

GUÍA PARA LA APLICACIÓN DE LOS PERFILES DE PROTECCIÓN EN LA ELABORACIÓN DE APLICACIONES CERTIFICABLES DE CREACIÓN Y VERIFICACIÓN DE FIRMA CON DNIE

**Tipo 2: para ordenadores personales con sistemas
operativos de propósito general**

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format).

Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección [Accesibilidad > Formación > Manuales y Guías](#) de la página <http://www.inteco.es>.

ÍNDICE

1.	INTRODUCCIÓN	7
2.	ACRÓNIMOS Y DEFINICIONES	9
3.	LA NORMA COMMON CRITERIA	12
3.1.	Procedimiento de Certificación	14
3.2.	Metodología de evaluación	15
4.	PERFILES DE PROTECCIÓN PARA APLICACIONES DE FIRMA CON DNIe	17
4.1.	Diferencias entre los dos tipos de perfiles	17
4.2.	Diferencias entre los dos niveles de garantía de seguridad	17
4.3.	Perfil de Protección para aplicaciones de firma Tipo 2	18
5.	PROCESO DE EVALUACIÓN	20
6.	CERTIFICACIÓN DE APLICACIONES SCVA TIPO 2	22
6.1.	Evidencias de garantía requeridas en la certificación EAL1	22
6.1.1.	Declaración de seguridad	23
6.1.1.1.	<i>Introducción a la Declaración de Seguridad</i>	24
6.1.1.2.	<i>Declaración de conformidad</i>	25
6.1.1.3.	<i>Definición de componentes extendidos</i>	27
6.1.1.4.	<i>Objetivos de seguridad del entorno operacional</i>	28
6.1.1.5.	<i>Requisitos de seguridad declarados</i>	29
6.1.1.6.	<i>Resumen de la especificación del TOE</i>	31
6.1.2.	Documentos de guía	31
6.1.2.1.	<i>Guía operativa</i>	32
6.1.2.2.	<i>Guía preparativa</i>	33
6.1.3.	Desarrollo	34
6.1.3.1.	<i>Especificación funcional básica</i>	35
6.1.4.	Soporte al ciclo de vida	37
6.1.4.1.	<i>Etiquetado</i>	38
6.1.4.2.	<i>Gestión de la Configuración</i>	39
6.1.5.	Pruebas	39
6.1.5.1.	<i>Pruebas independientes - conformidad</i>	40
6.1.6.	Análisis de vulnerabilidades	41
6.1.6.1.	<i>Test de vulnerabilidades</i>	41

6.2.	Evidencias de garantía requeridas en la certificación EAL3	43
6.2.1.	Declaración de seguridad	44
6.2.1.1.	<i>Introducción de la Declaración de Seguridad</i>	44
6.2.1.2.	<i>Declaración de conformidad</i>	46
6.2.1.3.	<i>Definición del problema de seguridad</i>	47
6.2.1.4.	<i>Objetivos de Seguridad</i>	48
6.2.1.5.	<i>Definición de componentes extendidos</i>	49
6.2.1.6.	<i>Requisitos de seguridad derivados</i>	50
6.2.1.7.	<i>Resumen de especificación del TOE</i>	52
6.2.2.	Documentos de guía	53
6.2.2.1.	<i>Guía operativa</i>	54
6.2.3.	Guía preparativa	56
6.2.4.	Desarrollo	56
6.2.4.1.	<i>Descripción de la arquitectura de seguridad</i>	57
6.2.4.2.	<i>Especificación funcional con resumen completo</i>	60
6.2.4.3.	<i>Documentos de diseño</i>	62
6.2.5.	Soporte al ciclo de vida	63
6.2.5.1.	<i>Documentación y sistemas de Gestión de la Configuración</i>	64
6.2.5.2.	<i>Gestión de la configuración: implementación</i>	66
6.2.5.3.	<i>Procedimientos de suministro</i>	67
6.2.5.4.	<i>Medidas de seguridad</i>	68
6.2.6.	Pruebas	69
6.2.6.1.	<i>Análisis de cobertura de los test</i>	70
6.2.6.2.	<i>Test: diseño básico</i>	71
6.2.6.3.	<i>Test de funcionalidad</i>	71
6.2.6.4.	<i>Muestra para test independientes</i>	73
6.2.7.	Análisis de vulnerabilidades	73
6.2.7.1.	<i>Análisis de vulnerabilidades</i>	74
7.	REQUISITOS DE SEGURIDAD FUNCIONAL	75
7.1.	FTP_SDI	75
7.1.1.	Transcripción del componente	75
7.1.2.	Descripción del componente	75
7.1.3.	Ejemplos de instanciación	76
7.1.4.	Ejemplos de implantación	76
7.1.5.	Recomendaciones de seguridad	77
7.2.	FTP_ITC.1.UD	78

7.2.1.	Transcripción del componente	78
7.2.2.	Descripción del componente	78
7.2.3.	Ejemplo de instanciación del requisito	79
7.2.4.	Ejemplo de implementación	79
7.2.5.	Recomendación de seguridad	83
7.3.	FTP_ITC.1.VAD	85
7.3.1.	Transcripción del componente	85
7.3.2.	Descripción del componente	85
7.3.3.	Ejemplo de instanciación del requisito	86
7.3.4.	Ejemplo de implementación	86
7.3.5.	Recomendación de seguridad	91
7.4.	FDP_RIP.1	92
7.4.1.	Transcripción del componente	92
7.4.2.	Descripción del componente	92
7.4.3.	Ejemplo de instanciación del requisito	92
7.4.4.	Ejemplo de implementación	92
7.4.5.	Recomendación de seguridad	93
7.5.	FPT_TST.1	94
7.5.1.	Transcripción del componente	94
7.5.2.	Descripción del componente	94
7.5.3.	Ejemplo de instanciación del requisito	94
7.5.4.	Ejemplo de implementación	95
7.5.5.	Recomendación de seguridad	96
7.6.	FDP_SVR.1	97
7.6.1.	Transcripción del componente	97
7.6.2.	Explicación del conceptual del requisito	97
7.6.3.	Ejemplo de instanciación del requisito	98
7.6.4.	Ejemplos de implementación de FDP_SVR.1.1	98
7.6.5.	Recomendación de seguridad	98
7.7.	FDP_ISD.1	99
7.7.1.	Transcripción del componente	99
7.7.2.	Explicación del conceptual del requisito	99
7.7.3.	Ejemplo de instanciación del requisito	99
7.7.4.	Ejemplo de implementación	100
7.7.5.	Recomendación de seguridad	100
7.8.	FDP_ITC.1	101

7.8.1.	Transcripción del componente	101
7.8.2.	Explicación conceptual del requisito	101
7.8.3.	Ejemplo de instanciación del requisito	101
7.8.4.	Ejemplo de implementación	102
7.8.5.	Recomendación de seguridad	102
7.9.	FCS_COP.1_SIGNATURE_CREATION_PROCESS	103
7.9.1.	Transcripción del componente	103
7.9.2.	Explicación del conceptual del requisito	103
7.9.3.	Ejemplo de instanciación del requisito	103
7.9.4.	Ejemplo de implementación	104
7.9.5.	Recomendación de seguridad	104
7.10.	FCS_COP.1_SIGNATURE_VERIFICATION	105
7.10.1.	Transcripción del componente	105
7.10.2.	Explicación del conceptual del requisito	105
7.10.3.	Ejemplo de instanciación del requisito	105
7.10.4.	Ejemplo de implementación	105
7.10.5.	Recomendación de seguridad	106
8.	REFERENCIAS	107

1. INTRODUCCIÓN

El propósito de este documento «Guía para la aplicación de los Perfiles de Protección en la elaboración de aplicaciones certificables de creación y verificación de firma con DNle, Tipo 2» es el de servir de referencia útil y detallada para facilitar la elaboración y posterior certificación de aplicaciones de creación y verificación de firma electrónica usando el DNle como dispositivo seguro de creación de firma, conforme a los Perfiles de Protección elaborados de acuerdo a la norma Common Criteria versión 3.1 release 2.

Para la elaboración de esta guía INTECO ha contado con la colaboración de un socio tecnológico especializado. Esta guía se elabora en el marco del Plan Avanza, financiada por la Secretaría de Estado para Telecomunicaciones y para la Sociedad de la Información (SETSI).

Este documento aporta información para facilitar la comprensión de la norma Common Criteria y la redacción de los documentos necesarios para solicitar la certificación; además determina los requisitos que han de satisfacerse en el proceso de desarrollo y los requisitos funcionales de seguridad que han de cumplir las aplicaciones de generación y verificación de firma electrónica que utilicen el DNle como dispositivo seguro de creación de firma. El contenido de la guía de implantación es:

- Introducción a la norma Common Criteria. Describe los conceptos claves de la norma Common Criteria y los recursos de los que dispone el desarrollador para conseguir la certificación de su producto. Incluye un apartado donde se indica dónde puede informarse el desarrollador sobre el procedimiento para certificar un producto conforme a la norma Common Criteria.
- Los Perfiles de Protección según Common Criteria. Indica de forma general su contenido y las diferencias entre los perfiles elaborados.
- Los Perfiles de Protección Tipo 2, describe el perfil de protección para aplicación de creación y verificación de firma electrónica Tipo 2.
- Evidencias de garantía requeridas en la certificación. Describe los entregables que deben ser proporcionados por el desarrollador para una certificación Common Criteria.
- Requisitos de seguridad funcional para la elaboración de un producto que cumpla con los Perfiles Tipo 2. Describe los requisitos funcionales y de garantía de seguridad para las aplicaciones de generación y verificación de firma electrónica Tipo 2.
- Referencias, describe documentación extra usada en la guía.

AVISO: todas las cuestiones relativas a la tecnología del DNle así como el procedimiento operativo a seguir para la petición y obtención del la guía de comandos y las claves para establecer el canal seguro con el DNle estarán disponibles en el Portal Oficial sobre el DNle <http://www.dnielectronico.es> del Cuerpo Nacional de Policía (DGP).

2. ACRÓNIMOS Y DEFINICIONES

Atributos de firma: es aquella información adicional que se firma junto con el documento a firmar del usuario.

CC (*Common Criteria for Information Technology Security Evaluation*): Criterios Comunes para la evaluación de la seguridad de las tecnologías de la información.

CEM (*Common Evaluation Methodology*): metodología común de evaluación.

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.

Conformidad demostrable: permite al autor de un PP describir un problema de seguridad común para ser resuelto y proporcionar unas guías genéricas para establecer los requerimientos necesarios para su resolución, sabiendo que puede haber más de una manera de especificarla. También es apropiada para un TOE donde existan, o puedan existir, un gran número de PP's, por lo que permite al autor del ST conformarlo con todos esos PP's de forma simultánea, ahorrando así trabajo.

Consistente: describe una relación entre dos o más entidades, indicando que no hay aparentemente contradicciones entre esas entidades.

CSP (*Certification Service Provider*): entidad legal o persona física que entrega certificados o proporciona otros servicios relativos a firma electrónica, definidos en el artículo 2.11 de la Directiva.

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, también referida como «Directiva».

DNle: Documento Nacional de Identidad, versión electrónica.

DTBS (*Data To Be Signed*): son los datos electrónicos completos (véase SD) que hay que firmar (incluyendo tanto los atributos del documento o datos a firmar, del usuario, como los de la firma).

DTBSR (*Data To Be Signed Representation*): son los datos enviados por la aplicación de creación de firma al SSCD para ser firmados y son:

- un valor matemático (*hash*) de los datos a ser firmados (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).

Enforcing: característica de una interfaz de hacer cumplir una propiedad o actividad.

Firma electrónica avanzada: firma electrónica que está vinculada al firmante de manera única, permite la identificación de éste, ha sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control y está vinculada a los datos a que se refiere, de modo que cualquier cambio ulterior de los mismos es detectable.

Firma electrónica reconocida: es una firma electrónica avanzada basada en un certificado reconocido y que ha sido creada por un SSCD.

Interfaz: medio por el cuál se interacciona con un componente o un módulo de la aplicación o producto.

Non-interfering: característica de una interfaz de no intervenir ni interferir en la aplicación de una propiedad o actividad.

Patrocinador: responsable de la petición de certificación y dar soporte en la evaluación. Esta figura puede ser desempeñada por el desarrollador o por una tercera parte.

PP (*Protection Profile*): perfil de protección. Es un documento formal que expresa un conjunto de requisitos de seguridad de un producto TI —independientemente de su implementación—, tanto de funcionamiento como de garantía, para cumplir con las necesidades específicas de los clientes.

SAR (*Security Assurance Requirement*): requisito de garantía de seguridad. Definen los criterios para evaluar los PP, ST y TOE, y las responsabilidades y actividades de garantía de seguridad para los desarrolladores y evaluadores. La parte 3 de CC es un catálogo jerárquico de SARs. La descripción de las unidades de la jerarquía es similar a la de los requisitos funcionales (SFR).

SCD (*Signature Creation Data*): datos de creación de firma.

SCVA (*Signature Creation and Verification Application*): aplicación de creación y verificación de firma electrónica. Los medios utilizados para la creación y verificación de firma electrónica, sin incluir el SSCD.

SD (*Signed Data*): el documento que el firmante pretende firmar electrónicamente.

SFR (*Security Functional Requirement*): requisito funcional de seguridad. Son exigencias a las funciones del TOE que aportan seguridad y cuyo comportamiento es observable. Los SFR tienen distintos propósitos:

- describir el comportamiento de seguridad esperado de un TOE,

- alcanzar los objetivos de seguridad marcados en el PP o en el ST,
- especificar las propiedades de seguridad que los usuarios pueden detectar por interacción directa o como respuesta a un estímulo,
- contrarrestar las amenazas en el entorno de operación del TOE, y
- cumplimentar las políticas y actitudes de seguridad identificadas por la organización.

En la parte 2 de la norma CC se organizan los SFR en una estructura jerárquica con: clases, familias, componentes y elementos.

SSCD (*Secure Signature Creation Device*): dispositivo seguro de creación de firma. Es el software o hardware configurado para aplicar los SCD y que cumple los requisitos establecidos en el anexo III de la Directiva.

ST (*Security Target*): declaración de seguridad. Es una respuesta de los desarrolladores a un PP —dependiente de la implementación— que se utiliza como base para el desarrollo del producto. El ST proporciona un diseño que incorpora los mecanismos, funciones y características para cumplir los requisitos del PP.

Supporting: característica de una interfaz de dar soporte a una propiedad o actividad para que pueda ser realizada correctamente.

SVD (*Signature Verification Data*): son los datos, como códigos o claves criptográficas públicas, que se utilizan para de verificar una firma electrónica.

TOE (*Target Of Evaluation*): un conjunto de software, *firmware* o hardware que se va a evaluar, acompañado de las guías de uso. Es un producto, sistema o red TI y su documentación asociada, que es el objeto de la evaluación. Es la implementación física del ST.

TSFI (*TOE Security Functionality Interface*): interfaz de la funcionalidad de seguridad, el medio por el cual las entidades externas proporcionan/reciben datos e invocan servicios.

VAD (*Verification Authentication Data*): 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.

3. LA NORMA COMMON CRITERIA

La norma Common Criteria¹ proporciona un marco estandarizado (metodología, notación y sintaxis) para especificar y verificar los requisitos funcionales de seguridad que debe cumplir un producto o sistema IT y las medidas de garantía aplicadas sobre los mismos, en sus diferentes fases de vida.

CC consiste en un marco normativo, aprobado como estándar internacional por ISO en 1999, para la evaluación de la seguridad con el siguiente cometido:

- que los usuarios puedan especificar sus necesidades,
- que los fabricantes e integradores puedan implementar y declarar los atributos de seguridad de sus productos y
- que los laboratorios puedan evaluar los productos y determinar si realmente tienen los atributos que declaran.

CC aporta la garantía de que el proceso de especificación, implementación y evaluación de productos de seguridad informática se ha realizado de una forma rigurosa y estandarizada.

La norma Common Criteria está dividida en tres partes:

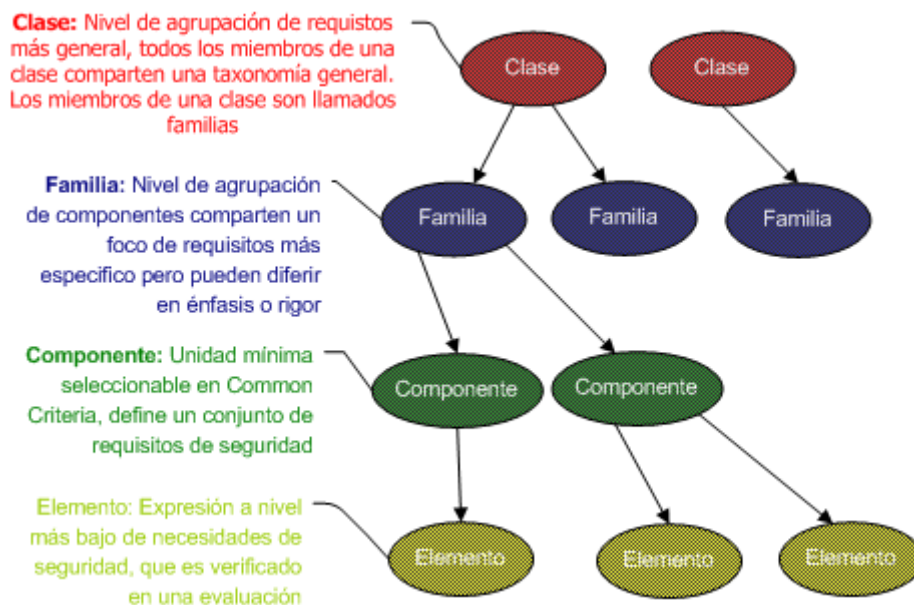
- 1) Introducción y modelo general. Define los conceptos y los principios generales de la evaluación de seguridad IT y proporciona un modelo de evaluación.
- 2) Componentes funcionales de seguridad. Establece el catálogo de requisitos funcionales de seguridad que sirven de plantillas para definir las funcionalidades de seguridad de un producto.
- 3) Componentes de garantía de seguridad. Establece el catálogo de requisitos de garantía de seguridad que debe cumplir la documentación, el producto a evaluar, el entorno de desarrollo y otras partes implicadas en la seguridad del producto. La parte 3 de Common Criteria también define el criterio de evaluación de los Perfiles de protección (PP), declaraciones de seguridad (ST) y otras evidencias de evaluación. También presenta siete paquetes de garantía predefinidos, los cuales son llamados niveles de garantía de evaluación (EALs).

¹ <http://www.commoncriteriaportal.org>

Common Criteria organiza los catálogos de requisitos de forma jerárquica, definiendo niveles jerárquicos de clase, familia y componente:

- **Clase funcional** es una agrupación de requisitos de seguridad que comparten un objetivo común. Las clases funcionales son agrupaciones de familias. A cada clase funcional se le asigna un nombre y una sigla de tres letras que comienza por «T».
- Las clases funcionales están divididas en **familias funcionales**. Éstas son agrupaciones de requisitos funcionales que comparten objetivos de seguridad pero que pueden diferir en el énfasis o rigor que les aplica; sus miembros son los componentes. También se les denomina con unas siglas de tres letras que se añaden a la sigla de la clase a la que pertenecen. Ej.: FCS_CKM.

Figura 1: Estructura modular de requisitos de seguridad



- Las familias funcionales están divididas en **componentes**. Éstos son los conjuntos de requisitos de seguridad específicos, se construyen a partir de los elementos; son las unidades más pequeñas que pueden seleccionarse para formar un PP, un ST o un paquete. Los componentes tienen un nombre y se identifican con un número que se añade a la familia a la que pertenecen. Existen relaciones jerárquicas entre componentes de una misma familia. Ej.: FCS_CKM.1
- Los componentes contienen **elementos**. Éstos se describen con un número único que se añade a la descripción del componente al que pertenecen

(Ej.:FCS_CKM.1.1). Son los bloques con los que se construyen los requisitos funcionales del PP.

