizar la inicialización, personalización u otras funciones administrativas del objeto de evaluación (TOE)

3. **S. Signatory** Usuario que posee el objeto de evaluación (TOE) y lo utiliza en su propio nombre o en nombre de la persona legal, física o jurídica, a la que representa.

Amenazas y sus agentes

S.OFFCARD **Atacante.** Una persona o un proceso actuando en su nombre localizado fuera del objeto de evaluación (TOE). El principal objetivo del atacante S.OFFCARD es acceder a información sensible de la Aplicación. El atacante tiene una capacidad de ataque alta y no conoce ningún secreto.

3.2 Hipótesis.

A.CGA Aplicación de generación de certificados confiable

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

A.SCA Aplicación de creación de firma confiable

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

3.3 Amenazas a los activos del producto.

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

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

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

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

T.SCD_Derive Deducción de los datos de creación de firma

29 Un atacante deduce los datos de creación de firma (SCD) de los datos conocidos públicamente, como los datos de verificación de firma (SVD) que

corresponden a los SCD o las firmas creadas por medio de los SCD o cualquier otro dato comunicado fuera del objeto de evaluación (TOE), que constituye una amenaza contra la confidencialidad de los SCD.

T.Sig_Forgery Falsificación de la firma electrónica

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

T.Sig_Repud Repudio de firmas

31 Si un atacante puede atacar cualquier activo con éxito, entonces el no repudio de la firma electrónica está comprometido.

32 El firmante puede negar haber firmado datos usando los datos de creación de firma (SCD) del objeto de evaluación (TOE) bajo su control aun cuando la firma se verifica con éxito con los datos de verificación de firma (SVD) contenidos en su certificado no revocado.

T.SVD_Forgery Falsificación de los datos de verificación de firma

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

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

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

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

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

3.4 Políticas de seguridad.

P.CSP_Qcert Certificado reconocido

36 El proveedor de servicios de certificación (CSP) usa una aplicación de generación de certificados (CGA) confiable para generar el certificado reconocido para los datos de verificación de firma (SVD) generados por el dispositivo seguro de creación de firma (SSCD). Los certificados reconocidos contienen, al menos, los elementos definidos en el Anexo I de la Directiva, es decir, el nombre del firmante y los SVD que se corresponden con los datos de creación de firma (SCD) implementados en el objeto de evaluación (TOE) bajo el único control del firmante. El CSP asegura el uso del TOE en las firmas a través del certificado o de otra información públicamente disponible.

P.Qsign Firmas electrónicas reconocidas

37 El firmante usa un sistema de creación de firma para firmar los datos con firmas electrónicas reconocidas. La aplicación de creación de firma (SCA) presenta los datos a ser firmados (DTBS) al firmante. La firma electrónica reconocida se basa en un certificado reconocido y la crea un dispositivo seguro de creación de firma (SSCD).

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

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

4 Objetivos de seguridad.

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

4.1 Objetivos de seguridad aplicables al producto.

40 Los objetivos de seguridad aplicables a la tarjeta DNIe son los siguientes. Estos objetivos contrarrestan las amenazas identificadas y cumplen con las políticas de seguridad e hipótesis definidas en el Perfil de Protección CWA14169

OT.EMSEC_Design Seguridad física en las emisiones

41 Diseñar y fabricar el objeto de evaluación (TOE) de manera que se pueda controlar la producción de emisiones inteligibles dentro de los límites especificados.

OT.Lifecycle_Security Seguridad del ciclo de vida

42 El objeto de evaluación (TOE) debe detectar los fallos de seguridad durante su inicialización, personalización y su uso operacional. El TOE debe proporcionar técnicas de destrucción seguras de los datos de creación de firma (SCD) en caso de regeneración.

OT.SCD_Secrecy Confidencialidad de los datos de creación de firma

43 La confidencialidad de los datos de creación de firma (SCD) (utilizados para la generación de la firma) está razonablemente garantizada contra ataques de alta capacidad.

OT.SCD_SVD_Corresp Correspondencia entre datos de verificación de firma (SVD) y datos de creación de firma (SCD)

44 El objeto de evaluación (TOE) debe garantizar la correspondencia entre los datos de verificación de firma (SVD) y los datos de creación de firma (SCD). El TOE debe verificar, bajo petición, la correspondencia entre los SCD almacenados en el TOE y los SVD, si han sido enviados al TOE.

OT.SVD_Auth_TOE El objeto de evaluación (TOE) garantiza la autenticidad de los datos de verificación de firma (SVD)

45 El objeto de evaluación (TOE) proporciona medios para permitir a la aplicación de generación de certificados (CGA) verificar la autenticidad de los datos de verificación de firma (SVD) exportados por ese TOE.

OT.Tamper_ID Detección de manipulación

46 El objeto de evaluación (TOE) posee características que detectan la manipulación física de un componente del sistema y utiliza dichas características para limitar las brechas de seguridad.

OT.Tamper_Resistance Resistencia a la manipulación

47 El objeto de evaluación (TOE) impide o resiste la manipulación física con dispositivos y componentes específicos del sistema.

OT.Init Generación de datos de creación de firma (SCD)/ datos de verificación de firma (SVD)

48 El objeto de evaluación (TOE) posee características de seguridad para garantizar que sólo los usuarios autorizados invocan la generación de los datos de creación de firma (SCD) y los datos de verificación de firma (SVD).

OT.SCD_Unique Unicidad de los datos de creación de firma

49 El objeto de evaluación (TOE) debe garantizar la calidad criptográfica del par datos de creación de firma (SCD)/ datos de verificación de firma (SVD) para la firma electrónica reconocida. Los SCD utilizados para la generación de firma sólo pueden producirse una vez en la práctica y no pueden reconstruirse a partir de los SVD. En ese contexto “sólo pueden producirse una vez en la práctica” significa que la probabilidad de dos SCD iguales es despreciablemente baja.

OT.DTBS_Integrity_TOE Verificación de la integridad de la representación de datos a ser firmados (DTBS)

50 El objeto de evaluación (TOE) debe verificar que la representación de datos a ser firmados (DTBS) recibida desde la aplicación de creación de firma (SCA) no ha sido alterada en el tránsito entre la SCA y el TOE. El propio TOE debe garantizar que la representación de DTBS no es alterada por el mismo TOE. Esto no entra en conflicto con el proceso de creación de firma donde los propios DTBS pueden ser objeto de un hash realizado por el TOE.

OT.Sigy_SigF Función de generación de firma sólo para el firmante legítimo

51 El objeto de evaluación (TOE) proporciona la función de generación de firma sólo para el firmante legítimo y protege los datos de creación de firma (SCD) contra su uso por parte de otros. El TOE debe resistir ataques con capacidad alta.

OT_Sig_Secure Seguridad criptográfica de la firma electrónica

52 El objeto de evaluación (TOE) genera firmas electrónicas, mediante técnicas de cifrado fuerte que no pueden ser falsificadas sin el conocimiento de los

datos de creación de firma (SCD). Los SCD no se pueden reconstruir utilizando las firmas electrónicas. Las firmas electrónicas deben resistir estos ataques incluso cuando se ejecutan con una capacidad de ataque alta.

4.2 Objetivos de seguridad aplicables al entorno.

53 Los objetivos de seguridad aplicables al entorno de operación de la tarjeta DNIe son los siguientes. Estos objetivos contrarrestan las amenazas identificadas y cumplen con las políticas de seguridad e hipótesis definidas en el Perfil de Protección CWA14169

OE.CGA_Qcert Generación de certificados reconocidos

54 La aplicación de generación de certificados (CGA) genera certificados reconocidos que incluyen:

a) El nombre del firmante que controla el objeto de evaluación (TOE).

b) Los datos de verificación de firma (SVD) que se corresponden con los datos de creación de firma (SCD) implementados en el objeto de evaluación (TOE) bajo el único control del firmante.

c) La firma electrónica avanzada del proveedor de servicios de certificación (CSP).

OE.SVD_Auth_CGA La aplicación de generación de certificados (CGA) verifica la autenticidad de los datos de verificación de firma (SVD)

55 La aplicación de generación de certificados (CGA) verifica que el dispositivo seguro de creación de firma (SSCD) es el remitente de los datos de verificación de firma (SVD) recibidos así como la integridad de dichos SVD. La CGA verifica la correspondencia entre los datos de creación de firma (SCD) en el SSCD del firmante y los SVD en el certificado reconocido.

