PPSCVA-T1, EAL1. Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 1, con control exclusivo de los interfaces con el firmante y nivel de evaluación de los requisitos de seguridad EAL1.

Índice

Control de versiones

V 1.0 Borrador del PP1 para evaluación.

V 2.0 Cambio de denominación de PP1 a PPSCVA-T1 EAL1.

Índice

Índice

Figuras

Tablas

INTRODUCCIÓN

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-T2 Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 2, agrupa los PP para EAL1 y EAL3.

Términos y abreviaturas

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

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

3 **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.

4 **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).

5 **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).

6 **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).

7 **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.

8 **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).

9 **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).

10 **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).

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

12 **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.

13 **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.

14 **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).

15 **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.

16 **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).

17 **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).

Referencia

18 **Título:** Perfil de Protección para la aplicación de creación y verificación de firma electrónica Tipo 1, con control exclusivo de los interfaces con el firmante y nivel de evaluación de los requisitos de seguridad EAL1

19 **Título corto**: PPSCVA-T1, EAL1

20 **Versión:** v 2.0

21 **Autor:** INTECO

22 **Fecha de publicación:** 18 de diciembre de 2008

Resumen del TOE

Uso del TOE

23 Este Perfil de Protección (PP) especifica los requisitos de seguridad para las aplicaciones de creación y verificación de firma electrónica (SCVA), que se deben usar con el **DNI-e** como dispositivo seguro de creación de firma (SSCD).

24 La SCVA y el SSCD son los "medios que el firmante debe mantener bajo su control exclusivo", tal como requieren la **Directiva** y la **Ley 59/2003** para la consideración de la firma electrónica como avanzada. Utilizando un SSCD, las aplicaciones que cumplan con este Perfil de Protección permiten crear y verificar firmas electrónicas reconocidas.

25 Este PP supone que la SCVA incluye todo el hardware, *firmware* y software necesarios para facilitar la funcionalidad requerida, incluyendo el interfaz con el firmante. Este modelo de aplicación se denomina "SCVA - Tipo 1".

26 La funcionalidad del TOE, 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.

27 La funcionalidad del TOE, 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.

28 En la implementación de la SCVA, algunos fabricantes pueden optar por utilizar una plataforma de propósito general (por ejemplo, un ordenador personal con un sistema operativo de propósito general), y este tipo de implementación se denomina “SCVA - Tipo 2”. En este caso, otro Perfil de Protección detalla los requisitos e hipótesis que se deben exigir a la plataforma de propósito general, de manera que una “SCVA - Tipo 2” pueda evaluarse de manera separada de la plataforma utilizada, véase el PP **PPSCVA-T2**.

Figura 1 - SCVA - Tipo 1

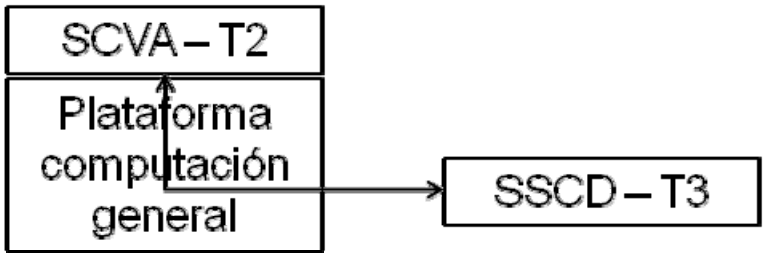


Figura 2 - SCVA - Tipo 2

29 Las comunicaciones entre la "SCVA - Tipo 1" y el **DNI-e** se suponen securizadas por la propia "SCVA - Tipo 1", cumpliendo además con los requisitos exigibles por el Perfil de Protección **CWA 14169** que se aplica al **DNI-e** .

30 Las comunicaciones entre una "SCVA - Tipo 2" y el **DNI-e** requieren de la colaboración del entorno. En esta configuración, es importante la securización de las comunicaciones entre el **DNI-e** y la SCVA, tal como requiere de nuevo el Perfil de Protección **CWA 14169**.