Los requisitos funcionales de seguridad se describen en la parte 2 de la norma Common Criteria version 3.1 release 2.

Los requisitos de garantía de seguridad se describen en la parte 3 de la norma Common Criteria version 3.1 release 2.

La certificación Common Criteria se basa en un proceso de evaluación independiente para verificar la confianza que se puede depositar en la declaración de cumplimiento de las funcionalidades de seguridad y las medidas de garantía aplicables en un producto IT.

El proceso de evaluación proporciona a los potenciales consumidores mecanismos para determinar si estos productos IT satisfacen sus necesidades de seguridad.

Para asegurar la comparabilidad de los resultados, el proceso de evaluación ha de ser realizado dentro de un marco de trabajo de un «esquema de evaluación», en nuestro caso el Organismo de Certificación articulado en el ámbito de actuación del Centro Criptológico Nacional.

La consistencia entre los marcos de trabajo reguladores de los distintos esquemas de evaluación se basa en:

- 4) Estar alineados mediante CCRAs (*Common Criteria Recognition Arrangement*); que permiten el reconocimiento internacional mutuo de los productos certificados bajo la norma Common Criteria siguiendo las condiciones descritas en <http://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf>.
- 5) Usar una metodología común para evaluar los productos o sistemas IT descrita en el CEM versión 3.1 revisión 2.

3.1. PROCEDIMIENTO DE CERTIFICACIÓN

El procedimiento operativo para la actividad de certificación de producto respecto a la norma Common Criteria se describe en la Orden PRE/2740/2007, de 19 de septiembre, que aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Adicionalmente, dispone la naturaleza y establecimiento de la contraprestación exigida por las acreditaciones y certificaciones, conforme a lo siguiente:

- Al amparo de lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, los ingresos procedentes de las acreditaciones de laboratorios y de las certificaciones de productos, tienen la naturaleza de tasas.

- Según lo establecido en el artículo 2.3 del Real Decreto 1287/2005, de 28 de octubre, por el que se modifica el Real Decreto 593/2002, de 28 de junio, que desarrolla el régimen económico presupuestario del Centro Nacional de Inteligencia, el establecimiento o modificación de la cuantía de los ingresos que tengan la naturaleza de tasas, así como la fijación de los diversos elementos de la correspondiente relación jurídico-tributaria, se harán con arreglo a lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos.

Para iniciar el proceso de evaluación, el patrocinador presentará al Organismo de Certificación una Solicitud de Evaluación debidamente cumplimentada, a la que se le deberá adjuntar:

- Declaración responsable de conocer y aceptar los términos y requisitos de la certificación solicitada.
- Declaración de Seguridad / Perfil de Protección.
- Justificante de pago de los precios públicos de certificación.
- Identificación del producto a evaluar.

Información: a fecha de publicación de esta guía no existen tasas aplicables a este proceso de certificación, por lo que el patrocinador no deberá presentar un Justificante de pago de los precios públicos de certificación. Si en algún momento fuera necesario el pago de dichas tasas, será el Organismo de Certificación el que determine su importe, haciendo público los precios en el Boletín Oficial del Estado.

El proceso de evaluación se realizará siguiendo lo establecido en el apartado «Proceso de Evaluación» y durante esta fase el patrocinador proporcionará las evidencias requeridas para la evaluación descritas en el apartado «Evidencias de garantía requeridas en la certificación EAL1» o en «Evidencias de garantía requeridas en la certificación EAL3», en función del nivel de evaluación solicitado.

Para más detalle, en el sitio web del CCN, <http://www.oc.ccn.cni.es>, apartado de documentos internos, se describen los procedimientos operativos que regulan la actividad de evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

3.2. METODOLOGÍA DE EVALUACIÓN

El proceso de certificación incluye la evaluación por un laboratorio acreditado del producto a certificar. El procedimiento para esta evaluación se describe en el apartado 7.

La metodología CEM estandariza las actividades, subactividades, acciones y unidades de trabajo para garantizar la seguridad.

Según la metodología, el evaluador debe contrastar el ST especificado por el proveedor o el cliente con el TOE.

Se recurre a los requisitos de garantía de seguridad (SAR) para asegurarse de que todos los requisitos funcionales de seguridad (SFR) del TOE, del entorno TI y externos cumplen que:

- están implementados,
- están implementados correctamente, y
- son suficientemente robustos y resistentes para contrarrestar las amenazas identificadas.

4. PERFILES DE PROTECCIÓN PARA APLICACIONES DE FIRMA CON DNIE

Los perfiles de protección son requisitos de seguridad, conforme al estándar CC, que han de contemplarse y cumplirse por las Aplicaciones de Creación y Verificación de firma con DNIE que quieran certificarse. Los requisitos que incluyen estos documentos adoptan también los criterios de la legislación nacional al efecto y la normativa y legislación europeas.

En INTECO, se han elaborado cuatro PP para aplicaciones de creación y verificación de firma con DNIE. Estos perfiles corresponden a dos tipos (Tipo 1 y Tipo 2) dependiendo de las características de la plataforma sobre la que se utilicen las aplicaciones que se generen. A su vez, para cada tipo se elaboran dos perfiles cada uno con un nivel de garantía de seguridad, EAL1 y EAL3.

Tabla 1: PP elaborados: tipos y niveles de evaluación

Tipo / Nivel garantía	EAL1	EAL3
Tipo 1	PPSCVA-T1-EAL1	PPSCVA-T1-EAL3
Tipo 2	PPSCVA-T2-EAL1	PPSCVA-T2-EAL3

4.1. DIFERENCIAS ENTRE LOS DOS TIPOS DE PERFILES

Los PP's sirven para definir el entorno y los requisitos de seguridad que son relevantes para los usuarios de un producto utilizado con un propósito particular. Se elaboraron dos tipos de perfiles:

- 1) Tipo 1: han de servir para certificar aplicaciones para plataformas con control exclusivo de los interfaces con el firmante como TDT, dispositivos portátiles tipo PDA o teléfonos móviles.
- 2) Tipo 2: han de servir para certificar aplicaciones para ordenadores personales con sistemas operativos de propósito general.

Los dos Tipos de perfiles comparten la funcionalidad, por lo que se puede decir que se trata de la misma aplicación sobre dos tipos de plataformas.

4.2. DIFERENCIAS ENTRE LOS DOS NIVELES DE GARANTÍA DE SEGURIDAD

Según CC, los niveles de garantía de seguridad o EAL (*Evaluation Assurance Level*) son indicativos de la profundidad y rigor necesarios en la evaluación. CC define siete niveles de garantía. Los niveles que se utilizan en estos perfiles son EAL1 y EAL3.

- 1) EAL 1: «probado funcionalmente». El análisis de las funciones de seguridad se realiza usando las especificaciones funcionales y el interfaz de la aplicación, para comprender el comportamiento de seguridad. El análisis se basa en pruebas independientes. Se aplica cuando se necesita cierta confianza sobre el correcto funcionamiento del TOE. Incluye evaluación del TOE tal y como se entrega al cliente, pruebas independientes contra una especificación y un examen de la documentación de guía suministrada. La evaluación de este nivel debe aportar la evidencia de que el TOE funciona de forma consistente con su documentación, y que ofrece una protección útil contra las amenazas identificadas.
- 2) EAL 3: «chequeado y probado con metodología». El análisis consiste en pruebas de «caja gris», confirmación independiente del resultado de las pruebas de desarrollo, búsqueda de vulnerabilidades obvias, control del entorno de desarrollo y gestión de la configuración de la aplicación. Se aplica en aquellas circunstancias en las que los proveedores o los usuarios precisan un nivel moderado de seguridad garantizada independiente, es necesario realizar una investigación profunda del TOE y su desarrollo pero no requiere reingeniería. Permite al proveedor minucioso obtener la máxima garantía de seguridad en fase de diseño sin alterar substancialmente las prácticas de desarrollo existentes.

En cuanto a los PP la diferencia fundamental entre los dos niveles de garantía de seguridad estriba en los requisitos de garantía, siendo en EAL3 mucho más numerosos que en EAL1 lo que supone un mayor nivel de profundidad en las pruebas relacionadas con el diseño.

4.3. PERFIL DE PROTECCIÓN PARA APLICACIONES DE FIRMA TIPO 2

Este Perfil de Protección (PP) especifica los requisitos de seguridad para las aplicaciones de creación y verificación de firma electrónica (SCVA) que utilizan el DNle como dispositivo seguro de creación de firma (SSCD) sobre una plataforma de propósito general confiable.

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 que la firma electrónica realizada sea considerada. Utilizando el DNle como SSCD, las aplicaciones que cumplan con este Perfil de Protección permitirán crear y verificar firmas electrónicas reconocidas.

Este PP supone que la SCVA no incluye todo el hardware, *firmware* y software necesarios para facilitar la funcionalidad de SCVA, sino que la SCVA utiliza una plataforma de propósito general confiable (por ejemplo, un ordenador personal con un sistema operativo de propósito general), incluyendo el necesario interfaz al firmante.

Este modelo de aplicación se denomina «SCVA - Tipo 2».

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 para 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 se 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.

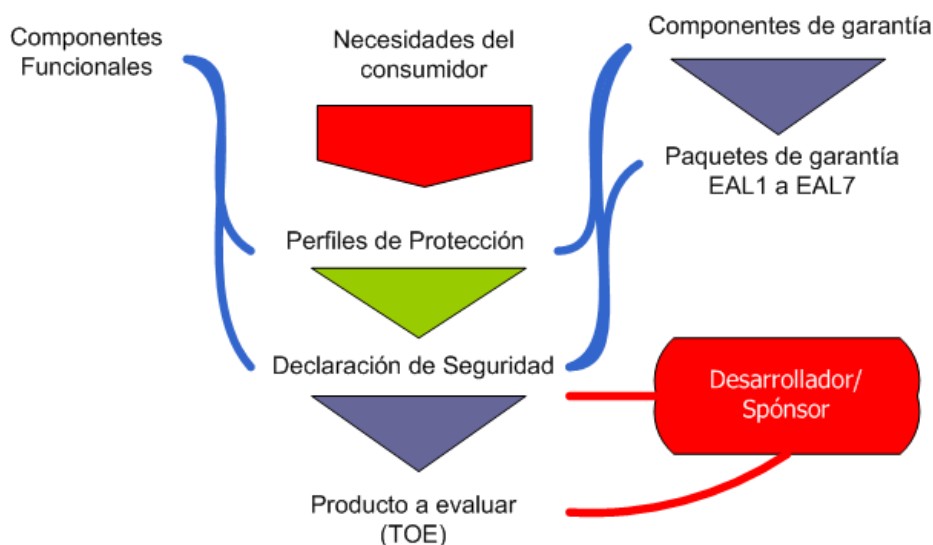
La funcionalidad del TOE, para la verificación de firma electrónica, incluye:

- 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 haya podido realizarse, e identificará las firmas que no han podido verificarse.

5. PROCESO DE EVALUACIÓN

El siguiente gráfico es un esquema del funcionamiento de una evaluación Common Criteria:

Figura 2: Entes en el proceso de evaluación



La evaluación se realizará sobre un producto o sistema IT conforme a una Declaración de Seguridad, o ST (de sus siglas en inglés *Security Target*), que establece un conjunto de requisitos y funcionalidades de seguridad. Este documento, la ST, debe incluir la conformidad con uno de los PP y además establecer un nivel de garantía de evaluación.

Cada nivel de garantía de evaluación establece como será evaluado un producto o sistema IT, indicando:

- 1) Las evidencias que el desarrollador debe presentar para la evaluación según se muestra en la figura 3.
- 2) El método que el evaluador utilizará para verificar cada uno de los componentes descritos en el nivel de garantía de evaluación, gracias a la metodología de evaluación CEM v3.1 release 2.

En el apartado siguiente se explica cómo una ST debe incluir la conformidad con un PP.

Figura 3: Grupos de evidencias en el proceso de evaluación



6. CERTIFICACIÓN DE APLICACIONES SCVA TIPO 2

El PP establece un conjunto de objetivos y requisitos de seguridad que debe cumplir la SCVA, es decir la aplicación de creación y verificación de firma electrónica, que según la definición del PP Tipo 2 no incluye todo el hardware, *firmware* y software necesarios para facilitar la funcionalidad de SCVA, sino que la SCVA utiliza una plataforma de propósito general confiable (por ejemplo, un ordenador personal con un sistema operativo de propósito general), incluyendo el necesario interfaz al firmante.

En el apartado de declaración de conformidad, el autor de la Declaración de Seguridad tiene que demostrar una conformidad demostrable con alguno de los Perfiles de Protección de Tipo 2, el PPSCVA-T2, EAL1 o el PPSCVA-T2, EAL3 según el nivel de garantía de seguridad del certificado que se desea obtener (EAL1 o EAL3).

Se establecen dos paquetes de garantía de evaluación para la SCVA:

- EAL1 (probado funcionalmente), es aplicable cuando se requiera cierta confianza del correcto funcionamiento, pero las amenazas a la seguridad no son vistas como algo serio.
- EAL3 (chequeado y probado con metodología), permite a un desarrollador concienciado obtener las máximas garantías al introducir procesos de ingeniería de seguridad en la fase de desarrollo sin alterar sustancialmente sus prácticas de desarrollo.

Para el cumplimiento de estos paquetes de garantía, los ST deben demostrar la conformidad con los PP 3 y 4, respectivamente.

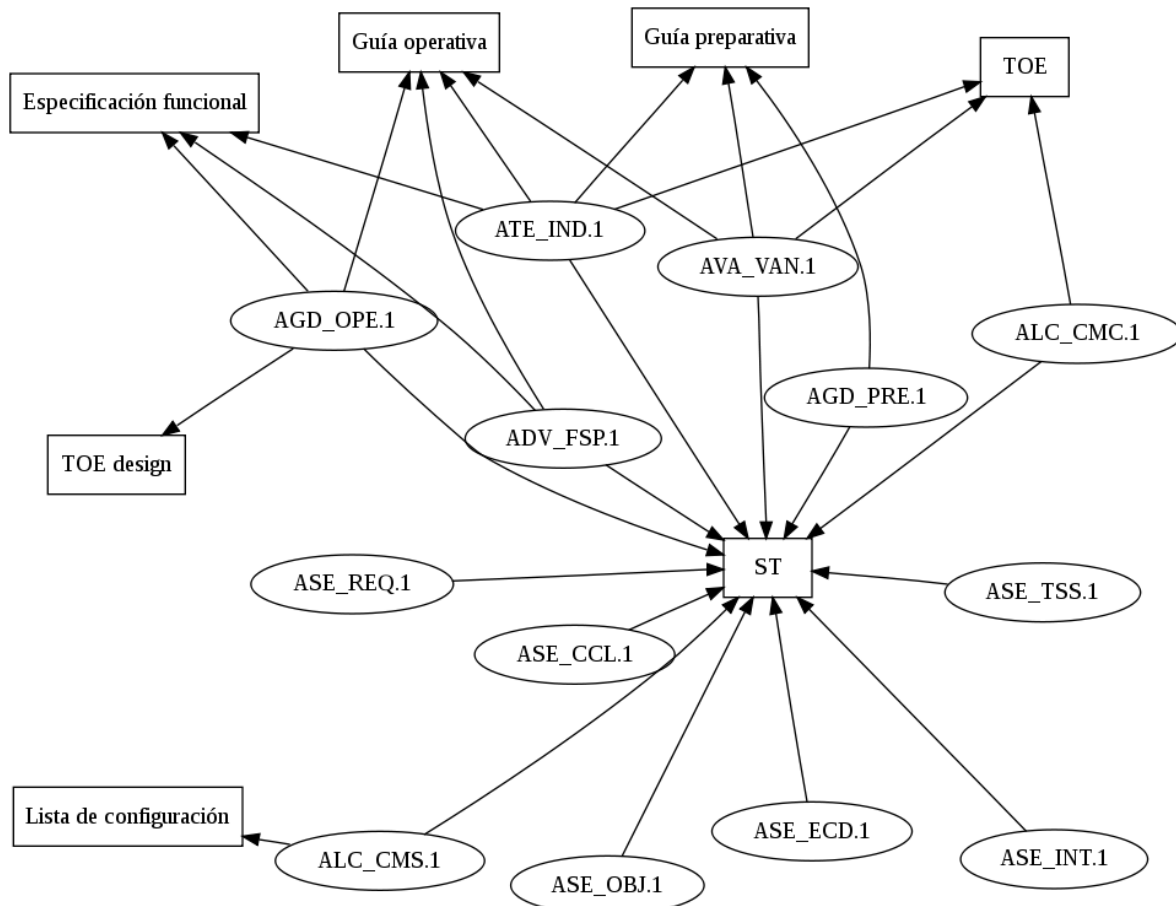
6.1. EVIDENCIAS DE GARANTÍA REQUERIDAS EN LA CERTIFICACIÓN EAL1

El siguiente gráfico muestra las evidencias de garantía requeridas en la certificación EAL 1 y los requisitos que tratan sobre ellas.

En la norma CC se define un campo *Input*, para cada componente de seguridad de garantía, que describe que evidencias a entregar para dar evidencias de cumplimiento.

Estas evidencias son: Declaración de Seguridad (ST), Especificación funcional, Guía operativa, Guía preparativa, TOE (objeto de evaluación, es decir la propia aplicación), Diseño del TOE y Lista de configuración.

Figura 4: Evidencias de garantía requeridas en la certificación EAL1



6.1.1. Declaración de seguridad

La Declaración de Seguridad es un documento completo y riguroso que define el producto a evaluar en base a los siguientes elementos: descripción, amenazas, hipótesis, objetivos de seguridad, requisitos funcionales y de garantía de seguridad y funcionalidades de seguridad.

Constituye uno de los grupos de evidencias en el proceso de evaluación.

Figura 5: Declaración de seguridad



A continuación se presentan las actividades que según la norma se exigen al desarrollador y el contenido que debe presentar:

6.1.1.1. Introducción a la Declaración de Seguridad

ASE_INT.1 ST Introduction

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

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

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

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

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

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

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

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

Guía de cumplimiento

La primera parte de la Declaración de Seguridad es la introducción. Esta debe contener los siguientes datos:

- referencia de la ST, de forma unívoca
- referencia del TOE, de forma unívoca
- resumen del TOE
- descripción del TOE
- resumen del TOE

El propósito del resumen del TOE es proporcionar suficiente información para que una persona que pueda estar interesada sepa que hace el producto a grandes rasgos:

- uso y las principales funcionalidades de seguridad del TOE
- tipo de TOE (en este caso, el tipo de TOE según el PP será Tipo 2)
- *firmware*, software, y hardware necesario para el funcionamiento del TOE

La descripción del TOE debe cubrir todos los aspectos del TOE incluidos en su resumen y abordarlos con mayor profundidad. Ha de estar redactada en forma narrativa y no debe adentrarse demasiado en los detalles técnicos. Además, tiene que describir el alcance físico y lógico del TOE, que en los TOEs de Tipo 2 estarán delimitados por el propio producto.

6.1.1.2. Declaración de conformidad

ASE_CCL.1 Conformance claims

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

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

Elementos del contenido y de presentación

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 ASE_CCL.1.2C 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 rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.*

ASE_CCL.1.7C *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.*

Guía de cumplimiento

Otro apartado indispensable de la Declaración de Seguridad es la declaración de conformidad. En ella se ha de expresar la conformidad del desarrollo con el Perfil de Protección que ha servido de referencia para el desarrollo y servirá igualmente de referencia para la evaluación.

