TITULO

DECLARACIÓN DE SEGURIDAD

VERSIÓN: RC5

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN

Torre de Cristal
Pº de la Castellana 259C
28046, Madrid

Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

INDICE DE CONTENIDO

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

1 ST Introduction

1.1 Referencias

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-e 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.

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

PPSCVA-T1 Perfil de Protección la aplicación de creación y verificación de firma electrónica Tipo 1, con control exclusivo de los interfaces con el firmante, agrupa los PP para EAL1 y EAL3.

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

1.2 Términos y abreviaturas

Aplicación de creación y verificación de firma electrónica (SCVA) — los medios utilizados para la **creación y verificación** de firma electrónica, sin incluir el SSCD.

Aplicación de generación de certificados (CGA) — es una colección de elementos, a nivel de aplicación, que solicita los datos de verificación de firma (SVD) del dispositivo seguro de creación de firma (SSCD) para la generación del certificado reconocido. La CGA estipula la generación del correspondiente par datos de creación de firma (SCD) / datos de verificación de firma (SVD) por el SSCD, si los SVD pedidos no han sido generados todavía por el SSCD. La CGA verifica la autenticidad de los SVD por medio de:

- La prueba de correspondencia de dispositivo seguro de creación de firma (SSCD) entre los datos de creación de firma (SCD) y los datos de verificación de firma (SVD).
- Verificando el remitente y la integridad de los datos de verificación de firma (SVD) recibidos.

Atributos de firma — es aquella información adicional que se firma junto con el mensaje de usuario.

Certificado — es una garantía electrónica que une los datos de verificación de firma (SVD) a una persona y confirma la identidad de esa persona, tal como se define en la **Directiva**, artículo 2.9.

Certificado reconocido — es el certificado que cumple los requisitos establecidos en el anexo I de la **Directiva** y es suministrado por un proveedor de servicios de certificación (CSP) que cumple los requisitos establecidos en el anexo II de la **Directiva** (definido en la **Directiva**, artículo 2.10).

Datos a ser firmados (DTBS) — son los datos electrónicos completos que hay que firmar (incluyendo tanto los atributos del mensaje del usuario como los de la firma).

Datos de autenticación de referencia (RAD) — son datos almacenados por el dispositivo seguro de creación de firma (SSCD) de forma permanente para la comprobación de los intentos de autenticación de los usuarios autorizados.

Datos de creación de firma (SCD) — Son los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear una firma electrónica (definido en la **Directiva**, artículo 2.4).

Datos de verificación de autenticación (VAD) — son datos de entrada de autenticación proporcionados por el usuario para la autenticación de su identidad bien sea demostrando el conocimiento o bien derivados de las características biométricas del usuario.

Datos de verificación de firma (SVD) — son los datos, como códigos o claves criptográficas públicas, que se utilizan para de verificar una firma electrónica (definidos en la **Directiva**, artículo 2.7).

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

Directiva — es la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica [1], también referida como "Directiva". en el resto del Perfil de Protección (PP).

Dispositivo seguro de creación de firma (SSCD) — es el software o hardware configurado para aplicar los datos de creación de firma (SCD) y que cumple los requisitos establecidos en el anexo III de la **Directiva**. (El término SSCD se define en la propia **Directiva** artículos 2.5 y 2.6).

Documento del Firmante (SD) — el documento en formato electrónico que el firmante pretende firmar electrónicamente.

Firma electrónica avanzada — (definida en la **Directiva**, artículo 2.2) es la firma electrónica que cumple los requisitos siguientes:

- Estar vinculada al firmante de manera única.
- Permitir la identificación del firmante.
- Haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control.
- Estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable.

Firma electrónica reconocida — es una firma electrónica avanzada basada en un certificado reconocido y que ha sido creada por un dispositivo seguro de creación de firma (SSCD) según la **Directiva**, artículo 5, párrafo 1.

Firmante — es la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa (definido en la **Directiva**, artículo 2.3).

Objeto de datos firmados (SDO) — son los datos electrónicos a los que se adjuntó la firma electrónica o a los que ésta se asoció lógicamente como método de autenticación.

Organismo notificado — Los Estados Miembros deben notificar a la Comisión y a los otros Estados Miembros los organismos nacionales (referidos como organismos notificados en este Perfil de Protección (PP)) que son responsables de la acreditación y supervisión, así como de los organismos referidos en el artículo 3(4) (**Directiva**, artículo 11(1b)). Nótese que los organismos a los que se refiere el artículo 3(4) determinan la conformidad de los dispositivos seguros de creación de firma electrónica, conforme a los requisitos establecidos en el Anexo III de la **Directiva**.

Proveedor de servicios de certificación (CSP) — es la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación a la firma electrónica (definido en la **Directiva**, artículo 2.11).

Representación de los datos a ser firmados (DTBSR) — (representación de datos a ser firmados (DTBS) son los datos enviados por la aplicación de creación de firma (SCA) al dispositivo seguro de creación de firma (SSCD) para firmar y son:

- Un valor matemático (*hash*) de los datos a ser firmados (DTBS); o un valor matemático (*hash*) de los DTBS o
- Un valor matemático (*hash*) intermedio de una primera parte de los datos a ser firmados (DTBS) y una parte restante de los DTBS o
- Los datos a ser firmados (DTBS).

