inDenova

Workflow empresarial
Firma Electrónica
Portal web corporativo
Videoconferencia web

Integración de sistemas
Facturación electrónica
Almacenamiento confidencial
Aplicaciones PDA

Título	**eSigna Crypto 2.1.1 - Declaración de Seguridad**

Realizado por	**Indenova SL**		
Fecha	09/02/2012	Versión	1.9

AENOR
ER
Madurez Software 2
ISO/IEC 15504

Dels Traginers, 14 - 2ºB
Pol. Ind. Vara de Quart
46014 Valencia
Tel. (34) 96 381 99 47
Fax (34) 96 381 99 48
indenova@indenova.com
http://www.indenova.com

Histórico de versiones

Versión	Fecha	Comentario
1.0	18/08/2011	Versión inicial
1.1	27/09/2011	Correcciones declaración de seguridad, añadido el apartado TOE Summary Specification
1.2	05/10/2011	Modificación funcionalidad webservice seguro
1.3	20/10/2011	Correcciones ESIG-OR-001, ESIG-OR-002, ESIG-OR-003, ESIG-OR-004
1.4	30/11/2011	Adaptación para PP-SCVA-T1
1.5	01/12/2011	Modificación para PP-SCVA-T2
1.6	22/12/2011	Modificaciones requisitos seguridad
1.7	16/01/2012	Correcciones ESIG-OR-001, ESIG-OR-002, ESIG-OR-003, ESIG-OR-004
1.8	31/01/2012	Correcciones ESIG-OR-009 y ESIG-OR-010
1.9	09/02/2012	Corrección versión navegador soportado

1 INTRODUCCION

El propósito de este ST es especificar los requisitos funcionales y de seguridad implementados por **eSigna Crypto 2.1.1**, que es el objetivo de la evaluación.

El producto **eSigna Crypto 2.1.1** es un sistema que permite realizar operaciones de firma y verificación empleando el **DNIe**.

El contenido de este documento se organiza en los siguientes apartados:

1. **Introducción:** proporciona información etiquetada y descriptiva sobre el ST y del TOE.
2. **Declaración de conformidad:** proporciona una descripción de los servicios del TOE, da una vista general de los usuarios de TOE que interactuarán con él y describe la disposición de las arquitecturas físicas y lógicas del sistema.
3. **Definición del problema de seguridad:** proporciona una definición del problema de seguridad, mostrando los activos, amenazas y políticas de seguridad que deben ser sostenidas por el TOE y su entorno operacional.
4. **Objetivos de seguridad:** contiene la solución al problema de seguridad, proporcionando los objetivos de seguridad para el TOE y su entorno.
5. **Definición de componentes extendidos:** incluye su definición.
6. **Requisitos de seguridad:** proporciona los requisitos de seguridad funcionales y de garantía para el TOE y su entorno.
7. **TOE Summary Specification:** en dicho apartado se describen las funciones de seguridad que satisfacen esos requisitos.
8. **Bibliografía y Acrónimos:** se incluye un glosario de términos utilizados en el documento y una lista de acrónimos.

1.1 IDENTIFICACIÓN DE LA DECLARACIÓN SEGURIDAD

Título:	eSigna Crypto 2.1.1 – Declaración de Seguridad
Versión:	1.9
Autor:	Indenova SL
Fecha:	09 de Febrero de 2012

1.2 IDENTIFICACIÓN DEL TOE

TOE:	eSigna Crypto 2.1.1
Versión:	2.1.1
Autor:	Indenova SL
Identificación CC:	Common Criteria v3.1
EAL:	Common Criteria v.3.1 EAL1

1.3 DESCRIPCIÓN GENERAL

El TOE referenciado en esta declaración de seguridad **eSigna Crypto 2.1.1** consiste una aplicación de creación y verificación de firma electrónica (SCVA) que emplea el **DNIe** como dispositivo seguro de creación de firma (SSCD).

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

- Seleccionar un documento o texto para firmar (SD)
- Seleccionar la política de firma a aplicar, los atributos de la firma, y el certificado a utilizar para la firma, y componer los DTBS
- Mostrar de manera no ambigua los DTBS al firmante, para un número determinado de formatos de documento electrónico, y de detectar formatos o construcciones problemáticas, en cuyo caso rechaza la operación de creación de firma de estos documentos
- 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
- Asociar la firma electrónica creada por el SSCD al propio documento firmado, o de facilitar la firma realizada como datos separados
- 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 formas válidas e inválidas, cuando el proceso de verificación haya podido realizarse, e identificará las firmas que no han podido verificarse.

Las comunicaciones entre la SCVA y el DNIe se suponen securizadas por la propia SCVA, cumpliendo además con los requisitos exigibles por el perfil de protección **CWA 14169** que se aplica al DNIe.

El TOE recibe el SD a través de uno de sus interfaces. El TOE dispone de interfaces de comunicaciones a redes confiables, vía HTTPS, y a interfaces a dispositivos locales, tales como discos o lectores de tarjetas de memoria como lectores de **DNIe** compatibles con **CWA 14169**. Un interfaz que siempre implementará el TOE es el interfaz propio al **DNIe**.

El TOE muestra el DTBS al firmante, de tal manera que su contenido no pueda ser malinterpretado, y que no tenga contenido oculto o ambiguo en su representación. En la declaración de seguridad se especifican los tipos de formato de documento electrónico que son capaces de presentar de manera fiable al firmante, y se detallan ciertos requisitos adicionales a esta presentación.

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

eSigna Crypto también es capaz de verificar una firma electrónica. Para ello, permite la selección de documentos firmados desde el sistema de ficheros local. El TOE mostrará al usuario si el documento seleccionado corresponde a un formato de firma válido para la verificación o no (en la declaración de seguridad se detallan los tipos de formato de firma válidos para la verificación). En el caso que el formato de firma a verificar sea válido, se mostrará al usuario el resultado de la firma.

En la siguiente figura se puede ver un resumen de los elementos que forman parte del TOE así como otros que son parte del entorno operacional:

