DECLARACIÓN DE SEGURIDAD

CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIE

MADRID A 18 DE JULIO DE 2012

	NOMBRE	FECHA
Elaborado por:	INTECO	11/06/2012
Revisado por:	INTECO	11/06/2012
Aprobado por:	INTECO/RED.ES	11/06/2012
Aprobado por:	DGMAPIAE	13/06/2012

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
0.1	10/05/2012	Creación del documento.	INTECO
1.0	15/05/2012	Revisión del documento.	INTECO
1.1	16/05/2012	Revisión del documento.	E&E
1.2	16/05/2012	Revisión del documento.	INTECO
1.3	16/05/2012	Revisión del documento.	Atos
1.4	16/05/2012	Revisión del documento.	INTECO
1.5	17/05/2012	Revisión del documento.	E&E
1.6	17/05/2012	Validación del documento.	INTECO
1.7	21/05/2012	Validación del documento.	INTECO
1.8	28/05/2012	Validación documento y cambio formato	MINHAP
1.9	04/06/2012	Validación y correcciones versionado	INTECO
1.10	06/06/2012	Control de cambios. Corrección nombre TOE	INTECO
1.11	13/06/2012	Control de cambios. Cambios de formato y ECD.	INTECO
1.12	26/06/2012	Hipótesis sobre el entorno operacional.	INTECO
1.13	18/07/2012	Hipótesis sobre el entorno operacional.	INTECO
1.14	18/07/2012	Corrección versionado	INTECO

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

1. INTRODUCCIÓN

1.1. REFERENCIAS LEGISLATIVAS Y NORMATIVAS

Ley 15/1999 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley 59/2003 Ley 59/2003, de 19 de diciembre, de firma electrónica.

DNI electrónico Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica. También referenciado como DNIe.

CWA 14169 Perfil de Protección - Dispositivo seguro de creación de firma electrónica "EAL4+" Tipo 3.

PPSCVA Perfil de Protección la aplicación de creación y verificación de firma electrónica, con control exclusivo de los interfaces con el firmante, agrupa los PP para EAL1 y EAL3 y los tipos T1 y T2 de aplicación.

CC Common Criteria for Information Technology Security Evaluation, v. 3.1, agrupa: CC Parte 1 *release* 3, julio de 2009, CC Parte 2 *release* 3, julio de 2009 y CC Parte 3 *release* 3, julio de 2009.

1.2. REFERENCIA DE LA DECLARACIÓN DE SEGURIDAD

1 **Título:** DECLARACIÓN DE SEGURIDAD – CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe.

2 **Versión:** 1.14

3 **Autor:** INTECO

4 **Fecha de publicación:** 18 de Julio de 2012

1.3. REFERENCIA DEL TOE

5 **Nombre:** CONTROLADOR JAVA DE LA SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS PARA EL DNIe.

6 **Versión:** 1.4

7 **Desarrollador:** INTECO, ATOS

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

1.4. RESUMEN DEL TOE

1.4.1. Tipo de TOE

8 El TOE es un "driver", que permite exportar servicios de acceso a los mecanismos y funcionalidad del DNI electrónico, normalizados conforme a la arquitectura de seguridad Java. Se puede considerar que es como una librería java que facilita el acceso al DNIe.

9 La solución construida se integra en la Arquitectura Java de Criptografía (JCA, Java Cryptography Architecture).

10 Dicha arquitectura permite que todas aquellas aplicaciones que invocan los servicios de acceso a tarjeta inteligente sobre la arquitectura JAVA puedan trabajar contra los DNI electrónicos de una manera transparente, siendo necesario únicamente que la aplicación se ajuste al estándar definido por el fabricante de la arquitectura JAVA.

11 La librería criptográfica para el DNIe permite llamadas relacionadas con la lectura de objetos del DNI electrónico (Acceso a Almacén de Claves) y firma. No están soportadas las funciones definidas de generación de claves, creación, modificación o borrado de ningún tipo de objetos del DNI electrónico.

12 Además se permite validar firmas RSA realizadas externa e internamente.

1.4.2. Uso del TOE

13 Tanto el TOE como las aplicaciones que lo invocan corren dentro de la máquina virtual de JAVA. El TOE es invocado y utilizado por aplicaciones confiables de generación de firma, o de autenticación, que son las que interactúan con el firmante, y que utilizan los servicios del DNI electrónico a través del TOE.