Sistema de creación de firma (SCS) — es el sistema global que crea una firma electrónica. El sistema de creación de firma se compone de la aplicación de creación de firma (SCVA) y del dispositivo seguro de creación de firma (SSCD).

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

1.3 ST reference

Título: Declaración de seguridad para el producto Crypto.X

Título corto: Declaración_Seguridad_CryptoX

Versión: RC5

Autor: Inixa del Principado, S.L.

Fecha de publicación: 8 de Febrero de 2012

1.4 TOE reference

Nombre: Crypto.X

Versión: 2.3.6.1

1.5 TOE overview

Crypto.X es una SCVA - Tipo 2, una aplicación de creación y verificación de firma electrónica utilizando el DNI-e.

Medidas de seguridad incluidas en el producto:

- Comprobación y validación de formato y de Documentos a Firmar o Validar, y comprobaciones periódicas de su integridad a lo largo de todo el proceso.
- Comprobación de la integridad del programa y procedimientos durante todo el proceso, tanto de forma automática como a petición del usuario.
- Control de confidencialidad del VAD y tratamiento seguro del mismo mediante un canal de comunicación seguro y lógicamente independiente.
- Sistema de seguridad mediante captchas para evitar la impersonación trivial de la voluntad expresa de firma del usuario.

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

La funcionalidad de Crypto.X, para la creación de firma electrónica, incluye:

- La capacidad de seleccionar un documento para firmar (SD).
- La capacidad de seleccionar la política de firma a aplicar, los atributos de la firma, y el certificado a utilizar para la firma, y componer los DTBS.
- La capacidad de mostrar de manera no ambigua los DTBS al firmante, para un número determinado de formatos de documento electrónico, y de detectar formatos o construcciones problemáticas, en cuyo caso rechaza la operación de creación de firma de estos documentos.
- La capacidad de requerir el VAD del firmante de manera explícita en cada operación de firma, y de autenticarlo frente al SSCD, y de mandar los DTBSR al mismo SSCD, si el firmante expresa su voluntad inequívoca de firmar el documento.
- La capacidad de asociar la firma electrónica creada por el SSCD al propio documento firmado, o de facilitar la firma realizada como datos separados.
- La capacidad de eliminar del ámbito de control de la SCVA el VAD y los demás datos de usuario asociados a una firma, tan pronto como dejan de ser necesarios para la realización de la misma.

La funcionalidad de Crypto.X, para la verificación de firma electrónica, incluye:

- La capacidad de seleccionar un documento firmado (SDO).
- La capacidad de seleccionar una política de certificación a aplicar.
- La capacidad de mostrar al usuario que solicita su verificación, de manera no ambigua, el SDO y los correspondientes atributos de la firma, para un número determinado de formatos de documento electrónico, y de detectar formatos o construcciones problemáticas, en cuyo caso rechaza la operación de verificación de firma de estos documentos.
- La capacidad de verificar la firma electrónica, conforme a la política de certificación seleccionada, y la capacidad de mostrar el resultado de la verificación al usuario que la ha solicitado. Este resultado deberá discriminar entre firmas válidas e inválidas, cuando el proceso de verificación ha podido realizarse, e identificará las firmas que no han podido verificarse.

Una "SCVA - Tipo 2" es una aplicación de creación y verificación de firma electrónica, e incluye la funcionalidad necesaria para verificar y crear una firma electrónica, utilizando el propio DNI-e, que es un elemento de uso obligado.

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

La "SCVA - Tipo 2" requiere de una plataforma de computación, fuera del ámbito del TOE, para el interfaz con el firmante, las comunicaciones con el DNI-e, y para acceder y utilizar recursos generales de computación, tales como CPU o memoria.

Esta plataforma de propósito general debe ser confiable, y será configurada y gestionada de tal manera.

El sistema operativo sobre el que corre el TOE es un Windows XP Bastionado.

La citada plataforma deberá cumplir unos requisitos mínimos de capacidad de computación y contener el hardware necesario para el funcionamiento del TOE. Estos elementos se enumeran a continuación:

- Procesador Intel Pentium 1 GHz o CPU con velocidad de procesado equivalente.
- Memoria RAM de al menos 256 Megabytes.
- Disco duro de al menos 3 Gigabytes.
- Monitor con una resolución mínima de 800x600.
- Un puerto USB como mínimo.
- Lector y grabador de CDs.
- Lector de tarjetas inteligentes USB que cumpla con el estándar USB CCID compatible con el DNI-e:
    - Debe cumplir el estándar ISO-7816 (1, 2 y 3).
    - Debe soportar tarjetas asíncronas en protocolos T=0 y T=1.
    - Debe soportar velocidades de comunicación mínimas de 9.600 bps.
    - Debe soportar los estándares API PC/SC, CSP, API PKCS#11.

La "SCVA - Tipo 2" requiere de un DNI-e como dispositivo seguro de creación de firma.

Los siguientes datos se reciben a través de uno de los interfaces de la SCVA. No se supone si estos interfaces lo son para entidades locales o remotas:

- El Documento del Firmante (SD), y

- Los Datos de verificación de firma (SVD).