El PP establece que la conformidad debe de ser **demostrable**, es decir: la Declaración de Seguridad (ST) puede contener secciones o partes distintas a las presentadas en el Perfil de Protección, si bien, para demostrar la conformidad, el autor de la Declaración de Seguridad debe proporcionar una justificación de porqué la Declaración de Seguridad es equivalente o más restrictiva al PP.

Algunos requisitos que debe cumplir esta declaración son:

- se ha de especificar cual es el tipo de TOE según el PP elegido (en este caso será Tipo 2)

- se especificará un paquete de garantía (EAL) mínimo según el PP usado
- la definición del problema de seguridad debe ser consistente con la especificada en el PP
- los objetivos de seguridad presentados en la ST han de ser consistentes con los presentes en el PP
- los requisitos de seguridad presentados en la ST han de ser consistentes con los presentes en el PP

Esto implica que los SFRs declarados en la ST deben ser al menos tan restrictivos como los declarados en el PP.

Recomendación de seguridad: una Declaración de Seguridad es equivalente o más restrictiva que un Perfil de Protección si:

- todos los producto a evaluar que satisfacen la PP, también satisfacen la ST
- todos los entornos operacionales que satisfacen la ST, también satisfacen el PP

Informalmente, la Declaración de Seguridad presenta las mismas o más restricciones para el TOE y presenta igual o menos restricciones para el entorno operacional.

6.1.1.3. Definición de componentes extendidos

ASE_ECD.1 Extended components definition

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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.*

Elementos del contenido y de presentación

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.*

Guía de cumplimiento

Estos elementos obligan al redactor de la Declaración de Seguridad a identificar los requisitos que no son extraídos de CC parte 2 y parte 3.

En este caso el PP tiene dos requisitos funcionales que no forman parte de CC parte 2 (FDP_SVR.1 y FDP_ISD.1), ya identificados en el PP. Haciendo una declaración de conformidad demostrable con el PP, según el apartado anterior, la identificación de los requisitos extendidos ya queda identificada.

En caso de querer añadir otros componentes, se aplicará lo que especifica la norma CC, tal y como establece los elementos de contenido y presentación de ASE_ECD.1.1C a ASE_ECD.1.5C.

6.1.1.4. Objetivos de seguridad del entorno operacional

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

ASE_OBJ.1 Security objectives for the operational environment

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

Guía de cumplimiento

La norma establece que se deben describir los objetivos de seguridad para el entorno.

Los PP de Tipo 2 definen los objetivos de seguridad para el entorno en el apartado «Objetivos de seguridad para el entorno operacional»; es suficiente copiar el contenido del PP a la ST para poder demostrar «conformidad demostrable».

En caso de cambiar el contenido se debe demostrar que los objetivos para el entorno son equivalentes o menos restrictivos.

Recomendación de seguridad: para demostrar la conformidad demostrable basta con reproducir el contenido de los objetivos de seguridad para el entorno.

6.1.1.5. Requisitos de seguridad declarados

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

ASE_REQ.1 Stated security requirements

Acciones que el desarrollador debe realizar

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.*

Elementos del contenido y de presentación

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.*

Guía de cumplimiento

Se deben describir al menos todos los requisitos funcionales y de garantía de seguridad que indica el PP de Tipo 2, esta referencia no tiene por que ser realizada de forma uniforme, es decir:

- los requisitos funcionales que no contienen operaciones pueden ser simplemente referenciados, y los que contienen operaciones reproducidos en la ST
- los SARs pueden ser todos referenciados, ya que no contienen operaciones

Por otra parte, a la hora de realizar una operación sobre un SFR, cada operación debe estar correctamente identificada y ésta se debe realizar correctamente.

Advertencia: las operaciones que pueden realizarse sobre un componente son:

- Asignación: permite la especificación de parámetros
- Iteración: permite que un componente puede ser utilizado más de una vez
- Selección: permite la especificación de uno o más ítems de una lista
- Refinamiento: permite la inclusión de detalles sobre ítems

En el caso de que las dependencias de un requisito no estén cubiertas éstas se deberán justificar de forma correcta.

En caso de cambiar o añadir requisitos de seguridad, se debe demostrar que en conjunto los requisitos son más restrictivos que los presentados en el PP Tipo 2.

Advertencia: si se suprime y no se añade un requisito de seguridad entonces la conformidad no es demostrable y generaría no conformidad con el PP.

Recomendación de seguridad: el capítulo «Requisitos de Seguridad Funcional» profundiza en el análisis de contenido para cada funcionalidad, presenta ejemplos y proporciona recomendaciones de seguridad.

6.1.1.6. Resumen de la especificación del TOE

ASE_TSS.1 TOE summary specification

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

Guía de cumplimiento

El resumen de la especificación del TOE detalla como el TOE cubre cada uno de los requisitos. Este resumen consiste en una descripción, dirigida a los usuarios, de cómo el TOE cubre cada requisitos, profundizando a nivel de diseño.

De la misma forma que la descripción del TOE ha de ser más detallada que el resumen del TOE, el resumen de la especificación del TOE debe explicar el funcionamiento del TOE de forma más minuciosa, es decir, a nivel de los mecanismos usados para satisfacer los requisitos funcionales de seguridad.

6.1.2. Documentos de guía

Documentos que describen cómo el usuario debe operar con el producto de manera que todas las acciones sean realizadas de manera segura:

Constituye uno de los grupos de evidencias en el proceso de evaluación.

Figura 6. Guías



El desarrollador debe proporcionar la siguiente documentación para la consecuente evaluación:

- guía de operativa
- guía preparativa

A continuación se presentan las acciones que según la norma se exigen al desarrollador y el contenido que debe presentar:

6.1.2.1. Guía operativa

AGD_OPE.1 Operational user guidance

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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.*

Guía de cumplimiento

El guía operativa (generalmente en forma de manual de usuario) describirá para cada uno de los roles de usuario posibles, todas las funciones y privilegios accesibles. Las guías o manuales de usuario han de contener avisos acerca de estas funciones y privilegios, explicando las consecuencias de realizar una operación, posibles consecuencias laterales y posibles interacciones con otras operaciones.

También se tienen que describir las interfaces disponibles para cada usuario. Una interfaz de usuario puede ser una interfaz gráfica. Para el caso actual, caso de TOE de Tipo 2, una de las interfaces más habituales serán las ventanas que ofrecen interacción con el usuario, o el sistema que se haya elegido.

En caso de que haya eventos en los que se precise la intervención del usuario, estos tendrán que ser descritos en los manuales o guías de usuario. También se explicará el protocolo a seguir para estos casos.

Si existen modos de operación diferentes, por ejemplo un modo de mantenimiento y otro general o de usuario, se deben explicar sus capacidades y su implicación en el funcionamiento seguro del TOE.

La guía operativa debe explicar cómo cubrir el objetivo O.SSCD y O.ITENV definido en el PP Tipo 2 y en caso de que en la ST se hayan definido otros objetivos de seguridad para el entorno adicionales, también deberá explicarse como cubrirlos.

6.1.2.2. Guía preparativa

AGD_PRE.1 Preparative procedures

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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.*

Guía de cumplimiento

La guía preparativa (generalmente en forma de manual de instalación) debe contener todos los pasos para iniciar el TOE de forma segura.

Esta guía preparativa debe contener procedimientos de instalación y especificaciones de cómo debe ser usado de forma segura en el entorno operacional.

6.1.3. Desarrollo

La documentación debe describir el diseño a nivel de interfaces mediante una especificación funcional.

La documentación de desarrollo constituye uno de los grupos de evidencias en el proceso de evaluación.

Figura 7: Desarrollo



A continuación se presentan las actividades que según la norma se exigen al desarrollador y el contenido que debe presentar:

6.1.3.1. Especificación funcional básica

ADV_FSP.1 Basic functional specification

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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.*

Elementos del contenido y de presentación

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

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

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

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

Guía de cumplimiento

En la especificación funcional básica se deben describir todos las interfaces, tanto las TSF-*enforcing*, es decir, las que sirven para hacer cumplir una actividad o propiedad, como las TSF-*supporting*, que dan soporte a una actividad o propiedad para que se pueda realizar.

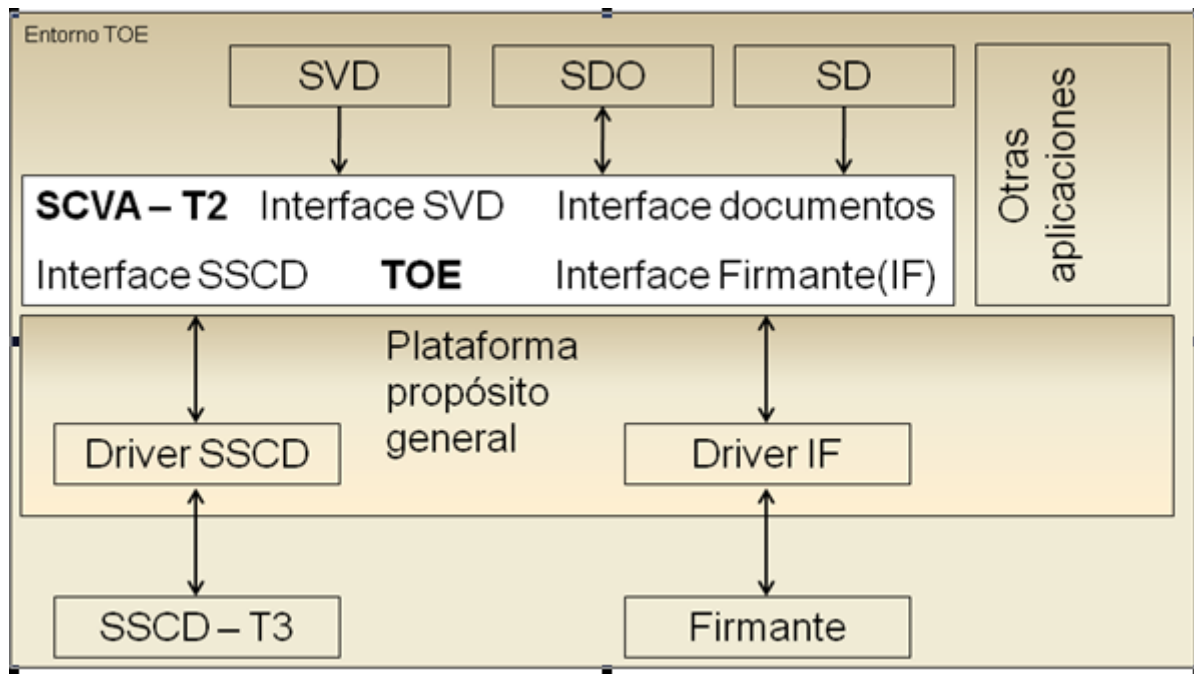
La descripción debe explicar el método de uso de cada una de las interfaces, incluyendo los parámetros de entrada y de salida.

Si una interfaz se define como TSF-*non-interfering*, se ha de justificar.

Las interfaces descritas como TSF-*enforcing* o TSF-*supporting* deben corresponderse con algún SFR, de forma que todos los aspectos de cada SFR deben ser cubiertos por interfaces. Cuando los SFR no actúen en los límites del TOE es aceptable que no queden cubiertos.

Las interfaces de un producto Tipo 2 deberán ser consistentes con la descripción de las interfaces del resumen del TOE, según queda definido en el PP Tipo 2.

Figura 8: Interfaces de la SCVA Tipo 2



6.1.4. Soporte al ciclo de vida

La documentación de soporte al ciclo de vida debe mostrar la adecuación de los procedimientos de seguridad usados durante las fases de desarrollo y mantenimiento del TOE. Constituye otro de los grupos de evidencias en el proceso de evaluación.

El desarrollador debe proporcionar la siguiente documentación para la consecuente evaluación:

- la aplicación.
- listado de configuración.

Figura 9: Gestión de la configuración



A continuación se presentan las acciones que según la norma se exigen al desarrollador y el contenido que debe presentar:

6.1.4.1. Etiquetado

ALC_CMC.1 Labelling of the TOE

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

Guía de cumplimiento

El TOE debe estar etiquetado con alguna referencia y ésta debe identificar unívocamente la versión de TOE.

La identificación del TOE debe corresponder con la presentada en la ST.

Recomendación de seguridad: típicos ejemplos de versionado de productos son:

- línea de comandos con parámetro versión
- cuadro de texto o advertencia tipo *Acerca de*

- al iniciar el producto éste presenta la versión por pantalla
- un etiquetado físico que indique versión

6.1.4.2. Gestión de la Configuración

ALC_CMS.1 TOE CM coverage

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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.*

Guía de cumplimiento

La lista de configuración debe identificar de forma única al TOE y todas las evidencias necesarias para realizar la evaluación.

6.1.5. Pruebas

Se han de aportar el producto y su documentación para verificar que el producto se comporta tal y como establece la declaración de seguridad. Este constituye otro de los grupos de evidencias en el proceso de evaluación.

El desarrollador debe proporcionar el producto a evaluar.

Figura 10: Pruebas



6.1.5.1. Pruebas independientes - conformidad

ATE_IND.1 Independent testing – conformance

ATE_IND.1 Independent testing - conformance

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

Guía de cumplimiento

El TOE debe presentarse en un estado conocido, esto implica que se ha de suministrar el TOE en un estado determinado, con las configuraciones completamente especificadas (esta es la forma más habitual en el caso de productos hardware).

En caso contrario el evaluador instalará el TOE desde cero siguiendo los procedimientos descritos en la guía de instalación (esta es la forma más habitual en el caso de productos software).

6.1.6. Análisis de vulnerabilidades

Se ha de presentar el producto para determinar si existen vulnerabilidades que exploten debilidades o fallos en el entorno operacional de uso.

Figura 11: Análisis de vulnerabilidades



Para cumplir con este grupo de evidencias el desarrollador debe facilitar el producto a evaluar.

6.1.6.1. Test de vulnerabilidades

AVA_VAN.1 Vulnerability survey

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

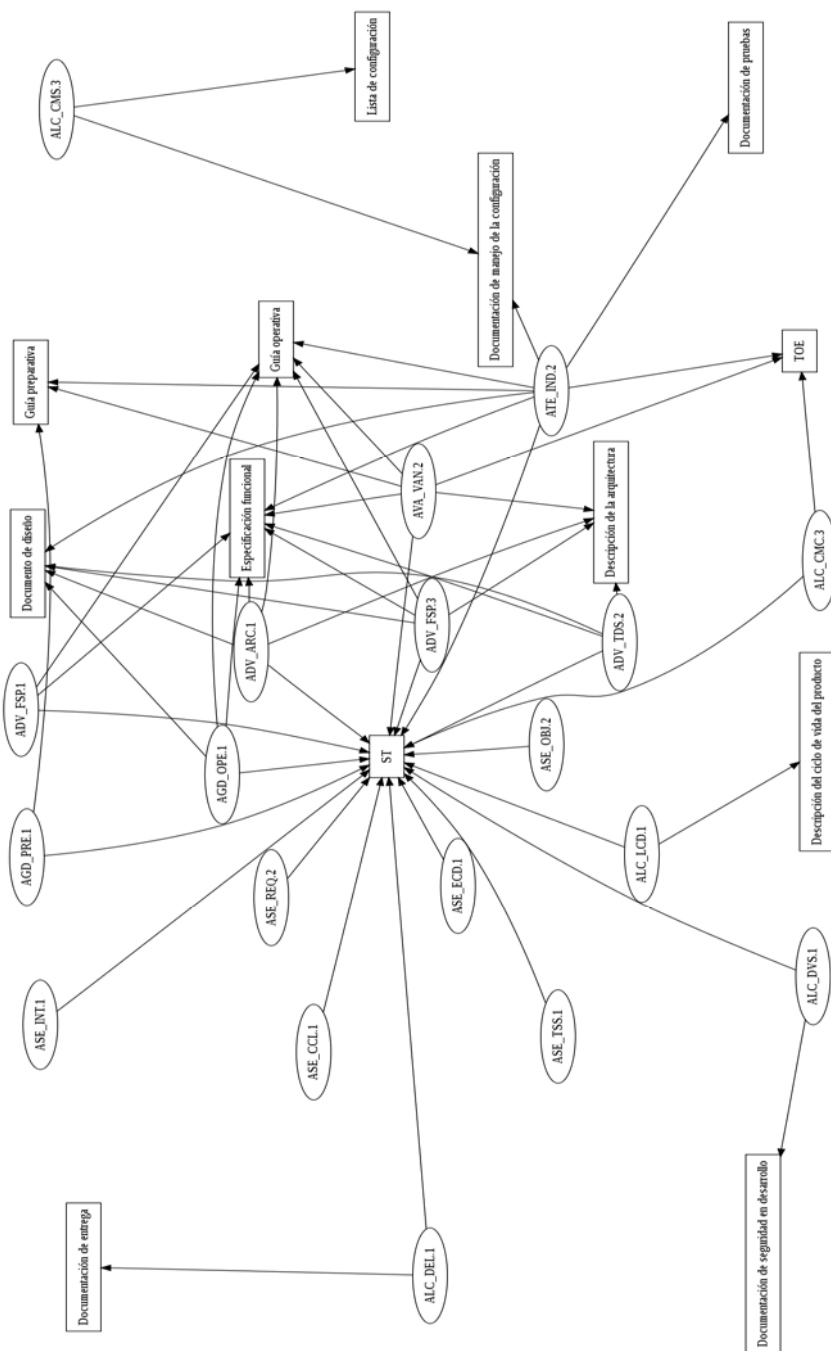
Guía de cumplimiento

Se proporcionará el TOE en un estado conocido, con las configuraciones completamente especificadas (esta es la forma más habitual en el caso de productos hardware).

En caso contrario el evaluador instalará el TOE desde cero siguiendo los procedimientos descritos en el manual de usuario (esta es la forma más habitual en el caso de productos software).

6.2. EVIDENCIAS DE GARANTÍA REQUERIDAS EN LA CERTIFICACIÓN EAL3

Figura 12: Evidencias de garantía requeridas en la certificación EAL3



6.2.1. Declaración de seguridad

Documento completo y riguroso que define el producto a evaluar en base a una descripción, unas amenazas, unas hipótesis, unos objetivos de seguridad, unos requisitos funcionales y de garantía de seguridad y unas funcionalidades de seguridad.

A continuación se presenta las acciones que el desarrollador debe realizar y el contenido que debe presentar:

6.2.1.1. Introducción de la Declaración de Seguridad

ASE_INT.1 ST Introduction

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

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

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

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

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

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

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

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

Figura 13: Declaración de seguridad



La Declaración de Seguridad es uno de los grupos de evidencias requeridos en el proceso de evaluación.

Guía de cumplimiento

La introducción de la ST debe contener los siguientes datos:

- referencia de la ST, de forma unívoca
- referencia del TOE, de forma unívoca
- resumen del TOE
- descripción del TOE

Resumen del TOE

La intención del resumen del TOE es proporcionar suficiente información para que una persona que pueda estar interesada sepa que hace el producto a grandes rasgos:

- uso y las principales funcionalidades de seguridad del TOE
- tipo de TOE (en este caso, el tipo de TOE según el PP será Tipo 2)
- *firmware*, software, y hardware necesario para el funcionamiento del TOE

Descripción del TOE

La descripción del TOE debe cubrir todos los aspectos del TOE incluidos en su resumen y abordarlos con mayor profundidad. Esta descripción ha de ser redactada en forma narrativa y no debe adentrarse demasiado en los detalles técnicos.

Además, tiene que describir el alcance físico y lógico del TOE, que en los TOEs de Tipo 2 el desarrollador deberá considerar cuales son los límites del producto.