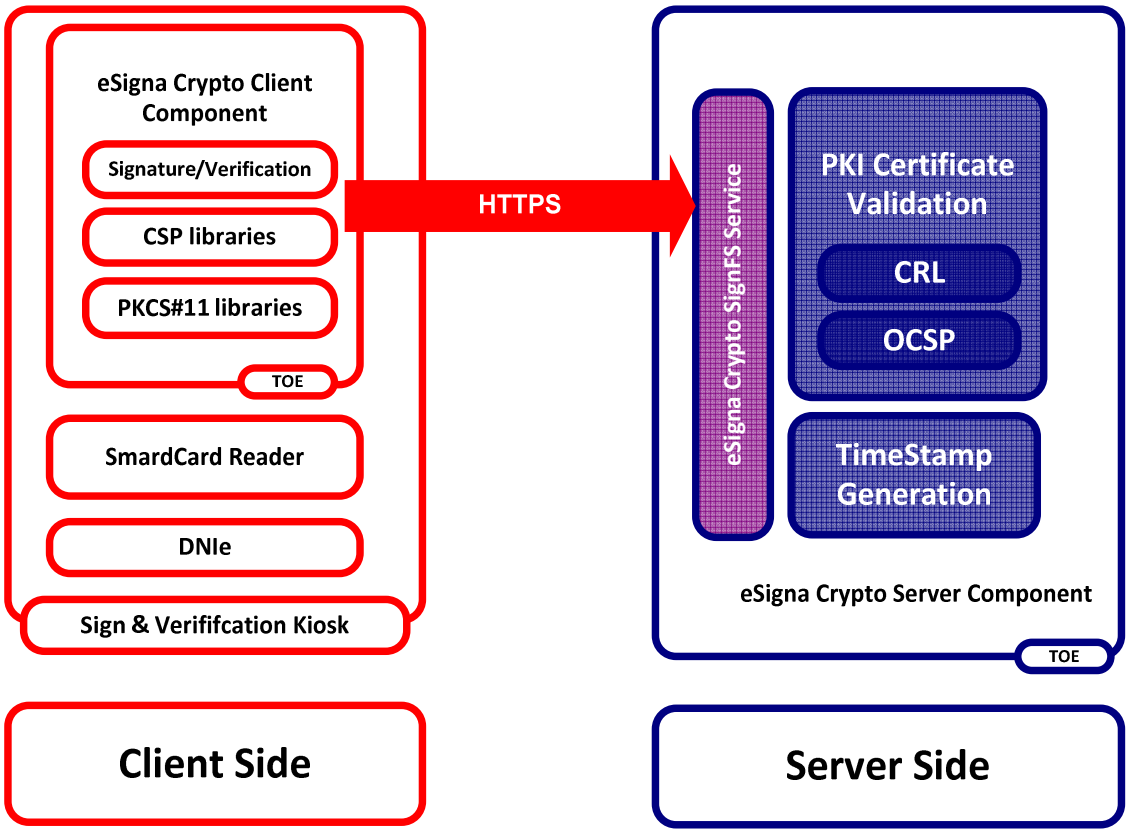


Figura 1. Arquitectura eSigna Crypto

La aplicación **eSigna Crypto 2.1.1** está compuesta por los siguientes componentes:

- **eSigna Crypto Client Component:** se trata de un componente que se ejecuta en el navegador web del cliente. Este componente se trata de un punto de entrada que incorpora la lógica de comunicación con el componente servidor **eSigna Crypto Server Component.**
- **eSigna Crypto Server Component:** este componte reside en servidor y se encarga básicamente de la composición del objeto XAdES. Este componente ofrece al **eSigna Crypto Client Component,** una interfaz web service a través la cual se comunica.

eSigna Crypto 2.1.1 es un servicio accesible a través de la web, en concreto a través de un navegador utilizando *Java Applets*. La parte cliente se encontrará desplegada en un entorno cerrado, un **kiosko de firma y verificación**, en el que los usuarios solamente puedan acceder a los servicios del sistema necesarios para la firma y verificación empleando el **DNIe**. En este caso, se dotará en la máquina cliente de la política de permisos necesaria para que los usuarios puedan acceder a dichos servicios. El usuario dispondrá de un directorio de trabajo en el que podrá almacenar las firmas realizadas y seleccionar los ficheros a verificar. La implementación y configuración de estas políticas se verán en mayor detalle en el **documento de instalación** o **guía preparativa**.

Los componentes web, *Java Applets*, son componentes que permiten su utilización en distintas plataformas y en cualquier sistema operativo para el cual exista una máquina virtual de Java. El usuario interacciona con el sistema a través de estos componentes, acoplados en una página web. Estos componentes corresponden con el componente **eSigna Crypto Client Component**. Este componente contiene la implementación de los servicios de criptografía básicos que requieren comunicación con el dispositivo de creación de firma, el **DNIe**, mediante **CSP** o **PKCS#11**. El acceso del componente cliente al **DNIe** se realizará empleando los **drivers CSP/ PKCS#11** distribuidos por el **Ministerio del Interior y la Dirección General de la Policía y de la Guardia Civil**. El proceso de intalación de estas librerías y manejadores se verá con mayor detalle en el **documento de instalación** o **guía preparativa**.

Cuando el usuario accede a la plataforma web por primera vez, el navegador procederá a la descarga automática de los *Java Applets* necesarios para realizar la operación de **firma electrónica**. Estos componentes se encuentran firmados adecuadamente con un certificado válido de firma de código.

eSigna Crypto Server Component contiene la implementación de servicios como validación CRL/OCSP de los certificados digitales y aplicación de sellados de tiempo opcionales.

La comunicación entre el **componente cliente** y **servidor** se realiza a utilizando un protocolo seguro **HTTPS** que proporciona **confidencialidad** en la transmisión de información crítica al **componente servidor** como son los **documentos del firmante, datos de verificación de firma** y **datos a ser firmados**. Respecto a los datos de **verificación de autenticación** como el PIN del **DNIe** o datos de **creación de firma** como la clave privada del **DNIe** nunca se transmiten a la parte servidora, preservando la confindencialidad de los mismos.

En el componente cliente, también se adoptan medidas para garantizar la **integridad** tanto del **documento del firmante** como de los **datos a ser firmados**. Para ello se realizan recalculos de resúmenes y verificación del certificado firmante en servidor.

El usuario puede firmar **una cadena de texto ASCII** o un **fichero en formato XML** que cumpla un esquema propio denominado **FormSchema.**

Los formatos de firma aceptados por **eSigna Crypto 2.1.1** son:

- **XAdES-BES**
- **XAdES-T**
- **XAdES-XL**

En el caso de formatos **XAdES-T** y **XAdES-XL** se aplica como autoridad de sellado de tiempo (TSA) la **ACCV**. La versión de **XAdES** generada es la **1.2.2**[1] **attached**. En el caso de los documentos **XML** se aplicará una firma **enveloped**, incluyéndola en un nodo **signatures**. En caso de firmar un mensaje **texto ASCII** se empleará siempre una firma **enveloping**.

En el caso de verificación de firma electrónica, se aceptarán los siguientes formatos de firma:

- **XAdES-BES**
- **XAdES-T**
- **XAdES-XL**

Se verificarán firmas **attached** tanto **enveloping** y **enveloped**, en formatos de **XAdES 1.2.2**. Se empleará el **DNIe** como dispositivo de verificación de la firma. Para ello, el usuario seleccionará un documento firmado de la carpeta de trabajo y procederá a su verificación.

[1] XML Advanced Electronic Signatures XAdES - ETSI TS 101 903 V1.2.2 (2004-04)

Elementos del entorno operacional del TOE

A continuación, se definen los elementos del entorno operacional del TOE:

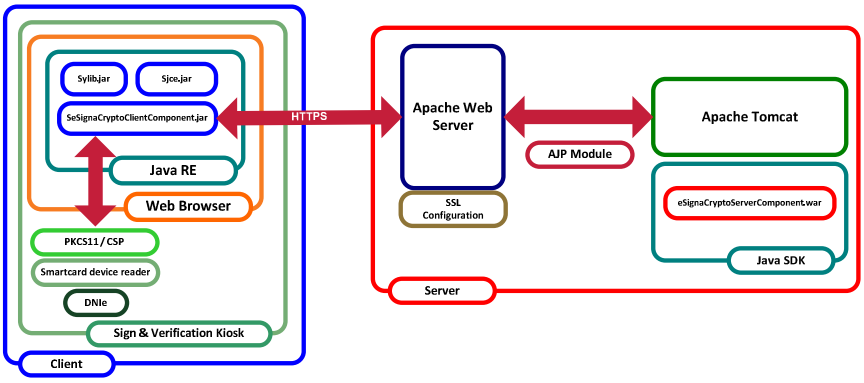


Figura 2. Elementos del entorno operacional

Parte cliente	
Sistema operativo	Microsoft Windows XP Professional
Plataforma hardware	Procesador: Doble núcleo 2GHz o superior Memoria: 2GB o superior Disco duro: 10GB o superior 3 Puertos USB 1.0 o superior disponibles
Navegador web	Internet Explorer 6
Máquina virtual de Java – plugin para navegador	Java Runtime Environment (JRE) versión 1.5 o superior
Dispositivo criptográfico – Lector de tarjetas inteligentes	Cumplimiento de los estándares ISO 7816 (1, 2 y 3) y los API PC/SC, CSP y PKCS#11
DNIe	DNIe del firmante/ verificador