14 El TOE establece un diálogo con el firmante para la captura de su consentimiento en el momento de realizar una firma electrónica/autenticación, y es capaz de notificar diferentes estados y resultados de error en la ejecución de sus operaciones.

1.4.3. Características de seguridad del TOE

15 El DNI electrónico requiere que las comunicaciones entre la aplicación y la tarjeta se realicen con un canal securizado. Este canal cifrado lo establece y lo gestiona el propio TOE de manera transparente para la aplicación, encargándose de su establecimiento, cifrado/descifrado de mensajes y, en su caso, destrucción de dicho canal.

16 Adicionalmente, el TOE recibe el PIN del usuario del DNI electrónico, necesario tanto para la realización de operaciones de firma como para la lectura de certificados privados. La lectura de certificados públicos no requiere la

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

presentación del PIN (para las versiones más actuales del DNIe). La solicitud y gestión del PIN es responsabilidad del TOE. En ningún caso se delegará esta responsabilidad en la aplicación que haga uso del driver. El TOE lo destruye de su ámbito de control cuando deja de ser necesario.

17 El TOE no entiende de tipos de documentos a firmar, ni incorpora visor de los datos a firmar o de su representación ("hash"), cuestiones que pertenecen al ámbito de las aplicaciones o el sistema de firma que utiliza este TOE.

18 Así mismo, el TOE permite la verificación de firma invocando a un proveedor externo de los servicios criptográficos.

1.4.4. Software y hardware requerido por el TOE

19 El TOE es un "driver" que se ejecuta e integra en una máquina con los siguientes requisitos:

1. JVM JSE 6 o superior

2. Al margen del hardware del ordenador de propósito general que se requiera para el correcto funcionamiento del Sistema Operativo que conforma el entorno del TOE, éste requiere de un lector de tarjetas inteligentes y del propio DNI electrónico. No hay más requisitos para el lector que su compatibilidad con el estándar ISO 7816 (1, 2 y 3), soporte para tarjetas asíncronas basadas en protocolos T=0 y T=1, velocidad de comunicación mínima de 9.600 bps y compatibilidad con JSE SmartCardIO (JSR-268).

Plataforma de pruebas utilizada en la evaluación de seguridad.

20 Para la evaluación se ha utilizado la siguiente plataforma de pruebas:

1. Windows 7

2. JVM 6u32

3. El TOE se integra con el cliente de @firma, utilizando el MiniApplet @firma y una página HTML simple de pruebas. El MiniApplet deberá ser publicado en un servidor Web.

1.5. DESCRIPCIÓN DEL TOE

1.5.1. Ámbito físico del TOE: Componentes

21 El TOE, una vez instalado, se compone de la siguiente librería:

DNIeJCAProvider.jar

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

1.5.2. Ámbito lógico del TOE

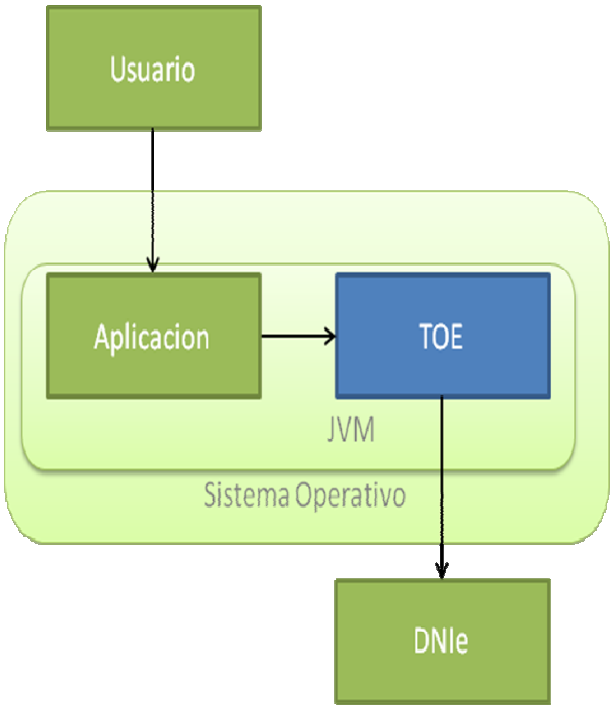

Ilustración 1-1

22 El TOE se ejecuta y usa como un driver en la máquina virtual de java que se esté ejecutando en el sistema operativo y es invocado por las aplicaciones java siguiendo los mecanismos que la máquina virtual de java provee. Las comunicaciones con el DNI electrónico se realizan igualmente a través del mismo sistema operativo, en particular mediando el uso de los correspondientes drivers del lector de tarjetas. Los diálogos con el usuario y la captura de sus entradas a través del teclado se realizan a través de las capacidades del interfaz de usuario del sistema operativo.