6.2.1.2. Declaración de conformidad

ASE_CCL.1 Conformance claims

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

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

Elementos del contenido y de presentación

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 ASE_CCL.1.2C 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 rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.*

ASE_CCL.1.7C *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.*

Guía de cumplimiento

El PP establece que la conformidad debe de ser demostrable, por tanto la Declaración de Seguridad puede contener secciones o partes distintas a las presentadas en el Perfil de Protección, si bien, para demostrar la conformidad con el PP, el autor de la Declaración de Seguridad debe proporcionar una justificación del porqué la Declaración de Seguridad es equivalente o más restrictiva que el PP.

Recomendación de seguridad: una Declaración de Seguridad es equivalente o más restrictiva que un perfil de protección si:

- todos los productos a evaluar que satisfacen el PP, también satisfacen la ST
- todos los entornos operacionales que satisfacen la ST, también satisfacen el PP

Es decir, la Declaración de Seguridad debe presentar al menos las mismas o más restricciones para el TOE y presenta igual o menos restricciones para el entorno operacional. Se ha de especificar cual es el tipo de TOE según el PP elegido (en este caso será Tipo 2).

Se especificará un paquete de garantía (EAL) mínimo según el PP usado.

La definición del problema de seguridad debe ser consistente con la especificada en el PP.

Los objetivos de seguridad presentados en la ST han de ser consistentes con los presentes en el PP.

Los requisitos de seguridad presentados en la ST han de ser consistentes con los presentes en el PP.

Esto implica que los SFRs declarados en la ST deben ser tan restrictivos o más que los declarados en el PP.

6.2.1.3. Definición del problema de seguridad

Se detallan según la norma las actividades que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

ASE_SPD.1 Security problem definition

Acciones que el desarrollador debe realizar

ASE_SPD.1.1D *The developer shall provide a security problem definition.*

Elementos del contenido y de presentación

ASE_SPD.1.1C *The security problem definition shall describe the threats.*

ASE_SPD.1.2C *All threats shall be described in terms of a threat agent, an asset, and an adverse action.*

ASE_SPD.1.3C *The security problem definition shall describe the OSPs.*

ASE_SPD.1.4C *The security problem definition shall describe the assumptions about the operational environment of the TOE.*

Guía de cumplimiento

Se deben describir las amenazas que pueden comprometer la seguridad del TOE. Para ello se detalla el agente que puede causar la amenaza, los recursos que pueden ser comprometidos por esa amenaza y las consecuencias de no resolver esa amenaza.

Se deben describir también las políticas organizativas de seguridad y las hipótesis de seguridad del entorno operacional del TOE, es decir las condiciones de seguridad bajo las que se utilizará el TOE.

Recomendación de seguridad: el PP Tipo 2 establece la descripción del problema de seguridad (apartado «Definición del Problema de Seguridad») y por tanto usando esta misma descripción, el autor de la Declaración de Seguridad demuestra conformidad demostrable.

6.2.1.4. Objetivos de Seguridad

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

ASE_OBJ.2 Security objectives

Acciones que el desarrollador debe realizar

ASE_OBJ.2.1D *The developer shall provide a statement of security objectives.*

ASE_OBJ.2.2D *The developer shall provide a security objectives rationale.*

Elementos del contenido y de presentación

ASE_OBJ.2.1C *The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.*

ASE_OBJ.2.2C *The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.*

ASE_OBJ.2.3C *The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.*

ASE_OBJ.2.4C *The security objectives rationale shall demonstrate that the security objectives counter all threats.*

ASE_OBJ.2.5C *The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.*

ASE_OBJ.2.6C *The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.*

Guía de cumplimiento

Se deben definir los objetivos de seguridad para el TOE y para el entorno operacional. La separación entre los objetivos del TOE y del entorno debe ser clara y se deben incluir los objetivos de seguridad presentados en el PP.

Cada uno de los objetivos de seguridad para el TOE debe corresponderse con al menos una política de seguridad organizativa o una amenaza. Cada uno de los objetivos de seguridad para el entorno debe corresponderse con al menos una amenaza, política de seguridad organizativa o hipótesis de seguridad.

Se debe razonar la cobertura por parte de cada uno de los objetivos de seguridad.

Cada una de las amenazas, políticas de seguridad organizativas y hipótesis debe corresponderse con al menos un objetivo de seguridad.

En caso de cambiar el contenido se debe demostrar que los objetivos para el TOE son equivalentes o más restrictivos y para el entorno son equivalentes o menos restrictivos.

Recomendación de seguridad: el PP Tipo 2 establece los objetivos de seguridad para el TOE y para el entorno operacional y la justificación de cobertura de estos objetivos, por tanto usando esta misma descripción (apartado «Objetivos de Seguridad del PP») el autor de la Declaración de Seguridad demuestra conformidad demostrable.

6.2.1.5. Definición de componentes extendidos

ASE_ECD.1 Extended components definition

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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.*

Elementos del contenido y de presentación

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

ASE_ECD.1.2C *The extended components definition shall dedine 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.*

Guía de cumplimiento

Estos elementos obligan al redactor de la Declaración de Seguridad a identificar los requisitos que no son extraídos de CC parte 2 y parte 3.

En este caso el PP tiene dos requisitos funcionales que no forman parte de CC parte 2 (FDP_SVR.1 y FDP_ISD.1), ya identificados en el PP. Haciendo una declaración de conformidad demostrable con el PP, la identificación de los requisitos extendidos ya queda identificada.

En caso de querer añadir otros componentes, se aplicará lo que especifica la norma CC, tal y como establece los elementos de contenido y presentación de ASE_ECD.1.1C a ASE_ECD.1.5C.

6.2.1.6. Requisitos de seguridad derivados

ASE_REQ.2 Derived security requirements

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

ASE_REQ.2.1D *The developer shall provide a statement of security objectives.*

ASE_REQ.2.2D *The developer shall provide a security objectives rationale.*

Elementos del contenido y de presentación

ASE_REQ.2.1C *The statement of security requirements shall describe the SFRs and the SARs.*

ASE_REQ.2.2C *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.2.3C *The statement of security requirements shall identify all operations on the security requirements.*

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C *Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.*

ASE_REQ.2.6C *The security requirements rationale shall trace each SFR back to the security objectives for the TOE.*

ASE_REQ.2.7C *The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.*

ASE_REQ.2.8C *The security requirements rationale shall explain why the SARs were chosen.*

ASE_REQ.2.9C *The statement of security requirements shall be internally consistent.*

Guía de cumplimiento

Se deben describir todos los requisitos funcionales y de garantía de seguridad que indica el PP, esta referencia no tiene por que ser realizada de forma uniforme, es decir:

- Los requisitos que no contienen operaciones pueden ser simplemente referenciados, y los que contienen operaciones deben reproducirse en la ST y completar las operaciones.
- Los SARs pueden ser todos referenciados, ya que no contienen operaciones.

Además, a la hora de realizar una operación sobre un SFR, cada operación debe estar correctamente identificada y se debe realizar de forma adecuada.

Recomendación de seguridad: las operaciones que pueden realizarse sobre un componente son:

- Asignación: permite la especificación de parámetros

- Iteración: permite que un componente pueda ser utilizado más de una vez
- Selección: permite la especificación de uno o más *ítems* de una lista
- Refinamiento: permite la inclusión de detalles sobre *ítems*

En el caso de que las dependencias de un requisito no estén cubiertas, se deberán justificar de forma correcta.

En caso de cambiar el añadir requisitos de seguridad, se debe demostrar que en conjunto los requisitos son más restrictivos que los presentados en el PP Tipo 2.

Advertencia: si se suprime o no se añade un requisito de seguridad entonces la conformidad no es demostrable y generaría no conformidad con el PP.

Recomendación de seguridad: el capítulo «Requisitos de Seguridad Funcional» de esta guía profundiza en el análisis de contenido para cada funcionalidad, presenta ejemplos y aporta recomendaciones de seguridad.

6.2.1.7. Resumen de especificación del TOE

ASE_TSS.1 TOE summary specification

Se detallan según la norma las actividades que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

Guía de cumplimiento

El resumen de la especificación del TOE explicará como se cubren cada uno de los requisitos. Este resumen será una descripción, dirigida a los usuarios, de cómo el TOE cubre cada uno de los requisitos, profundizando a nivel de diseño.

De la misma forma que la descripción del TOE ha de ser más detallada que el resumen del TOE, el resumen de la especificación del TOE debe explicar el funcionamiento del TOE de

forma más minuciosa, a nivel de los mecanismos usados para satisfacer los requisitos funcionales de seguridad.

6.2.2. Documentos de guía

Documentos que describen cómo el usuario debe operar con el producto de manera que todas las acciones sean realizadas de manera segura:

Figura 14: Guías



Los documentos de guía son otro de los grupos de evidencias necesarias en el proceso de evaluación.

El desarrollador debe proporcionar la siguiente documentación para la consecuente evaluación:

- guía de operativa
- guía preparativa

A continuación se presentan las acciones que según la norma se exigen al desarrollador y el contenido que debe presentar:

6.2.2.1. Guía operativa

AGD_OPE.1 Operational user guidance

Se detallan según la norma las actividades que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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.*

Guía de cumplimiento

Para cada uno de los roles de usuario posibles, el manual de usuario describirá todas las funciones y privilegios accesibles.

Las guías operativas (generalmente en forma de manuales de usuario) han de contener avisos acerca de estas funciones y privilegios, explicando las consecuencias de realizar una operación, posibles consecuencias laterales y posibles interacciones con otras operaciones.

La guía operativa tiene que describir las interfaces disponibles para cada usuario. Una interfaz de usuario puede ser una interfaz gráfica.

Para el caso actual, caso de TOE de Tipo 2, una de las interfaces más habituales serán las ventanas que ofrecen interacción con el usuario, o el sistema que se haya elegido.

En caso que haya eventos en los que se precise la intervención del usuario, estos tendrán que ser descritos en los manuales o guías de usuario. También se explicará el protocolo a seguir para estos casos.

Si existen modos de operación diferentes, por ejemplo un modo de mantenimiento y otro general o de usuario, se deben explicar sus capacidades y su implicación en el funcionamiento seguro del TOE.

La guía operativa debe explicar cómo cubrir el objetivo O.SSCD y O.ITENV definido en el PP Tipo 2 y en caso de que en la ST se hayan definido otros objetivos de seguridad para el entorno adicionales, también deberá explicarse como cubrirlos.

6.2.3. Guía preparativa

AGD_PRE.1 Preparative procedures

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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.*

Guía de cumplimiento

La guía preparativa (generalmente en forma de manual de instalación) debe contener todos los pasos para iniciar el TOE de forma segura.

Esta guía preparativa debe contener procedimientos de instalación y especificaciones de cómo debe ser usado de forma segura en el entorno operacional.

6.2.4. Desarrollo

La documentación debe describir el diseño a nivel de interfaces, subsistemas y demostrar que las funcionalidades no son evitables y se autoprotegen.

Figura 15: Desarrollo



Los documentos de desarrollo son otro de los grupos de evidencias necesarios en el proceso de evaluación.

El desarrollador debe proporcionar la siguiente documentación para la consecuente evaluación:

- especificación funcional
- descripción del problema de seguridad
- diseño del producto

A continuación se presentan las actividades que según la norma se exigen al desarrollador y el contenido que debe presentar:

6.2.4.1. Descripción de la arquitectura de seguridad

ADV_ARC.1 Security Architecture Description

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

ADV_ARC.1.1D *The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.*

ADV_ARC.1.2D *The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.*

ADV_ARC.1.3D *The developer shall provide a security architecture description of the TSF.*

Elementos del contenido y de presentación

ADV_ARC.1.1C *The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.*

ADV_ARC.1.2C *The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.*

ADV_ARC.1.3C *The security architecture description shall describe how the TSF initialisation process is secure.*

ADV_ARC.1.4C *The security architecture description shall demonstrate that the TSF protects itself from tampering.*

ADV_ARC.1.5C *The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.*

Guía de cumplimiento

La descripción de la arquitectura de seguridad debe explicar en base a un documento cómo el TOE se auto-protege de los ataques y modificaciones.

También en este documento se ha de explicar cómo el TOE hace aplicar la separación de dominios prevista en el PP y cómo asegura que los requisitos funcionales de seguridad no se pueden violar.

Este documento debe proporcionar el mismo nivel de detalle que el presentado en la especificación del diseño y en la especificación funcional.

Recomendación de seguridad: Ejemplo de descripción de la arquitectura de seguridad en el apartado de separación de dominios de seguridad para una aplicación software sobre Linux:

La aplicación software se agrupa en un TOE de Tipo 2 según el PP, y por tanto el entorno IT será confiable.

En este caso el entorno IT será el sistema operativo por lo que consideramos que el contexto sobre el que se ejecuta el núcleo y los procesos de *root* son confiables.

Para la separación de dominios se definen tres áreas:

Generación del ejecutable

Para mejorar la seguridad contra desbordamientos de *buffer* del producto se ha compilado con la opción *-fstack-protector* de *gcc*.

Instalación

El usuario propietario del binario instalado será *root*, el binario tendrá el bit *suid* activado y los permisos serán los correctos (rwsr-xr-x). El bit *suid* forzará a que el programa se ejecute como *root* e impedirá los ataques de inyección de bibliotecas vía *LD_PRELOAD*, impedirá el *debug* del proceso vía *ptrace()* y permitirá que se pueda realizar la operación *mlock()*.

Tiempo de ejecución: Auto-protección inicial

- 1) La aplicación cargará la imagen de la aplicación mediante la *syscall execve*. En este momento se cargará la imagen del programa en memoria. A continuación el */lib/ld-linux.so.2* carga la librería *opensc* (PKCS#15) y esta por su parte carga el driver del DNIe.
- 2) *ld-linux.so* pasa la ejecución al punto de entrada de la aplicación.
- 3) Se instalan los manejadores de señales (*syscall sigaction*).
- 4) La aplicación verifica que se está ejecutando con permisos de *root* (*getresuid*).
- 5) Se bloquea la memoria del proceso en RAM mediante la *syscall mlockall()*, de esta forma se previene que el VAD llegue al *swap*.
- 6) Cuando la aplicación ha hecho las verificaciones anteriores, esta baja los privilegios al mismo nivel que el usuario que ha llamado al programa (*syscall setreuid()*).
- 7) En caso de que se haya detectado alguna violación de seguridad, se presenta un mensaje explicativo del error y cierra la aplicación.
- 8) Se comprobará que no existan descriptores de fichero abiertos mediante la lectura del directorio */proc/self/fd/* (se comprobará que sólo existan los descriptores 0, 1 y 2, en caso de que existan más se cierran).

Tiempo de ejecución: Auto-protección durante la ejecución normal

Esta fase de protección se encarga de proteger a la aplicación tanto cuando esta pretende acceder a un recurso como cuando un evento generado fuera de la aplicación debe ser entregado a la aplicación.

Tiempo de ejecución: Acceso a ficheros

Al usar la *syscall open*, se debe usar el flag *O_CLOEXEC* para cerrar los ficheros si el proceso hace un *exec*. Todos los accesos a ficheros deben libres de condiciones de carrera (ataques TOCTTOU -*Time Of Check To Time Of Use*-) mediante la creación segura de ficheros (uso de la *syscall open* con los flags *O_CREAT|O_EXCL*). Cuando se abren ficheros ya existentes, la *syscall open* también debería usar el flag *O_NOFOLLOW* para evitar ataques de falseamiento de identidad de ficheros con enlaces simbólicos.

Tiempo de ejecución: Señales

El producto debe ignorar todas las señales o abortar correctamente al recibir una señal no esperada.

También debe ser capaz de manejar correctamente las señales recibidas durante el gestión de una señal (el tratamiento de señales debe ser atómico puesto que puede ser interrumpido por otra señal).

6.2.4.2. Especificación funcional con resumen completo

ADV_FSP.3 Functional specification with complete summary

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

ADV_FSP.3.1D *The developer shall provide a functional specification.*

ADV_FSP.3.2D *The developer shall provide a tracing from the functional specification to the SFRs.*

Elementos del contenido y de presentación

ADV_FSP.3.1C *The functional specification shall completely represent the TSF.*

ADV_FSP.3.2C *The functional specification shall describe the purpose and method of use for all TSFI.*

ADV_FSP.3.3C *The functional specification shall identify and describe all parameters associated with each TSFI.*

ADV_FSP.3.4C *For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.*

ADV_FSP.3.5C *For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.*

ADV_FSP.3.6C *The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.*

ADV_FSP.3.7C *The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.*

Guía de cumplimiento

El resumen completo o descripción debe explicar el método de uso de cada una de las interfaces, incluyendo parámetros de entrada y de salida.

Se debe presentar una especificación funcional que detalle todas las funcionalidades de seguridad (TSFs) y cómo éstas son utilizadas por medio de las interfaces (TSFIs) sin dejar TSFs o partes de TSFs sin cubrir.

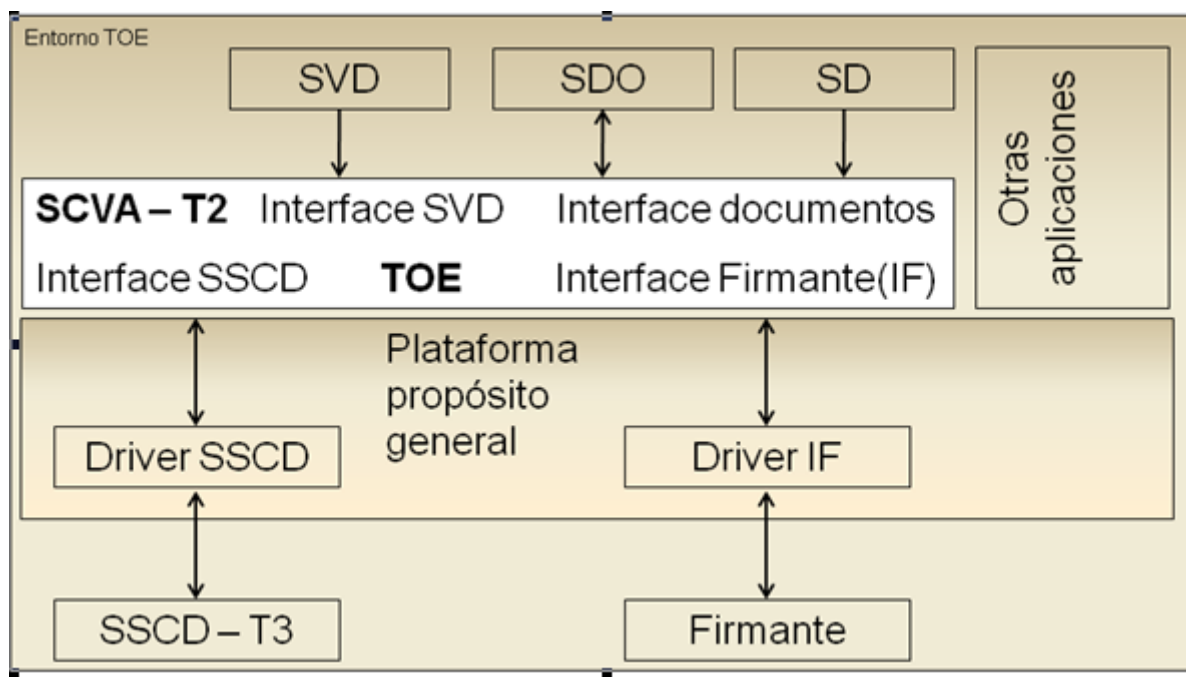
La especificación funcional incluirá una descripción de las acciones derivadas de la instanciación de las interfaces-*enforcing* y los mensajes de error derivados de su utilización.

Igualmente esta especificación debe incluir la descripción de las acciones asociadas a las interfaces para las interfaces *supporting* y *non interfering*.

Las interfaces descritas como *TSF-supporting* se deben corresponder con algún SFR, todos los aspectos de cada SFR deben ser cubiertos por interfaces.