Parte servidora	
Sistema operativo	Ubuntu 10.04 LTS
Plataforma hardware	Procesador: Doble núcleo 2GHz o superior

	Memoria: 2GB o superior Disco duro: 10GB o superior
Servidor web	Apache HTTP Server 2.0 o superior
Contenedor web JavaEE	Apache Tomcat 7.0
Máquina virtual Java	Java Development Kit (JDK) versión 6

1.4 DESCRIPCIÓN DEL TOE

1.4.1 ALCANCE FÍSICO DEL TOE

En la siguiente tabla se especifican los componentes que forman parte del TOE y que, por lo tanto, son objetos de la evaluación:

Parte cliente	
Client Component	SeSignaCryptoClientComponent.jar
Parte servidora	
Server Component	eSignaCryptoServerComponent.war

El elemento **SeSignaCryptoClientComponent.jar** es un archivo JAR que contiene el componente Java Applet que se ejecuta en el navegador y que interactúa con la parte servidora. Las dependencias de esta librería como son Sjce.jar y Sylib.jar no forman parte del TOE.

El elemento **eSignaCryptoServerComponent.war** es un archivo WAR que contiene la implementación web service de los servicios de criptografía relacionados con la firma electrónica. Este WAR dispone de dependencias de librería de terceros y de Indenova SL que no forman parte de la evaluación del TOE.

1.4.2 ALCANCE LÓGICO DEL TOE

La funcionalidad del TOE es la firma electrónica empleando formatos **XAdES-BES**, **XAdES-T** y **XAdES-XL** y la verificación de las mismas mediante **DNIe**. En el caso de los formatos avanzados **XAdES-T** y **XAdES-XL** se le aplicarán de forma automática un sellado de tiempo utilizando el servicio de la **ACCV** (Autoridad Certificadora de la Comunidad Valenciana).

Los datos objeto a firmar pueden ser:

- Un documento XML que valide un formato determinado de Indenova S.L
- Una cadena de texto

Para ello el usuario introducirá el objeto a firmar, tanto si es una cadena de texto o un documento XML, e indicará si el formato es texto plano o XML, el formato de firma (**XAdES-BES**, **XAdES-T** o **XAdES-XL**) y si desea que el resultado de la firma se almacene en disco o no.

Cuando el usuario introduce el mensaje a firmar, se le mostrará una visualización especial que no permita la ocultación o falsificación de esos datos. Para ello se utilizará una representación en **UNICODE** junto al resumen **SHA-1** de los mismos. El sistema incorpora mecanismos para detectar formatos de datos objeto incorrectos.

El TOE dispone, además, de mecanismos de control para verificar la integridad de los diferentes datos de usuario:

- Comunicación vía **HTTPS**: el documento a firmar, los atributos de firma, datos a firmar y el documento firmado viajan sobre un protocolo seguro de manera que se garantiza la integridad de los mismos.
- Verificación de los datos originales con los originales extraídos de la firma utilizando la comparación de resúmenes **SHA-1.**
- Protección del **PIN** del DNIe mediante la desasignación de memoria de los objetos que contienen información sobre el mismo.

La comunicación entre el componente cliente y el **DNIe** se realiza empleando un canal confiable según especifica el estándar **CWA 14890-1** en el que, los datos a firmar y el PIN, quedan protegidos por el mismo.

Tras el resultado de la firma, se presentará al usuario el resultado de la misma y se almacenará el fichero resultado de firma **XAdES** en un el sistema de ficheros del usuario en el caso de haber seleccionado la opción correspondiente. El usuario además podrá comparar el mensaje original a firmar con el extraido de la firma, sus resúmenes **SHA-1** y la visualización en formato **UNICODE** para evitar cualquier tipo de ambigüedad en lo que se refiere al mensaje objeto de firma.

El usuario podrá verificar documentos firmados empleando formatos **XAdES-BES**, **XAdES-T** y **XAdES-XL attached** (**enveloping** o **enveloped**) **versión 1.2.2** utilizando como dispositivo de verificación el **DNIe**. Para ello, el usuario seleccionará un fichero firmado del directorio de trabajo, y se procederá a su verificación. En el caso de que el fichero firmado cumpla con los requisitos de formato de firma, se mostrará el resultado de la verificación.

Antes de efectuar las operaciones de firma y/o verificación y bajo petición del usuario, se realizarán testeos que comprobarán la integridad de los componentes cliente y servidor, integridad de las librerias de comunicación con el **DNIe**, testeo de comunicación con componente servidor y pruebas básicas de firma utilizando un certificado embebido en el componente contra servidor.

2 DECLARACIÓN DE CONFORMIDAD

2.1 CONFORMIDAD CON RESPECTO A LA NORMA COMMON CRITERIA

[CC-1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 July 2009. Part 1: Introduction and general model.

[CC-2] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 July 2009. Part 2: Functional security components.

[CC-3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 July 2009. Part 3: Assurance security components.

Esta declaración de seguridad se ha redactado conforme a la norma Common Criteria **[CC-1]**, **[CC-2] extendida** y **[CC-3].**

2.2 CONFORMIDAD RESPECTO A OTROS PERFILES DE PROTECCIÓN

Esta declaración de seguridad declara también el cumplimiento del Perfil de Protección para la aplicación y verificación de firma electrónica Tipo 2, con nivel de evaluación de requisitos EAL1:

[PPSCVA-T2-EAL1] Perfil Protección SCVA Tipo 2 EAL 1, v.2.0

Esta declaración de seguridad está basada siguiendo la distribución de secciones incluidas en el perfil **[PPSCVA-T2-EAL1]**. Existen secciones que son réplicas exactas, como son las siguientes:

3. DEFINICIÓN DEL PROBLEMA DE SEGURIDAD

4. OBJETIVOS DE SEGURIDAD

5. DEFINICIÓN DE COMPONENTES EXTENDIDOS

6.2. REQUISITOS DE GARANTÍA DE SEGURIDAD

6.3. JUSTIFICACIÓN DE LOS REQUISITOS FUNCIONALES DE SEGURIDAD

6.4. DEPENDENCIAS DE LOS REQUISITOS FUNCIONALES DE SEGURIDAD

6.5. JUSTIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD

La sección **6.1. REQUISITOS FUNCIONALES DE SEGURIDAD** se ha adaptado para incorporar los mapeos correspondientes de la SCVA **eSigna Crypto.**

3 DEFINICIÓN DEL PROBLEMA DE SEGURIDAD

3.1 ACTIVOS A PROTEGER POR ESIGNA CRYPTO

A.DSCVA

La **integridad y representación no ambigua** del **documento del firmante** (SD), así como de sus representaciones intermedias, como los **datos a ser firmados** (DTBS), mientras se remite al **DNIe** y están en posesión de la SCVA.

De igual manera, **la integridad de todos los datos de usuario necesarios para las operaciones de creación o verificación de firma**, tales como:

- **Datos de creación de firma** (SCD) – clave privada para realizar una operación de firma electrónica
- Los **datos de verificación de la firma** (SVD) – clave pública asociada
- **Las políticas de firma aplicadas**
- Los **datos de verificación de autenticación** (VAD)

A.SCVA

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

A.VAD

La **confidencialidad** de los **datos de verificación de autenticación** (VAD), que se transmiten al **DNIe** para la realización de la operación de firma. En este caso, el número de identificación personal (PIN).