23 Todas las comunicaciones del TOE están, por tanto, mediadas por el sistema operativo y la máquina virtual de java en el que se instala y/o utiliza el driver.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

2. DECLARACIONES DE CONFORMIDAD

2.1. CONFORMIDAD RESPECTO A LA NORMA CC

24 Esta Declaración de Seguridad cumple con lo indicado en la norma **CC** versión 3.1, Parte 2 release 3 extendida, y Parte 3 release 3, para un nivel de evaluación EAL1.

2.2. CONFORMIDAD RESPECTO A PERFILES DE PROTECCIÓN

25 Esta Declaración de Seguridad no declara el cumplimiento de ningún Perfil de Protección.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

3. OBJETIVOS DE SEGURIDAD

3.1. OBJETIVOS DE SEGURIDAD PARA EL ENTORNO OPERACIONAL

26 El entorno en que se ejecuta el TOE debe garantizar que no se ejecutan aplicaciones maliciosas que interfieran en el funcionamiento del TOE o la interacción con el usuario, sin embargo el canal de comunicaciones con el DNIe sí puede ser objeto de ataques, incluyendo el lector del DNIe y sus comunicaciones con el ordenador.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

4. DEFINICIÓN DE COMPONENTES EXTENDIDOS

4.1. OPERATION ACKNOWLEDGE (FDP_OAK)

4.1.1. Family behaviour

27 This extended family defines the mechanisms for TSF-mediated display a message to the user of the driver without misleading or ambiguous interpretation, allowing the user to verify that the operation is the requested one and allowing the user to acknowledge the operation when the requested operation is a signature generation or an authentication.

4.1.2. Component levelling

FDP_OAK: OPERATION ACKNOWLEDGE	1

28 FDP_OAK.1 defines the mechanisms for TSF-mediated display a message to the user of the driver without misleading or ambiguous interpretation, allowing the user to verify that the operation is the requested one and allowing the user to acknowledge the operation when the requested operation is a signature generation or an authentication.

29 **Management: FDP_OAK.1**

30 There are no management activities foreseen.

31 **Audit: FDP_OAK.1**

32 The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Success and failure of the capture of the will to sign.

FDP_OAK.1 OPERATION ACKNOWLEDGE

Dependencies: No dependencies.

FDP_OAK.1.1 The TSF shall warn the user of the purpose for which the PIN is requested when the requested operation is a signature generation or an authentication. The user shall also be warned even if the PIN has not been requested to perform any of the above mentioned operations.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

FDP_ OAK.1.2 The TSF shall prompt the signatory with a non trivial challenge to capture his/her will to sign, so the signatory cannot trivially be impersonated.

4.2. DELEGATED CRYPTOGRAPHIC OPERATION (FCS_COP.2)

4.2.1. Family behaviour

33 In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. This family should be included whenever there are requirements for cryptographic operations to be performed.

34 Typical cryptographic operations include data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement.

35 Component 2 has been added as an extended component to fulfil the aforementioned TOE requirement.

4.2.2. Component levelling

36 FCS_COP.1 Cryptographic operation, as specified in CC Part 2.

37 FCS_COP.2 Delegated cryptographic operation, requires a cryptographic operation to be performed by an entity external to the TOE, in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

38 **Management: FCS_COP.1, FCS_COP.2**

39 There are no management activities foreseen.

40 **Audit: FCS_COP.1, FCS_COP.2**

41 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

42 a) Minimal: Success and failure, and the type of cryptographic operation.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

43 b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

FCS_COP.2 DELEGATED CRYPTOGRAPHIC OPERATION

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.2.1 The TSF shall invoke an external entity to perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

5. REQUISITOS DE SEGURIDAD DEL TOE

5.1. REQUISITOS FUNCIONALES DE SEGURIDAD

5.1.1. FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product 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 The TSF shall permit [selection] **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment] **creación de firma electrónica con el DNI electrónico**.