OE.HI_VAD Protección de los datos de verificación de autenticación (VAD)

56 Si un dispositivo externo proporciona el interfaz humano (HI) para la autenticación del usuario, este dispositivo garantizará la confidencialidad y la integridad de los datos de verificación de autenticación (VAD) según lo necesite el método de autenticación empleado.

OE.SCA_Data_Intend Datos que se pretenden firmar

57 La aplicación de creación de firma (SCA)

a) genera la representación de datos a ser firmados (DTBS) de los datos que han sido presentados como DTBS, y que el firmante pretende firmar, en un formato apropiado para su firma por el objeto de evaluación (TOE),

b) envía la representación de datos a ser firmados (DTBS) al objeto de evaluación (TOE) y permite que el TOE verifique la integridad de dicha representación y

c) adjunta la firma producida por el objeto de evaluación (TOE) a los datos o la proporciona separadamente.

5 Requisitos de seguridad.

5.1 Requisitos de seguridad aplicables al producto.

5.1.1 Requisitos funcionales.

FCS_CKM.1 Generación de claves criptográficas

FCS_CKM.1.1 **La TSF debe generar las claves criptográficas de acuerdo con el algoritmo de generación de claves criptográficas especificado [RSA PKCS#1 v1.5, Miller-Rabin como test de primalidad] y con un tamaño de claves criptográficas especificado [1024 a 2048 bits] que cumpla lo siguiente: RSA, PKCS#1 v1.5**

FCS_CKM.4 Destrucción de claves criptográficas

FCS_CKM.4.1 **La TSF debe destruir las claves criptográficas en caso de regeneración de los datos de creación de firma (SCD) de acuerdo con un método de destrucción de claves criptográficas especificado [borrado de la memoria] que cumpla lo siguiente: [puesta a cero de la zona de memoria ocupada por las claves (ver** FDP_RIP.1 Subset residual information protection**)]**

FCS_COP.1 Operación criptográfica

FCS_COP.1.1/CORRESP **La TSF debe realizar la verificación de la correspondencia datos de creación de firma (SCD)/ datos de verificación de firma (SVD) de acuerdo con un algoritmo criptográfico especificado [SHA1, RSA, 3DES CBC] y con los tamaños de claves criptográficas [1024 a 2048 para cifra asimétrica, 16 ó 24 bytes para cifra simétrica] que cumplan lo siguiente: SHA1, RSA, 3DES CBC.**

FCS_COP.1.1/SIGNING **La TSF debe realizar la generación de firma electrónica de acuerdo con un algoritmo criptográfico especificado [SHA1, RSA, 3DES CBC] y con los tamaños de claves criptográficas [1024 a 2048 para cifra asimétrica, 16 ó 24 bytes para cifra simétrica] que cumplan lo siguiente: SHA1, RSA, 3DES CBC**

FDP_ACC.1 Control de acceso parcial

FDP_ACC.1.1 / SFP de Transferencia de datos de verificación de firma (SVD) **La TSF debe aplicar la SFP de Transferencia de datos de verificación de firma (SVD) en la exportación de los SVD por parte del Usuario.**

FDP_ACC.1.1 / SFP de Inicialización de datos de creación de firma (SCD) **La TSF debe aplicar la SFP de Inicialización en la generación del par datos de creación de firma (SCD)/ datos de verificación de firma (SVD) por parte del Usuario.**

FDP_ACC.1.1 / SFP de Personalización **La TSF debe aplicar la SFP de Personalización en la creación de los datos de autenticación de referencia (RAD) por parte del Administrador.**

FDP_ACC.1.1 / SFP de creación de firma **La TSF debe aplicar la SFP de creación de firma en:**

1. El envío de la representación de datos a ser firmados (DTBS) por parte de la aplicación de creación de firma (SCA)

2. La firma de la representación de datos a ser firmados (DTBS) por parte del Firmante

FDP_ACF.1 Control de acceso basado en atributo de Seguridad

58 Los atributos de seguridad para el usuario, los componentes del *objeto de evaluación (TOE)* y los estados relacionados son

Usuario, sujeto u objeto con el que está asociado el atributo	Atributo	Estado
Atributo General		
Usuario	Rol	Administrador, Firmante
Atributo de inicialización		
Usuario	Gestión de *datos de creación de firma (SCD)/ datos de verificación de firma (SVD)*	Autorizada, no autorizada
Atributo de creación de firma		
datos de creación de firma (SCD)	*datos de creación de firma (SCD)* operacional	No, sí
Datos a ser firmados (DTBS)	Enviados por una *aplicación de creación de firma (SCA)* autorizada	No, sí

FDP_ACF.1.1 / SFP de Inicialización **La TSF debe aplicar la SFP de Inicialización a objetos basándose en el atributo General y en el atributo de inicialización.**

FDP_ACF.1.2 / SFP de Inicialización **La TSF debe aplicar las siguientes reglas para determinar si una operación entre sujetos y objetos controlados está permitida:**

El usuario con el atributo de seguridad "rol" establecido como "Administrador" o como "Firmante" y con el atributo de seguridad "Gestión de datos de creación de firma (SCD)/ datos de verificación de firma (SVD)" establecido como "autorizado" tiene permiso para generar el par SCD/ SVD.

FDP_ACF.1.3 / SFP de Inicialización **La TSF debe autorizar explícitamente el acceso de sujetos a objetos basándose en las siguientes reglas adicionales: ninguna.**

FDP_ACF.1.4 / SFP de Inicialización **La TSF debe negar explícitamente el acceso de sujetos a objetos basándose en la regla:**

El usuario con el atributo de seguridad "rol" establecido como "Administrador" o como "Firmante" y con el atributo de seguridad "Gestión de datos de creación de firma (SCD)/ datos de verificación de firma (SVD) establecido como "No autorizado" no tiene permiso para generar el par SCD/ SVD

FDP_ACF.1.1 / SFP de Transferencia de datos de verificación de firma (SVD) **La TSF debe aplicar la SFP de Transferencia de datos de verificación de firma (SVD) a objetos basándose en el atributo General.**

FDP_ACF.1.2 / SFP de Transferencia de datos de verificación de firma (SVD) **La TSF debe aplicar las siguientes reglas para determinar si una operación entre sujetos y objetos controlados está permitida:**

El usuario con el atributo de seguridad "rol" establecido como "Administrador" o como "Firmante" está autorizado a exportar los datos de verificación de firma (SVD).

FDP_ACF.1.3 / SFP de Transferencia de datos de verificación de firma (SVD) **La TSF debe autorizar explícitamente el acceso de sujetos a objetos basándose en las siguientes reglas adicionales: ninguna.**

FDP_ACF.1.4 / SFP de Transferencia de datos de verificación de firma (SVD) **La TSF debe negar explícitamente el acceso de sujetos a objetos basándose en la regla: ninguna.**

FDP_ACF.1.1 / SFP de Personalización **La TSF debe aplicar la SFP de Personalización a objetos basándose en el atributo General.**

FDP_ACF.1.2 / SFP de Personalización **La TSF debe aplicar las siguientes reglas para determinar si una operación entre sujetos y objetos controlados está permitida:**

El usuario con el atributo de seguridad "rol" establecido como "Administrador" está autorizado a crear los datos de autenticación de referencia (RAD).

FDP_ACF.1.3 / SFP de Personalización **La TSF debe autorizar explícitamente el acceso de sujetos a objetos basándose en las siguientes reglas adicionales: ninguna.**

FDP_ACF.1.4 / SFP de Personalización **La TSF debe negar explícitamente el acceso de sujetos a objetos basándose en la regla: ninguna.**

FDP_ACF.1.1 / SFP de Creación de firma **La TSF debe aplicar la SFP de Creación de firma a objetos basándose en el atributo General y en el atributo de Creación de firma.**

FDP_ACF.1.2 / SFP de Creación de firma **La TSF debe aplicar las siguientes reglas para determinar si una operación entre sujetos y objetos controlados está permitida:**

El usuario con el atributo de seguridad "rol" establecido como "Firmante" está autorizado a crear firmas electrónicas para los datos a ser firmados (DTBS) enviados por una aplicación de creación de firma (SCA) autorizada con los datos de creación de firma (SCD) del Firmante cuyo atributo de seguridad "SCD operacional" está establecido como "sí".