El Objeto de datos firmados (SDO) es un resultado de la funcionalidad de creación de firma del TOE, y se exporta a través de uno de los interfaces de la SCVA, sin que se suponga si es una exportación local o remota. El SDO se recibe como entrada para realizar la funcionalidad de verificación de firma, también a través de uno de sus interfaces, y de nuevo sin distinguir sobre si es una importación local o remota.

El TOE descansa en su entorno para comunicarse con el firmante, así como con el DNI-e.

Mientras que los SD, SDO y SVD se reciben probablemente de una entidad externa, nada impide que el propio firmante los introduzca directamente a través del interfaz que posee la SCVA, ni que los lea a través del mismo interfaz. En todo caso, no hay hipótesis de seguridad relativas a estas entidades externas que facilitan o reciben el SD, SDO y SVD.

1.6 Descripción del TOE

1.6.1 Alcance físico del producto

El TOE incluye los siguientes componentes:

- Binarios Crypto·X (CryptoX.exe , CryptoXH.dll)
- Binarios del driver del DNIe: UsrDNIeCertStore.dll y dniecsp.dll

1.6.2 Alcance lógico del producto

A continuación se describe el alcance lógico del producto:

- Implementa medidas de seguridad para comprobar el formato del texto que se desea firmar, detectando cualquier modificación o error de integridad en el mismo antes de realizar la firma.
- Provee un canal de comunicación seguro entre sí mismo y el DNI-e para la creación de firma.
- Permite la autenticación del firmante utilizando el DNI-e.
- Implementa medidas de seguridad para liberar los recursos utilizados tras la creación/verificación de firma.
- Implementa medidas de seguridad de auto comprobación para garantizar el correcto funcionamiento y la no alteración. Estas medidas se realizan durante el arranque inicial, periódicamente durante su operación normal, y bajo petición del usuario.
- Implementa un visor seguro el cual permite visualizar el texto a firmar previamente.
- Provee un sistema de seguridad que evita la impersonación del firmante y que permite al usuario expresar su voluntad para llevar a cabo la operación.
- Únicamente acepta para la firma documentos de texto almacenados en ficheros con extensión .txt y de no más de 5000 caracteres en formato ASCII restringido a los caracteres con códigos desde 0x30 a 0x7E ambos excluidos.
- Importa firmas en formato PKCS7 en un fichero situado en el mismo directorio y con el mismo nombre (extensión .p7s) que el archivo firmado.
- Crea firmas en formato PKCS7 utilizando el hash SHA-1 del documento a firmar utilizando certificados de firma del DNI-e con longitud mínima de 2048 bits.
- Verifica tanto la firma del documento como el certificado que firma.

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

2 Conformance Claims

2.1 CC Conformance Claim

Se cumple con la norma CC versión 3.1 R3, metodología CEM 3.1, R3. Se cumple además la conformidad con la parte 2 extendida de la norma, así como con la parte 3 de la norma.

2.2 PP Claim

Se cumple estrictamente con el perfil de protección con título "Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2 con nivel de evaluación de los requisitos de seguridad EAL1" y de nombre corto PPSCVA-T2, EAL1 del INTECO, versión v 2.0 del 18 de Diciembre del año 2008.

2.3 Conformance Rationale

- El tipo de TOE es el mismo que en el perfil de protección referenciado.
- La definición del problema de seguridad está directamente correlacionada con el perfil de protección referenciado
- Los objetivos de seguridad son comunes con el perfil de protección referenciado.
- El uso del TOE es el mismo que en el perfil de protección referenciado.
- Los registros funcionales son los mismos que en el mencionado perfil de protección.
- Las operaciones se han resuelto de manera conforme al perfil de protección.

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

3 Definición del problema de seguridad

3.1 Activos del TOE

Activos a proteger por la SCVA

A. DSCVA

La integridad y representación no ambigua del Documento del Firmante (SD), así como de sus representaciones intermedias, como los DTBS, mientras se remite al DNI-e y están en posesión de la SCVA. De igual manera, la integridad de todos los datos de usuario necesarios para las operaciones de creación o verificación de firma, tales como los atributos de la firma, los SVD, las políticas de firma aplicadas y el VAD.

A.SCVA

La integridad de la funcionalidad de la SCVA, de manera que se garantice que su comportamiento fiable no se puede modificar.

A.VAD

La confidencialidad de los Datos de verificación de autenticación (VAD), que se transmiten al DNI-e para la realización de la operación de firma.

3.2 Amenazas

Amenazas soportadas por la SCVA

T.DSCVA

Un atacante modifica cualquiera de los datos de usuario que intervienen en la creación o verificación de firma, mientras están en posesión de la SCVA, o durante el proceso de remisión al DNI-e para la realización de la firma.

Un atacante es capaz de incluir información en el SD, que no se muestra por la SCVA al firmante, y que aún siendo conforme con el formato de documento electrónico del SD, que se firma de manera inadvertida. Esta amenaza compromete el activo A.DSCVA

Un atacante es capaz de incluir información en el SDO, que no se muestra por la SCVA al firmante, y que aún siendo conforme con el formato de documento electrónico del SDO, se verifica de manera inadvertida. Esta amenaza compromete el activo A. DSCVADSCVA.

T.SCVA

Un atacante es capaz de tomar el control del proceso de firma, engañando al firmante, o abusando de los medios de firma, de manera que puede obtener firmas electrónicas sin el consentimiento del titular legítimo del DNI-e.