5.1.2. FDP_OAK.1 OPERATION ACKNOWLEDGE

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_OAK.1.1 The TSF shall warn the user of the purpose for which the PIN is requested when the requested operation is a signature generation or an authentication. The user shall also be warned even if the PIN has not been requested to perform any of the above mentioned operations.

FDP_ OAK.1.2 The TSF shall prompt the signatory with a non trivial challenge to capture his/her will to sign, so the signatory cannot trivially be impersonated.

5.1.3. 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 [selection] **deallocation of the resource** from the following objects [assignment] **PIN**

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

5.1.4. FCS_COP.1 Cryptographic operation

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 The TSF shall perform [assignment] **operaciones de resumen** in accordance with a specified cryptographic algorithm [assignment] **SHA-1, SHA-256, SHA-384, SHA-512** and cryptographic key sizes [assignment] **N/A** that meet the following: [assignment] **None**.

5.1.5. FCS_COP.2 DELEGATED CRYPTOGRAPHIC OPERATION

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.2.1 The TSF shall invoke an external entity to perform [assignment] **verificación de firma** in accordance with a specified cryptographic algorithm [assignment] **RSA** and cryptographic key sizes [assignment] **512, 1024, 2048 4096, 8192 or 16384 bits** that meet the following: [assignment] **None**.

5.1.6. FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation.

FDP_ITC.1.1 The TSF shall enforce the [assignment] **ninguna** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment] **ninguna**

Nota de aplicación: No se aplica ninguna política.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

Los datos de usuario que requiere el TOE para la verificación de firma serán el texto o mensaje, la firma y el certificado (clave pública) utilizado para la verificación.

5.2. REQUISITOS DE GARANTÍA DE SEGURIDAD

44 El desarrollo y evaluación del TOE se realizará conforme al siguiente nivel de garantía:

- EAL1

5.2.1. ASE_CCL.1 Conformance claims

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

5.2.2. ASE_ECD.1 Extended components definition

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

5.2.3. ASE_INT.1 ST introduction

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

5.2.4. ASE_OBJ.1 Security objectives for the operational environment

Developer action elements:

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

Content and presentation elements:

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

5.2.5. ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_REQ.1.1D The developer shall provide a statement of security requirements.

ASE_REQ.1.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C The statement of security requirements shall be internally consistent.

5.2.6. ASE_TSS.1 TOE summary specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

5.2.7. ADV_FSP.1 Basic functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

5.2.8. AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance 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.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

5.2.9. AGD_PRE.1 Preparative procedures

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

5.2.10. ALC_CMC.1 Labelling of the TOE

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labeled with its unique reference.

5.2.11. ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

5.2.12. ATE_IND.1 Independent testing - conformance

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

5.2.13. AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative Procedures

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C The TOE shall be suitable for testing.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

5.3. JUSTIFICACIÓN DE LOS REQUISITOS DE GARANTÍA DE SEGURIDAD

45 La garantía de seguridad deseada para este tipo de TOE según las exigencias del mercado es la proporcionada por el nivel de evaluación EAL1.

5.4. DEPENDENCIAS DE LOS REQUISITOS FUNCIONALES DE SEGURIDAD

46 A continuación se proporciona la justificación para aquellos requisitos funcionales de seguridad en los que no se han satisfecho las dependencias definidas en la parte 2 de Common Criteria:

- FCS_COP.1: Los algoritmos de resumen no utilizan claves, por lo tanto no es necesario ni introducir, ni generar ni destruir ninguna clave justificándose la no inclusión de las dependencias.

- Para satisfacer FCS_COP.2 DELEGATED CRYPTOGRAPHIC OPERATION, el TOE no necesita, ni crear, ni destruir claves (la no destrucción de la clave pública no afecta a la seguridad del TOE), por lo que no se requiere ni FCS_CKM.1 ni FCS_CKM.4. Sin embargo, el TOE debe importar los datos de entrada necesarios para la verificación de la firma, de forma que el requisito presenta una dependencia de FDP_ITC.1 Import of user data without security attributes.