FDP_ACF.1.3 / SFP de Creación de firma **La TSF debe autorizar explícitamente el acceso de sujetos a objetos basándose en las siguientes reglas adicionales: ninguna.**

FDP_ACF.1.4 / SFP de Creación de firma **La TSF debe negar explícitamente el acceso de sujetos a objetos basándose en la regla:**

a) El usuario con el atributo de seguridad "rol" establecido como "Firmante" no está autorizado a crear firmas electrónicas para los datos a ser firmados (DTBS) que no hayan sido enviados por una aplicación de creación de firma (SCA) autorizada con los datos de creación de firma (SCD) del Firmante cuyo atributo de seguridad " SCD operacional" esté establecido como "sí".

b) El usuario con el atributo de seguridad "rol" establecido como "Firmante" no está autorizado a crear firmas electrónicas para los datos a ser firmados (DTBS) enviados por una aplicación de creación de firma (SCA) autorizada con los datos de creación de firma (SCD) del Firmante cuyo atributo de seguridad "SCD operacional" está establecido como "No".

FDP_ETC.1 Exportación de datos de usuario sin atributos de seguridad

FDP_ETC.1.1 / Transferencia de datos de verificación de firma (SVD) **La TSF debe aplicar la Transferencia de datos de verificación de firma (SVD) al exportar los datos de usuario, controlados por SFP(s), fuera del TSC.**

FDP_ETC.1.2 / Transferencia de datos de verificación de firma (SVD) **La TSF debe exportar los datos de usuario sin sus atributos de seguridad asociados.**

FDP_ITC.1 Importación de datos de usuario sin atributos de seguridad

FDP_ITC.1.1/DTBS **La TSF debe aplicar la SFP de Creación de firma cuando se importen datos de usuario, controlados bajo la SFP, desde fuera del TSC.**

FDP_ITC.1.2/DTBS **La TSF debe ignorar cualquier atributo de seguridad asociado con los datos de usuario cuando se importen desde fuera del TSC.**

FDP_ITC.1.3/DTBS **La TSF debe aplicar las siguientes reglas cuando se importen datos de usuario controlados bajo la SFP desde fuera del TSC: la representación de datos a ser firmados (DTBS) debe ser enviada por una aplicación de creación de firma (SCA) autorizada.**

FDP_RIP.1 Protección parcial de la información residual

FDP_RIP.1.1 **La TSF debe garantizar que cualquier contenido de información anterior de un recurso no está disponible tras la liberación del recurso para los siguientes objetos: datos de creación de firma (SCD), datos de verificación de autenticación (VAD), datos de autenticación de referencia (RAD).**

FDP_SDI.2 Supervisión de la integridad de los datos almacenados y acción

59 Los siguientes datos guardados de forma permanente por el objeto de evaluación (TOE) tienen el atributo de dato de usuario “datos permanentes almacenados con integridad verificada”

1. **Datos de creación de firma (SCD)**
2. **Datos de autenticación de referencia (RAD)**
3. **Datos de verificación de firma (SVD) (si están almacenados permanentemente por el objeto de evaluación (TOE))**

FDP_SDI.2.1 / Permanente **La TSF debe supervisar los datos de usuario almacenados dentro del TSC contra error de integridad en todos los objetos, basándose en los siguientes atributos: datos permanentes almacenados con integridad verificada**.

FDP_SDI.2.2 / Permanente **Ante la detección de un error de integridad de los datos, la TSF debe**

1. Prohibir el uso de datos alterados

2. Informar al Firmante del error de integridad

60 La representación de datos a ser firmados (DTBS) almacenada temporalmente por el objeto de evaluación (TOE) tiene el atributo de dato de usuario "datos almacenados con integridad verificada"

FDP_SDI.2.1 / DTBS **La TSF debe supervisar los datos de usuario almacenados dentro del TSC contra error de integridad en todos los objetos, basándose en los siguientes atributos: datos almacenados con integridad verificada.**

FDP_SDI.2.2 / DTBS **Ante la detección de un error de integridad de los datos, la TSF debe**

1. Prohibir el uso de datos alterados

2. Informar al Firmante del error de integridad

FDP_UIT.1 Integridad del intercambio de datos

FDP_UIT.1.1 / Transferencia de datos de verificación de firma (SVD) **La TSF debe aplicar la SFP de Transferencia de datos de verificación de firma (SVD) para poder transmitir datos de usuario de una manera protegida contra errores de modificación e inserción.**

FDP_UIT.1.2 / Transferencia de datos de verificación de firma (SVD) **La TSF debe poder determinar a la recepción de los datos de usuario si ha habido modificación e inserción.**

FDP_UIT.1.1 / DTBS del objeto de evaluación (TOE) **La TSF debe aplicar la SFP de Creación de firma para poder recibir la representación de datos a ser firmados (DTBS) de una manera protegida contra errores de modificación, borrado e inserción.**

FDP_UIT.1.2 / DTBS del objeto de evaluación (TOE) **La TSF debe poder determinar, a la recepción de los datos de usuario, si ha habido modificación, borrado e inserción.**

FIA_AFL.1 Gestión de fallos de autenticación

FIA_AFL.1.1 **La TSF debe detectar cuándo ocurren [3] intentos de autenticación infructuosos en lo relativo a intentos consecutivos de autenticación fallidos.**

FIA_AFL.1.2 **Cuando el número definido de intentos de autenticación infructuosos haya sido alcanzado o superado, la TSF debe bloquear los datos de autenticación de referencia (RAD).**

FIA_ATD.1 Definición del atributo de usuario

FIA_ATD.1.1 **La TSF debe mantener la siguiente lista de atributos de seguridad que pertenecen a los usuarios individuales: datos de autenticación de referencia (RAD).**

FIA_UAU.1 Secuencia de autenticación

FIA_UAU.1.1 **La TSF debe permitir que se realicen las siguientes acciones**

1. Identificación del usuario mediante la TSF exigido por FIA_UID.1.

2. Establecer un canal confiable entre el usuario local y el objeto de evaluación (TOE) mediante la TSF exigido por FTP_TRP.1 / objeto de evaluación (TOE).

3. Establecer una canal confiable entre la aplicación de creación de firma (SCA) y el objeto de evaluación (TOE) mediante la TSF exigido por FTP_ITC.1 / Importación de datos a ser firmados (DTBS).

En nombre del usuario antes de que el usuario se autentique

FIA_UAU.1.2 **La TSF debe exigir que cada usuario sea autenticado con éxito antes de permitir cualquier otra acción mediada por la TSF en nombre de ese usuario.**

FIA_UID.1 Secuencia de identificación

FIA_UID.1.1 **La TSF debe permitir que se realicen las siguientes acciones en nombre del usuario antes de que el usuario se identifique:**

1. Establecer un canal confiable entre el usuario local y el objeto de evaluación (TOE) mediante la TSF exigido por FTP_TRP.1 / TOE.

2. Establecer un canal confiable entre la aplicación de creación de firma (SCA) y el objeto de evaluación (TOE) mediante la TSF exigido por FTP_ITC.1 / Importación de datos a ser firmados (DTBS).

FIA_UID.1.2 **La TSF debe exigir que cada usuario se identifique con éxito antes de permitir cualquier otra acción mediada por la TSF en nombre de ese usuario.**

FMT_MOF.1 Gestión del comportamiento de las funciones de seguridad

FMT_MOF.1.1 **La TSF debe restringir la capacidad de habilitar la función de creación de firma al Firmante.**

FMT_MSA.1 Gestión de los atributos de seguridad

FMT_MSA.1.1 / Administrador **La TSF debe aplicar la SFP de Inicialización para restringir la capacidad de modificar los atributos de seguridad Gestión de datos de creación de firma (SCD) / datos de verificación de firma (SVD) al Administrador.**

FMT_MSA.1.1 / Firmante **La TSF debe aplicar la SFP de Creación de firma para restringir la capacidad de modificar los atributos de seguridad datos de creación de firma (SCD) operacional al Firmante.**

FMT_MSA.2 Atributos de seguridad seguros

FMT_MSA.2.1 **La TSF debe garantizar que sólo se aceptan valores seguros para los atributos de seguridad.**

FMT_MSA.3 Inicialización de atributos estáticos

FMT_MSA.3.1 **La TSF debe aplicar la SFP de Inicialización y la SFP de Creación de firma para proporcionar los valores por defecto restrictivos de los atributos de seguridad que se usan para aplicar la SFP.**

Refinamiento: El atributo de seguridad de los datos de creación de firma (SCD) "SCD operacional" se fija como "No" después de la generación de los datos de creación de firma (SCD).

FMT_MSA.3.2 **La TSF debe permitir al Administrador especificar valores iniciales alternativos para sustituir los valores predefinidos cuando se genera un objeto o información**.