Lo mismo aplica al proceso de verificación de firmas, forzando falsos positivos o negativos. Esta amenaza incluye una posible modificación del propio TOE, de manera que se altere su funcionalidad. Esta amenaza compromete el activo A.SCVA.

T.VAD

Un atacante compromete la confidencialidad del VAD, perdiendo su titular el control del exclusivo del DNI-e. Esta amenaza compromete el activo A.VAD.

3.3 Hipótesis

Entorno de computación

AS.ITENV

La plataforma de propósito general que la "SCVA - Tipo 2" necesite para operar y para facilitar los interfaces de firmante y con el **DNI-e**, facilita las protecciones y mecanismos de seguridad adecuados para proteger los activos de la SCVA (A.DSCVA, A.VAD y A.SCVA).

Nota: Esto implica que las vulnerabilidades que sean eficaces a través del entorno de uso de la SCVA, pero que no explotan una vulnerabilidad propia de la construcción u operación de la SCVA, no se consideran que afecten a la certificación de la misma, sino que deben resolverse mediante la configuración y uso de un entorno adecuado para la misma. Cómo configurar una plataforma de propósito general de manera que no presente formas de ataque a los activos de la SCVA es una tarea ardua, fuera del alcance de este PP.

3.4 Políticas organizativas

Dispositivo Seguro de Creación de Firma

P.SSCD

El dispositivo seguro de creación de firma que usa la SCVA será el **DNI-e**.

Algoritmos criptográficos

P.CRYPTO

Los algoritmos criptográficos que realice la SCVA, así como el certificado seleccionado para crear o verificar una firma deberán ser tales que se verifiquen y produzcan firmas reconocidas con el **DNI-e**.

Protección de Datos de Carácter Personal

P.LOPD

La SCVA avisará al firmante sobre el hecho de que datos suyos de carácter personal se incluyen en la firma, tal como la realiza el **DNI-e**.

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN

Torre de Cristal
Pº de la Castellana 259C
28046, Madrid

Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

4 Objetivos de seguridad

4.1 Objetivos de seguridad para el TOE

O.INT

Garantizar la integridad de los DTBS, así como de todos los datos de usuario necesarios para la creación o verificación de las firmas electrónicas.

O.CONF

Garantizar la confidencialidad del VAD, de manera que se garantice a su titular legítimo el control exclusivo de la funcionalidad de firma del DNI-e.

O.CONT

Garantizar la integridad del propio TOE, de manera que su funcionalidad no se pueda comprometer.

O.STEGA

Definir un conjunto de formatos de documento electrónico que sean representables de manera no ambigua, y limitar la capacidad de firma a los documentos basados en estos formatos. Incluir un visor seguro de documentos, que detecte y rechace cualquier información oculta o de representación ambigua.

O.CRYPTO

Los algoritmos criptográficos que realice la SCVA, así como el certificado seleccionado para crear o verificar una firma deberán ser tales que se verifiquen y produzcan firmas reconocidas con el DNI-e.

O.LOPD

La SCVA avisará al firmante sobre el hecho de que datos suyos de carácter personal se incluyen en la firma, tal como la realiza el DNI-e.

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

4.2 Objetivos de seguridad para el entorno operacional

O.SSCD

El dispositivo seguro de creación de firma que usa la SCVA será el DNI-e.

O.ITENV

La plataforma de propósito general que la "SCVA - Tipo 2" necesita para operar y para facilitar los interfaces de firmante y con el DNI-e, facilita las protecciones y mecanismos de seguridad adecuados para proteger los activos de la SCVA (A.DSCVA, A.VAD y A.SCVA), mediante una combinación eficaz de medidas de índole técnico, de procedimientos y de securización de su entorno.

4.3 Justificación de los objetivos de seguridad

Objetivos de seguridad del TOE

En la siguiente tabla se presenta la correspondencia entre los objetivos de seguridad del TOE y las amenazas y políticas de seguridad, tal y como se especifican en la definición de problema de seguridad:

	T,DSCVA	**T.SCVA**	**T.VAD**	**P.CRYPTO**	**P.LOPD**
O.INT	X				
O.CONF			X		
O.CONT		X			
O.STEGA	X				
O.CRYPTO				X	
O.LOPD					X

Tabla 1: Correspondencia de los objetivos de seguridad del TOE

Como se puede ver, la correspondencia cumple con las propiedades requeridas:

No existen objetivos espurios: cada objetivo de seguridad se corresponde con, al menos, una amenaza o una OSP o una hipótesis.

La correspondencia es completa con respecto a la definición del problema de seguridad: cada amenaza, OSP o hipótesis se corresponde, al menos, con un objetivo de seguridad.

La correspondencia es correcta: las hipótesis se asocian siempre al entorno operacional del TOE y los objetivos de seguridad del TOE no se corresponden con ninguna hipótesis.

Para contrarrestar la amenaza T.DSCVA, O.INT asegura la integridad de los datos de usuario necesarios para la realización de las operaciones de creación o verificación de firma. O.STEGA a su vez, asegura que el SD es de un tipo seguro, tal que no pueda inducir a error al usuario firmante.

Para contrarrestar la amenaza T.SCVA, O.CONT asegura la integridad del TOE, por lo que evita que éste pueda ser comprometido por un atacante. Es importante mencionar que esta protección deberá ser efectiva únicamente para el potencial de ataque especificado.