31 La SCVA recibe el SD a través de uno de sus interfaces, y el tipo y número de éstos no se detalla en este PP. La SCVA puede tener interfaces de comunicaciones, por ejemplo una conexión a una red no confiable, o interfaces a dispositivos locales, tales como discos o lectores de tarjetas de memoria. Un interfaz que siempre implementará la SCVA es el interfaz propio al **DNI-e**.

32 La SCVA puede incluir la funcionalidad de creación y edición de los SDs, pero esta funcionalidad no se incluye en este Perfil de Protección, que supone que los SDs se crean externamente, y que las firmas electrónicas, en los SDOs, se exportan para su uso posterior.

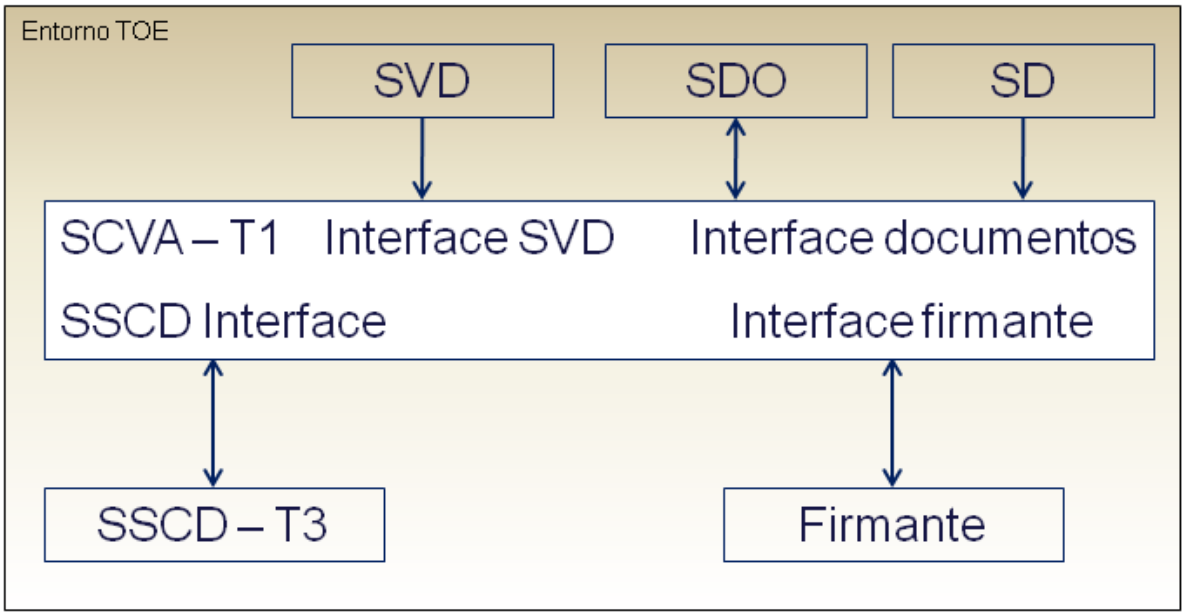


Figura 3 - SCVA - Tipo 1, Interfaces

33 La SCVA necesita mostrar el DTBS al firmante, de tal manera que su contenido no pueda ser malinterpretado, y que no tenga contenido oculto o ambiguo en su representación. Para ello, se requiere que la Declaración de Seguridad de las SCVA que pretendan cumplir con este PP especifiquen los tipos de formato de documento electrónico que son capaces de presentar de manera fiable al firmante, y se detallan ciertos requisitos adicionales a esta presentación.

34 De igual manera, se requiere la voluntad expresa del firmante para que la SCVA solicite una firma al **DNI-e**. Este PP incluye requisitos para el proceso y secuencia de mostrar el DTBS al firmante, y de solicitar y confirmar la voluntad expresa del mismo. Además, la SCVA solicita el VAD al firmante, e inicia y ordena la operación de firma, que realiza en todo caso el **DNI-e**.

35 Este PP no incluye requisitos para controlar el acceso a los SD, ni a los documentos firmados, sino que los aspectos regulados de la SCVA únicamente se refieren a la labor de interfaz entre el firmante y el **DNI-e**, solicitando y transmitiendo el VAD, tal como se requiere para la realización de una firma. Por ello, no se definen tipos de usuarios, o roles, excepto el propio firmante, que no se autentica frente a la SCVA, sino frente al **DNI-e**.