FMT_MTD.1 Gestión de datos de TSF

FMT_MTD.1.1 **La TSF debe restringir la capacidad de modificar los datos de autenticación de referencia (RAD) al Firmante.**

FMT_SMF.1 Especificación de funciones de gestión

FMT_SMF.1.1 **La TSF debe ser capaz de ejecutar las siguientes funciones de gestión de la seguridad: operaciones de pre y personalización.**

FMT_SMR.1 Roles de seguridad

FMT_SMR.1.1 **La TSF debe mantener los roles Administrador y Firmante.**

FMT_SMR.1.2 **La TSF debe poder asociar usuarios con roles.**

FPT_AMT.1 Pruebas de la máquina abstracta

FPT_AMT.1.1 **La TSF debe ejecutar una colección de pruebas [durante el arranque inicial] para demostrar el correcto funcionamiento de las hipótesis de seguridad dadas por la máquina abstracta subyacente a la TSF.**

FPT_EMSEC.1 Emisiones del objeto de evaluación (TOE)

FPT_EMSEC.1.1 **El objeto de evaluación (TOE) no debe emitir [información sobre el consumo de potencia del circuito integrado ni los tiempos de ejecución de comandos] en exceso de [información no útil] permitiendo el acceso a los datos de autenticación de referencia (RAD) y a los datos de creación de firma (SCD).**

FPT_EMSEC.1.2 **La TSF debe garantizar que [S.OFFCARD] es incapaz de utilizar los siguientes interfaces [contactos VCC, GND, IO] para obtener acceso a los datos de autenticación de referencia (RAD) y a los datos de creación de firma (SCD).**

FPT_FLS.1 Fallo con preservación del estado seguro

FPT_FLS.1.1 **La TSF debe conservar un estado seguro cuando ocurran los siguientes tipos de fallos: cualquier ataque de protocolo de comunicaciones, alteraciones de la alimentación VCC.**

FPT_PHP.1 Detección pasiva de ataque físico

FPT_PHP.1.1 **La TSF debe proporcionar detección inequívoca de manipulación física que pueda comprometer la seguridad de la TSF.**

FPT_PHP.1.2 **La TSF debe proporcionar la capacidad para determinar si se ha producido alguna manipulación física en los dispositivos o en los elementos de la TSF.**

FPT_PHP.3 Resistencia al ataque físico

FPT_PHP.3.1 **La TSF debe resistir [manipulación física y sondas físicas] de [la TSF] respondiendo automáticamente de manera que la TSP no sea violada.**

FPT_TST.1 Pruebas de TSF

FPT_TST.1.1 **La TSF debe realizar una serie de auto-tests [durante el arranque inicial, a petición del usuario autorizado] [con VCC] que demuestren el correcto funcionamiento de la TSF.**

FPT_TST.1.2 **La TSF debe proporcionar a los usuarios autorizados la capacidad de verificar la integridad de los datos de TSF**

FPT_TST.1.3 **La TSF debe proporcionar a los usuarios autorizados la capacidad para verificar la integridad del código ejecutable de TSF almacenado.**

FTP_ITC.1 Canal confiable inter - TSF

FTP_ITC.1.1 / Transferencia de datos de verificación de firma (SVD) **La TSF debe proporcionar un canal de comunicación, entre sí misma y una aplicación de generación de certificados (CGA) confiable remota, que sea distinto lógicamente de otros canales de comunicación y que proporcione la identificación segura de sus extremos y la protección de los datos del canal contra su modificación o pérdida de confidencialidad.**

FTP_ITC.1.2 / Transferencia de datos de verificación de firma (SVD) **La TSF debe permitir a [el producto de tecnología de la información (IT) confiable remoto] iniciar la comunicación a través del canal confiable.**

FTP_ITC.1.3 / Transferencia de datos de verificación de firma (SVD) **La TSF o la aplicación de generación de certificados (CGA) debe iniciar la comunicación a través del canal confiable para la exportación de datos de verificación de firma (SVD).**

FTP_ITC.1.1 / Importación de datos a ser firmados (DTBS) **La TSF debe proporcionar un canal de comunicación, entre sí misma y un producto de tecnología de la información (IT) confiable remoto, que sea distinto lógicamente de otros canales de comunicación y que proporcione la identificación segura de sus extremos y la protección de los datos del canal contra su modificación o pérdida de confidencialidad.**

FTP_ITC.1.2 / Importación de datos a ser firmados (DTBS) **La TSF debe permitir a la aplicación de creación de firma (SCA) iniciar la comunicación a través del canal confiable.**

FTP_ITC.1.3 / Importación de datos a ser firmados (DTBS) **La TSF o la aplicación de creación de firma (SCA) debe iniciar la comunicación a través del canal confiable para firmar la representación de datos a ser firmados (DTBS).**

FTP_TRP.1 Trusted path

61 Véase Perfil de Protección CWA14169.

5.1.2 Requisitos de garantía.

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

a) EAL4

b) AVA_VLA.4

c) AVA_MSU.3

d) ALC_FLR.1

63 Por tanto, los requisitos de garantía aplicables son:

ACM_AUT.1 Automatización parcial de la Gestión de la Configuración

Dependencias: **ACM_CAP.4 Generation support and acceptance procedures**

Acciones del fabricante:

ACM_AUT.1.1D **The developer shall use a CM system.**

ACM_AUT.1.2D **The developer shall provide a CM plan.**

Contenido y presentación de elementos de evidencias:

ACM_AUT.1.1C **The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.**

ACM_AUT.1.2C **The CM system shall provide an automated means to support the generation of the TOE.**

ACM_AUT.1.3C **The CM plan shall describe the automated tools used in the CM system.**

ACM_AUT.1.4C **The CM plan shall describe how the automated tools are used in the CM system.**

ACM_CAP.4 Soporte a la generación y procedimientos de aceptación

Dependencias: **ALC_DVS.1 Identification of security measures**

Acciones del fabricante:

ACM_CAP.4.1D **The developer shall provide a reference for the TOE.**

ACM_CAP.4.2D **The developer shall use a CM system.**

ACM_CAP.4.3D **The developer shall provide CM documentation.**

Contenido y presentación de elementos de evidencias:

ACM_CAP.4.1C **The reference for the TOE shall be unique to each version of the TOE.**

ACM_CAP.4.2C **The TOE shall be labelled with its reference.**

ACM_CAP.4.3C **The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.**

ACM_CAP.4.4C **The configuration list shall uniquely identify all configuration items that comprise the TOE.**

ACM_CAP.4.5C **The configuration list shall describe the configuration items that comprise the TOE.**

ACM_CAP.4.6C **The CM documentation shall describe the method used to uniquely identify the configuration items.**

ACM_CAP.4.7C **The CM system shall uniquely identify all configuration items.**

ACM_CAP.4.8C **The CM plan shall describe how the CM system is used.**

ACM_CAP.4.9C **The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.**

ACM_CAP.4.10C **The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.**

ACM_CAP.4.11C **The CM system shall provide measures such that only authorised changes are made to the configuration items.**

ACM_CAP.4.12C **The CM system shall support the generation of the TOE.**

ACM_CAP.4.13C **The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.**

ACM_SCP.2 Cobertura del seguimiento de problemas por parte de la Gestión de la Configuración

Dependencias: **ACM_CAP.4 Generation support and acceptance procedures**

Acciones del fabricante:

ACM_SCP.2.1D **The developer shall provide a list of configuration items for the TOE.**

Contenido y presentación de elementos de evidencias:

ACM_SCP.2.1C **The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.**

ADO_DEL.2 Detección de modificación

Dependencias: **ACM_CAP.4 Generation support and acceptance procedures**

Acciones del fabricante:

ADO_DEL.2.1D **The developer shall document procedures for delivery of the TOE or parts of it to the user.**

ADO_DEL.2.2D **The developer shall use the delivery procedures.**

Contenido y presentación de elementos de evidencias:

ADO_DEL.2.1C **The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.**

ADO_DEL.2.2C **The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.**

ADO_DEL.2.3C **The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.**

ADO_IGS.1 Procedimientos de instalación, generación y arranque

Dependencias: **AGD_ADM.1 Administrator guidance**

Acciones del fabricante:

ADO_IGS.1.1D **The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.**

Contenido y presentación de elementos de evidencias:

ADO_IGS.1.1C **The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.**

ADV_FSP.2 Interfaces externos totalmente definidos

Dependencias:: **ADV_RCR.1 Informal correspondence demonstration**

Acciones del fabricante:

ADV_FSP.2.1D **The developer shall provide a functional specification.**

Contenido y presentación de elementos de evidencias:

ADV_FSP.2.1C **The functional specification shall describe the TSF and its external interfaces using an informal style.**