Las interfaces de un producto Tipo 2 deberán ser consistentes con la descripción de las interfaces del resumen del TOE, definido en el resumen del PP Tipo 2

Figura 16: Interfaces de la SCVA Tipo 2



6.2.4.3. Documentos de diseño

ADV_TDS.2 Architectural design

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

ADV_TDS.2.1D *The developer shall provide the design of the TOE.*

ADV_TDS.2.2D *The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.*

Elementos del contenido y de presentación

ADV_TDS.2.1C *The design shall describe the structure of the TOE in terms of subsystems.*

ADV_TDS.2.2C *The design shall identify all subsystems of the TSF.*

ADV_TDS.2.3C *The design shall describe the behaviour of each SFR noninterfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.*

ADV_TDS.2.4C *The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.*

ADV_TDS.2.5C *The design shall summarise the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems.*

ADV_TDS.2.6C *The design shall summarise the behaviour of the SFR-supporting subsystems.*

ADV_TDS.2.7C *The design shall provide a description of the interactions among all subsystems of the TSF.*

ADV_TDS.2.8C *The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.*

Guía de cumplimiento

El desarrollador debe proporcionar los documentos de diseño del TOE. Los documentos de diseño deben incluir una descripción de los subsistemas, y explicar por qué los subsistemas que no alteran los SFR no afectan a la seguridad del producto.

Los documentos de diseño han de incluir una descripción del comportamiento de los subsistemas que implementan los SFR.

Estos documentos también han de incluir un resumen del comportamiento de los subsistemas que ayudan a la implementación de los SFR y los que o tienen incidencia en ellos.

Igualmente se debe proporcionar una descripción que explique la relación entre el comportamiento del TOE y las operaciones a través de sus interfaces. Esta relación se debe corresponder con el nivel más bajo de descomposición presentado en el diseño.

6.2.5. Soporte al ciclo de vida

La documentación de soporte al ciclo de vida debe mostrar la adecuación de los procedimientos de seguridad usados durante las fases de desarrollo y mantenimiento del TOE.

Los documentos de Gestión de la Configuración son uno de los grupos de evidencias necesarios para la evaluación.

Figura 17: Gestión de la configuración



El desarrollador proporcionará la siguiente documentación para la consecuente evaluación:

- documentación del sistema de gestión de configuración
- documentación del proceso de entrega
- identificación de las medidas de seguridad aplicadas en el sitio de desarrollo
- documentación del modelo de ciclo de vida

A continuación se presentan las actividades que según la norma se exigen al desarrollador y el contenido que debe presentar:

6.2.5.1. Documentación y sistemas de Gestión de la Configuración

ALC_CMC.3 Authorisation controls

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

ALC_CMC.3.1D *The developer shall provide the TOE and a reference for the TOE.*

ALC_CMC.3.2D *The developer shall provide the CM documentation.*

ALC_CMC.3.3D *The developer shall use a CM system.*

Elementos del contenido y de presentación

ALC_CMC.3.1C *The TOE shall be labelled with its unique reference.*

ALC_CMC.3.2C *The CM documentation shall describe the method used to uniquely identify the configuration items.*

ALC_CMC.3.3C *The CM system shall uniquely identify all configuration items.*

ALC_CMC.3.4C *The CM system shall provide measures such that only authorised changes are made to the configuration items.*

ALC_CMC.3.5C *The CM documentation shall include a CM plan.*

ALC_CMC.3.6C *The CM plan shall describe how the CM system is used for the development of the TOE.*

ALC_CMC.3.7C *The evidence shall demonstrate that all configuration items are being maintained under the CM system.*

ALC_CMC.3.8C *The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.*

Guía de cumplimiento

El desarrollador debe identificar unívocamente al TOE, es decir, este ha de tener una referencia única en todos los documentos, interfaces, etc. Una referencia única al TOE normalmente es el nombre del producto (debe ser el mismo que el presentado en la ST) y la versión del mismo.

La documentación del sistema de gestión de la configuración describirá el método usado para identificar cada uno de los elementos de configuración.

El sistema de gestión de la configuración tiene que identificar todos los elementos de configuración de forma única (véase la Recomendación de Seguridad a continuación).

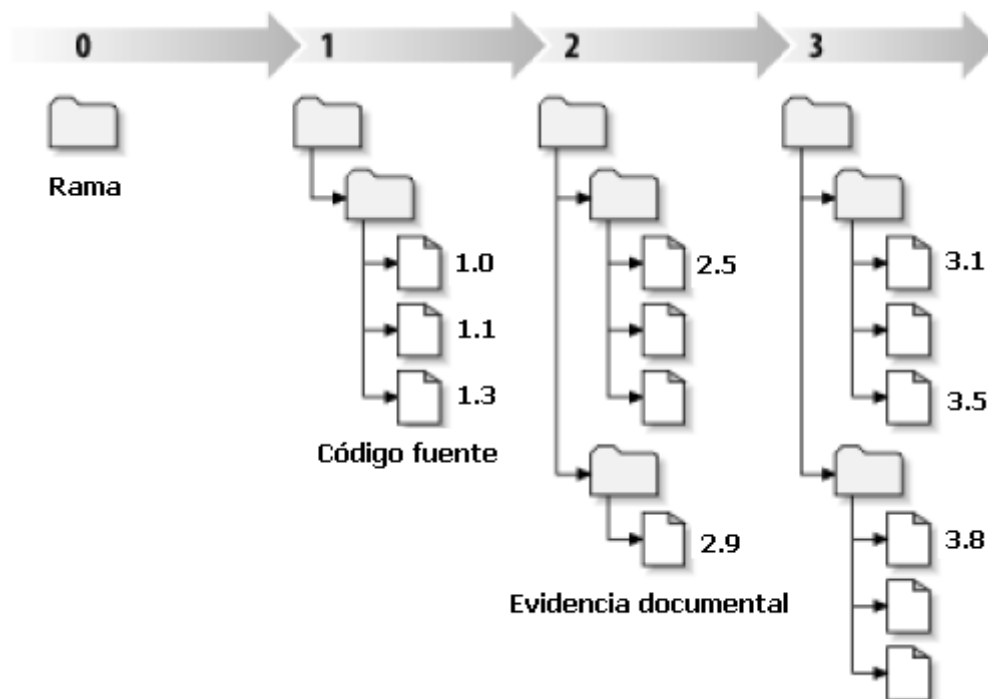
El sistema de gestión de la configuración también ha de proporcionar un método que controle la actualización de los elementos de configuración.

La documentación del sistema de gestión de la configuración incluirá un plan de gestión de la configuración. Este plan debe describir cómo se usa el sistema de gestión de la configuración durante el desarrollo del TOE.

Se han de presentar evidencias que demuestren que todos los elementos de configuración están controlados por el sistema de gestión de configuración y demostrar que el sistema de gestión de la configuración está siendo operado como establece el plan de gestión de la configuración.

Recomendación de seguridad: un ejemplo de herramienta que permite establecer un plan de gestión de configuración es Subversion, dónde:

- la versión de un producto se establece por cada rama del sistema Subversion.
- la versión de cada uno de los ítems de la representación de implementación (código fuente) se establece en un fichero o carpeta de una rama.
- la versión de cada una de las evidencias requeridas para cubrir los requisitos de garantía se definen en un fichero o carpeta de una rama.



NOTA: Subversion es un ejemplo de herramienta gratuita de gestión de la configuración que se puede encontrar en <http://subversion.tigris.org>.

6.2.5.2. Gestión de la configuración: implementación

ALC_CMS.3 Implementation representation CM coverage

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

ALC_CMS.3.1D *The developer shall provide a configuration list for the TOE.*

Elementos del contenido y de presentación

ALC_CMS.3.1C *The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.*

ALC_CMS.3.2C *The configuration list shall uniquely identify the configuration items.*

ALC_CMS.3.3C *For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.*

Guía de cumplimiento

El desarrollador debe proporcionar un listado de configuración del TOE.

Este listado debe contener identificadores unívocos para:

- TOE
- las evidencias de evaluación requeridas por los SAR
- las partes que componen el TOE
- la representación de la implementación del TOE (código fuente, diagramas, esquemáticos,...)

6.2.5.3. Procedimientos de suministro

ALC_DEL.1 Delivery procedures

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

ALC_DEL.1.1D *The developer shall document procedures for delivery of the TOE or parts of it to the consumer.*

ALC_DEL.1.2D *The developer shall use the delivery procedures.*

Elementos del contenido y de presentación

ALC_DEL.1.1C *The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.*

Guía de cumplimiento

El desarrollador debe documentar y usar o demostrar que tiene activos los procedimientos de entrega del TOE al consumidor.

La documentación debe detallar los procedimientos necesarios para mantener la seguridad al entregar el TOE al consumidor.

6.2.5.4. Medidas de seguridad

ALC_DVS.1 Identification of security measures

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

Guía de cumplimiento

El desarrollador debe producir documentación que garantice que el desarrollo se realiza de forma segura y que se mantienen, manteniendo la confidencialidad e integridad del diseño y la implementación del TOE.

Modelo de ciclo de vida

ALC_LCD.1 Developer defined life-cycle model

Acciones que el desarrollador debe realizar

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

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

Elementos del contenido y de presentación

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

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

Guía de cumplimiento

El desarrollador debe establecer el modelo del ciclo de vida usado para el desarrollo y mantenimiento del TOE.

Este modelo ha de estar plasmado en la documentación de definición del ciclo de vida.

6.2.6. Pruebas

Se han de entregar el producto y su documentación con el fin de asegurar que el producto se comporta tal y como establece la declaración de seguridad.

Este grupo de evidencias también es necesario para el proceso de evaluación.

Figura 18: Pruebas



El desarrollador debe proporcionar la siguiente documentación para la consecuente evaluación:

- documentación de la cobertura de las pruebas
- documentación de las pruebas
- producto a evaluar operativo

A continuación se presentan las actividades que según la norma se exigen al desarrollador y el contenido que debe presentar:

6.2.6.1. Análisis de cobertura de los test

ATE_COV.2 Analysis of coverage

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

ATE_COV.2.2C *The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.*

Guía de cumplimiento

El desarrollador aportará un análisis de la cobertura del conjunto de las pruebas realizadas. Este análisis tiene que demostrar que se han comprobado mediante pruebas todas las TSFIs de la especificación funcional.

6.2.6.2. Test: diseño básico

ATE_DPT.1 Testing: basic design

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

ATE_DPT.1.1C *The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.*

ATE_DPT.1.2C *The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.*

Guía de cumplimiento

El desarrollador aportará un análisis de la profundidad del conjunto de las pruebas realizadas y presentará la correspondencia entre los subsistemas detallados en la documentación de desarrollo y las pruebas realizadas. Este análisis debe demostrar que se han comprobado mediante pruebas todos los subsistemas descritos en el diseño del TOE.

6.2.6.3. Test de funcionalidad

ATE_FUN.1 Functional testing

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

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

Elementos del contenido y de presentación

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

ATE_FUN.1.2C *The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.*

ATE_FUN.1.3C *The expected test results shall show the anticipated outputs from a successful execution of the tests.*

ATE_FUN.1.4C *The actual test results shall be consistent with the expected test results.*

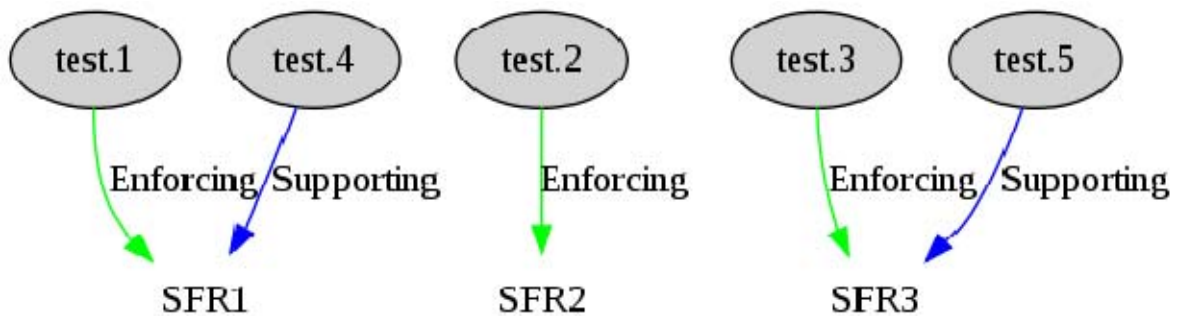
Guía de cumplimiento

El desarrollador realizará las pruebas de las funcionalidades de seguridad del TOE y documentará los resultados.

También aportará documentación detallada para cada uno de los siguientes apartados:

- requisitos iniciales del escenario de test
- procedimientos a seguir
- resultados esperados
- resultados obtenidos en las pruebas
- cobertura del SFR
- tipo de cobertura (*enforcing, supporting, non-interfering*).

Figura 19: Cobertura de pruebas sobre requisitos funcionales



La figura anterior muestra un ejemplo de demostración de cobertura, dónde mediante enlace descriptivo, *enforcing* o *supporting*, se presenta la cobertura entre los requisitos funcionales de seguridad descritos en la declaración de seguridad y las pruebas realizadas.

6.2.6.4. Muestra para test independientes

ATE_IND.2 Independent testing - sample

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

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

Guía de cumplimiento

El desarrollador proporcionará el TOE en un estado conocido, especificando completamente sus configuraciones (esta es la forma más habitual en el caso de productos hardware).

En caso contrario el evaluador instalará el TOE desde cero siguiendo los procedimientos descritos en el manual de usuario (esta es la forma más habitual en el caso de productos software).

6.2.7. Análisis de vulnerabilidades

Se proporcionará el producto para determinar si existen vulnerabilidades que exploten debilidades o fallos en el entorno operacional de uso.

Figura 20: Análisis de vulnerabilidades



El desarrollador debe proporcionar el producto a evaluar. Este es uno de los grupos de evidencias necesarios para la evaluación.

6.2.7.1. Análisis de vulnerabilidades

AVA_VAN.2 Vulnerability analysis

Se detallan según la norma las acciones que el desarrollador debe realizar y los elementos de contenido que debe incluir para cumplir este requisito. Estas se acompañan de una guía de cumplimiento para facilitar la tarea del desarrollador.

Acciones que el desarrollador debe realizar

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

Elementos del contenido y de presentación

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

Guía de cumplimiento

El desarrollador proporcionará el TOE en un estado conocido, especificando completamente sus configuraciones (esta es la forma más habitual en el caso de productos hardware).

En caso contrario el evaluador instalará el TOE desde cero siguiendo los procedimientos descritos en el manual de usuario (esta es la forma más habitual en el caso de productos software).

7. REQUISITOS DE SEGURIDAD FUNCIONAL

Este apartado describe cada una de las funcionalidades de seguridad descritas en el PP, para cada una de éstas se incluye:

- una transcripción de los componentes presentados en el PP
- una descripción técnica aclarativa del propio componente
- ejemplos de instanciación, dónde se detallan el contenido de las operaciones a realizar en los componentes presentados
- ejemplos de implementación
- recomendaciones de seguridad

7.1. FTP_SDI

7.1.1. Transcripción del componente

This component monitors data stored on media for integrity errors.

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:integrity errors] on all objects, based on the following attributes: [assignment: atributos de los datos de usuario].*

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].*

7.1.2. Descripción del componente

El producto a evaluar se acompañará de un mecanismo para verificar la integridad de los siguientes datos de usuario:

- documento a firmar
- atributos de firma
- datos a firmar
- representación de los datos a firmar

- clave pública
- documento firmado
- PIN

Además, si se detecta un error de integridad, se debe interrumpir el proceso de creación de firma y notificar el error al usuario.

7.1.3. Ejemplos de instanciación

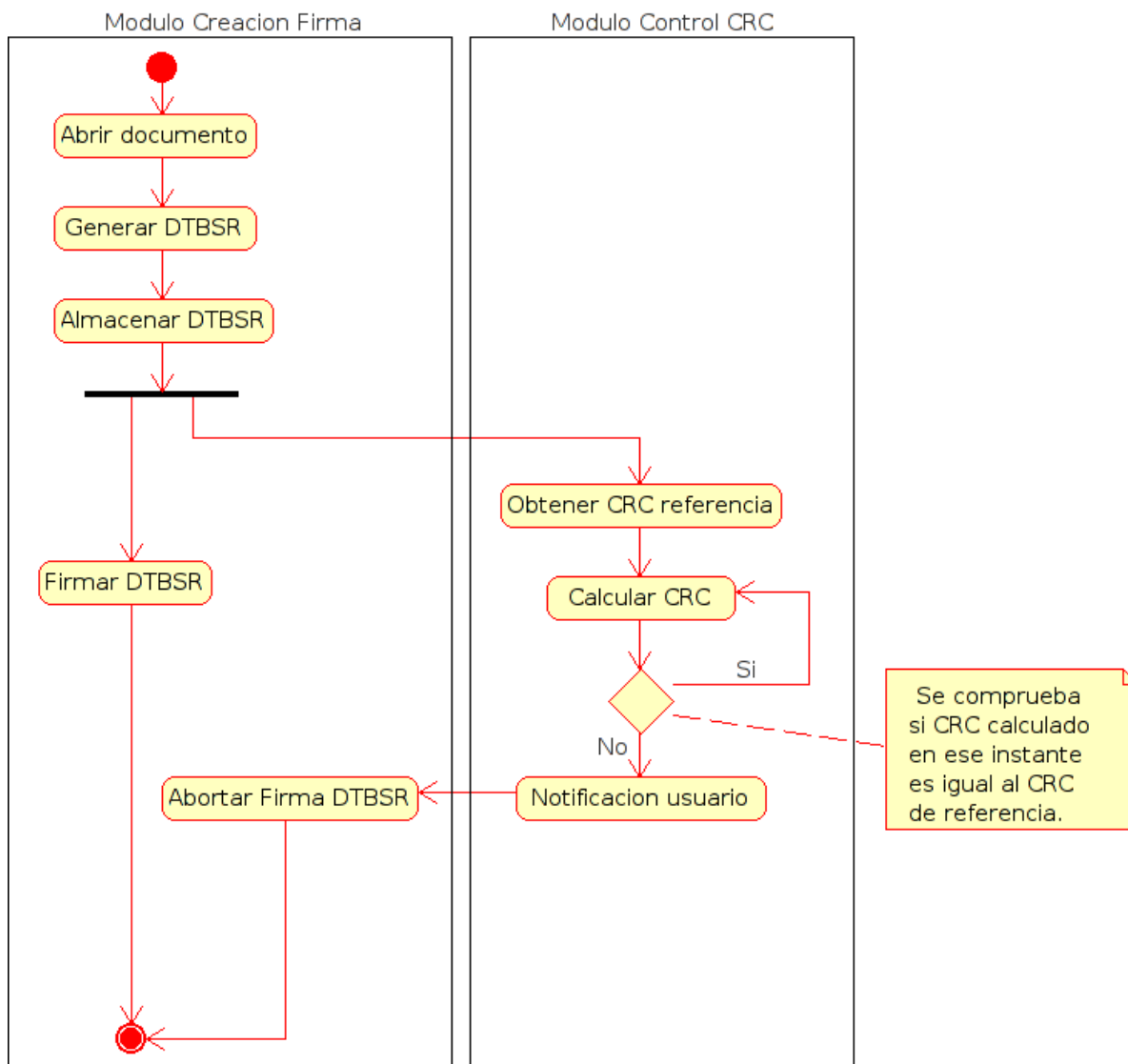
El requisito presenta las siguientes operaciones:

- Asignación: [*integrity errors*], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.
- Asignación: [atributos de los datos de usuario], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.
- Asignación: [interrumpir la operación de creación/verificación de firma y notificar al firmante], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.

7.1.4. Ejemplos de implantación

A continuación se presenta un ejemplo de implantación de este requisito:

Figura 21: Control CRC mediante módulo software



Mediante un hilo se revisa si el CRC del DTBSR ha cambiado y si hay una desviación se generará una interrupción que permitirá informar al usuario del problema.