La amenaza T.VAD se contrarresta directamente por O.CONF.

Las políticas de seguridad organizativa P.CRYPTO y P.LOPD, se abordan directamente por O.CRYPTO y O.LOPD respectivamente.

La política de seguridad P.SSCD se aborda directamente con el objetivo de seguridad del entorno O.SSCD, al determinar este que el DNI-e será el dispositivo seguro de creación de firma que utiliza la SCVA.

Objetivos para el entorno

La siguiente tabla muestra la correspondencia trivial entre los objetivos de seguridad del entorno del TOE y la política de seguridad aplicable e hipótesis, tal y como se especifica en la definición del problema de seguridad:

	P.SSCD	**AS.ITENV**
O.SSCD	X	
O.ITENV		X

Tabla 2: Correspondencia de los objetivos de seguridad del entorno

La hipótesis de seguridad AS.ITENV se aborda directamente con el objetivo de seguridad para el entorno operacional O.ITENV al estipular que la plataforma de propósito general debe facilitar las protecciones y mecanismos de seguridad adecuados para proteger los activos de la SCVA.

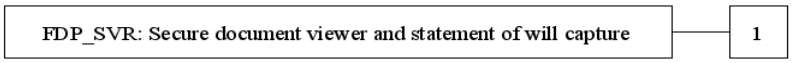
5 Definición de componentes extendidos

Secure document viewer and statement of will capture (FDP_SVR)

Family Behaviour

This extended family defines the mechanisms for TSF-mediated displaying of an SD or an SDO to the signatory without misleading or ambiguous interpretation, and for a secure and non misleading capture of the signature will to sign or for the signature verification process. This family also ensures that the signatory is informed about the personal data that is to be incorporated into the electronic signature, which can later be retrieved and accessed outside the TSF control.

Component levelling



Management

No management activities apply.

Audit

No audit requirements apply.

FDP_SVR.1 Secure viewer and SCVA interface

Hierarchical to: No other components

Dependencies: No dependencies.

User application notes

This extended component is used to specify the mechanisms for TSF-mediated displaying of an SD or an SDO to the signatory without misleading or ambiguous interpretation, and for a secure and non misleading capture of the signature will to sign, and of the signature verification process.

FDP_SVR.1.1 The TSF shall provide a secure SD or SDO viewer, so that no steganographed or misleading data is inadvertently signed / verified by the signatory. This goes beyond the limitations on accepted file formats, by ensuring that

All document elements are shown (no document parts outside the signatory view)

All document elements can be seen (drawing size appreciable and readable)

FDP_SVR.1.2 The TSF shall warn the signatory about the personal data that is to be incorporated into the electronic signature, with the following message: **La realización de una firma electrónica implica el tratamiento de los datos de carácter personal contenidos en los certificados, y serán comunicados a todas las entidades con acceso a este documento firmado, ante las que podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición conforme lo estipulado en la Ley Orgánica de Protección de datos.**

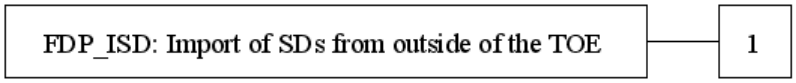
FDP_SVR.1.3 The TSF shall prompt the signatory with a non trivial challenge to capture his/her will to sign, so the signatory cannot trivially be impersonated.

Import of SDs from outside of the TOE (FDP_ISD)

Family Behaviour

This extended family defines the mechanisms for TSF-mediated importing of user data into the TOE, which has to comply with a number of restrictions.

Component levelling



Management

No management activities apply.

Audit

No audit requirements apply

FDP_ISD.1 Import of Signer's Document

Hierarchical to: No other components

Dependencies: No dependencies.

User application notes

This extended component is used to specify the import of user data as SD, which has to comply with a number of restrictions.

FDP_ISD.1.1 The TSF shall only accept for signature documents based in one of the following electronic formats [assignment: *relación de formatos de documento electrónico (a_1)*] when importing user data, as SDs, or SDOs, from outside of the TOE, which comply with the following [assignment: *definición de las reglas de contenido y presentación de los formatos indicados (a_2)*]

(a_1) el autor de la declaración de seguridad especificará la relación de formatos de documento electrónico que el TOE es capaz de interpretar y mostrar de manera no ambigua.

(a_2) el autor de la declaración de seguridad especificará la lista de reglas aplicables a los formatos de documento electrónico que permiten su interpretación y presentación de manera no ambigua al firmante.

FDP_ISD.1.2 The TSF shall reject the import of any document not fully conformant to the previously defined electronic file formats and shall show to the signatory an alert message including the full report of those nonconformities detected.

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN

Torre de Cristal
Pº de la Castellana 259C
28046, Madrid

Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

6 Requisitos de seguridad del TOE

Requisitos funcionales de seguridad

Requisitos para garantizar la integridad de los datos de usuario

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data (SD, Signature Attributes, DTBS, DTBSR, SVD, SDO, VAD) stored in containers controlled by the TSF for [assignment: **La TSF realiza una comprobación del texto a firmar una vez se ha importado correctamente, detectando cualquier modificación o error de integridad en el mismo antes de realizar la firma**] on all objects, based on the following attributes: [assignment: **La TSF utiliza el hash SHA1 del texto a firmar para monitorizar su integridad**].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: **interrumpir la operación de creación/verificación de firma, y notificar al firmante**].