36 Las implementaciones típicas de las “SCVA - Tipo 1” probablemente incluyan medidas de control de acceso para proteger los SDs y SDOs, pero las propiedades y características de seguridad aplicables a esta funcionalidad deberán ser objeto de desarrollo en las correspondientes Declaraciones de Seguridad.

37 La “SCVA - Tipo 1” es también capaz de verificar una firma electrónica. Para ello, se necesita acceso a los SVD correspondientes, que se deben facilitar a la SCVA. La SCVA garantiza que el documento firmado no puede

ser mal interpretado, de manera que este PP impone requisitos sobre la seguridad de los formatos de documento electrónico que la SCVA es capaz de interpretar de manera fiable, e incluye una serie de requisitos a la representación de estos documentos.

Tipo de TOE

38 Una “SCVA - Tipo 1” es una aplicación de creación y verificación de firma electrónica, e incluye todo el hardware, *firmware* y software necesario para crear y verificar una firma electrónica, excluyendo el propio **DNI-e**, que es un elemento de uso obligado para la SCVA.

Hardware y software no incluido en el TOE

39 La “SCVA - Tipo 1” requiere de un **DNI-e** como dispositivo seguro de creación de firma.

40 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).

41 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.

42 El TOE debe contener el interfaz directo con el firmante.

43 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.

DECLARACIONES DE CONFORMIDAD

Conformidad respecto a la norma CC

CC Common Criteria for Information Technology Security Evaluation, v. 3.1, agrupa: CC Parte 1 *release* 1 septiembre de 2006, CC Parte 2 *release* 2 septiembre de 2007 y CC Parte 3 *release* 2 septiembre de 2007.

CEM Common Methodology for Information Technology Security Evaluation, v. 3.1, *release* 2, septiembre 2007.

44 Este Perfil de Protección cumple con lo indicado en la norma **CC** versión 3.1, Parte 1 *release* 1, Parte 2 *release* 2 extendida, y Parte 3 *release* 2 conforme.

Este Perfil de Protección, y las declaraciones de seguridad que declaren su cumplimiento, se deberán evaluar utilizando la metodología de evaluación definida en 2 septiembre de 2007.

45 **CEM** v3.1, *release* 2.

Conformidad respecto a otros PP

46 Este PP no declara el cumplimiento de ningún otro PP. Es conforme al nivel de evaluación EAL1, tal como define **CC** en su parte 3.

Declaraciones de conformidad con respecto a este PP

47 Este PP requiere que la conformidad al mismo se declare de manera **demostrable**, tal como se define en la norma **CC**.

DEFINICIÓN DEL PROBLEMA DE SEGURIDAD

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, el VAD y el SDO.

- **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.

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, 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.DSCVA**.

- **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**.

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**.

OBJETIVOS DE SEGURIDAD

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**.

Objetivos de seguridad para el entorno operacional

- **O.SSCD**;

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

Justificación de los objetivos de seguridad

Objetivos de seguridad del TOE

48 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

49 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.

50 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.

51 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.

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

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

Objetivos del entorno

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

Tabla 2 Correspondencia de los objetivos de seguridad del entorno

	P.SSCD
O.SSCD	X

55 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.

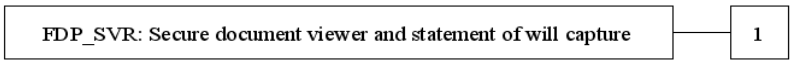
DEFINICIÓN DE COMPONENTES EXTENDIDOS

Secure document viewer and statement of will capture (FDP_SVR)

Family Behaviour

56 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

57 No management activities apply.

Audit

58 No audit requirements apply.

FDP_SVR.1 Secure viewer and SCVA interface

Hierarchical to: No other components

Dependencies: No dependencies.

User application notes

59 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, or for the signature verification process.