3.2 AMENAZAS

T.DSCVA

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

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

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

T.SCVA

Un **atacante** es capaz de **tomar el control del proceso de firma**, engañando al firmante, o abusando de los medios de firma, de manera que puede obtener firmas electrónicas sin el consentimiento del titular legítimo del **DNIe**. Lo mismo aplica al proceso de verificación de firmas, forzando falsos positivos o negativos.

Esta amenaza incluye una posible modificación del propio TOE, de manera que se altere su funcionalidad. Esta amenaza compromete el activo **A.SCVA**.

T.VAD

Un **atacante compromete la confidencialidad del VAD**, perdiendo su titular el control del exclusivo del **DNIe**. Esta amenaza compromete el activo **A.VAD**.

3.3 POLÍTICAS ORGANIZATIVAS DE SEGURIDAD

P.SSCD

El dispositivo seguro de creación de firma que usa la SCVA será el **DNIe**.

P.CRYPTO

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

P.LOPD

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

3.4 HIPÓTESIS

AS.ITENV

La plataforma de propósito general que la SCVA-Tipo2 necesita para operar y para facilitar los interfaces de firmante y con el **DNIe**, facilita las protecciones y mecanismos de seguridad adecuados para proteger los activos de la SCVA (**A.DSCVA**, **A.VAD** y **A.SCVA**).

4 OBJETIVOS DE SEGURIDAD

Esta declaración de seguridad se basa y cumple los objetivos de seguridad conforme a los definidos en el perfil de protección **[PPSCVA-T2-EAL1].**

4.1 OBJETIVOS DE SEGURIDAD PARA EL TOE

O.INT

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

O.CONF

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

O.CONT

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

O.STEGA

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

O.CRYPTO

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

O.LOPD

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

4.2 OBJETIVOS DE SEGURIDAD PARA EL ENTORNO OPERACIONAL

O.SSCD

El **dispositivo seguro de creación de firma** que usa la SCVA será el **DNIe**.

O.ITENV

La plataforma de propósito general que la **SCVA-Tipo2** necesita para operar y para facilitar los interfaces de firmante y con el **DNIe**, facilita las protecciones y mecanismos de seguridad adecuados para proteger los activos de la **SCVA** (**A.DSCVA**, **A.VAD** y **A.SCVA**), mediante una combinación eficaz de medidas de índole técnico, de procedimientos y de securización de su entorno.

4.3 JUSTIFICACIÓN DE LOS OBJETIVOS

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

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

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

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

- **La correspondencia es completa con respecto a la definición del problema de seguridad**: cada amenaza, OSP o hipótesis se corresponde, al menos, con un objetivo de seguridad.
- **La correspondencia es correcta**: las hipótesis se asocian siempre al entorno operacional del TOE y los objetivos de seguridad del TOE no se corresponden con ninguna hipótesis.

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

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

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

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

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

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

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

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

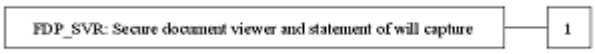
5 DEFINICIÓN DE COMPONENTES EXTENDIDOS

5.1 FDP_SVR - SECURE DOCUMENT VIEWER AND STATEMENT OF WILL CAPTURE

Family Behaviour

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

Component levelling



Management

No management activities apply.

Audit

No audit requirements apply.

FDP_SVR.1 Secure viewer and SCVA interface

Hierarchical to: No other components

Dependencies: No dependencies.

User application notes

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

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

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

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

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

5.2 FDP_ISD - IMPORT OF SDS FROM OUTSIDE OF THE TOE

Family Behaviour

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

Component levelling

FDP_ISD: Import of SDs from outside of the TOE	1

Management

No management activities apply.

Audit

No audit requirements apply.

FDP_ISD.1 Import of Signer's Document

Hierarchical to: No other components

Dependencies: No dependencies.

User application notes

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

FDP_ISD.1.1 The TSF shall only accept for signature documents based in one of the following electronic formats [assignment: **RELACIÓN DE FORMATOS DE DOCUMENTO ELECTRÓNICO**] when importing user data, as SDs, or SDOs, from outside of the TOE, which comply with the following [assignment: **DEFINICIÓN DE LAS REGLAS DE CONTENIDO Y PRESENTACIÓN DE LOS FORMATOS INDICADOS**].

Asignación: [**RELACIÓN DE FORMATOS DE DOCUMENTO ELECTRÓNICO**] el autor de la declaración de seguridad especificará la relación de formatos de documento electrónico que el TOE es capaz de interpretar y mostrar de manera no ambigua.

Asignación: [**DEFINICIÓN DE LAS REGLAS DE CONTENIDO Y PRESENTACIÓN DE LOS FORMATOS INDICADOS**] el autor de la declaración de seguridad especificará la lista de reglas aplicables a los formatos de documento electrónico que permiten su interpretación y presentación de manera no ambigua al firmante.

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

6 REQUISITOS DE SEGURIDAD

Esta declaración de seguridad se basa y cumple los requisitos de seguridad conforme a los definidos en el perfil de protección **[PPSCVA-T2-EAL1].**

6.1 REQUISITOS FUNCIONALES DE SEGURIDAD

6.1.1 FDP_SDI.2 - STORED DATA INTEGRITY MONITORING AND ACTION

Transcripción del componente

FDP_SDI.2.1 The TSF shall monitor user data (SD, Signature Attributes, DTBS, DTBSR, SVD, SDO, VAD) stored in containers controlled by the TSF for [assignment: **ERRORES DE INTEGRIDAD**] on all objects, based on the following attributes: [assignment: **ATRIBUTOS DATOS USUARIO**].

Asignación: [**ERRORES DE INTEGRIDAD**] Durante el proceso de firma si se ha realizado una alteración del documento o texto a firmar y al finalizar el proceso de firma si se ha alterado el documento que se ha firmado.

Durante el proceso de verificación, si se ha alterado el documento firmado a verificar.

Asignación: [**ATRIBUTOS DATOS USUARIO**] Comprobación de resúmenes SHA-1 del documento o texto original (SD) con el extraído de la firma.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: **DETECCIÓN ERROR INTEGRIDAD**].

Asignación: [**DETECCIÓN ERROR INTEGRIDAD**] Interrumpir la operación de creación/verificación de firma, y notificar al firmante.

6.1.2 FTP_ITC.1.UD - INTER-TSF TRUSTED CHANNEL

Transcripción del componente

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and **the SSCD** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: **LA TSF**] to initiate communication via the trusted channel.

Selección: [**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.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: **CREACIÓN Y VERIFICACIÓN DE LA FIRMA**].

Asignación: [**CREACIÓN Y VERIFICACIÓN DE LA 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.

6.1.3 FTP_ITC.1.VAD - INTER-TSF TRUSTED CHANNEL/VAD

Transcripción del componente

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and **the SSCD** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: **LA TSF**] to initiate communication via the trusted channel.

Selección: [**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.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: **AUTENTICACIÓN DE FIRMANTE PRESENTANDO EL VAD AL DNIE**].

Asignación: [**AUTENTICACIÓN DE FIRMANTE PRESENTANDO EL VAD AL DNIE**] Contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.

6.1.4 FDP_RIP.1 - SUBSET RESIDUAL INFORMATION PROTECTION

Transcripción del componente

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**].

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.