FTP_ITC.1.UD Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and **the SSCD** 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: **la TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: **creación y verificación de firma**].

Requisitos para garantizar la confidencialidad de los VAD

FTP_ITC.1.VAD Inter-TSF trusted channel/VAD

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and **the SSCD** 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: **la TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: **autenticación de firmante, presentando el VAD al DNI-e**].

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: **deasignación del recurso para**] the following objects: [assignment: **VAD**]

Requisitos para garantizar el control del proceso de creación y verificación de firmas

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests [selection**: durante el arranque inicial, periódicamente durante su operación normal, y, por petición del firmante**] to demonstrate the correct operation of [selection: **la TSF**].

FPT_TST.1.2 The TSF shall provide the signatory with the capability to verify the integrity of [selection: **los datos de la TSF**].

FPT_TST.1.3 The TSF shall provide the signatory with the capability to verify the integrity of stored TSF executable code.

FDP_SVR.1 **Secure viewer and SCVA interface**

FDP_SVR.1.1 The TSF shall provide a secure SD viewer, so that no steganographed or misleading data is inadvertently signed by the signatory. This goes beyond the limitations on accepted file formats, by ensuring that

- All document elements are shown (no document parts outside the signatory view)
- All document elements can be seen (drawing size appreciable and readable)

FDP_SVR.1.2 The TSF shall warn the signatory about the personal data that is to be incorporated into the electronic signature, with the following message: **La realización de una firma electrónica implica el tratamiento de los datos de carácter personal contenidos en los certificados, y serán comunicados a todas las entidades con acceso a este documento firmado, ante las que podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición conforme lo estipulado en la Ley Orgánica de Protección de datos.**

FDP_SVR.1.3 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.

Requisitos para importar el SD y datos de usuario relacionados

FDP_ISD.1 Import of Signer's Document

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

FDP_ISD.1.1 The TSF shall only accept for signature documents based in one of the following electronic formats [assignment: **El TOE es capaz de interpretar de manera no ambigua textos de no más de 5000 caracteres en formato ASCII restringido a los caracteres con códigos desde 0x30 a 0x7E ambos excluídos**] when importing user data, as SDs, from outside of the TOE, which comply with the following [assignment: **El texto se encontrará en un fichero de texto en formato ASCII y extensión txt.**

Sólo se admiten caracteres ASCII con códigos desde 0x30 a 0x7E ambos excluídos.

El texto se presentará de manera no ambigua en letra negra sobre fondo claro.]

FDP_ISD.1.2 The TSF shall reject the import of any document not fully conformant to the previously defined electronic file formats and shall show to the signatory an alert message including the full report of those nonconformities detected.

FDP_ITC.1 Import of user data without security attributes

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: **Para la creación de firma: Documento del Firmante. Para la verificación de firma: Firma en formato PKCS7 en un fichero situado en el mismo directorio y con el mismo nombre (distinta extensión) que el archivo firmado]**

Requisitos criptográficos para la creación y verificación de la firma electrónica

FCS_COP.1_SIGNATURE_CREATION_PROCESS Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: **Hash SHA-1 del documento y firma RSA de dicho hash creando el fichero de firma PKCS7**] in accordance with a specified cryptographic algorithm [assignment: **Hash SHA-1, PKCS #7**] and cryptographic key sizes [assignment: **Para certificados de firma una longitud mínima de 2048 bits**] that meet the following: [assignment: **ninguna**]

FCS_COP.1_SIGNATURE_VERIFICATION Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: **Comprobación de la firma RSA y del certificado que firma, y comprobación de que el Hash SHA-1 se corresponde con el documento firmado**] in accordance with a specified cryptographic algorithm [assignment: **SHA-1, PKCS #7**] and cryptographic key sizes [assignment: **Para certificados de firma una longitud mínima de 2048 bits**] that meet the following: [assignment: **ninguna**].

Requisitos de garantía de seguridad

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

- EAL1

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

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 of evidence 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 categorization of interfaces as SFR-non-interfering.

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

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 of evidence 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.

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence 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.

ALC_CMC.1 Labeling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

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

Content and presentation of evidence elements:

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

ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence 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.

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence 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 summarize 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.

ASE_CCL.1 Conformance claims

Dependencies:

ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

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 of evidence 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.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence elements:

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

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 of evidence 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.

ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements:

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

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 of evidence 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.

ASE_TSS.1 TOE summary specification

Dependencies:

ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

ATE_IND.1 Independent testing - conformance

Dependencies:

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation of evidence elements:

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

AVA_VAN.1 Vulnerability survey

Dependencies:

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation of evidence elements:

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

Justificación de los requisitos de seguridad

Justificación de los requisitos funcionales de seguridad

1 La tabla siguiente muestra la relación entre los objetivos de seguridad del TOE y los requisitos funcionales de seguridad aplicables:

	O.INT	O.CONF	O.CONT	O.STEGA	O.CRYPTO	O.LOPD
FDP_SDI.2 Stored data integrity monitoring and action	X					

