Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN COMERCIAL

DEPARTAMENTO DOCUMENTOS DE IDENTIFICACIÓN-TARJETAS

DECLARACIÓN DE SEGURIDAD – DRIVER DNI ELECTRÓNICO SMART CARD MODULE

MADRID A 7 DE DICIEMBRE DE 2011

	NOMBRE	FECHA
Elaborado por:	Real Casa de la Moneda. Fábrica Nacional de Moneda y Timbre.	07/12/2011
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
0.9	05/10/2011	Creación del documento	FNMT
1.0	07/12/2011	Modificación del documento de acuerdo a los informes de observación recibidos durante la evaluación.	FNMT

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.

Card Module http://msdn.microsoft.com/en-us/library/dd627652%28v=VS.85%29.aspx

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 para "Driver DNI electrónico Smart Card Module".

2 **Versión:** 1.0

3 **Autor:** FNMT

4 **Fecha de publicación:** 7 de Diciembre de 2011

1.3. REFERENCIA DEL TOE

5 **Nombre:** "Driver DNI electrónico Smart Card Module".

6 **Versión:** 1.0

7 **Autor:** FNMT

8 **Fecha de publicación:** 5 de octubre de 2011

1.4. RESUMEN DEL TOE

1.4.1. Tipo de TOE

9 El TOE es un "driver", que permite exportar servicios de acceso a los mecanismos y funcionalidad del DNI electrónico, normalizados conforme a la especificación de interfaz de nivel de aplicación propietaria de Microsoft, "Smart Card Module". Dicho interfaz permite que todas aquellas aplicaciones que invocan los servicios de acceso a tarjeta inteligente sobre la arquitectura Microsoft Windows puedan trabajar contra los DNI electrónicos de una manera transparente, siendo necesario únicamente que la aplicación se ajuste al estándar definido por el fabricante del sistema operativo Microsoft Windows.

10 Conforme a la definición del "Smart Card Module", la librería criptográfica desarrollada por la FNMT-RCM para el DNIe soporta todas las llamadas del estándar, si bien sólo están permitidas aquellas relacionadas con la lectura de objetos del DNI electrónico y firma. No están soportadas las funciones definidas de generación de claves, creación, modificación o borrado de ningún tipo de objetos del DNI electrónico.

1.4.2. Uso del TOE

11 El TOE requiere de su instalación en el sistema de firma electrónica, según las restricciones que cada sistema operativo establece. 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.

12 El TOE establece un diálogo con el firmante para la captura de su consentimiento en el momento de realizar una firma electrónica, 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

13 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.

14 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 presentación del PIN. La adquisición de este PIN corresponde a las aplicaciones que invocan el TOE, y el TOE lo destruye de su ámbito de control cuando deja de ser necesario.

15 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.

1.4.4. Software y hardware requerido por el TOE

16 El TOE es un "driver" que se instala e integra en las siguientes versiones del sistema operativo "Microsoft Windows":

1. Microsoft Windows 7 32 bits
2. Microsoft Windows 7 64 bits

17 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, y velocidad de comunicación mínima de 9.600 bps.

1.5. DESCRIPCIÓN DEL TOE

1.5.1. Componentes del TOE

18 El TOE, una vez instalado, se compone de los siguientes ficheros o librerías dinámicas y versiones:

DNIeCMx86.dll	v1.0.0.0, para la arquitectura 32bits del sistema operativo
DNIeCMx64.dll	v1.0.0.0, para la arquitectura 64bits del sistema operativo