6.1.5 FPT_TST.1 - TSF TESTING

Transcripción del componente

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: **DURANTE EL ARRANQUE INICIAL, POR PETICIÓN DEL FIRMANTE Y PERIÓDICAMENTE DURANTE SU OPERACIÓN NORMAL**] to demonstrate the correct operation of [selection: **LA TSF**].

Selección: [**DURANTE EL ARRANQUE INICIAL, POR PETICIÓN DEL FIRMANTE Y PERIÓDICAMENTE DURANTE SU OPERACIÓN NORMAL**] contenido ya establecido por el autor del Perfil de Protección que no requiere de asignación por parte del autor de la declaración de seguridad.

Selección: [**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.

FPT_TST.1.2 The TSF shall provide the signatory with the capability to verify the integrity of [selection: **LOS DATOS DE LA TSF**].

Selección: [**LOS DATOS DE 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.

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

6.1.6 FDP_SVR.1 - SECURE VIEWER AND SCVA INTERFACE

Transcripción del componente

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.

6.1.7 FDP_ISD.1 - IMPORT OF SIGNER'S DOCUMENT

Transcripción del componente

FDP_ISD.1.1 The TSF shall only accept for signature documents based in one of the following electronic formats [assignment: **FORMATOS DE DOCUMENTO ELECTRÓNICO**] when importing user data, as SDs, from outside of the TOE, which comply with the following [assignment: **DEFINICIÓN DE REGLAS DE CONTENIDO Y PRESENTACIÓN DE LOS FORMATOS DE DOCUMENTO ELECTRÓNICO**]

Asignación: [**FORMATOS DE DOCUMENTO ELECTRÓNICO**] El TOE es capaz de interpretar y mostrar de manera no ambigua, los siguientes formatos de documento electrónico: **texto plano ASCII**, y subconjunto limitado **XML.**

Asignación: [**DEFINICIÓN DE REGLAS DE CONTENIDO Y PRESENTACIÓN DE LOS FORMATOS DE DOCUMENTO ELECTRÓNICO**] En caso de formato de **texto plano ASCII** se comprobará si los bytes que conforman el mensaje a firmar sigue el **código ASCII** y en el caso de tratarse de un **documento XML** se validará contra un esquema XSD propio tal y como sigue la recomendación **XML Schema de W3C**.

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.

6.1.8 FDP_ITC.1 - IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

Transcripción del componente

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

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.

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**].

Asignación: [**REGLAS ADICIONALES DE CONTROL DE LA IMPORTACIÓN**] No se aplica ninguna política propia, se siguen los estándares marcados por el ETSI XAdES (XML Advanced Electronic Signatures). Los datos de usuario que requiere el TOE para el proceso de firma serán el texto o mensaje a firmar, el formato del texto o mensaje, el formato/subformato de firma y el PIN del DNIe. Para el proceso de verificación, el usuario deberá facilitar un documento firmado y el PIN para el acceso al dispositivo criptográfico, DNIe.

6.1.9 FCS_COP.1_SIGNATURE_CREATION_PROCESS - CRYPTOGRAPHIC OPERATION

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**].

Asignación: [**RELACIÓN DE OPERACIONES CRIPTOGRÁFICAS**] hashSHA1(data), cipherSHA1RSA(data, privateKey).

Asignación: [**ALGORITMOS CRIPTOGRÁFICOS**] **SHA-1** y **RSA.**

Asignación: [**TAMAÑOS DE CLAVE**] **Tamaño clave empleada en RSA: 2048 bits.**

Asignación: [**RELACIÓN DE NORMAS**] Ninguna.

6.1.10 FCS_COP.1_SIGNATURE_VERIFICATION - CRYPTOGRAPHIC OPERATION

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**].

Asignación: [**RELACIÓN DE OPERACIONES CRIPTOGRÁFICAS**] hashSHA1(data), decipherSHA1RSA(data, publicKey)

Asignación: [**ALGORITMOS CRIPTOGRÁFICOS**] **SHA-1**y **RSA.**

Asignación: [**TAMAÑOS DE CLAVE**] **Tamaño de clave empleada en RSA: 2048 bits.**

Asignación: [**RELACIÓN DE NORMAS**] Ninguna.

6.2 REQUISITOS DE GARANTÍA DE SEGURIDAD

El desarrollo y evaluación del TOE se realizará conforme al siguiente nivel de garantía: EAL1.

ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation of evidence elements:

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

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

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

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

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

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

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

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence elements:

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

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

ALC_CMC.1 Labeling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

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

Content and presentation of evidence elements:

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

ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence elements:

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

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

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

ASE_INT.1.6C The TOE overview shall identify any non-TOE

hardware/software/firmware required by the TOE.

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

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

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements

Developer action elements:

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

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

Content and presentation of evidence elements:

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

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

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

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

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

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

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

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

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

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

ASE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence elements:

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation of evidence elements:

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

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

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

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

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

ASE_REQ.1 Stated security requirements

Dependencies: ASE_ECD.1 Extended components definition

Developer action elements:

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

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

Content and presentation of evidence elements**:**

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

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

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

ASE_REQ.1.4C All operations shall be performed correctly.

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

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

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

ATE_IND.1 Independent testing - conformance

Dependencies: ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation of evidence elements:

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

AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures

Developer action elements:

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

Content and presentation of evidence elements:

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

6.3 JUSTIFICACIÓN DE LOS REQUISITOS FUNCIONALES DE SEGURIDAD

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

	O.INT	O.CONF	O.CONT	O.STEGA	O.CRYPTO	O.LOPD
FDP_SDI.2	X					
FTP_ITC.1.UD	X					
FTP_ITC.1.VAD		X				
FDP_RIP.1		X				
FPT_TST.1			X			
FDP_SVR.1				X		X
FDP_ISD.1				X	X	
FDP_ITC.1					X	
FCS_COP.1_SIGNATURE_CREATION					X	
FCS_COP.1_SIGNATURE_VERIFICATION					X	

La correspondencia específica como cada SFR se corresponde con cada objetivo de seguridad, demostrando que:

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

Para satisfacer el objetivo **O.INT**, el TOE deberá monitorizar la integridad de los activos correspondientes, tal y como requiere **FDP_SDI.2 Stored data integrity monitoring and action**, y durante su envío al **DNIe**, tal y como requiere **FTP_ITC.1.UD Inter-TSF trusted channel**.

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

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

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

Se aborda el objetivo **O.CRYPTO** mediante los SFRs **FCS_COP.1_SIGNATURE_CREATION Cryptographic operation** y **FCS_COP.1_SIGNATURE_VERIFICATION Cryptographic operation** para el proceso de creación y verificación de firma electrónica respectivamente.

Estos requisitos necesitan importar los datos de entrada necesarios para la realización de las operaciones criptográficas correspondientes, como se requiere en **FDP_ITC.1 Import of user data without security attributes** y **FDP_ISD.1 Import of Signer's Document**. El requisito **FDP_ISD.1 Import of Signer's Document** es un requisito funcional extendido, que se diferencia principalmente de **FDP_ITC.1 Import of user data without security attributes** en la especificación de la acción que debe ser llevada a cabo cuando no se cumplen las reglas de importación definidas.