FTP_ITC.1.UD Inter-TSF trusted channel	X					
FTP_ITC.1.VAD Inter-TSF trusted channel/VAD		X				
FDP_RIP.1 Subset residual information protection		X				
FPT_TST.1 TSF testing			X			
FDP_SVR.1 Secure viewer and SCVA interface				X		X
FDP_ISD.1 Import of Signer's Document				X	X	
FDP_ITC.1 Import of user data without security attributes					X	
FCS_COP.1_SIGNATURE_CREATION Cryptographic operation					X	
FCS_COP.1_SIGNATURE_VERIFICATION Cryptographic operation					X	

Tabla 1 Correspondencia Requisitos de seguridad vs. Objetivos de seguridad

2 La correspondencia especifica cómo cada SFR se corresponde con cada objetivo de seguridad demostrando que:

- No existen SFR espurios: cada SFR se corresponde con, al menos, un objetivo de seguridad.
- La correspondencia es completa con respecto a los objetivos de seguridad del TOE: cada objetivo de seguridad se corresponde, al menos, con un SFR.

3 Para satisfacer el objetivo O.INT, el TOE deberá monitorizar la integridad de los activos correspondientes, tal y como requiere FDP_SDI.2 Stored data integrity monitoring and

action, y durante su envío al DNI-e, tal y como requiere FTP_ITC.1.UD Inter-TSF trusted channel.

4 La confidencialidad de los VAD, O.CONF, se consigue asegurando que éstos no se vean comprometidos durante su transmisión al DNI-e, tal y como requiere FTP_ITC.1.VAD Inter-TSF trusted channel/VAD, y asegurando la no disponibilidad de los mismos, cuando el TOE libere los recursos que los almacenaban, tal y como requiere FDP_RIP.1 Subset residual information protection.

5 Para asegurar la integridad del TOE de forma que su funcionalidad no se vea comprometida, tal y como requiere O.CONT, se especifica el requisito FPT_TST.1 TSF testing, que define una monitorización de la integridad del mismo TOE.

6 O.STEGA se aborda en primera instancia por FDP_ISD.1 Import of Signer's Document, que exige una serie de propiedades de seguridad al SD y el SDO, y posteriormente por la funcionalidad de confianza del visor que se especifica en FDP_SVR.1 Secure viewer and SCVA interface.

7 Se aborda el objetivo O.CRYPTO mediante los SFRs FCS_COP.1_SIGNATURE_CREATION Cryptographic operation y FCS_COP.1_SIGNATURE_VERIFICATION Cryptographic operation para el proceso de creación y verificación de firma electrónica respectivamente. Estos requisitos necesitan importar los datos de entrada necesarios para la realización de las operaciones criptográficas correspondientes, como se requiere en FDP_ITC.1 Import of user data without security attributes y FDP_ISD.1 Import of Signer's Document. El requisito FDP_ISD.1 Import of Signer's Document es un requisito funcional extendido, que se diferencia principalmente de FDP_ITC.1 Import of user data without security attributes en la especificación de la acción que debe ser llevada a cabo cuando no se cumplen las reglas de importación definidas.

8 El objetivo de seguridad O.LOPD se consigue de manera trivial mediante el visor seguro, FDP_SVR.1 Secure viewer and SCVA interface, en el que se incluye el aviso requerido.

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
Torre de Cristal
Pº de la Castellana 259C
28046, Madrid
Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com

Dependencias de los requisitos funcionales de seguridad

9 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:

- 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.

- Para satisfacer FCS_COP.1_SIGNATURE_CREATION Cryptographic operation, el TOE el TOE debe realizar las operaciones criptográficas establecidas en este requisito sobre los datos importados mediante el requisito FDP_ISD.1 Import of Signers's Document.

- Para satisfacer FCS_COP.1_SIGNATURE_VERIFICATION el TOE debe importar la clave pública (FDP_ITC.1 Import of user data without security attributes) y el documento firmado (FDP_ISD.1 Import of Signers's Document) y mediante el algoritmo descrito en el requisito verificar la firma.

- Justificación de no inclusión de dependencia FCS_CKM.4: En el proceso de creación de firma el TOE no se requiere de la creación ni la importación de claves públicas, por tanto la destrucción de la clave pública no aplica. Además en el proceso de verificación de firma, la destrucción de clave pública importada mediante FDP_ITC.1 tampoco aplica. Ya que los algoritmos de clave pública se autoprotegen de posibles alteraciones de la clave pública y por tanto la destrucción de ésta no aplica.

Justificación de los requisitos de seguridad de garantía

10 La garantía de seguridad deseada para este tipo de TOE es la proporcionada por el nivel de evaluación EAL1.

7 TOE Summary Specification

El TOE realiza una comprobación del texto a firmar una vez que se ha importado éste correctamente. Para llevar a cabo esta comprobación el TOE realiza las siguientes operaciones:

- Se obtiene el hash SHA1 del fichero que contiene el texto a firmar previa realización de la firma.
- Se obtiene el hash SHA1 del fichero que contiene el texto a firmar tras realizar la firma.
- Se comparan los dos hash, y si no son iguales se detecta una manipulación no permitida.

Para realizar el hash no se utiliza el texto importado en memoria, sino que el hash se realiza utilizando el fichero que contiene el texto a firmar, fichero que se mantiene bloqueado a nivel del sistema operativo durante todo el proceso.

Ante cualquier detección de modificación del texto, se interrumpe la operación y se notifica al usuario.