1.5.2. Ámbito lógico del TOE

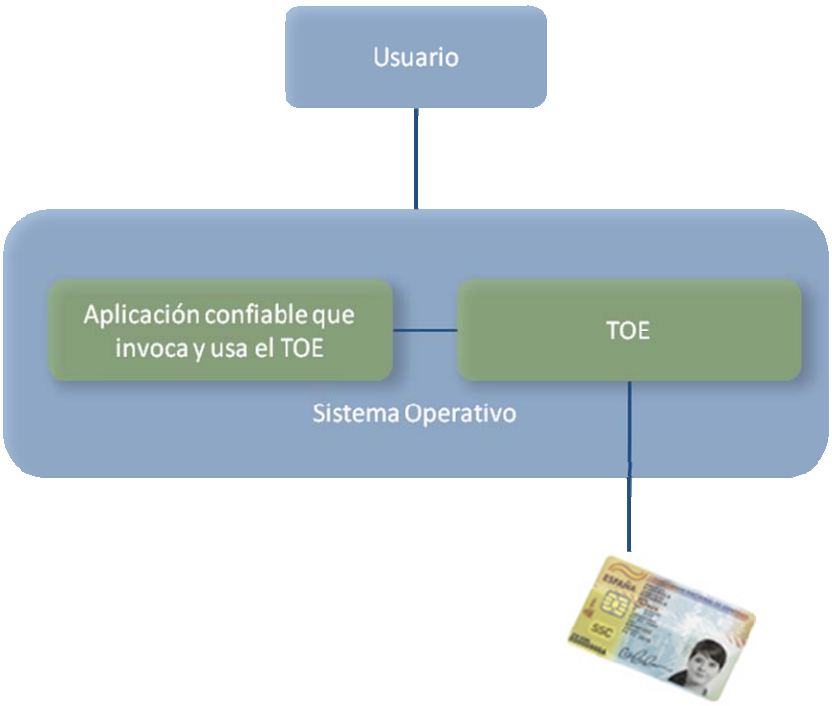


Ilustración 1-1

19 El TOE se instala e integra como un driver en el sistema operativo, y es invocado por las aplicaciones siguiendo los mecanismos que el propio sistema operativo establece. 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.

20 Todas las comunicaciones del TOE están, por tanto, mediadas por el sistema operativo en el que se instala y utiliza.

2. DECLARACIONES DE CONFORMIDAD

2.1. CONFORMIDAD RESPECTO A LA NORMA CC

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

22 No se utilizan requisitos extendidos en la formulación de esta Declaración de Seguridad, por lo que todos los requisitos funcionales indicados lo son según se definen en la norma CC, Parte 2.

2.2. CONFORMIDAD RESPECTO A PERFILES DE PROTECCIÓN

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

3. OBJETIVOS DE SEGURIDAD

3.1. OBJETIVOS DE SEGURIDAD PARA EL ENTORNO OPERACIONAL

24 **OE.ENTORNO SEGURO;**

La plataforma de propósito general sobre la que se instala y opera el TOE es confiable y no es fuente de ataques, incluyendo las aplicaciones que invocan y usan el TOE.

No requiere confianza y puede ser objeto de ataques, el canal de comunicaciones con la tarjeta, esto es, el lector de tarjetas y sus comunicaciones con el ordenador de propósito general, ya sea por cable, wireless o por red.

4. DEFINICIÓN DE COMPONENTES EXTENDIDOS

25 Ninguno.

5. REQUISITOS DE SEGURIDAD DEL TOE

5.1. REQUISITOS FUNCIONALES DE SEGURIDAD

5.1.1. FTP_ITC.1 Inter-TSF trusted channel

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and **"el DNI electrónico"** 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 ***"the TSF"*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **"creación de firma electrónica"**.

5.2. REQUISITOS DE GARANTÍA DE SEGURIDAD

26 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.

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.

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.

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 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.

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.

6. ESPECIFICACIÓN RESUMIDA DEL TOE

6.1. FTP_ITC.1 INTER-TSF TRUSTED CANNEL

27 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 envía 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.).

28 En cuanto a los algoritmos criptográficos utilizados en el driver para la implementación del canal seguro, se utiliza RSA para todo tipo de operaciones criptográficas.

ANEXO I. TRAZA DE TSFIS A SFRS

29 La funcionalidad de que consta el TOE responde al estándar Windows Smart Card Minidriver Specification versión 7.06. De este modo, las aplicaciones usuarias del TOE son las responsables de la invocación de las funciones implementadas por el mismo, cuyo objetivo final es la comunicación con el Lector de DNI electrónico.

30 Dada esta característica, la especificación funcional del TOE es el propio estándar Windows Smart Card Minidriver Specification versión 7.06, por lo que los interfaces accesibles del TOE son los definidos en él, y listados a continuación:

A. INITIALIZATION AND DECONSTRUCT

CardAcquireContext
Initialize communication between the Base CSP/KSP and the card minidriver.

CardDeleteContext
Reverses the effect of CardAcquireContext and severs the communication between the Base CSP/KSP and the card minidriver.

B. CARD PIN OPERATIONS

CardAuthenticatePin
Submits a PIN value as a string to the card to establish the user's identity and to satisfy access conditions for an operation to be undertaken on the user's behalf.