7.1.5. Recomendaciones de seguridad

Recomendación de seguridad: en el caso de garantía de evaluación EAL3, la implantación de controles de integridad debe demostrar que no es posible evadir estos controles y por tanto el cumplimiento en código almacenado en RAM es técnicamente complejo.

7.2. FTP_ITC.1.UD

7.2.1. Transcripción del componente

This component should be used when a trusted communication channel between the TSF and another trusted IT product is required. FTP_ITC.1 requires that the TSF provide a trusted communication channel between itself and another trusted IT product.

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 [assignment: 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].*

7.2.2. Descripción del componente

El producto a evaluar debe crear un canal confiable con el dispositivo de creación de firma segura, el DNle para proceder a la firma de un documento.

Las características del canal confiable deben ser:

- separación lógica de otros canales de comunicación
- garantizar la identidad de los dos extremos del canal confiable
- asegurar protección frente a la modificación y a la alteración de los datos transmitidos por el canal confiable

Para el establecimiento del canal seguro, en primer lugar, se realiza un intercambio de las claves públicas entre la tarjeta y el terminal mediante certificados que serán verificados por ambas partes. A continuación se utiliza un protocolo de autenticación mutua, con intercambio de semillas para la derivación de una semilla común que dé lugar a las claves de sesión de cifrado y autenticación.

Una vez concluido el protocolo para el establecimiento de las claves de sesión comunes todos los mensajes deben transmitirse securizados.

Las dos opciones disponibles para el intercambio de claves están basadas en la especificación *Application Interface for smart cards used as Secured Signature Creation Devices Part 1*, y son las siguientes:

- 1) autenticación con intercambio de claves (descrita en el capítulo 8.4 de CWA 14890-1)
- 2) autenticación de dispositivos con protección de la privacidad, (descrita en el capítulo 8.5 de CWA 14890-1)

La derivación de las claves de sesión de cifrado y autenticado es conforme a la computación de claves de sesión de una clave semilla (descrita en el capítulo 8.8 de CWA 14890-1).

7.2.3. Ejemplo de instanciación del requisito

El requisito presenta las siguientes operaciones:

- Asignación: [la TSF], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.
- Asignación: [creación de firma], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.

7.2.4. Ejemplo de implementación

El ejemplo instanciado es el protocolo de transporte de clave, y la consecuente derivación de la clave de sesión, detallado en capítulo 8.4 y 8.8 de CWA 14890:

Figura 22: Protocolo de transporte de clave (Fase 1: Reconocimiento de la clave pública de la aplicación por el DNIe)

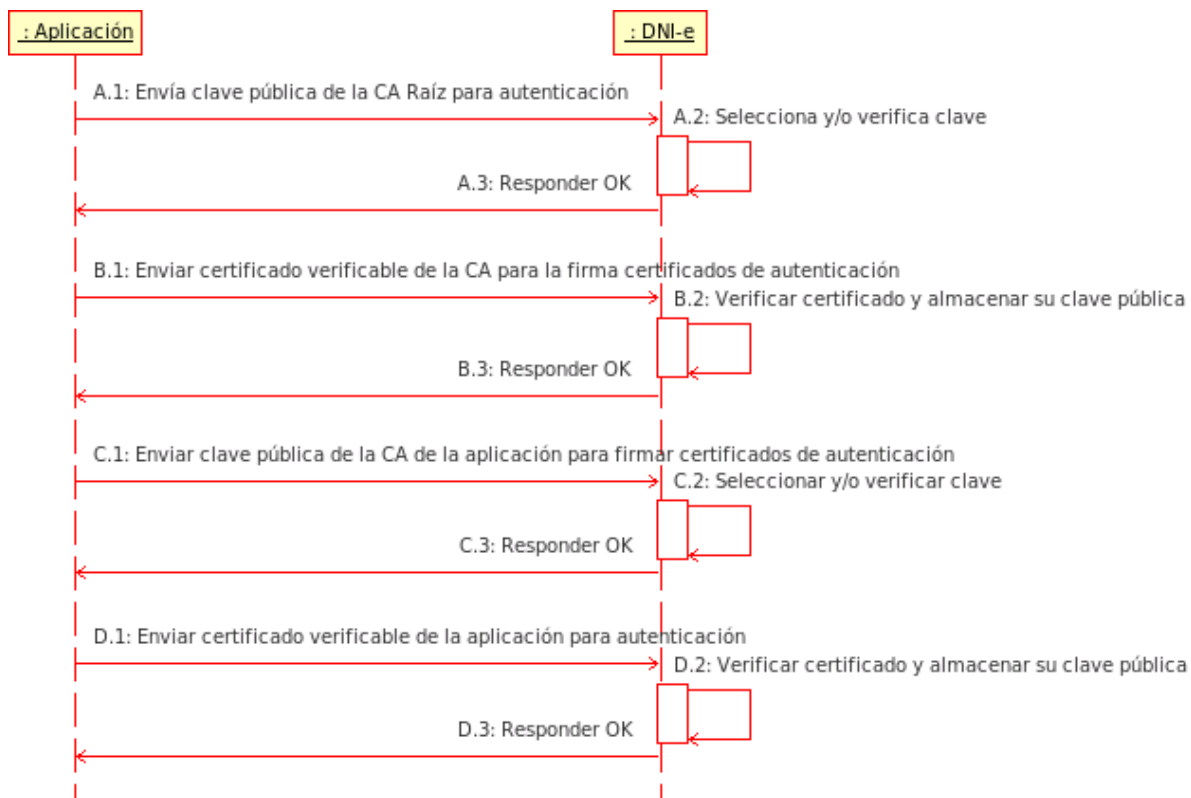


Figura 23: Protocolo de transporte de clave (Fase 2: Reconocimiento de la clave pública del DNLe por la aplicación)

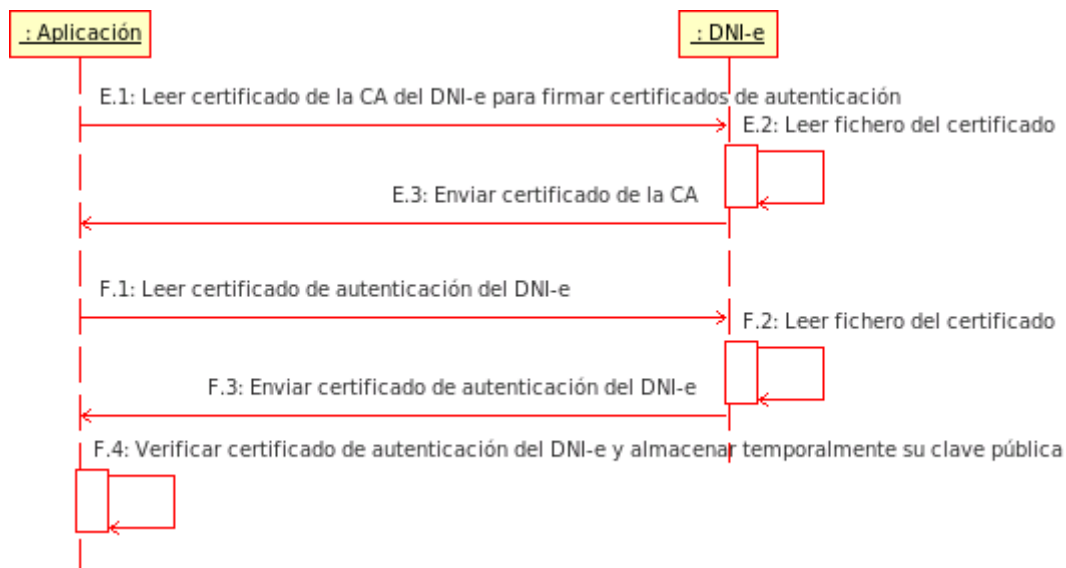


Figura 24: Protocolo de transporte de clave (Fase 3: Autenticación del DNLe por parte de la aplicación)

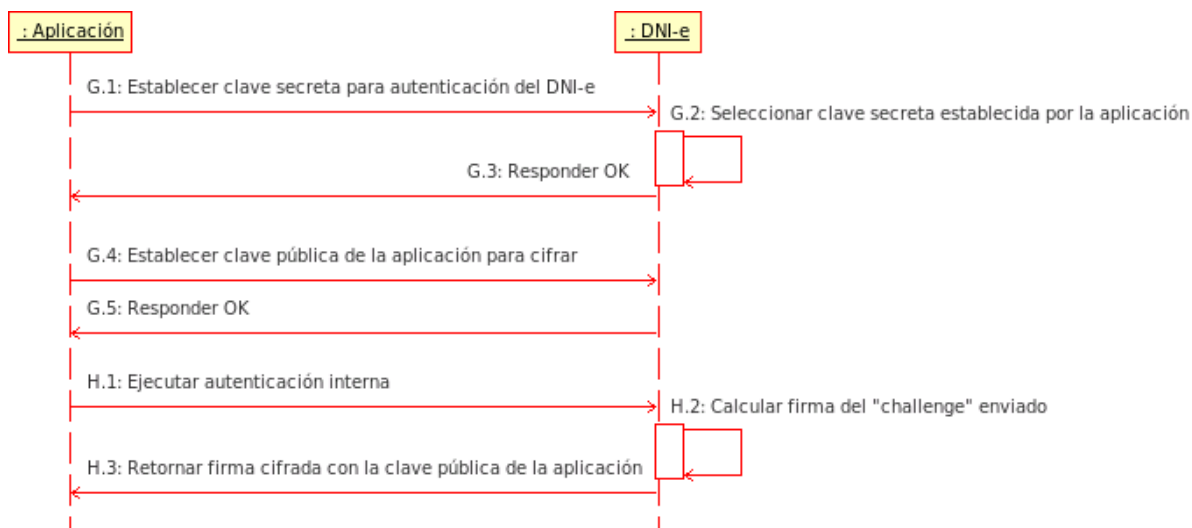


Figura 25: Protocolo de transporte de clave (Fase 4: Autenticación de la aplicación por parte del DNIe. Autenticación a dos bandas completada)

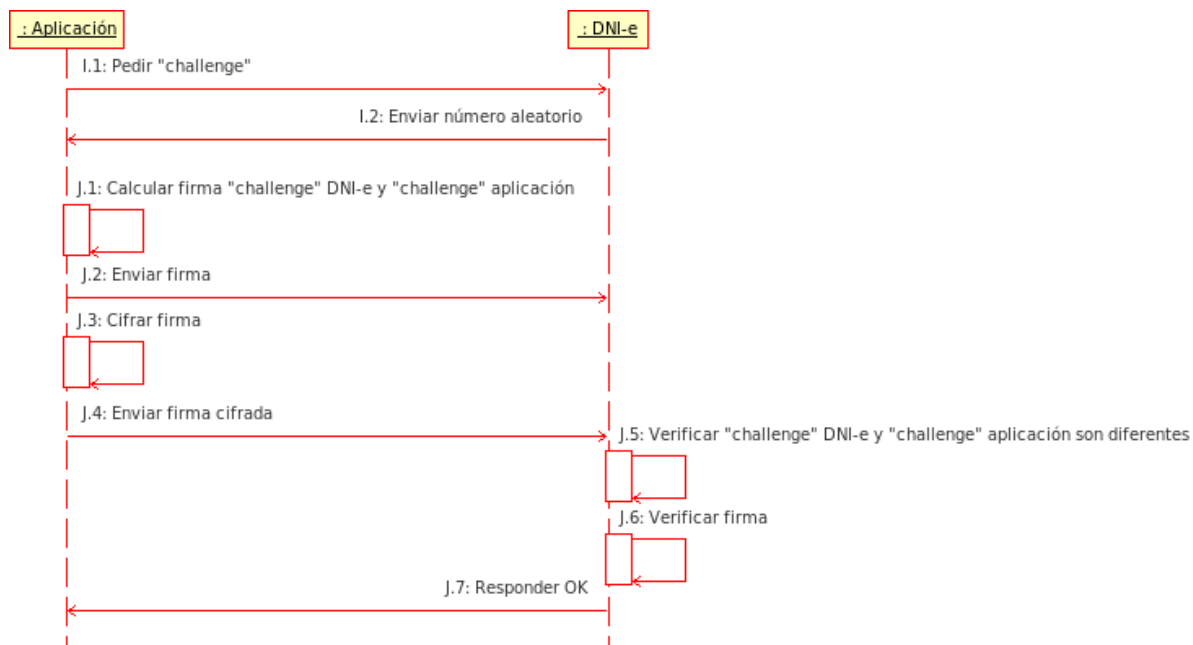
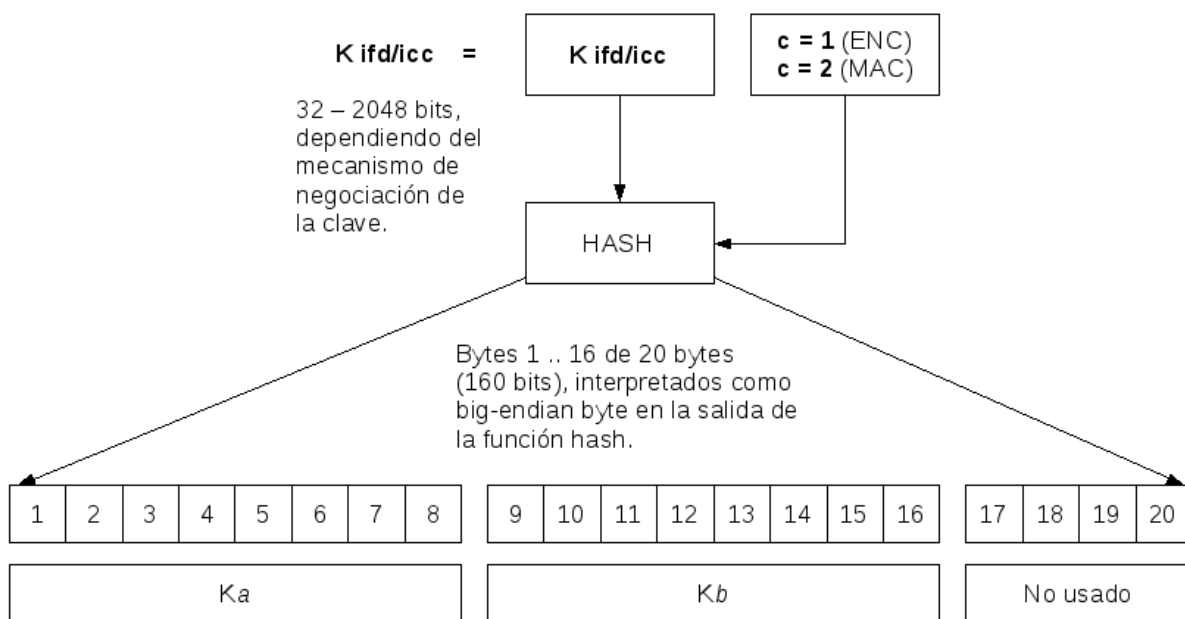


Figura 26: Protocolo de transporte de clave (Fase 5: Derivación de claves de sesión)



7.2.5. Recomendación de seguridad

Advertencia: el canal de comunicación entre el producto a evaluar y el DN_{Ie} debe ser distinto al resto de canales de comunicación usados por el dispositivo en la autenticación del firmante.

Información: la DGP establecerá en la política de certificación el criterio de aceptación de las autoridades de certificación raíz aceptadas para firmar las claves públicas utilizadas por las aplicaciones.

AVISO: todas las cuestiones relativas a la tecnología del DNle así como el procedimiento operativo a seguir para la petición y obtención del la guía de comandos y las claves para establecer el canal seguro con el DNle estarán disponibles en el Portal Oficial sobre el DNle <http://www.dnielectronico.es> del Cuerpo Nacional de Policía (DGP).
utilizadas por las aplicaciones.

7.3. FTP_ITC.1.VAD

7.3.1. Transcripción del componente

This component should be used when a trusted communication channel between the TSF and another trusted IT product is required. FTP_ITC.1 requires that the TSF provide a trusted communication channel between itself and another trusted IT product.

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 [assignment: 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 DNle].*

7.3.2. Descripción del componente

El producto a evaluar debe crear un canal confiable con el dispositivo de creación de firma segura, el DNle, para la autenticación del firmante presentando un PIN al DNle. Las características del canal seguro son:

- separación lógica de otros canales de comunicación
- proporcionar aseguramiento de la identificación de los puntos originarios del canal
- asegurar protección frente a la modificación y la alteración de datos que son transmitidos por el canal

Para el establecimiento del canal seguro, en primer lugar, se realiza un intercambio de las claves públicas de la tarjeta y el terminal mediante certificados que serán verificados por ambas partes. A continuación se realiza un protocolo de autenticación mutua, con intercambio de semillas para la derivación de una semilla común que dé lugar a las claves de sesión de cifrado y autenticado.

Una vez concluido el protocolo para el establecimiento de la semilla común todos los mensajes deben transmitirse securizados.

Las dos opciones disponibles para el intercambio de claves están basadas en la especificación *Application Interface for smart cards used as Secured Signature Creation Devices Part 1*, y son las siguientes:

- 3) autenticación con intercambio de claves (descrita en el capítulo 8.4 de CWA 14890-1)
- 4) autenticación de dispositivos con protección de la privacidad, (descrita en el capítulo 8.5 de CWA 14890-1)

La derivación de las claves de sesión de cifrado y autenticado es conforme a la computación de claves de sesión de una clave semilla (descrita en el capítulo 8.8 de de CWA 14890-1).

7.3.3. Ejemplo de instanciación del requisito

El requisito presenta las siguientes operaciones:

- Asignación: [la TSF], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.
- Asignación: [autenticación de firmante, presentando el VAD al DNle], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.