Para proveer un canal de comunicación seguro entre sí mismo y el DNI-e (tanto para la creación como para la verificación de firma) el TOE utiliza los servicios criptográficos que proporciona el sistema operativo Windows XP SP3 a través de CAPICOM; junto con el CSP del DNI-e.

El TOE permite la autenticación del firmante utilizando el DNI-e, para lo cual previa realización de la firma se le solicita el código PIN de su DNI-e.

Tanto en la realización como en la verificación de la firma, el TOE libera los recursos utilizados al realizar ambas operaciones. Estos recursos se liberan utilizando los servicios criptográficos que proporciona el sistema operativo Windows XP SP3 a través de CAPICOM.

Para garantizar el correcto funcionamiento, el TOE implementa medidas de seguridad de auto comprobación, las cuales lleva a cabo de la siguiente forma:

- Previo arranque del TOE se calcula el hash SHA1 de los siguientes elementos: CryptoX.exe, UsrDNIeCertStore.dll y dnicsp.dll. Para el elemento CryptoXH.dll en lugar del hash SHA1 se obtiene su tamaño en bytes. Los valores obtenidos se comparan con los valores obtenidos en el momento de la compilación de la versión proporcionada. Si cualquiera de estos valores no coinciden se notifica al usuario y se interrumpe el arranque del TOE.
- Durante todo el tiempo que el TOE está ejecutándose se realiza también la verificación indicada anteriormente, de esta forma si durante la ejecución normal del TOE se realiza una modificación este hecho se notifica al usuario y se interrumpe el TOE.
- También se le permite al usuario que realice ésta comprobación cuando él lo vea necesario utilizando para ello un interfaz del TOE.

Para garantizar los datos que se van a firmar el TOE proporciona un visor seguro, este visor muestra el texto en color negro sobre fondo blanco y únicamente muestra caracteres imprimibles. De esta forma el usuario puede ver el texto que va a firmar in lugar a dudas.

Para que el usuario pueda expresar su voluntad de llevar a cabo la operación, el TOE muestra un Captcha que el usuario debe validar a través de un botón. Una vez que ha validado el Captcha el usuario tiene que aceptar la operación a través de otro botón de la interfaz. De esta forma se garantiza la voluntad expresa de realizar la operación, y se evita la impersonación del firmante.

Mediante un texto que se muestra previa realización de la firma, se notifica al usuario acerca de que sus datos van a ser incorporados en una firma digital. El texto que se le muestra es el siguiente:

"La realización de una firma electrónica implica el tratamiento de los datos de carácter personal contenidos en los certificados, y serán comunicados a todas las entidades con acceso a este documento firmado, ante las que podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición conforme lo estipulado en la Ley Orgánica de Protección de datos."

El TOE verifica de manera no ambigua el texto a firmar. Para comprobar este texto realiza las siguientes operaciones:

- Comprueba que la extensión del archivo es .txt.
- Comprueba que se traba de un archivo de texto.
- Cuenta el número de caracteres que contiene el fichero, y únicamente admite aquellos con un máximo de 5000 caracteres.
- Únicamente permite que contenga caracteres ASCII comprendidos entre los códigos 0x30 y 0x7E ambos excluídos, para llevar a cabo esta comprobación recorre todo el fichero y comprueba uno a uno cada carácter.

Si se detecta cualquier anomalía en el texto a firmar, se notifica al usuario el error encontrado mediante un mensaje.

Para la realización de una firma digital el TOE lleva a cabo los siguientes pasos:

- Mediante un diálogo le solicita al usuario que seleccione el archivo a firmar.
- Una vez seleccionado se le muestra en el visor seguro.
- Tras esto, el usuario tiene que validar el Captcha mostrado mediante un botón. Tras ser validado se activa el botón que le permite expresar su deseo de firma.
- Como se dijo en el paso anterior, una vez validado el Captcha el usuario presiona el botón Aceptar. En esta misma pantalla al usuario se le notifica que sus datos van a ser incorporados a una firma digital.
- En este momento es cuando se carga el certificado de firma del DNI-e, para lo cual el usuario deberá introducir su PIN.
- Una vez seleccionado el certificado se obtiene el Hash SHA-1 del documento y se firma dicho Hash utilizando el DNI-e. Esta firma de realiza en formato PKCS7 y se almacena en un fichero localizado en el mismo directorio que el archivo firmado, pero al que se le añade la extensión .p7s.

Para realizar la verificación de una firma el TOE lleva a cabo los siguientes pasos:

- Mediante un diálogo le solicita al usuario que seleccione el archivo original que desea verificar.

- Una vez seleccionado el fichero a verificar, el TOE busca en el mismo directorio un fichero que tenga el mismo nombre que el fichero a verificar, pero con la extensión .p7s (es decir, si el fichero firmado es *PruebaFirma.txt* buscará un fichero denominado *PruebaFirma.txt.p7s*)
- Una vez hecho lo anterior, el TOE utilizando los servicios criptográficos de Windows XP SP3 comprueba la firma y el certificado que firma, para ello verifica que el Hash SHA-1 se corresponde con el documento firmado.

Editado e impreso por INIXA

Las observaciones a este documento deben dirigirse a :
INIXA | TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN

Torre de Cristal
Pº de la Castellana 259C
28046, Madrid

Tel: 902 875 876
Fax: 984 188 823
e-mail: info@inixa.com