CardDeauthenticate
Is an optional export that should be provided if it is possible within the card minidriver to efficiently reverse the effect of authenticating a user or administrator without resetting the card.

CardAuthenticateEx
Handles PIN authentication operations to the card.

CardDeauthenticateEx
Efficiently reverse the effect of an authentication operation without resetting the card.

C. PUBLIC DATA OPERATIONS

CardGetFileInfo
Retrieves information about a file, specifically its size and ACL information.

CardEnumFiles
Returns name information about available files in a directory as a multistring list.

CardQueryFreeSpace
Determines the amount of available card storage space.

D. CARD CAPABILITIES (MINIDRIVER VERSION 5 AND EARLIER)

CardQueryCapabilities
Queries the card and card-specific minidriver combination for the functionality that is provided at this level, such as certificate or file compression.

E. CARD AND CONTAINER PROPERTIES

CardGetContainerProperty
Takes a LPWSTR that indicates which parameter is being requested. Then it returns data written into the pbData parameter.

CardGetProperty
Takes a LPWSTR that indicates which parameter is being requested. The function returns data in the pbData parameter.

F. KEY CONTAINER

CardGetContainerInfo
Queries the specified key container for more information about which keys are present, such as its key specification.

G. CRYPTOGRAPHIC OPERATIONS

CardRSADecrypt
Performs an RSA decryption operation on the passed buffer by using the private key that a container index refers to.

CardSignData
Signs a block of unpadded data.

CardQueryKeySizes
Returns the public key sizes that are supported by the card in use.

31 El resto de interfaces descritos en el estándar Windows Smart Card Minidriver v 7.06 no son implementados por el driver, por lo que quedan fuera del ámbito de la evaluación.

32 Los interfaces ejercitan la funcionalidad de seguridad del TOE definida por el requisito funcionalidad de seguridad FTP_ITC.1 del modo en que se muestra en la siguiente tabla:

		FTP_ITC.1
Initialization and Deconstruct	CardAcquireContext	
	CardDeleteContext	
Card PIN Operations	CardAuthenticatePin	X

	CardDeauthenticate	X
	CardAuthenticateEx	X
	CardDeauthenticateEx	X
Public Data Operations	CardGetFileInfo	X
	CardEnumFiles	X
	CardQueryFreeSpace	X
Card Capabilities (Minidriver Version 5 and Earlier)	CardQueryCapabilities	X
Card and Container Properties	CardGetContainerProperty	X
	CardGetProperty	X
Key Container	CardGetContainerInfo	X
Cryptographic Operations	CardRSADecrypt	X
	CardSignData	X
	CardQueryKeySizes	X

ANEXO II. ACEPTACIÓN E INSTALACIÓN DEL TOE EN SU ENTORNO OPERACIONAL

A. ACEPTACIÓN DEL TOE

33 El procedimiento a seguir para la aceptación segura del TOE se basa en la verificación del número de versión del driver por parte del personal que efectúa la descarga del mismo, de modo que sea capaz de identificar que se trata de la versión evaluada.

B. INSTALACIÓN DEL TOE

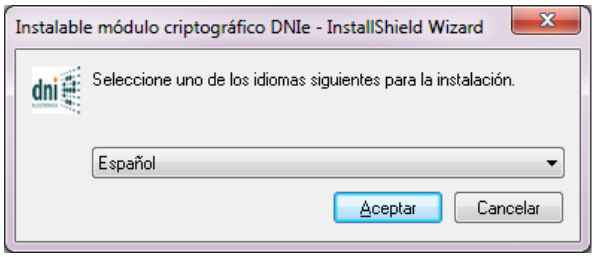
34 La instalación se realiza mediante un asistente desarrollado con la herramienta comercial InstallShield (fuera del ámbito de la evaluación). Este asistente guía al usuario mediante una interface gráfica durante la instalación de los drivers necesarios para poder usar su DNIe en el equipo.