7.3.4. Ejemplo de implementación

El ejemplo instanciado es la autenticación de dispositivo con protección de la privacidad, y la consecuente derivación de la clave de sesión, detallado en capítulo 8.5 y 8.8 de CWA 14890:

Figura 27: Autenticación de dispositivo con protección de la privacidad (Fase 1: Intercambio de parámetros de Diffie-Hellman)

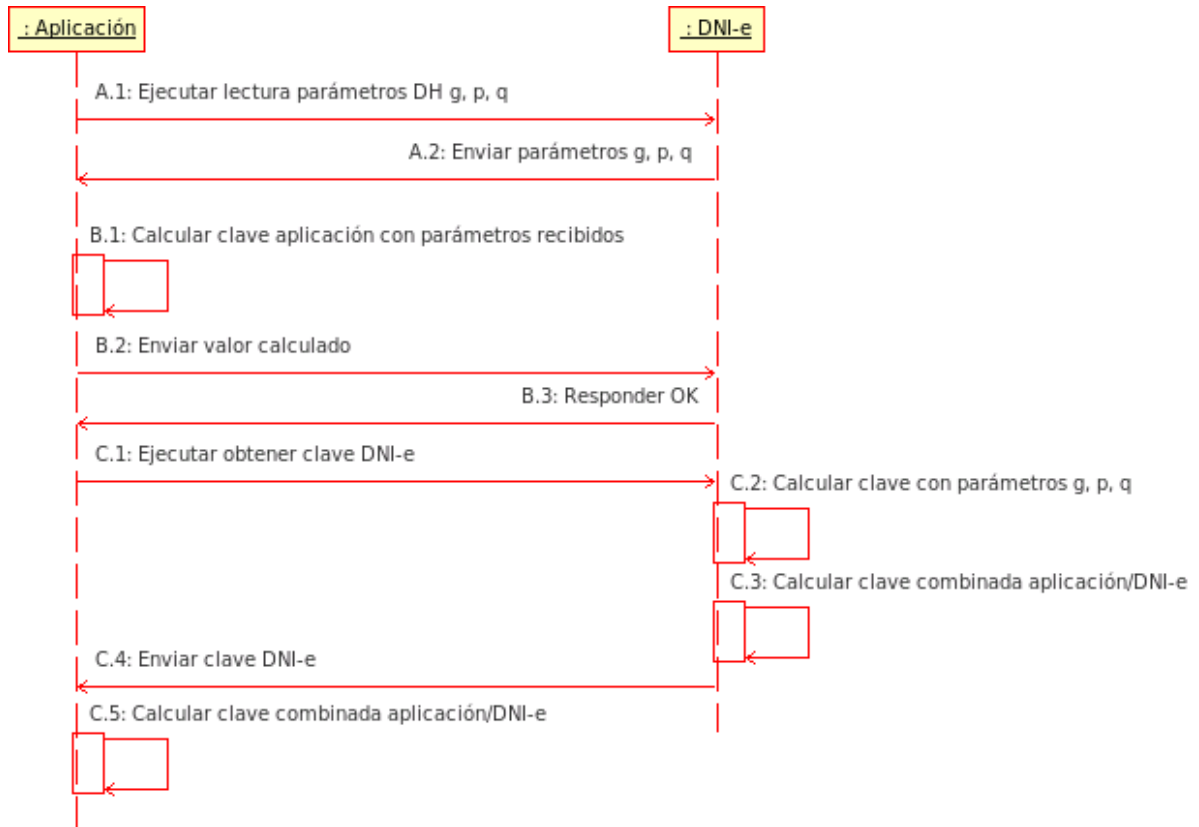


Figura 28: Autenticación de dispositivo con protección de la privacidad (Fase 2: Reconocimiento de la clave pública del DNle por la aplicación)

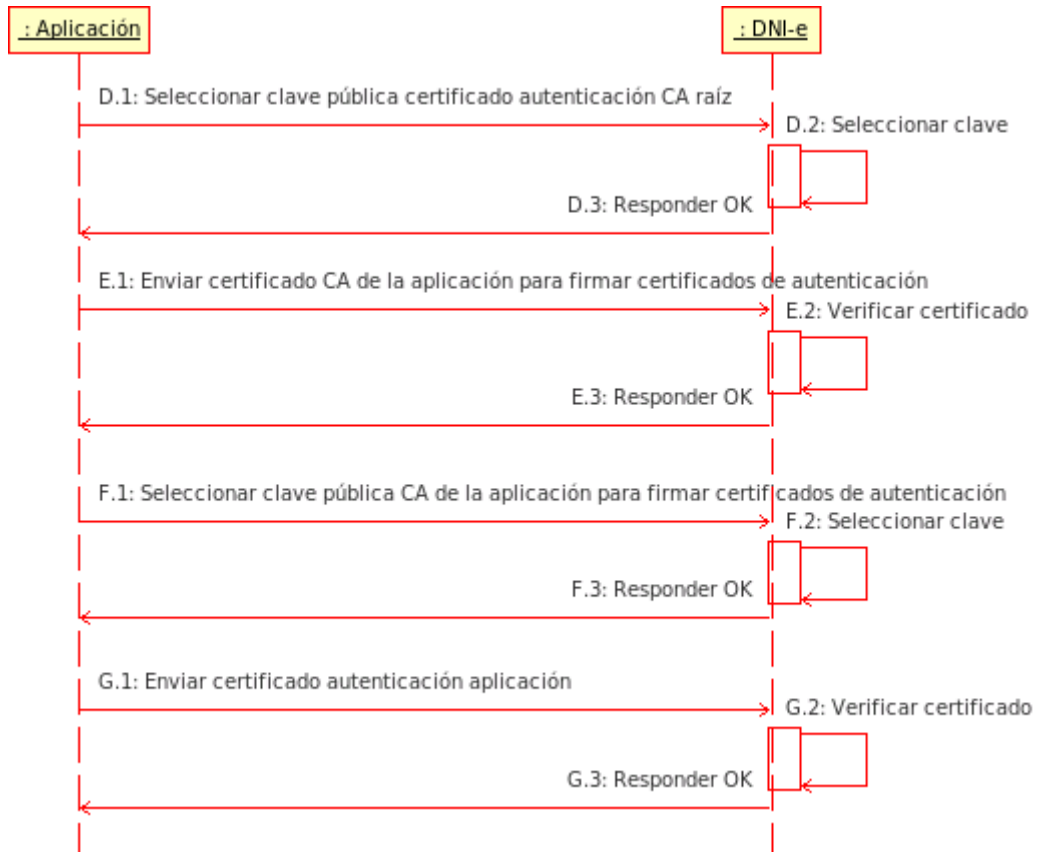


Figura 29: Autenticación de dispositivo con protección de la privacidad (Fase 3: Autenticación del DNle por parte de la aplicación – Cifrado activado)

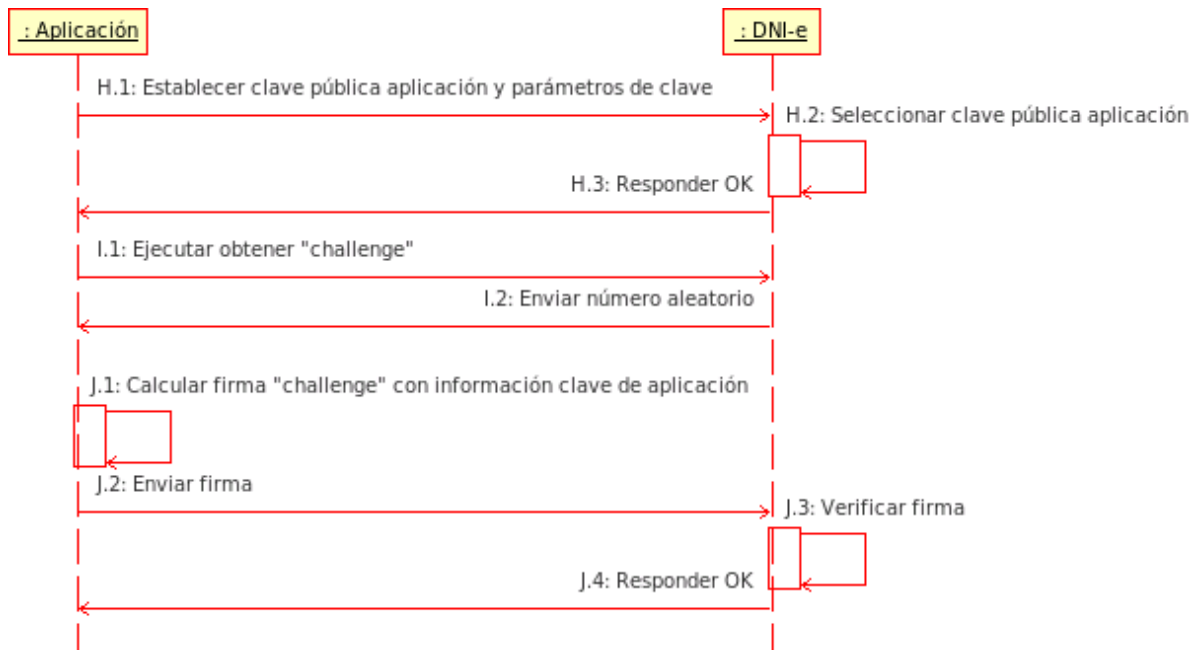


Figura 30: Autenticación de dispositivo con protección de la privacidad (Fase 4: Reconocimiento de la clave pública del DNle por parte de la aplicación)

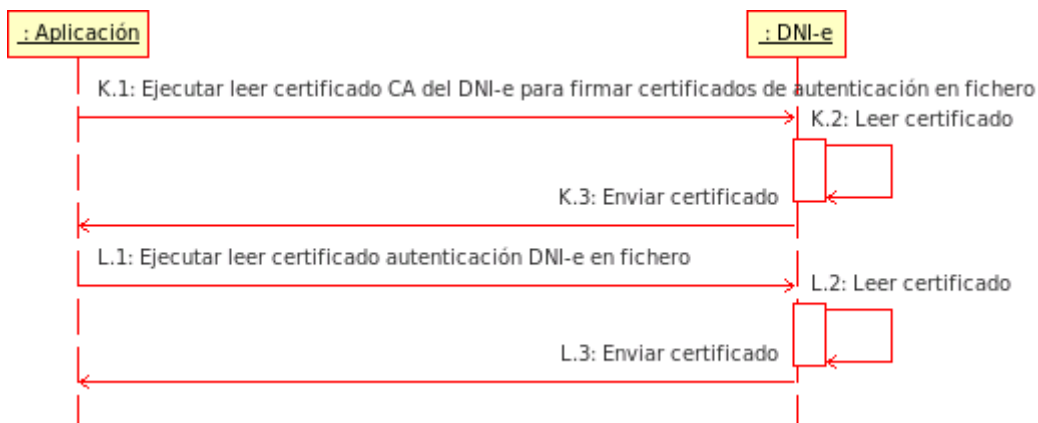


Figura 31: Autenticación de dispositivo con protección de la privacidad (Fase 5: Autenticación de la aplicación por parte del DNI-e. Autenticación a dos bandas completa)

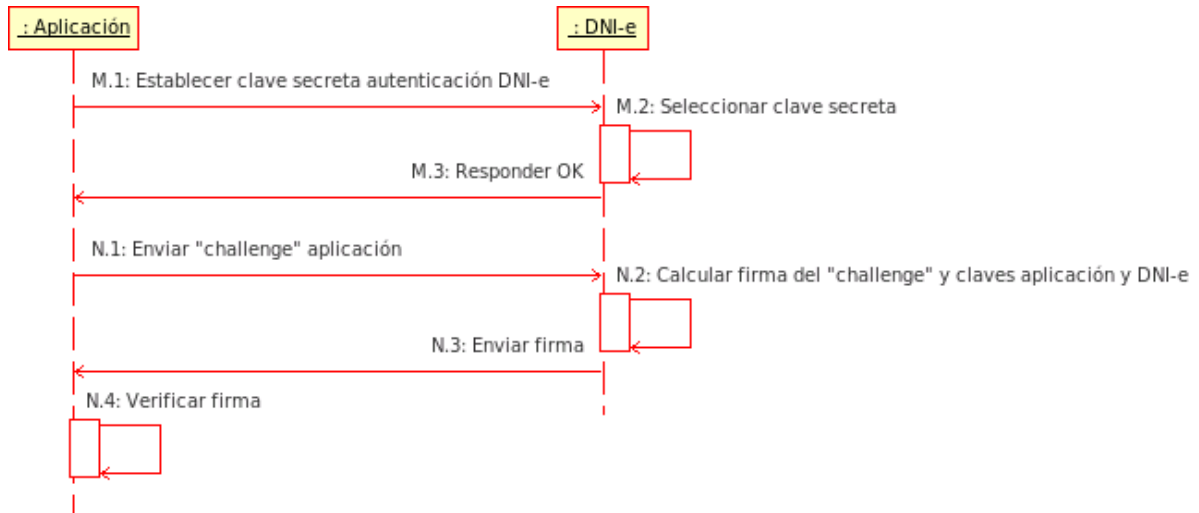
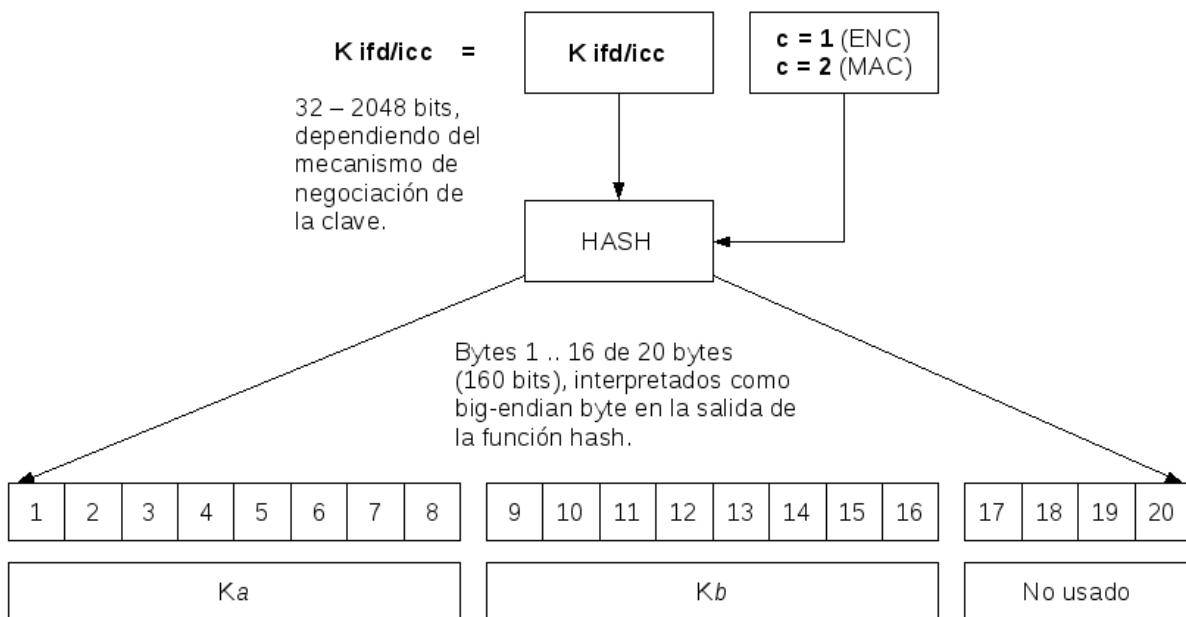


Figura 32: Autenticación de dispositivo con protección de la privacidad (Fase 6: Derivación de claves de sesión)



7.3.5. Recomendación de seguridad

Advertencia: el canal de comunicación entre el producto a evaluar y el DNle debe ser distinto al resto de canales de comunicación usados por el dispositivo en la autenticación del firmante.

Información: la DGP establecerá en la política de certificación el criterio de aceptación de las autoridades de certificación raíz aceptadas para firmar las claves públicas utilizadas por las aplicaciones.

AVISO: todas las cuestiones relativas a la tecnología del DNle así como el procedimiento operativo a seguir para la petición y obtención de la guía de comandos y las claves para establecer el canal seguro con el DNle estarán disponibles en el Portal Oficial sobre el DNle <http://www.dnielectronico.es> del Cuerpo Nacional de Policía (DGP).

7.4. FDP_RIP.1

7.4.1. Transcripción del componente

This component requires that, for a subset of the objects in the TOE, the TSF will ensure that there is no available residual information contained in a resource allocated to those objects or deallocated from those objects.

FDP_RIP.1 *Requires that the TSF ensure that any residual information content of any resources is unavailable to a defined subset of the objects controlled by the TSF upon the resource's allocation or deallocation.*

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

7.4.2. Descripción del componente

El producto a evaluar debe garantizar que el PIN no quede almacenado una vez haya finalizado la operación de firma. Es decir, se debe desasignar el recurso del producto a evaluar que almacena temporalmente el PIN y verificar que a pesar de haber sido desasignado el recurso este no permanezca accesible.

7.4.3. Ejemplo de instanciación del requisito

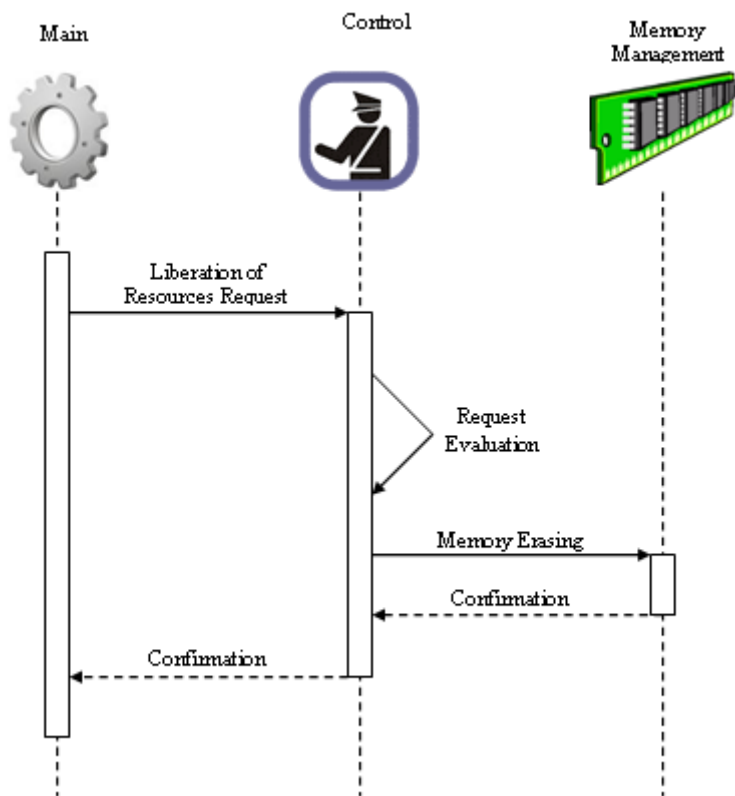
El requisito presenta las siguientes operaciones:

- Selección: [desasignación del recurso para], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.
- Asignación: [VAD], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.

7.4.4. Ejemplo de implementación

Esta guía presenta el siguiente ejemplo de diagrama de secuencia para implementar el requisito:

Figura 33: Desasignación del PIN



7.4.5. Recomendación de seguridad

Recomendación de seguridad: en caso de SCVA Tipo 2, si se usa un driver conforme con PKCS#11, la desasignación del PIN no es posible, ya que en la implantación de PKCS#11 no existe/define un método de liberalización de objetos de PIN.

7.5. FPT_TST.1

7.5.1. Transcripción del componente

This component provides support for the testing of the critical functions of the TSF's operation by requiring the ability to invoke testing functions and check the integrity of TSF data and executable code.

It is acceptable for the functions that are available to the authorised user for periodic testing to be available only in an on-line or maintenance mode. Controls should be in place to limit access during these modes to authorised users.

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 authorised users with the capability to verify the integrity of [selection: los datos de la TSF].*

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

7.5.2. Descripción del componente

El producto a evaluar debe garantizar que se realizan una serie de operaciones de autotesting durante:

- el arranque inicial, y/o
- periódicamente durante su operación normal, y/o
- por petición del firmante,

para asegurar el correcto funcionamiento del producto. Además, aportaré un método para verificar la integridad de todos los parámetros de configuración del producto y del código ejecutable.

7.5.3. Ejemplo de instanciación del requisito

El requisito presenta las siguientes operaciones:

- Selección: [durante el arranque inicial, periódicamente durante su operación normal, y, por petición del firmante], contenido seleccionable el desarrollador decide entre las opciones que se presentan pudiendo seleccionar una o más de una.

- Selección: [la TSF], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación.
- Selección: [los datos de la TSF], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación.

7.5.4. Ejemplo de implementación

Esta guía presenta distintos ejemplos de pruebas de las funcionalidades de seguridad.