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

6.4 DEPENDENCIAS DE LOS REQUISITOS FUNCIONALES DE SEGURIDAD

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

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

- Para satisfacer **FCS_COP.1_SIGNATURE_CREATION Cryptographic operation**, el TOE debe realizar las operaciones criptográficas establecidas en este requisito sobre los datos importados mediante el requisito **FDP_ISD.1 Import of Signers's Document**.
- Para satisfacer FCS_**COP.1_SIGNATURE_VERIFICATION** el TOE debe importar la clave pública (**FDP_ITC.1 Import of user data without security attributes**) y el documento firmado (**FDP_ISD.1 Import of Signers's Document**) y mediante el algoritmo descrito en el requisito verificar la firma.
- Justificación de no inclusión de dependencia **FCS_CKM.4**: En el proceso de creación de firma el TOE no se requiere de la creación ni la importación de claves públicas, por tanto la destrucción de la clave pública no aplica. Además en el proceso de verificación de firma, la destrucción de clave pública importada mediante **FDP_ITC.1** tampoco aplica. Ya que los algoritmos de clave pública se autoprotegen de posibles alteraciones de la clave pública y por tanto la destrucción de ésta no aplica.

6.5 JUSTIFICACIÓN DE LOS REQUISITOS DE GARANTÍA DE SEGURIDAD

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

7 TOE SUMMARY SPECIFICATION

En este apartado se definen cómo se instancian en el TOE los requisitos de seguridad establecidos en el apartado anterior.

7.1 FDP_SDI.2 - STORED DATA INTEGRITY MONITORING AND ACTION

El TOE dispone de un mecanismo de control para verificar la integridad de los siguientes datos de usuario:

Documento a firmar: antes de realizar la firma, una vez seteados los datos a ser firmados (cadena de texto **ASCII** o **XML** que valida un esquema propio de Indenova - **FormSchema**) se realiza un resumen **SHA-1** de ese objeto. Una vez realizada la firma, se comprueba que el resumen **SHA-1** de los datos originales coincide con el resumen de los datos firmados, extraidos de la firma. En el caso que no coincidan, se lanzará al usuario un mensaje de error indicando que los datos firmados no coinciden con los originales**.** Además de

este recurso, se emplean dos mecanismos adicionales para preservar la integridad de dichos datos:

- El objeto o mensaje SOAP que se envía al servidor (interfaz webservice) y que incluye el mensaje a firmar, atributos de firma, etc ... se firma con un **certificado embebido** en la parte cliente, **eSigna Crypto Client Component.**
- La comunicación entre **eSigna Crypto Cient Component y eSigna Crypto Server Component** se realiza sobre una capa de transporte segura **SSL/TLS**.

Atributos de la firma: por extensión, se garantiza la integridad ya que los atributos de firma se firman y se envian via HTTPS.

Datos a firmar: en el sistema el usuario solamente se firma el del nodo XAdES **SignedInfo**, cuyo resultado se verifica en la parte cliente y el contenido se establece al nodo XAdES **SignatureValue**, contenido necesario para completar el firmado. Por extensión, se garantiza la **integridad** ya que los datos a firmar se firman y se envian via HTTPS (ver Figura 3).

Representación de los datos a firmar: se muestra un campo de texto donde se especifica los datos que se van a firmar junto al resumen **SHA-1** calculado. Una vez firmados los datos, además del anterior campo, se mostrará el documento firmado, el documento original extraido y su resumen **SHA-1**.

Documento firmado: por extensión, se garantiza la integridad ya que el documento firmado se envia via HTTPS.

PIN: el pin que protege al **DNIe** no se transmite en ningún momento al servidor, tanto en procesos de firma o verificación. El componente **eSigna Crypto Client Component** solicita el PIN al usuario **solamente** en el momento de realizar la firma o verificación. Una vez efectuada la firma o verificación, la instancia del *Java Applet* se destruye, impidiendo que esa información resida en el sandbox de la máquina virtual de Java.

Datos a verificar: en el sistema el usuario selecciona un documento firmado desde el sistema de ficheros local. Este documento firmado se envía al componente servidor **eSigna Crypto Server Component** y es éste el que verifica si el formato de firma es correcto, extrae la firma del documento (contenido del nodo XAdES **SignatureValue)** junto con los valores originales firmados (nodo XAdES **SignedInfo**). Estos datos los recibe el componente cliente **eSigna Crypto Client Component**, el cual verifica la firma utilizando la clave pública del **DNIe.** Los datos a verificar se envían vía HTTPS con lo que queda garantizada la integridad de los mismos (ver Figura 4).

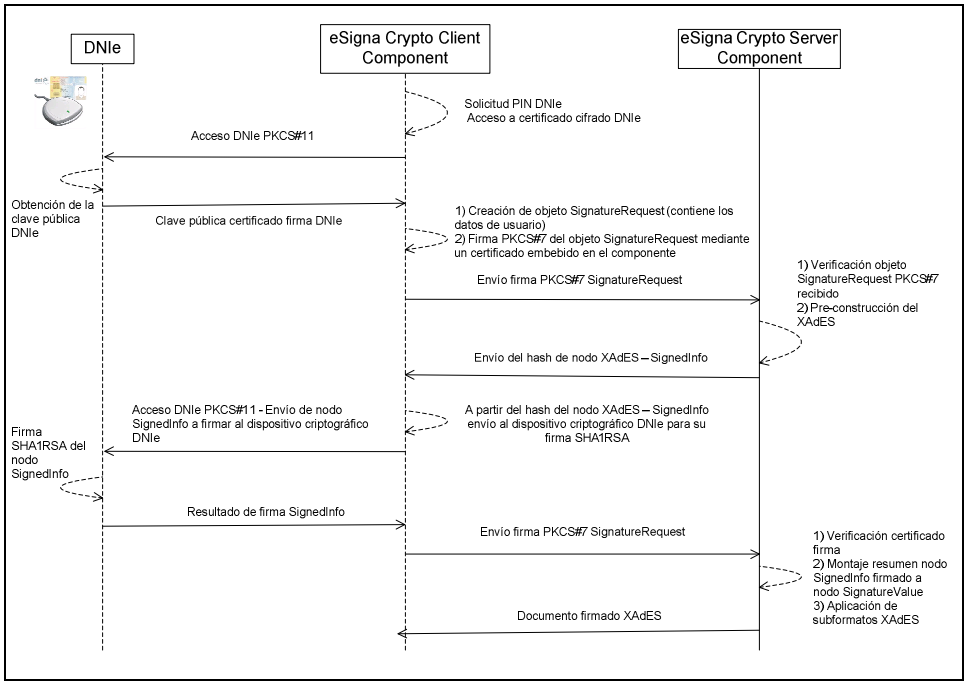


Figura 3. Detalle del proceso de firma

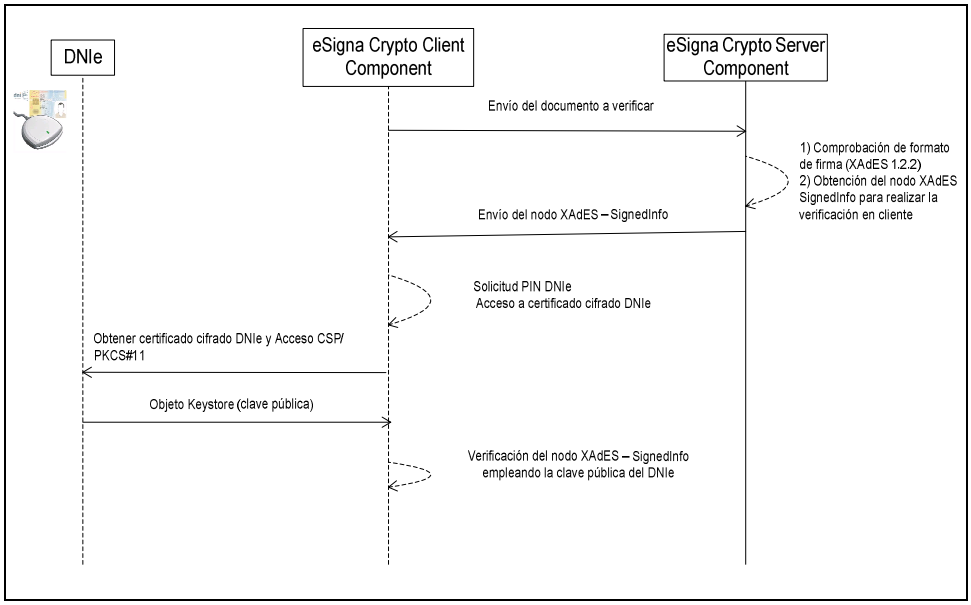


Figura 4. Detalle del proceso de verificación

7.2 FTP_ITC.1.UD - INTER-TSF TRUSTED CHANNEL

El sistema cumple este requisito de seguridad ya que el TOE accede al **DNIe**, a través de **CSP** o directamente a través de una librería **PKCS#11** para la conectividad con **DNIe**.