35 Los pasos a seguir durante la instalación son los siguientes:

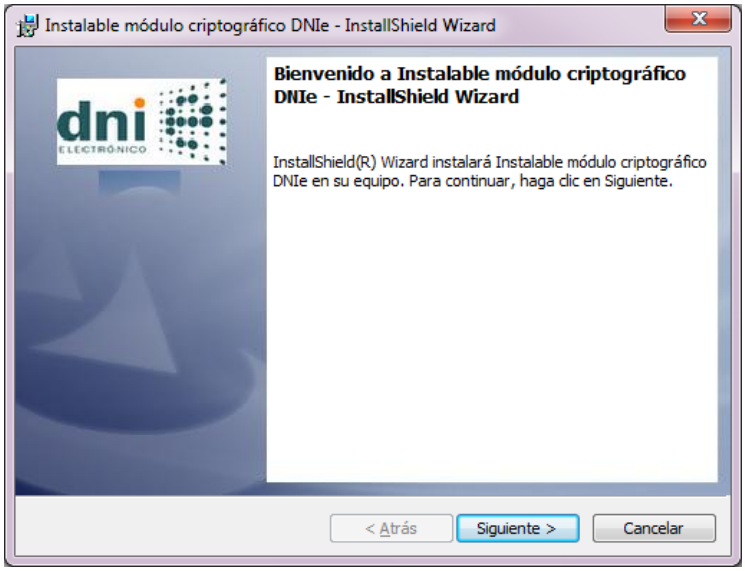
1. Ejecutar el instalador de drivers del DNI electrónico (el cual tiene un formato ejecutable de Windows)

2. El sistema operativo solicitará permisos de administración para llevar a cabo la instalación. Para seguir con la misma es necesario Aceptar la instalación con dichos permisos.

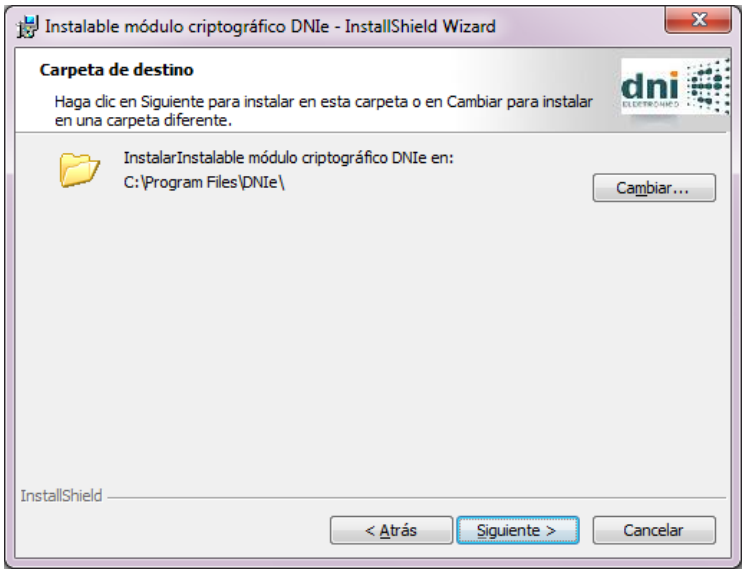
3. Seleccionar el idioma para la instalación:



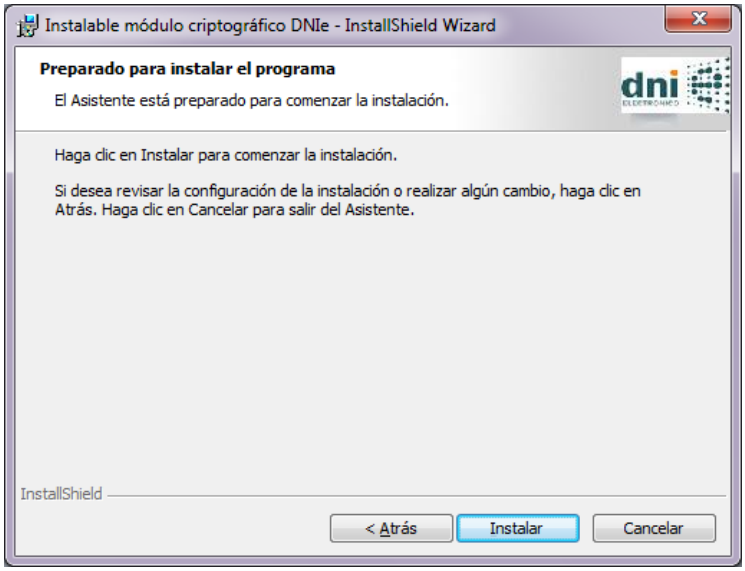
4. Seguir los pasos de la instalación, tal y como se muestra en las siguientes pantallas:



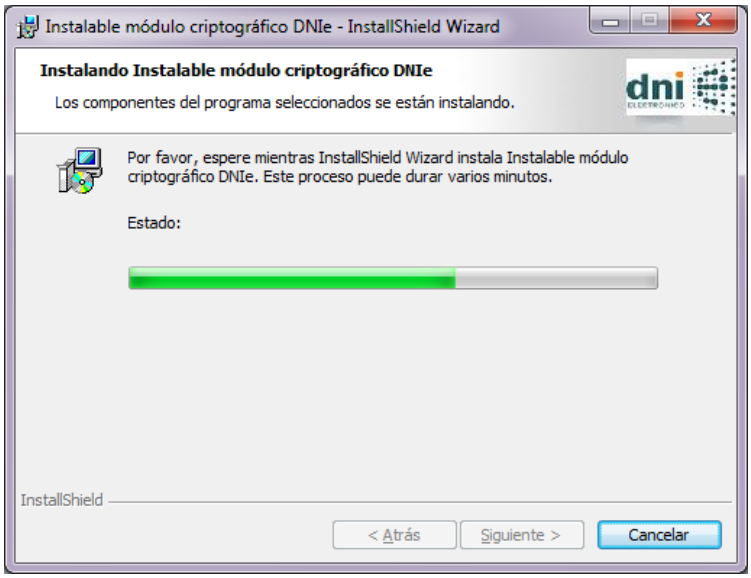
(Seleccionar Siguiente)



(Seleccionar Siguiente)

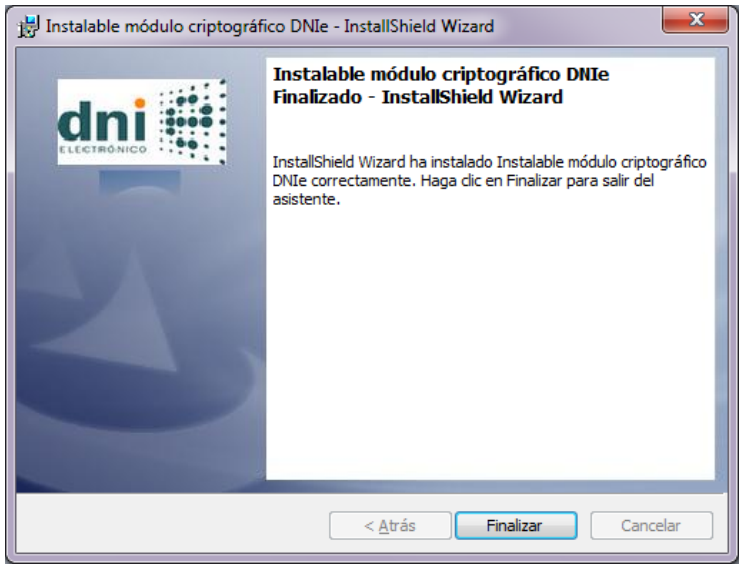


(Seleccionar Instalar)

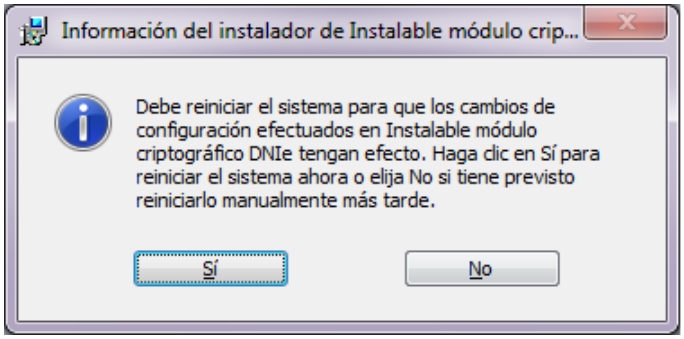


(Esperar hasta que la instalación termine)

(Seleccionar Install)



(Seleccionar Finalizar)



(Seleccionar Sí)

C. APLICACIONES USUARIAS DEL TOE

36 Una vez instalado el TOE en su entorno operacional, éste puede ser utilizado por aplicaciones usuarias. En lo relativo a dichas aplicaciones, tienen que ser confiables. La plataforma sobre la que se instala el TOE será utilizada por personal confiable y estará libre de software malicioso.