ADV_FSP.2.2C **The functional specification shall be internally consistent.**

ADV_FSP.2.3C **The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.**

ADV_FSP.2.4C **The functional specification shall completely represent the TSF.**

ADV_FSP.2.5C **The functional specification shall include rationale that the TSF is completely represented.**

ADV_HLD.2 Diseño de alto nivel de aplicación de la seguridad

Dependencias: **ADV_FSP.2 Fully defined external interfaces**

ADV_RCR.1 Informal correspondence demonstration

Acciones del fabricante:

ADV_HLD.2.1D **The developer shall provide the high-level design of the TSF.**

Contenido y presentación de elementos de evidencias:

ADV_HLD.2.1C **The presentation of the high-level design shall be informal.**

ADV_HLD.2.2C **The high-level design shall be internally consistent.**

ADV_HLD.2.3C **The high-level design shall describe the structure of the TSF in terms of subsystems.**

ADV_HLD.2.4C **The high-level design shall describe the security functionality provided by each subsystem of the TSF.**

ADV_HLD.2.5C **The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.**

ADV_HLD.2.6C **The high-level design shall identify all interfaces to the subsystems of the TSF.**

ADV_HLD.2.7C **The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.**

ADV_HLD.2.8C **The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.**

ADV_HLD.2.9C **The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.**

ADV_IMP.1 Implementación de la TSF

Dependencias: **ADV_LLD.1 Descriptive low-level design**

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1 Well-defined development tools

Acciones del fabricante:

ADV_IMP.1.1D **The developer shall provide the implementation representation for a selected subset of the TSF.**

Contenido y presentación de elementos de evidencias:

ADV_IMP.1.1C **The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.**

ADV_IMP.1.2C **The implementation representation shall be internally consistent.**

ADV_LLD.1 Diseño descriptivo de bajo nivel

Dependencias: **ADV_HLD.2 Security enforcing high-level design**

ADV_RCR.1 Informal correspondence demonstration

Acciones del fabricante:

ADV_LLD.1.1D **The developer shall provide the low-level design of the TSF.**

Contenido y presentación de elementos de evidencias:

ADV_LLD.1.1C **The presentation of the low-level design shall be informal.**

ADV_LLD.1.2C **The low-level design shall be internally consistent.**

ADV_LLD.1.3C **The low-level design shall describe the TSF in terms of modules.**

ADV_LLD.1.4C **The low-level design shall describe the purpose of each module**.

ADV_LLD.1.5C **The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.**

ADV_LLD.1.6C **The low-level design shall describe how each TSP-enforcing function is provided.**

ADV_LLD.1.7C **The low-level design shall identify all interfaces to the modules of the TSF.**

ADV_LLD.1.8C **The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.**

ADV_LLD.1.9C **The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.**

ADV_LLD.1.10C **The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.**

ADV_RCR.1 Demostración informal de correspondencia

Dependencias: **No hay dependencias**

Acciones del fabricante:

ADV_RCR.1.1D **The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.**

Contenido y presentación de elementos de evidencias:

ADV_RCR.1.1C **For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.**

ADV_SPM.1 Modelo informal de política de seguridad del objeto de evaluación (TOE)

Dependencias: **ADV_FSP.2 Fully defined external interfaces**

Acciones del fabricante:

ADV_SPM.1.1D **The developer shall provide a TSP model.**

ADV_SPM.1.2D **The developer shall demonstrate correspondence between the functional specification and the TSP model.**

Contenido y presentación de elementos de evidencias:

ADV_SPM.1.1C **The TSP model shall be informal.**

ADV_SPM.1.2C **The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.**

ADV_SPM.1.3C **The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.**

ADV_SPM.1.4C **The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.**

AGD_ADM.1 Manual del administrador

Dependencias: **ADV_FSP.2 Fully defined external interfaces**

Acciones del fabricante:

AGD_ADM.1.1D **The developer shall provide administrator guidance addressed to system administrative personnel.**

Contenido y presentación de elementos de evidencias:

AGD_ADM.1.1C **The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.**

AGD_ADM.1.2C **The administrator guidance shall describe how to administer the TOE in a secure manner.**

AGD_ADM.1.3C **The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.**

AGD_ADM.1.4C **The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.**

AGD_ADM.1.5C **The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.**

AGD_ADM.1.6C **The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.**

AGD_ADM.1.7C **The administrator guidance shall be consistent with all other documentation supplied for evaluation.**

AGD_ADM.1.8C **The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.**

AGD_USR.1 Manual de usuario

Dependencias: **ADV_FSP.2 Fully defined external interfaces**

Acciones del fabricante:

AGD_USR.1.1D **The developer shall provide user guidance.**

Contenido y presentación de elementos de evidencias:

AGD_USR.1.1C **The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.**

AGD_USR.1.2C **The user guidance shall describe the use of user-accessible security functions provided by the TOE.**

AGD_USR.1.3C **The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.**

AGD_USR.1.4C **The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.**

AGD_USR.1.5C **The user guidance shall be consistent with all other documentation supplied for evaluation.**

AGD_USR.1.6C **The user guidance shall describe all security requirements for the IT environment that are relevant to the user.**

ALC_DVS.1 Identificación de las medidas de seguridad

Dependencias: **No hay dependencias**

Acciones del fabricante:

ALC_DVS.1.1D **The developer shall produce development security documentation.**

Contenido y presentación de elementos de evidencias:

ALC_DVS.1.1C **The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.**

ALC_DVS.1.2C **The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.**

ALC_FLR.1 Subsanación básica de errores

Dependencias: **No hay dependencias**

Acciones del fabricante:

ALC_FLR.1.1D **The developer shall provide flaw remediation procedures addressed to TOE developers.**

Contenido y presentación de elementos de evidencias:

ALC_FLR.1.1C **The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.**

ALC_FLR.1.2C **The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.**

ALC_FLR.1.3C **The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.**

ALC_FLR.1.4C **The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.**

ALC_LCD.1 Modelo de ciclo de vida definido por el fabricante

Dependencias: **No hay dependencias**

Acciones del fabricante:

ALC_LCD.1.1D **The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.**

ALC_LCD.1.2D **The developer shall provide life-cycle definition documentation.**

Contenido y presentación de elementos de evidencias:

ALC_LCD.1.1C **The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.**

ALC_LCD.1.2C **The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.**

ALC_TAT.1 Herramientas de desarrollo bien definidas

Dependencias: **ADV_IMP.1 Subset of the implementation of the TSF**

Acciones del fabricante:

ALC_TAT.1.1D **The developer shall identify the development tools being used for the TOE.**

ALC_TAT.1.2D **The developer shall document the selected implementation-dependent options of the development tools.**

Contenido y presentación de elementos de evidencias:

ALC_TAT.1.1C **All development tools used for implementation shall be well-defined.**

ALC_TAT.1.2C **The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.**

ALC_TAT.1.3C **The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.**

ATE_COV.2 Análisis de cobertura

Dependencias: **ADV_FSP.2 Fully defined external interfaces**

ATE_FUN.1 Functional testing

Acciones del fabricante:

ATE_COV.2.1D **The developer shall provide an analysis of the test coverage.**

Contenido y presentación de elementos de evidencias:

ATE_COV.2.1C **The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.**

ATE_COV.2.2C **The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.**

ATE_DPT.1 Pruebas: diseño de alto nivel

Dependencias: **ADV_HLD.2 Security enforcing high-level design**

ATE_FUN.1 Functional testing

Acciones del fabricante:

ATE_DPT.1.1D **The developer shall provide the analysis of the depth of testing.**

Contenido y presentación de elementos de evidencias:

ATE_DPT.1.1C **The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.**

ATE_FUN.1 Pruebas funcionales

Dependencias: **No hay dependencias**

Acciones del fabricante:

ATE_FUN.1.1D **The developer shall test the TSF and document the results.**

ATE_FUN.1.2D **The developer shall provide test documentation.**

Contenido y presentación de elementos de evidencias:

ATE_FUN.1.1C **The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.**

ATE_FUN.1.2C **The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.**

ATE_FUN.1.3C **The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.**

ATE_FUN.1.4C **The expected test results shall show the anticipated outputs from a successful execution of the tests.**

ATE_FUN.1.5C **The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.**

ATE_IND.2 Pruebas independientes - muestra

Dependencias: **ADV_FSP.2 Fully defined external interfaces**

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

Acciones del fabricante:

ATE_IND.2.1D **The developer shall provide the TOE for testing.**

Contenido y presentación de elementos de evidencias:

ATE_IND.2.1C **The TOE shall be suitable for testing.**

ATE_IND.2.2C **The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.**

AVA_MSU.3 Análisis y pruebas para estados inseguros

Dependencias: **ADO_IGS.1 Installation, generation, and start-up procedures**

ADV_FSP.2 Fully defined external interfaces

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Acciones del fabricante:

AVA_MSU.3.1D **The developer shall provide guidance documentation.**

AVA_MSU.3.2D **The developer shall document an analysis of the guidance documentation.**

Contenido y presentación de elementos de evidencias:

AVA_MSU.3.1C **The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.**

AVA_MSU.3.2C **The guidance documentation shall be complete, clear, consistent and reasonable.**

AVA_MSU.3.3C **The guidance documentation shall list all assumptions about the intended environment.**

AVA_MSU.3.4C **The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).**

AVA_MSU.3.5C **The analysis documentation shall demonstrate that the guidance documentation is complete.**

AVA_SOF.1 Evaluación de la fortaleza de función de seguridad del objeto de evaluación (TOE)

Dependencias: **ADV_FSP.2 Fully defined external interfaces**

ADV_HLD.2 Security enforcing high-level design

Acciones del fabricante:

AVA_SOF.1.1D **The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.**

Contenido y presentación de elementos de evidencias:

AVA_SOF.1.1C **For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.**

AVA_SOF.1.2C **For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.**

AVA_VLA.4 Altamente resistente

Dependencias: **ADV_FSP.2 Fully defined external interfaces**

ADV_HLD.2 Security enforcing high-level design

ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Acciones del fabricante:

AVA_VLA.4.1D **The developer shall perform a vulnerability analysis.**

AVA_VLA.4.2D **The developer shall provide vulnerability analysis documentation.**

Contenido y presentación de elementos de evidencias:

AVA_VLA.4.1C **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.**

AVA_VLA.4.2C **The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.**

AVA_VLA.4.3C **The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.**

AVA_VLA.4.4C **The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.**

AVA_VLA.4.5C **The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.**

AVA_VLA.4.6C **The vulnerability analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.**

5.2 Requisitos de seguridad aplicables al entorno.

5.2.1 Requisitos de seguridad aplicables al entorno de las TI.

5.2.1.1 Aplicación de generación de certificados

FCS_CKM.2 Distribución de claves criptográficas

FCS_CKM.2.1/CGA **La TSF debe distribuir las claves criptográficas de acuerdo con un método de distribución de claves criptográficas especificado certificado reconocido que cumpla lo siguiente: distribución con integridad y no repudio.**

FCS_CKM.3 Acceso a claves criptográficas

FCS_CKM.3.1/CGA **La TSF debe realizar la importación de los datos de verificación de firma (SVD) de acuerdo con un método de acceso a las claves criptográficas especificado de importación a través de un canal confiable que cumpla lo siguiente: [integridad, confidencialidad y autenticación].**

FDP_UIT.1 Integridad del intercambio de datos

FDP_UIT.1.1 / Importación de datos de verificación de firma (SVD) **La TSF debe aplicar la SFP de Importación de datos de verificación de firma (SVD) para poder recibir datos de usuario de una manera protegida contra errores de modificación e inserción.**

FDP_UIT.1.2 / Importación de datos de verificación de firma (SVD) **La TSF debe ser capaz de determinar, a la recepción de los datos de usuario, si ha ocurrido modificación e inserción.**

FTP_ITC.1 Canal confiable inter – TSF

FTP_ITC.1.1 / Importación de datos de verificación de firma (SVD) **La TSF debe proporcionar un canal de comunicación, entre sí misma y un producto de tecnología de la información (IT) confiable remoto, que sea distinto lógicamente de otros canales de comunicación y que proporcione la identificación segura de sus extremos y la protección de los datos del canal contra su modificación o pérdida de confidencialidad.**

FTP_ITC.1.2 / Importación de datos de verificación de firma (SVD) **La TSF debe permitir a [el producto de tecnología de la información (IT) confiable remoto] iniciar la comunicación a través del canal confiable.**

FTP_ITC.1.3 / Importación de datos de verificación de firma (SVD) **La TSF o el objeto de evaluación (TOE) debe iniciar la comunicación a través del canal confiable para la importación de datos de verificación de firma (SVD).**

5.2.1.2 Aplicación de creación de firma

FCS_COP.1 Funcionamiento criptográfico

FCS_COP.1.1/SCA_HASH **La TSF debe realizar el hash de los datos a ser firmados (DTBS) de acuerdo con un algoritmo criptográfico especificado [SHA1] y con ningún tamaño de claves criptográficas que cumpla lo siguiente: SHA1.**

FDP_UIT.1 Integridad del intercambio de datos

FDP_UIT.1.1 / DTBS de la SCA **La TSF debe aplicar la SFP de Creación de firma para poder transmitir datos de usuario de una manera protegida contra errores de modificación, borrado e inserción.**

FDP_UIT.1.2 / DTBS de la SCA **La TSF debe ser capaz de determinar, a la recepción de los datos de usuario, si ha ocurrido modificación, borrado e inserción**.

FTP_ITC.1 Canal confiable inter – TSF

FTP_ITC.1.1 / DTBS de la SCA **La TSF debe proporcionar un canal de comunicación, entre sí misma y un producto de tecnología de la información (IT) confiable remoto, que sea distinto lógicamente de otros canales de comunicación y que proporcione identificación segura de sus extremos y protección de los datos del canal contra la modificación o la pérdida de confidencialidad.**

FTP_ITC.1.2 / DTBS de la SCA **La TSF debe permitir a la TSF iniciar la comunicación a través del canal confiable.**

FTP_ITC.1.3 / DTBS de la SCA **La TSF o el objeto de evaluación (TOE) debe iniciar la comunicación a través del canal confiable para firmar la representación de datos a ser firmados (DTBS) mediante el dispositivo seguro de creación de firma (SSCD).**

FTP_TRP.1 Trusted path

64 Se necesitará una ruta confiable entre el objeto de evaluación (TOE) y la aplicación de creación de firma (SCA) sólo si no es el propio TOE, sino la SCA la que proporciona el interfaz humano (HI) para la autenticación del usuario.

FTP_TRP.1.1 / SCA **La TSF debe proporcionar una ruta de comunicación, entre sí misma y los usuarios locales, que sea lógicamente distinta de otras rutas de comunicación y proporcione identificación segura de sus extremos y protección de los datos comunicados contra la modificación o la pérdida de confidencialidad.**

FTP_TRP.1.2 / SCA **La TSF debe permitir a [los usuarios locales] iniciar la comunicación a través de la ruta confiable**.

FTP_TRP.1.3 / SCA **La TSF debe exigir el uso de la ruta confiable para [la autenticación inicial del usuario], [ninguno].**

5.2.2 Requisitos de seguridad aplicables al entorno ajeno a las TI.

R. Administrator_Guide **Aplicación del Manual de Administrador**

65 La implementación de los requisitos del Anexo II de la Directiva, "Requisitos para los proveedores de servicio de certificación que emitan certificados reconocidos" establece, en el punto e), que los empleados del proveedor de servicios de certificación (CSP) u otras entidades relevantes deben seguir el manual de administrador dado para el objeto de evaluación (TOE). La adecuada supervisión del CSP o de otras entidades relevantes debe garantizar que se cumple lo estipulado por la Directiva.

R.Sigy_Guide **Aplicación del Manual de Usuario**

66 La implementación, por parte del proveedor de servicios de certificación (CSP), de los requisitos del Anexo II de la Directiva "Requisitos para los proveedores de servicio de certificación que emitan certificados reconocidos" establece, en el punto k), que el firmante debe seguir el manual de usuario dado para el objeto de evaluación (TOE).

R.Sigy_Name **Nombre del firmante en el Certificado reconocido**

67 El proveedor de servicios de certificación (CSP) debe verificar la identidad de la persona para la que se emite un certificado reconocido de acuerdo con el punto d) del Anexo II de la Directiva "Requisitos para los proveedores de servicio de certificación que emitan certificados reconocidos". El CSP debe verificar que esta persona mantiene el dispositivo seguro de creación de firma (SSCD) que almacena los datos de creación de firma (SCD) correspondientes a los datos de verificación de firma (SVD) que se deben incluir en el certificado reconocido.

6 Síntesis de la especificación del producto

6.1 Especificación funcional

CMD Manual de comandos Sistema Operativo DNIe

ST19WL34 SECURITY TARGET, SMD_ST19WL34_ST_05_001_V01.01

68 El manual CMD es la especificación técnica y descripción funcional del Sistema Operativo DNIe, en su versión evaluada.