Figura 34: Verificación del hash de los parámetros de configuración

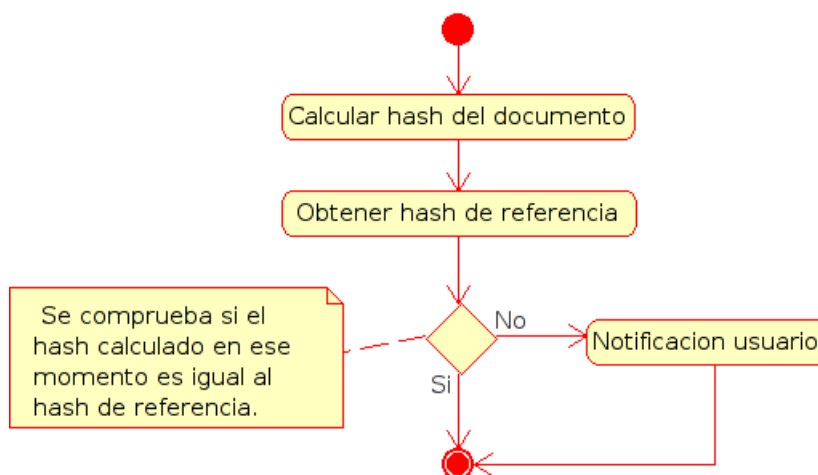
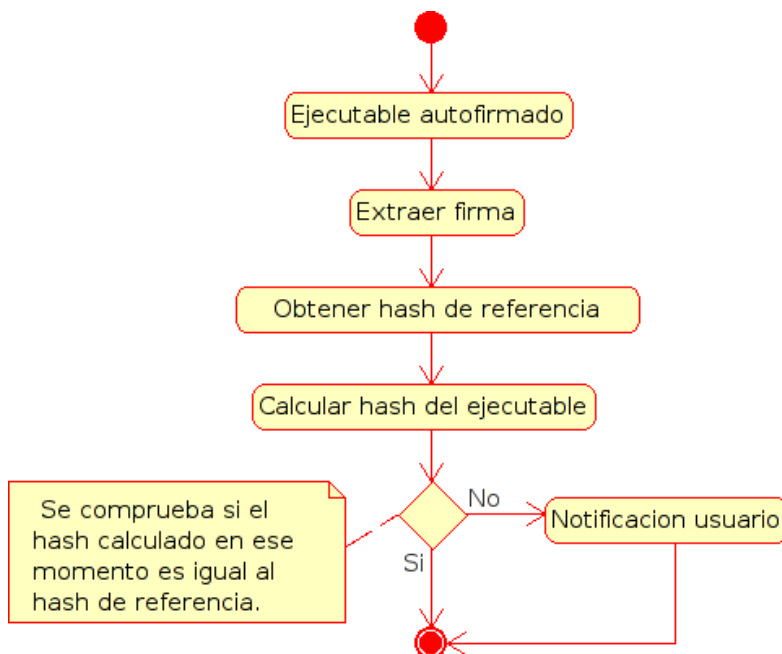


Figura 35: Verificación de código autofirmado



7.5.5. Recomendación de seguridad

Advertencia: usando métodos que proporcionan las plataformas de propósito general se puede separar dominios y comprobar la integridad del código ejecutable, un ejemplo típico es la virtualización.

7.6. FDP_SVR.1

7.6.1. Transcripción del componente

This extended component is used to specify the mechanisms for TSFmediated display of an SD 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 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.*

7.6.2. Explicación del conceptual del requisito

El producto a evaluar aportará un visor de documentos seguro, este visor debe mostrar al firmante el documento a firmar impidiendo la ocultación y/o falsificación de datos.

Este visor debe mostrar de manera correcta todos los objetos del documento, impidiendo que partes del documento no se muestren o no se visualicen correctamente.

Además el visor debe mostrar un mensaje de alerta (según lo indicado en FDP_SVR.1.2) informando del tratamiento y comunicación que se realizará sobre los datos personales que se incluirán en la firma electrónica.

Por último el visor debe confirmar la voluntad de firmar el documento mediante una captura de la voluntad expresa.

7.6.3. Ejemplo de instanciación del requisito

No existen operaciones a realizar sobre los SFR.

7.6.4. Ejemplos de implementación de FDP_SVR.1.1

Esta guía proporciona distintos ejemplos de implementación del requisito:

Texto plano UTF-8

Se presentará el texto en el visor y se representará de forma no ambigua mediante el uso de colores de fondo y la representación hexadecimal de los caracteres no representables por la interfaz de usuario y se avisará al usuario de su existencia mediante un cuadro de mensaje.

XML

Se presentará el fichero XML cómo un árbol en el que sean visibles todos los elementos, atributos, texto, instrucciones de procesamiento, secciones CDATA y comentarios. También se proporcionará una visión del XML como documento de texto plano.

Ejemplo de implementación de FDP_SVR.1.2

Mediante el interfaz de usuario del TOE se puede presentar un cuadro de mensaje que permita cancelar la operación de firma antes de realizar-la.

El mensaje a mostrar es:

«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.»

7.6.5. Recomendación de seguridad

Recomendación de seguridad: usar formatos normalizados y apoyados por una norma internacional de estandarización.

7.7. FDP_ISD.1

7.7.1. Transcripción del componente

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] when importing user data, as SDs or SDOs, from outside of the TOE, which comply with the following [assignment: de_nición de las reglas de contenido y presentación de los formatos indicados].*

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.*

7.7.2. Explicación del conceptual del requisito

El producto a evaluar debe proporcionar un mecanismo para importar el documento a firmar (SD) y el documento firmado (SDO).

Las reglas que gestionarán el mecanismo de importación serán establecidas por el autor de la declaración de seguridad.

Si se detecta un error en la importación se generará una alerta incluyendo no conformidades detectadas.

7.7.3. Ejemplo de instanciación del requisito

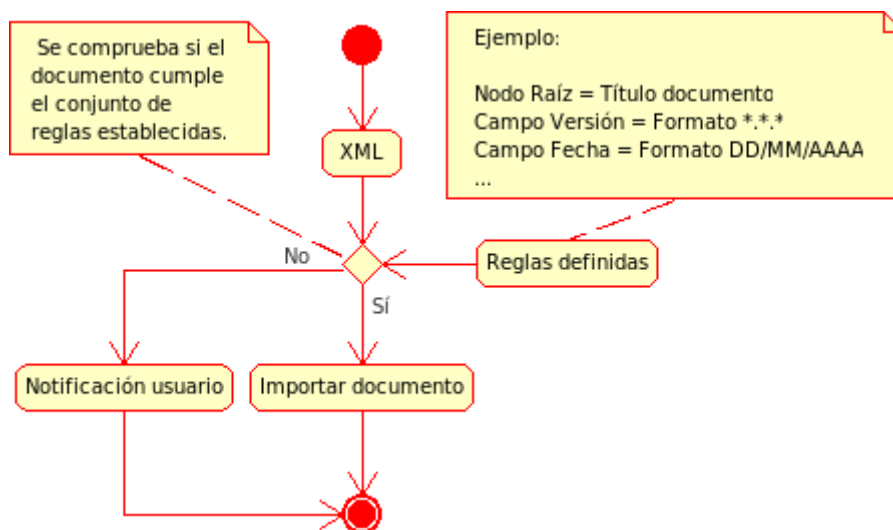
El requisito presenta las siguientes operaciones:

- Asignación: [relación de formatos de documento electrónico (a_1)], esta asignación permite establecer diferentes formatos. Ejemplos de estos pueden ser XML, PDF, etc.
- Asignación: [definición de las reglas de contenido y presentación de los formatos indicados (a_2)], esta asignación está ligada con la relación de formatos anterior y pueden ser: conformidad con XML Schema o DTD, conformidad con ISO 15929 e ISO 15930, etc.

7.7.4. Ejemplo de implementación

Esta guía presenta el siguiente ejemplo de diagrama de actividad para implementar el requisito:

Figura 36: Importación de documento a firmar (SD)



7.7.5. Recomendación de seguridad

Recomendación de seguridad: en el caso del SDO la regla de importación además debe satisfacer la correcta verificación de la firma.

7.8. FDP_ITC.1

7.8.1. Transcripción del componente

This component is used to specify the import of user data that does not have reliable (or any) security attributes associated with it. This function requires that the security attributes for the imported user data be initialised within the TSF. It could also be the case that the PP/ST author specifies the rules for import. It may be appropriate, in some environments, to require that these attributes be supplied via a trusted path or a trusted channel mechanism.

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].*

7.8.2. Explicación conceptual del requisito

El producto a evaluar incorporará un mecanismo para importar la política de certificación y otros datos de usuario necesarios para la creación o verificación de firmas.

Las reglas que gestionarán el mecanismo de importación serán establecidas por el autor de la declaración de seguridad.

7.8.3. Ejemplo de instanciación del requisito

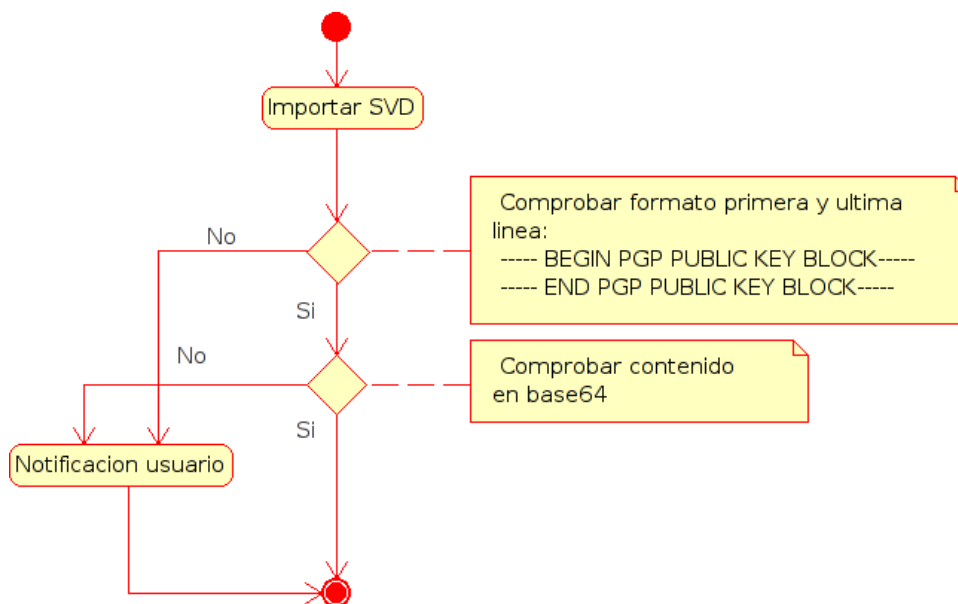
El requisito presenta las siguientes operaciones:

- Asignación: [ninguna], contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.
- Asignación: [reglas adicionales de control de la importación (a_1)], contenido a completar por el autor de la declaración de seguridad, especificando las reglas de importación de los datos de usuario, que se aplicarán en la importación de la política de certificación, SVD, y otros datos de usuario necesarios para la creación o verificación de firmas.

7.8.4. Ejemplo de implementación

El ejemplo presenta un filtro para la importación de la clave pública:

Figura 37: Importación de clave pública basada en formato



7.8.5. Recomendación de seguridad

Advertencia: el contenedor de dónde extraer la clave pública debe ser el DNle.

7.9. FCS_COP.1_SIGNATURE_CREATION_PROCESS

7.9.1. Transcripción del componente

This component requires the cryptographic algorithm and key size used to perform specified cryptographic operation(s) which can be based on an assigned standard.

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

7.9.2. Explicación del conceptual del requisito

El producto a evaluar incluirá la capacidad de guiar el proceso de generación de firma, creando un valor único generado a partir de la función resumen de un documento a ser firmado (DTBS). Posteriormente a la generación de esta representación única (DTBSR), ésta será enviada al DNle que lo firmará con un protocolo asimétrico con una longitud de clave especificada y que cumpla con el estándar RSA.

7.9.3. Ejemplo de instanciación del requisito

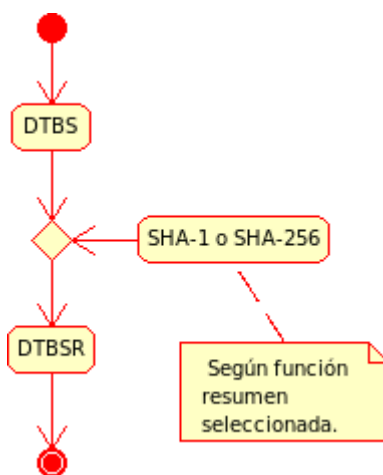
El requisito presenta las siguientes operaciones:

- Asignación: [relación de operaciones criptográficas], contenido a completar por el autor de la declaración de seguridad, especificando las operaciones criptográficas que realiza la SCVA para la generación de la función resumen, siendo éstas conformes con las aceptadas por el dispositivo de creación de firma, DNle.
- Asignación: [relación de operaciones criptográficas], contenido a completar por el autor de la declaración de seguridad, actualmente el DNle soportará SHA-1 y SHA-256.
- Asignación: [tamaños de clave], contenido a completar el autor de la declaración de seguridad, la función resumen SHA-1 y SHA-256 no utilizan clave por tanto el tamaño de claves será NULL.
- Asignación: [relación de normas], contenido ha completar el autor de la declaración de seguridad, las normas a aplicar para la función resumen SHA-1 es *FIPS 180-1 Secure Hash Algorithm* y para la función resumen SHA-256 es *FIPS 180-2 Secure Hash Algorithm*.

7.9.4. Ejemplo de implementación

Esta guía presenta el siguiente ejemplo de diagrama de actividad para implementar el requisito:

Figura 38: Generación del DTBSR



7.9.5. Recomendación de seguridad

Recomendación de seguridad: en el momento de publicarse esta guía la DGP recomienda el uso de SHA-256, aunque mantiene SHA-1 por motivos de compatibilidad con aplicaciones que tengan esta limitación.

7.10. FCS_COP.1_SIGNATURE_VERIFICATION

7.10.1. Transcripción del componente

This component requires the cryptographic algorithm and key size used to perform specified cryptographic operation(s) which can be based on an assigned standard.

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

7.10.2. Explicación del conceptual del requisito

El producto a evaluar debe proporcionar la capacidad de verificación de documentos firmados usando un protocolo asimétrico con una longitud de clave especificada y que cumpla con el estándar RSA.

7.10.3. Ejemplo de instanciación del requisito

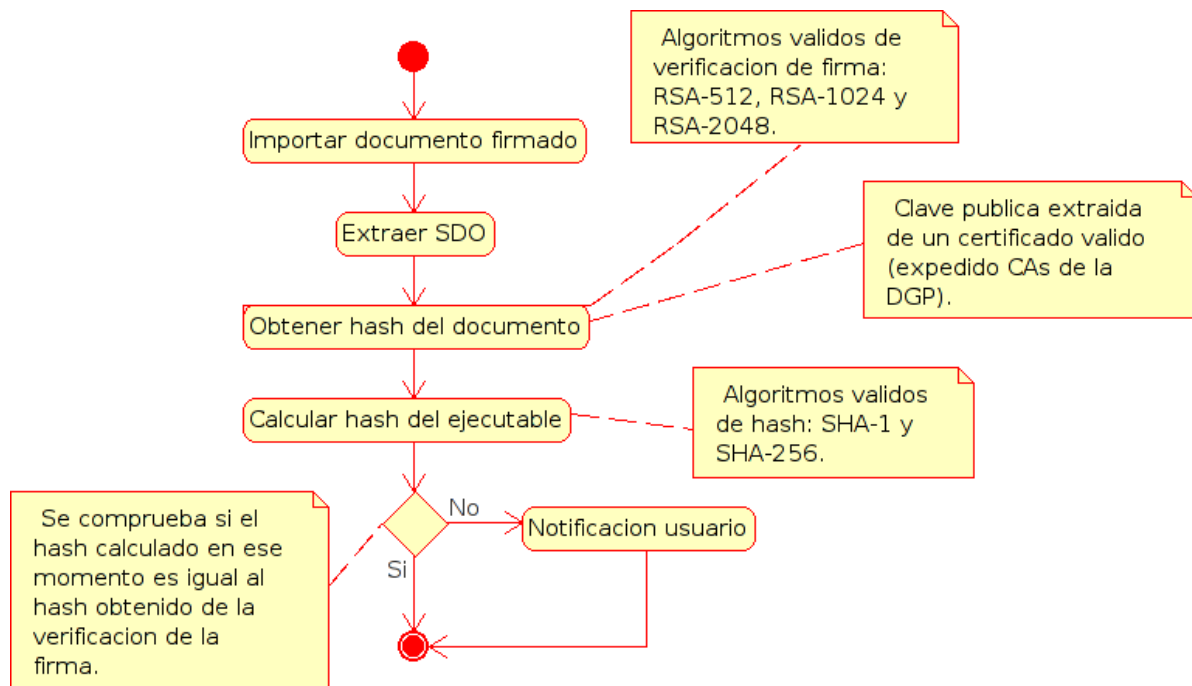
El requisito presenta las siguientes operaciones:

- Asignación: [relación de operaciones criptográficas], contenido a completar por el autor de la declaración de seguridad, especificando las operaciones criptográficas que realiza la SCVA para la verificación de la firma electrónica, siendo éstas conformes con las proporcionadas en la creación por el dispositivo de creación de firma, DNle.
- Asignación: [algoritmos criptográficos], contenido a completar por el autor de la declaración de seguridad, actualmente el DNle utiliza RSA.
- Asignación: [tamaños de clave], contenido a completar el autor de la declaración de seguridad, especificando el tamaño de las claves a utilizar, actualmente el DNle válida 512 bits, 1024 bits y 2048 bits.
- Asignación: [relación de normas], contenido ha completar el autor de la declaración de seguridad, en el momento de publicarse esta guía el DNle utiliza el estándar PKCS#1.

7.10.4. Ejemplo de implementación

Esta guía presenta un ejemplo de verificación de firma:

Figura 39: Verificación de un documento firmado siguiendo la política de clave pública del DNI electrónico



7.10.5. Recomendación de seguridad

Recomendación de seguridad: la longitud de clave 512 bits para el algoritmo RSA se considera insegura.

8. REFERENCIAS

- 1) España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, 14 de diciembre de 1999.
- 2) España. Ley 59/2003, de 19 de diciembre, de firma electrónica DNle. *Boletín Oficial del Estado*, 20 de diciembre de 2003.
- 3) España. 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. *Boletín Oficial del Estado*, 24 de diciembre 2005.
- 4) CEN. Dispositivo seguro de creación de firma electrónica EAL4+. CWA 14169. Bruselas: CEN, marzo 2004.
- 5) CEN. Interfaz de aplicación para tarjetas inteligentes usadas como dispositivos de creación de firma segura. CWA 14890. Bruselas: CEN, marzo 2004.
- 6) Infraestructura de clave pública DNI electrónico, proyecto de declaración de prácticas y políticas de certificación, versión 1.0, 6 de marzo 2006
- 7) INTECO. 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. PPSCVA-T1-EAL1. Madrid: INTECO, 2008.
- 8) INTECO. 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. PPSCVA-T1-EAL3. Madrid: INTECO, 2008.
- 9) INTECO. 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 PPSCVA-T2-EAL1. Madrid: INTECO, 2008.
- 10) INTECO. 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 PPSCVA-T2-EAL3. Madrid: INTECO, 2008.

- 11) ISO/IEC. Text for ISO/IEC 3rd WD 15446. Information Technologies - Security Techniques. Guide for the production of protection profiles and security targets. JTC 1/SC27 N5792. Berlin: ISO/IEC, 14 de septiembre 2007.
- 12) Common Criteria. Common Criteria for Information Security Evaluation. Part 1: Introduction and general model. V. 3.1, Release 1 [en línea] CCMB-2006-09-001. <http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf>, [consulta:25/11/2008]
- 13) Common Criteria. Common Criteria for Information Security Evaluation. Part 2: Security Functional Requirements. V. 3.1, Release 2 [en línea] CCMB-2007-09-002 <http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf> [consulta:25/11/2008]
- 14) Common Criteria. Common Criteria for Information Security Evaluation. Part 3 Security Assurance Requirements. V. 3.1, Release 2 [en línea] CCMB-2007-09-003 <http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R2.pdf> [consulta:25/11/2008]
- 15) Common Criteria. Common Methodology for Information Security Evaluation. V. 3.1 Release 2, CCMB-2007-09-004 [en línea] <http://www.commoncriteriaportal.org/public/files/cemv3.1.pdf> [consulta:25/11/2008]
- 16) Herrmann, D.S. Using the Common Criteria for IT Security Evaluation, Auerbach Pub., 2003.