FDP_SVR.1.1 The TSF shall provide a secure SD and 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.**

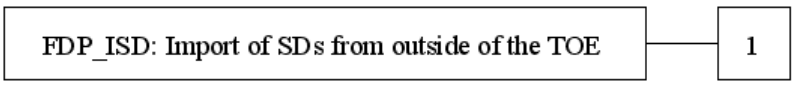
FDP_SVR.1.3 The TSF shall prompt the signatory with a non trivial challenge to capture his/her will to sign, so the signatory cannot trivially be impersonated.

Import of SDs from outside of the TOE (FDP_ISD)

Family Behaviour

60 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

61 No management activities apply.

Audit

62 No audit requirements apply.

FDP_ISD.1 Import of Signer's Document

Hierarchical to: No other components

Dependencies: No dependencies.

User application notes

63 This extended component is used to specify the import of user data as SD or SDO, 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)*]

64 (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.

65 (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.

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: *errores de integridad (a_1)*] on all objects, based on the following attributes: [assignment: *atributos de los datos de usuario (a_2)*].

66 (a_1) el autor de la declaración de seguridad especificará los errores de integridad que detecta la TSF.

67 (a_2) el autor de la declaración de seguridad especificará los atributos, propiedades o condiciones que se utilizan para la monitorización de la 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

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, 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)*]

68 (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.

69 (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.

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: *reglas adicionales de control de la importación (a_1)*].

70 (a_1) el autor de la declaración de seguridad especificará las reglas de importación de los datos de usuario, que se aplicarán en la, política de certificación, SVD, y otros datos de usuario necesarios para la creación o verificación de firmas.

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: *relación de operaciones criptográficas (a_1)*] in accordance with a specified cryptographic algorithm [assignment: *algoritmos criptográficos (a_2)*] and cryptographic key sizes [assignment: *tamaños de clave (a_3)*] that meet the following: [assignment: *relación de normas (a_4)*].

71 (a_1) el autor de la declaración de seguridad especificará las operaciones criptográficas que realiza la SCVA para el proceso de creación de la firma electrónica, sobre los datos de usuario.

72 (a_2) el autor de la declaración de seguridad especificará los algoritmos criptográficos que implementa la SCVA para que el resultado sea la creación de una firma reconocida conforme con las especificaciones del DNI-e.

73 (a_3) el autor de la declaración de seguridad especificará los tamaños de las claves a utilizar, que deben ser apropiados para cada algoritmo y su uso esperado.

74 (a_4) el autor de la declaración de seguridad especificará la relación de normas o estándares que satisface la implementación de los algoritmos criptográficos definidos.

FCS_COP.1_SIGNATURE_VERIFICATION Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *relación de operaciones criptográficas (a_1)*] in accordance with a specified cryptographic algorithm [assignment: *algoritmos criptográficos (a_2)*] and cryptographic key sizes [assignment: *tamaños de clave (a_3)*] that meet the following: [assignment: *relación de normas (a_4)*].

75 (a_1) el autor de la declaración de seguridad especificará las operaciones criptográficas que realiza la SCVA para verificación de la firma electrónica, sobre los datos de usuario.

76 (a_2) el autor de la declaración de seguridad especificará los algoritmos criptográficos que implementa la SCVA.

77 (a_3) el autor de la declaración de seguridad especificará los tamaños de las claves a utilizar, que deben ser apropiados para cada algoritmo y su uso esperado.

78 (a_4) el autor de la declaración de seguridad especificará la relación de normas o estándares que satisface la implementación de los algoritmos criptográficos definidos.

Requisitos de garantía de seguridad

79 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:

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

80 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 3 Correspondencia Requisitos de seguridad vs. Objetivos de seguridad

81 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.

82 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.

83 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.

84 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.

85 **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*.

86 Se aborda el objetivo **O.CRYPTO** mediante los SFRs *FCS_COP.1_SIGNATURE_CREATION_PROCESS Cryptographic operation* y *FCS_COP.1_SIGNATURE_VERIFICATION Cryptographic operatio*n 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.

87 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. Dependencias de los requisitos funcionales de seguridad.

Dependencias de los requisitos funcionales de seguridad

88 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**: 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

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