69 Se relacionan en este apartado los requisitos funcionales de la declaración de seguridad con los comandos o funciones que, conforme se detallan en CMD, dan cumplimiento a los mismos.

70 Dicho manual de comandos, CMD, es la especificación funcional de los interfaces de la tarjeta DNIe. Conforme al párrafo 228 de la primera parte de la norma CC, segunda frase, *"Note that the functional information provided as part of the TOE summary specification could be identical in some cases to the information to be provided for the TOE as part of the ADV_FSP requirements"*, no se repetirá en esta sección tal información del manual de comandos, sino que se referencian los apartados aplicables del mismo.

71 El cumplimiento de los siguientes requisitos funcionales se garantiza por la plataforma de la tarjeta DNIe, la familia de chip ST19WL34, como se detalla en su declaración de seguridad ST19WL34. Por trazabilidad con el resto de documentación, se establece el nombre de F_CHIP para la función de seguridad del TOE que representa a las funciones de seguridad del chip en las que descansan los siguientes requisitos:

a) FPT_PHP.1 Passive detection of physical attack

b) FPT_PHP.3 Resistance to physical attack

c) FDP_SDI.2 Stored data integrity monitoring and action (Sólo para FDP_SDI.2/Persistent, no para FDP_SDI.2/DTBS)

d) FPT_AMT.1 Abstract machine testing - **FPT_AMT.1.1**

e) FPT_TST.1 TSF testing - **FPT_TST.1.3**

72 El siguiente requisito funcional de seguridad no es implementado directamente por la interfaz funcional de la tarjeta, sino que se corresponde con funcionalidad interna del diseño. Por trazabilidad con el resto de documentación, se establece el nombre de F_DIS para la función de seguridad que no es implementada directamente por comandos sino que

existe debido a la arquitectura y el diseño del propio Sistema Operativo y sobre la que descansa el siguiente requisito.

a) FPT_FLS.1 Failure with preservation of secure state

73 Los siguientes requisitos funcionales de seguridad no son implementados directamente por la interfaz funcional de la tarjeta, sino que se corresponde con funcionalidad interna del diseño. Se da cumplimiento a estos requisitos con la función de seguridad definida para el caso anterior, esto es, F_DIS:

a) FDP_ACF.1.1/Initialisation SFP

b) FDP_ACF.1.1/Personalisation SFP

c) FIA_ATD.1.1

d) FMT_SMR.1

74 El siguiente requisito funcional de seguridad no es implementado directamente por la interfaz funcional de la tarjeta, debiendo ser comprobado su cumplimiento a través de pruebas de caja negra específicas. Denominaremos F_EMSEC a la función de seguridad que da cumplimiento al requisito:

a) FPT_EMSEC.1 TOE Emanation

75 Se indican en la tabla siguiente los restantes requisitos funcionales de esta declaración de seguridad la relación de comandos o funciones.

Tabla 3 Requisitos vs. descripción funcional

Nombre	Comando
FCS_CKM.1.1	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas
FCS_CKM.4.1	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas
FCS_COP.1.1/CORRESP	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas, comandos de realización y verificación de firma electrónica

Nombre	Comando
FCS_COP.1.1/SIGNING	Comandos de establecimiento de canal, comandos de realización y verificación de firma electrónica
FDP_ACC.1.1/SVD Transfer SFP	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas.
FDP_ACC.1.1/Initialisation SFP	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas.
FDP_ACC.1.1/Personalisation SFP	Comandos de establecimiento de canal, comandos de gestión de la seguridad.
FDP_ACC.1.1/Signature-creation SFP	Comandos de establecimiento de canal, comandos de realización y verificación de firma electrónica.
FDP_ACF.1.2/Initialisation SFP	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas.
FDP_ACF.1.3/Initialisation SFP	
FDP_ACF.1.4/Initialisation SFP	
FDP_ACF.1.1/SVD Transfer SFP	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas.
FDP_ACF.1.2/SVD Transfer SFP	
FDP_ACF.1.3/SVD Transfer SFP	
FDP_ACF.1.4/SVD Transfer SFP	

Nombre	Comando
FDP_ACF.1.2/Personalisation SFP	Comandos de establecimiento de canal, comandos de gestión de la seguridad, comandos de gestión de ficheros.
FDP_ACF.1.3/Personalisation SFP	
FDP_ACF.1.4/Personalisation SFP	
FDP_ACF.1.1/Signature-creation SFP	Comandos de establecimiento de canal, comandos de realización y verificación de firma electrónica.
FDP_ACF.1.2/Signature-creation SFP	
FDP_ACF.1.3/Signature-creation SFP	
FDP_ACF.1.4/Signature-creation SFP	
FDP_ETC.1.1/SVD Transfer	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas
FDP_ETC.1.2/SVD Transfer	
FDP_ITC.1.1/DTBS	Comandos de establecimiento de canal, comandos de realización y verificación de firma electrónica
FDP_ITC.1.2/DTBS	
FDP_ITC.1.3/DTBS	
FDP_RIP.1.1	Comandos de realización y verificación de firma electrónica, comandos de gestión de la seguridad.

Nombre	Comando
FDP_SDI.2.1/DTBS	Comandos de establecimiento de canal, comandos de realización y verificación de firma electrónica.
FDP_SDI.2.2/DTBS	
FDP_UIT.1.1/SVD Transfer	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas.
FDP_UIT.1.2/SVD Transfer	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas.
FDP_UIT.1.1/TOE DTBS	Comandos de establecimiento de canal, Comandos de realización y verificación de firma electrónica.
FDP_UIT.1.2/TOE DTBS	Comandos de establecimiento de canal, Comandos de realización y verificación de firma electrónica.
FIA_AFL.1.1	Comandos de la gestión de la seguridad.
FIA_AFL.1.2	
FIA_UAU.1.1	Comandos de establecimiento de canal.
FIA_UAU.1.2	Comandos de la gestión de la seguridad.
FIA_UID.1.1	Comandos de establecimiento de canal.
FIA_UID.1.2	Comandos de la gestión de la seguridad.

Nombre	Comando
FMT_MOF.1.1	Comandos de establecimiento de canal, comandos de gestión de ficheros.
FMT_MSA.1.1/Administrador	Comandos de establecimiento de canal, comandos de gestión de ficheros.
FMT_MSA.1.1/Signatory	Comandos de establecimiento de canal, comandos de gestión de ficheros.
FMT_MSA.2.1	Comandos de gestión de ficheros.
FMT_MSA.3.1	Comandos de gestión y utilización de claves criptográficas.
FMT_MSA.3.2	Comandos de gestión de ficheros.
FMT_MTD.1.1	Comandos de gestión de la seguridad.
FMT_SMF.1.1	Comandos de gestión de la seguridad, comandos de gestión de ficheros.
FPT_TST.1.1	Comandos de pruebas de la funcionalidad.
FPT_TST.1.2	
FTP_ITC.1.1/SVD Transfer	Comandos de establecimiento de canal, comandos de gestión y utilización de claves criptográficas.
FTP_ITC.1.2/SVD Transfer	

Nombre	Comando
FTP_ITC.1.3/SVD Transfer	
FTP_ITC.1.1/DTBS import	Comandos de establecimiento de canal, comandos de realización y verificación de firma electrónica.
FTP_ITC.1.2/DTBS import	
FTP_ITC.1.3/DTBS import	

76 Existe una función de lectura de eventos que tiene como objetivo informar al usuario del contenido del registro de auditoría. Es especialmente relevante en aquellos casos en los que se produce un evento grave (fallo de integridad o detección de anomalías por los sensores). Por lo tanto, esta función de seguridad puede ser usada por el usuario para obtener información de sucesos y forma parte del cumplimiento de los requisitos FDP_SDI.2, FPT_FLS.1, FPT_PHP.1, FPT_PHP.3, FPT_AMT.1.1 y FPT_TST.1

77 Todos los requisitos funcionales de seguridad exigibles al TOE se demuestran satisfechos con las funciones o comandos de la misma.

6.1.1 Fortaleza de mecanismos

78 El cumplimiento del Perfil de Protección CWA14169 exige fortaleza alta para los mecanismos de seguridad del DNIe.

79 En particular, los requisitos funcionales de la clase FIA utilizan mecanismos probabilísticos o permutacionales, para los cuales es necesaria la comprobación de su fortaleza.

80 Nótese que en la tarjeta inteligente, la identificación es implícita a la autenticación, por cuanto se supone un dispositivo de un sólo usuario, y su posesión implica la identidad del usuario.