Estos APIs crean un canal confiable (según especifica el **CWA 14890-1**) desde la aplicación al dispositivo de creación de firma, para proceder a la **firma de un documento**.

7.3 FTP_ITC.1.VAD - INTER-TSF TRUSTED CHANNEL/VAD

El sistema cumple este requisito de seguridad ya que el TOE accede al **DNIe**, a través de un módulo **CSP** o directamente a través de una librería **PKCS#11** para la conectividad con **DNIe**.

Estos APIs crean un canal confiable (**CWA 14890-1**) desde la aplicación al dispositivo de creación de firma para proceder a la firma de un documento presentando un PIN al **DNIe.**

7.4 FDP_RIP.1 - SUBSET RESIDUAL INFORMATION PROTECTION

Para el acceso al DNIe podemos emplear el **CSP** o atacar directamente al dispositivo criptográfico mediante una librería **PKCS#11**.

El componente **eSigna Crypto Client Component** solicita el PIN al usuario **solamente** en el momento de realizar la firma. Una vez efectuada la firma, la variable asociada al PIN se destruye además, la instancia del *Java* Applet se destruye, impidiendo que esa información resida en el sandbox de la máquina virtual de Java. El PIN solo ha permanecido en memoria durante el tiempo estrictamente necesario para realizar el proceso.

En el caso de emplear la librería **PKCS#11**, la desasignación del PIN en dicha librería no es posible, ya que en la implementación de **PKCS#11** no existe/no se define un método para la liberación de objetos que manejan datos como el PIN. En el caso de acceso mediante **CSP**, es el propio driver del **DNIe** el que realiza esta operación.

7.5 FPT_TST.1 - TSF TESTING

A nivel del componente **eSigna Crypto Client Component** presenta una serie de operaciones de comprobación que se ejecutan siempre que se

cargue el componente *Java Applet* (previamente a la operación de firma y verificación), periódicamente y bajo petición del usuario/firmante/verificador. Este testeo realiza las siguientes operaciones:

- **Comprobación** de librerias necesarias para la comunicación **eSigna Crypto Client Component** y dispositivo criptográfico **DNIe**.
- **Comprobación** de la integridad de las librerias necesarias para la comunicación **eSigna Crypto Client Component** y dispositivo criptográfico.
- **Comprobación** de la integridad del componente cliente **eSigna Crypto Client Component**.
- **Comprobación** de la integridad del componente servidor **eSigna Crypto Server Component.**
- **Comprobación** comunicación entre **eSigna Crypto Client Component** y dispositivo criptográfico.
- **Testeo de conectividad**: comprueba la conectividad con el componente **eSigna Crypto Server Component.**
- **Firma de un mensaje**: se realiza una firma en formato **XAdES-BES** de una cadena concreta empleando para ello el certificado embebido en el **eSigna Crypto Client Component.** Para este caso de prueba, se efectua el siguiente proceso:

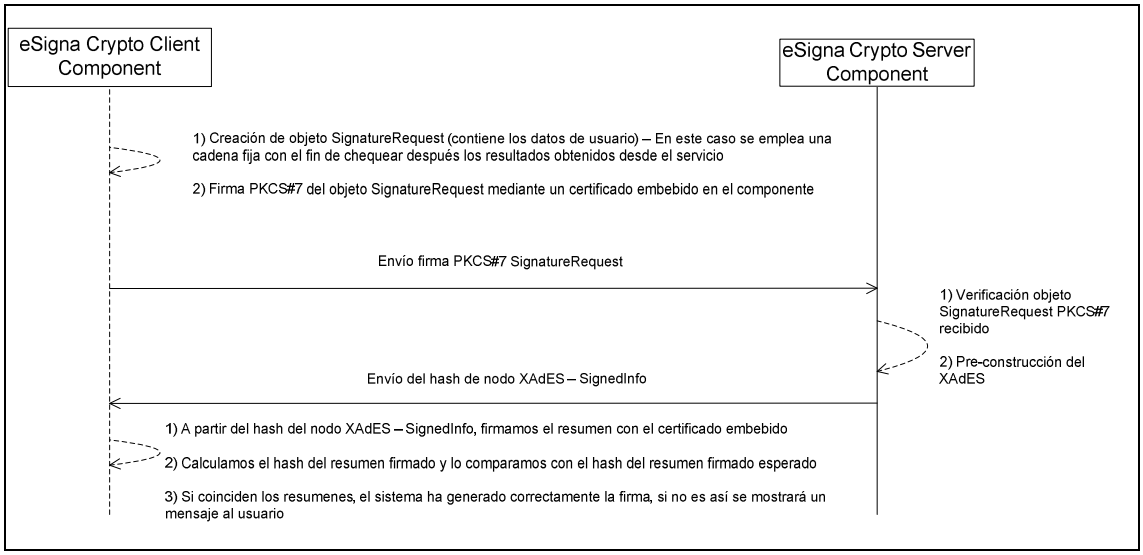


Figura 5. Testeo Firma de mensaje

La integridad del componente **eSigna Crypto Client Component** queda asegurada ya que el componente *Java Applet* se encuentra firmado con un certificado de firma de código y, además, el componente cliente realiza una comprobación en la que se aplica un resumen **MD5** sobre el componente desplegado en el servidor y comprueba que no se ha alterado comparando el valor del resumen con uno esperado. El componente cliente **eSigna Crypto Client Component** también verifica la integridad de las librerias que acceden al **DNIe** aplicando un resumen **MD5** sobre las mismas y comparando sus valores con los esperados.

La integridad del componente **eSigna Crypto Server Component** queda asegurada ya que el componente cliente realiza una comprobación en la que se aplica un resumen **MD5** sobre el componente desplegado en el servidor y comprueba que no se ha alterado comparando el valor del resumen con uno esperado.

7.6 FDP_SVR.1 - SECURE VIEWER AND SCVA INTERFACE

eSigna Crypto Client Component aportará un visor de documentos seguro, que mostrará en formato de texto plano **UNICODE** el mensaje a firmar, impidiendo la ocultación y/o falsificación de datos.

El componente **eSigna Crypto Client Component** mostrará al usuario una ventana que mostrará el siguiente mensaje: **"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."** La ventana incorpora la opción de **Aceptar** y **Cancelar**: la opción de **Cancelar** permite cancelar la operación de firma antes de realizarla. La opción **Aceptar** permite continuar con el proceso de firma.

El usuario puede seleccionar dos fuentes para el mensaje firmante:

- **Introduciendo el texto plano en formato ASCII en un elemento HTML textarea.**
- **Introduciendo el contenido de un fichero XML que cumpla el esquema FormSchema**. El formato de representación será **ASCII**.