- FDP_ITC.1 Import of user data without security attributes: el TOE no implementa ninguna política ni función de control de acceso o de control de flujo, por lo que no se requieren las dependencias de FDP_ACC o FDP_IFC. Asimismo, los atributos de seguridad que se definen en FMT_MSA.3 necesarios en estas funciones de control de acceso o control de flujo, no se utilizan en el TOE.

47 Para el resto de requisitos las dependencias se han satisfecho.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

6. ESPECIFICACIÓN RESUMIDA DEL TOE

6.1. FTP_ITC.1 INTER-TSF TRUSTED CHANNEL

48 El canal cifrado de usuario se establece de acuerdo a la norma CWA 14890-1. En dicha norma se definen tanto el formato de las firmas electrónicas y los certificados que permiten establecer el canal, y el interfaz de comandos que debe seguirse para la creación del mismo. Para destruir el canal basta con que una aplicación haga un reset contra la tarjeta o, simplemente, que se envíe un mensaje securizado mal formado (por ejemplo el envío de un comando no securizado, un error en el byte de clase CLA, cheksum incorrecto, etc.).

49 En cuanto a los algoritmos criptográficos utilizados en el driver para la implementación del canal seguro, se utiliza una combinación de DES y Triple-DES junto con RSA y huellas digitales SHA1.

6.2. FDP_OAK.1 OPERATION ACKNOWLEDGE

50 El Driver informará al usuario de la finalidad para la cual está solicitando el PIN en cada momento, esto es, que en la propia solicitud de introducción del PIN se mostrará al usuario una breve explicación de para qué operación se está solicitando dicho PIN. En el momento de la firma digital se solicitará confirmación al usuario indicando además qué certificado se está utilizando para realizar la operación criptográfica de firma.

51 Aún en el caso de que no fuera necesaria la introducción del PIN (por existir ya un canal seguro establecido y haberse presentado previamente el PIN a la tarjeta) para la realización de una operación de este tipo, se informará al usuario de que está a punto de realizar esta operación, de forma que pueda expresar su conformidad o no conformidad en este sentido. Resulta de interés que en todo caso, esta información que será mostrada al usuario sea lo más homogénea posible.

52 El consentimiento y expresión de voluntad de firma (will of sign) se realizará presentando un diálogo al usuario, en el que se le informará de la operación que está a punto de realizar y se le solicitará el PIN en caso de ser necesario. Sin embargo, la responsabilidad de presentar al usuario qué información está firmando queda delegada en la aplicación de terceros que hace uso del driver.

6.3. FDP_RIP.1 SUBSET RESIDUAL INFORMATION PROTECTION

53 El Driver borrará de memoria el PIN del usuario una vez se lo haya enviado al DNIe. El driver no hará uso del cacheo del PIN. Esto evitará que un atacante pueda obtener el PIN de manera fraudulenta. De esta manera el driver solicitará el PIN al usuario toda vez que éste necesite iniciar el proceso de verificación de usuario en la tarjeta, con el fin de acceder a la parte privada del DNIe.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06

6.4. FCS_COP.1 CRYPTOGRAPHIC OPERATION & FCS_COP.2 DELEGATED CRYPTOGRAPHIC OPERATION

54 El Driver permitirá hacer resúmenes (SHA-1, SHA-256, SHA-384, SHA-512) de los datos de forma interna y enviárselos al DNI para que realice la firma del resumen.

55 Además el driver permite la invocación de operaciones de verificación de firmas RSA realizadas externa e internamente. La operación de verificación de firma se delega en el proveedor por defecto instalado en la máquina virtual de Java o en el proveedor SunRsaSign (Proveedor criptográfico preinstalado en las JVM de Oracle, OpenJDK y Apple) si el proveedor por defecto no pudiese realizar la operación.

6.5. FDP_ITC.1 IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

56 El Driver recibirá los datos necesarios para realizar la verificación de las firmas RSA realizadas externa e internamente. Los datos de usuario que requiere el TOE para la verificación de firma serán el texto o mensaje, la firma y el certificado (clave pública) utilizado para la verificación.

MARÍA DE MOLINA, 50
28071 MADRID
TEL.: 91 273 24 08
FAX.: 91 273 24 06