81 Aunque los mecanismos de acceso a los activos protegidos se detallan en CMD, a continuación se enumeran los mecanismos de seguridad en los que descansa el acceso.

82 Mecanismos de identificación/autenticación en función del rol:

a) El usuario firmante tiene en su poder tres elementos de identificación/autenticación, éstos son, el PIN (secuencia de entre 4 y 16 bytes), clave APP (secuencia de bytes entre 8 y 20 bytes) y/o realiza una autenticación biométrica con huella dactilar (se trata de una operación de verificación, no identificación, puesto que se compara con la plantilla del titular de la tarjeta). Estos mecanismos son implementados en las funciones de seguridad "Verify", "External Authenticate" y "BIO Verify" respectivamente.

b) El usuario administrador tiene en su poder un elemento de identificación/autenticación que consiste en una clave privada cuya parte pública ha sido firmada por una CA en la que confía la tarjeta. Lo que autenticará al usuario como administrador es la firma con esta clave privada de los desafíos que solicite a la tarjeta. Este mecanismo de identificación es implementado en las funciones de seguridad que intervienen en el establecimiento del canal seguro: "Get Chip Info", "Get Challenge", "Manage Security Environment", "Perform Security Operation", "Internal Authentication", "External Authentication"

83 La combinación de estos mecanismos de identificación/autenticación con las políticas de comunicaciones y de seguridad definidas para la tarjeta DNIe, dan como resultado los siguientes mecanismos o formas de acceder a la tarjeta, que, por supuesto, se requerirán en función del activo protegido al que se quiera acceder y serán una combinación entre la identificación/autenticación necesaria y los canales de comunicación necesarios.

84 De esta manera, para los activos a proteger definidos en el Perfil de Protección CWA14169 y con la ayuda de las políticas de seguridad definidas, extraemos los siguientes mecanismos o formas de acceso

a) Presentación de PIN bajo un canal seguro de usuario (user channel): Este mecanismo de acceso combinado, utilizado por ejemplo para el acceso a la funcionalidad de firma, consta de la presentación de un PIN, siendo obligatorio realizar la presentación bajo un canal seguro de usuario.

b) Presentación de PIN bajo un canal seguro de administrador (PRO): Este mecanismo de acceso combinado consta de la presentación de un PIN, siendo obligatorio realizar la presentación bajo un canal seguro de administrador.

c) Presentación de clave APP y autenticación biométrica bajo un canal seguro de administrador (PRO): Este mecanismo de acceso combinado consta de la presentación del resultado de una operación con una clave APP, una autenticación biométrica y siendo obligatorio realizar estas operaciones bajo un canal seguro de administrador.

d) Firma de desafío con clave privada de administrador al objeto del establecimiento de canal seguro de administración. Con la firma de estos desafíos solicitados a la tarjeta, el administrador se identifica y autentica al objeto de establecer un canal seguro de administración. El administrador completa su identificación/autenticación y obtiene los privilegios de acceso una vez que el canal ha sido establecido

85 La fortaleza de cada una de las cuatro formas o mecanismos de acceso antes enumerados es alta.

6.2 Garantía de seguridad

86 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.

Tabla 4 Documentación y requisitos de garantía de seguridad.

Componente	Documento
ACM_AUT.1 Partial CM automation	Documentación de gestión de proyectos y gestión de la configuración
ACM_CAP.4 Generation support and acceptance procedures	
ACM_SCP.2 Problem tracking CM coverage	Lista de elementos de la configuración – Versión 1.0, Revisión 2
ALC_FLR.1 Basic flaw remediation	Procedimientos de clasificación de fallos y corrección de éstos
ADO_DEL.2 Detection of modification	Procedimientos de aceptación y entrega

Componente	Documento
ADO_IGS.1 Installation, generation, and start-up procedures	Procedimientos de instalación y puesta en marcha
ADV_FSP.2 Fully defined external interfaces	Manual de Comandos
ADV_HLD.2 Security enforcing high-level design	Diseño de Alto Nivel
ADV_IMP.1 Subset of the implementation of the TSF	Código fuente y mapas de memoria de tarjeta inteligente “DNIe”
ADV_LLD.1 Descriptive low-level design	Diseño de Bajo Nivel
ADV_RCR.1 Informal correspondence demonstration	Análisis de la correspondencia de los elementos representativos de las funciones de seguridad de la tarjeta DNIe
ADV_SPM.1 Informal TOE security policy model	Declaración de seguridad, Políticas se acceso a la tarjeta.
AGD_ADM.1 Administrator guidance	Manual del administrador, Manual de Comandos
AGD_USR.1 User guidance	Guía de referencia básica
ALC_DVS.1 Identification of security measures	Descripción de la Medidas de Seguridad para el Desarrollo y la Producción del DNIe
ALC_LCD.1 Developer defined life-cycle model	Ciclo de vida de la tarjeta DNIe

Componente	Documento
ALC_TAT.1 Well-defined development tools	Herramientas y técnicas para el desarrollo del Sistema Operativa de la tarjeta DNIe
ATE_COV.2 Analysis of coverage	Análisis de la cobertura de las pruebas para la especificación funcional
ATE_DPT.1 Testing: high-level design	Documentación de pruebas
ATE_FUN.1 Functional testing	
ATE_IND.2 Independent testing - sample	
AVA_MSU.3 Analysis and testing for insecure states	Documentación de análisis de vulnerabilidades
AVA_SOF.1 Strength of TOE security function evaluation	
AVA_VLA.4 Highly resistant	

7 Cumplimiento de "Perfiles de Protección".

87 Esta declaración de seguridad supone la segunda fase de la posible cadena de certificaciones de la seguridad de una tarjeta inteligente.

88 Se apoya en la certificación del chip, y satisface los requisitos adicionales requeridos para el cumplimiento del Perfil de Protección CWA14169.

7.1 Perfil de Protección CWA14169

7.1.1 Referencia.

89 CWA 14169:2004 (E), Secure Signature-Creation Device Type 3.

7.1.2 Adaptación y operaciones fijadas.

90 Todas las operaciones del PP están definidas en esta declaración de seguridad.

7.1.3 Incrementos sobre el Perfil de Protección.

91 Se incrementa el nivel de garantía de la seguridad de la evaluación con el componente ALC_FLR.1 Basic flaw remediation, de utilidad para el cumplimiento de los requisitos relativos al mantenimiento del registro y actuaciones relativas a la seguridad del producto certificado requeridas por el Organismo de Certificación.

8 Justificaciones.

8.1 Suficiencia de los objetivos de seguridad.

92 Véase Perfil de Protección CWA14169.

8.2 Adecuación de los requisitos de seguridad.

93 Véase Perfil de Protección CWA14169.

8.3 Justificación de la síntesis funcional.

8.3.1 Combinación de los comandos de la tarjeta.

94 La relación de comandos de la tarjeta DNIe, especificada en CMD, es ortogonal, en el sentido de que la funcionalidad de cada comando, tal como se especifica, es única, y no hay solapamientos de funcionalidad ni efectos laterales o secundarios no documentados.

95 La relación de requisitos funcionales de seguridad exigidos por esta declaración de seguridad y los comandos y propiedades de la tarjeta DNIe especificados en el apartado 6, “Síntesis de la especificación del producto”, es completa y única, no pudiendo establecerse otra correspondencia, de manera que es la única combinación de comandos que satisface los requisitos funcionales.

8.3.2 Fortaleza de las funciones

96 La fortaleza de función alta, para el mecanismo de PIN, es válida en aplicación de la metodología de análisis del CEM, para un tamaño de PIN de 4 dígitos.

8.3.3 Medidas de garantía de seguridad.

97 Las medidas de garantía de seguridad satisfacen los requisitos del nivel de evaluación exigido, EAL4+, tal como se deduce del análisis de su contenido y presentación.

8.4 Justificación del cumplimiento de Perfiles de Protección.

98 El requisito **FMT_SMF.1 Specification of Management Functions** no está incluido inicialmente en el Perfil de Protección CWA14169. Este requisito se incorpora a esta declaración de seguridad en cumplimiento de la versión de la norma de evaluación utilizada, CC/CEM 2.2, que lo exige por

dependencia de varios componentes de la clase FMT, que sí están demandados por el PP.

99 La incorporación del requisito **FMT_SMF.1 Specification of Management Functions** no exige de la modificación de los objetivos de seguridad a satisfacer, por cuanto se trata de una exigencia para el correcto soporte a los demás requisitos de la clase FMT que se requieren en el Perfil de Protección CWA14169, que son los que directamente satisfacen los objetivos de seguridad demandados en dicho PP.