Una vez el usuario ha introducido el texto o XML en el textarea aparecerán los siguientes elementos:

- Un elemento **HTML textarea** que contendrá la representación **UNICODE** del texto **ASCII** seleccionado.
- Otro **elemento HTML textarea** el **resumen SHA-1** del mensaje o fichero **XML**.

Cuando el usuario realiza el click sobre el botón **Firmar** y acepta la confirmación de voluntad mostrada, se procederá al firmado del mensaje o XML. Cuando ha finalizado el proceso correctamente, aparecerán los siguientes elementos:

- Un **elemento HTML textarea** el **contenido del fichero XAdES** resultado de la firma. Se mostrará en formato **ASCII.**
- Un **elemento HTML textarea que contendrá** el mensaje original extraido de la firma en formato **UNICODE.**
- Otro **elemento HTML textarea** que mostrará el **resumen SHA-1** del mensaje o XML.

De esta manera, el firmante puede observar que el mensaje o fichero XML firmado coincide con el original, bien visualizando su contenido en los campos textarea o bien comprobando los resúmenes **SHA-1.**

Estos elementos HTML textarea emplearán los siguientes estilos a nivel de visualización:

- Fuente: **Courier Bold**, tamaño de 10 píxeles.
- Fondo del área de texto: HTML 4.0 Color **Gold.**
- Los elementos HTML textarea que muestren el resultado de la firma (texto XAdES, texto original extraido de la firma en ASCII, original extraido en UNICODE y resumen SHA-1) aparecerán en modo lectura, impidiendo la modificación de los mismos por el usuario. Tambien estarán protegidos los elementos textarea relacionados con la visualización UNICODE del texto del mensaje original y el resumen SHA-1 del mismo.

Antes del proceso de firma, se le solicitará al usuario que introduzca un código visualizado en una imagen (captcha) que garantizará la voluntad expresa del firmante, impidiendo que un proceso automático realice este proceso.

7.7 FDP_ISD.1 - IMPORT OF SIGNER'S DOCUMENT

eSigna Crypto soporta dos formatos de mensajes/documentos:

- **Texto plano ASCII** – se presentará en un área de texto. El texto introducido será **ASCII**. Otra área de texto mostrará la representación en **UNICODE** del texto introducido.
- **XML** – el usuario puede cargar un **XML** que valide un esquema propio de Indenova, **FormSchema** siguiendo la recomendación

XML Schema [2]. En el caso de que no valide de forma correcta, se devuelve un mensaje de error al usuario indicando que el **XML** no cumple el esquema asociado. Una vez el usuario cargue el **XML**, se mostrará en un área de texto el contenido en formato **ASCII** y en otro área de texto se mostrará la representación **UNICODE** del mismo.

7.8 FDP_ITC.1 - IMPORT OF USER DATA WITHOUT SECURITY ATTRIBUTES

Este TOE, los procesos de creación y verificación de firma no requieren la importación de políticas de certificación. El formato de firma es el determinado por el estándar del **XAdES ETSI TS 101 903 versión 1.2.2** [3]. El usuario selecciona el subformato de **XAdES** a firmar: BES, T o XL.

Para la operación de firma, el usuario introduce un texto que puede tratarse de texto plano en **formato ASCII** o un texto en **formato XML** que cumple el esquema **XSD FormSchema**. Además del mensaje de firma, el usuario selecciona el formato del mensaje a firmar y el formato de firma. El dispositivo criptográfico **DNIe** realiza una firma **SHA1WithRSA** empleando la **clave privada** del certificado de firma del **DNIe**, a partir del nodo **SignedInfo** de **XAdES** nodo que contiene, entre otros elementos, el resumen **SHA-1** en Base64 del texto/mensaje a firmar. El acceso a la clave privada del **DNIe** se realiza mediante el **PIN** que el usuario introduce previamente al proceso de firma.

Para la verificación, el usuario selecciona el documento firmado mediante un selector. El dispositivo criptográfico **DNIe** emplea una verificación **SHA1WithRSA** utilizando la clave pública del **DNIe** (obtenida gracias al **PIN** que el usuario introduce previamente al momento de la verificación), el resultado de la firma contenido en el nodo **SignatureValue** de **XAdES** y los datos a verificar contenidos en el nodo **XAdES SignedInfo**. Estos valores (**SignatureValue** y **SignedInfo**) se extraen del documento firmado.

7.9 FCS_COP.1_SIGNATURE_CREATION_PROCESS - CRYPTOGRAPHIC OPERATION

A la hora de crear la firma se utiliza una operación de cifrado **SHA1WithRSA** utilizando una clave de **2048 bits** (clave privada del **DNIe)**.

---

[2] W3C XML Schema recommendation : http://www.w3.org/TR/xmlschema-0/

[3] XML Advanced Electronic Signatures XAdES - ETSI TS 101 903 V1.2.2 (2004-04) *http://uri.etsi.org/01903/v1.2.2/ts_101903v010202p.pdf*

El objeto que se firma en **eSigna Crypto Client Component** es el hash del nodo **SignedInfo** de XAdES, el cual se utiliza a posteriori para acabar de formar el fichero XAdES.

Estas operaciones criptográficas se implementan utilizando el proveedor PKCS#11 **SunPKCS#11.**

7.10 FCS_COP.1_SIGNATURE_VERIFICATION - CRYPTOGRAPHIC OPERATION

Se emplea un descifrado **SHA1WithRSA** utilizando la clave pública de **2048 bits** del firmante obtenida del **DNIe** para verificar la firma contenida en el nodo XAdES **SignatureValue** con el valor del nodo XAdES **SignedInfo** para obtener el resultado de la verificación.

Estas operaciones criptográficas se implementan utilizando el proveedor PKCS#11 **SunPKCS#11.**

8 BIBLIOGRAFÍA Y ACRÓNIMOS

8.1 BIBLIOGRAFÍA

[X509]	ITU-T standard for a public key infrastructure form single sign-on and privilege management infrastructure
[CWA 14890-1]	Application Interface for smart cards used as Secure Signature Creation Devices

8.2 ACRÓNIMOS

XAdES	XML Advanced Electronic Signatures
XAdES-BES	XAdES – Basic Electronic Signature
XAdES-T	XAdES – Timestamp
XAdES-XL	XAdES – eXtended Long-term
XMLDSig	XML Digital Signature
Java EE	Java Enterprise Edition
SOAP	Simple Object Access Protocol

CA	Certificate Authority
SD	Signed Data – documento que el firmante pretende firmar electrónicamente
DTBS	Data To Be Signed – datos electrónicos completos que hay que firmar, incluyendo tantos los atributos del documento o datos a firmar, del usuario como los de la firma
SVD	Signature Verification Data – datos (código o claves criptográficas públicas) que se utilizan para verificar una firma electrónica
SCVA	Signature Creation and Verification Application
DNIe	Documento Nacional de Identidad, versión electrónica
VAD	Verification Authentication Data – 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
TOE	Target Of Evaluation
TSF	TOE Security Functionality
DTBSR	Data To Be Signed Representation
SSCD	Secure Signature Creation Device
SFR	Security Functional Requirement
SDO	Signed Data Object
DTD	Document Type Definition
XSD	XML Schema Definition
CSP	Cryptographic Service Provider
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
ACCV	Autoritat de Certificació de la Comunitat Valenciana
TSA	Time-Stamping Authority
PPT	Pliego de prescripciones técnicas para el desarrollo de eSigna Crypto.