

# MANUAL DE USUARIO DE LA UTILIDAD DE COPIA, FIRMA Y VALIDACIÓN ELECTRÓNICA eCoFirma v1.4.0

Madrid, 29 de abril de 2013

# Índice

<b>PRELUDIO .....</b>	<b>3</b>
<b>1. INTRODUCCIÓN .....</b>	<b>4</b>
<b>2. REQUISITOS .....</b>	<b>6</b>
<b>3. VISTA RÁPIDA DE LA UTILIDAD.....</b>	<b>7</b>
<b>4. CONFIGURACIÓN DE LA UTILIDAD .....</b>	<b>12</b>
4.1. CONFIGURACIÓN DE LA UTILIDAD MEDIANTE ASISTENTE DE CONFIGURACIÓN .....	12
4.2. CONFIGURACIÓN DE LA APLICACIÓN DE FORMA MANUAL.....	19
<b>5. USO DE LA UTILIDAD .....</b>	<b>48</b>
5.1. FIRMA ELECTRÓNICA DE UN ARCHIVO .....	48
5.2. VALIDACIÓN DE UNA FIRMA .....	54
5.3. LANZAR VALIDACIONES RECURSIVAS .....	62
5.4. HERRAMIENTA ESTENOGRÁFICA .....	63
5.5. PROTECCIÓN DE DOCUMENTOS .....	68
5.6. CÁLCULO DE HUELLAS DIGITALES .....	71
5.7. FIRMA MÚLTIPLE Y CONTRAFIRMA .....	72
<b>6. MANEJO DE ERRORES .....</b>	<b>75</b>
<b>7. ENLACES DE INTERÉS .....</b>	<b>77</b>

## Preludio

La firma electrónica consiste en un proceso de encriptación de información que, por medio de una transmisión de confianza, identifica con garantías al dueño de la firma realizada, y asegura la integridad del contenido firmado.

Para realizar dicha codificación se emplea la infraestructura de clave pública (PKI), que consiste en una forma asimétrica de encriptar y desencriptar información, es decir, que en lugar de utilizar una contraseña única, existen dos claves, una de carácter público y otra privada, que se complementan. Lo codificado con clave privada sólo puede ser decodificado con la clave pública correspondiente y viceversa.

En la firma electrónica, el emisor utiliza su clave privada para codificar los datos a firmar, envía el resultado al receptor y éste procede a validarla empleando la clave pública del emisor, que va adjunta en la propia firma. Partiendo de la premisa de que la clave original es privada, se demuestra que los datos fueron firmados realmente por el emisor, que está identificado mediante el certificado que está asociado a las claves.

La entidad que emitió el certificado garantiza la veracidad de éste. Así pues, el receptor de un documento firmado, para validarlo completamente, debe comprobar que el contenido criptográfico corresponde, y a continuación reconstruir la cadena de confianza (se trata de una cadena de firmas electrónicas) hasta alcanzar un punto en el cual decide confiar, ya que se le ofrecen suficientes garantías. Por ejemplo, porque ha alcanzado hasta el certificado raíz del DNIe y confía en la DGP.

Los objetivos que se alcanzan de éste modo son:

- **Autenticidad:** El receptor del mensaje puede asegurar la identidad del emisor gracias al mecanismo de par de claves, encriptando datos mediante la clave privada, de forma que cualquiera lo pueda desencriptar con la clave pública para comparar si el resultado coincide con el contenido firmado.
- **Integridad:** El sistema asegura que la información no fue alterada desde el momento en el que el emisor lo firmó, gracias a los mecanismos de huella, con los cuales, si se produce una alteración, la huella o hash cambia.
- **No repudio:** Garantía de que el emisor o el receptor no rechazan la información, gracias a la asociación que existe entre el par de claves y el certificado emitido por una autoridad certificadora.
- **Política de firma:** Es posible que la firma incluya una política de firma. Dicha política consiste en una serie de criterios extra que la firma debe cumplir, definidos en otros contextos.

En resumen, para construir una firma electrónica, se requiere:

- Disponer de los **datos originales** a firmar.
- Disponer de un **certificado electrónico** asociado a un par de claves criptográficas que haya sido emitido por una autoridad certificadora que sea de confianza para el receptor de la firma.
- Disponer de las **herramientas** que posibilitan la firma.

## 1. Introducción

El objetivo de este documento es presentar la aplicación de un componente cómodo, sencillo, versátil y de gran fiabilidad que permite generar documentos firmados electrónicamente con los más avanzados sistemas de firma digital. Siguiendo los estándares internacionales en vigor actualmente, XADES 1.3.2 y con validación de firma, se cubren gran parte de los aspectos requeridos en la firma digital actual.

El aplicativo y servicios desarrollados permitirán generar documentos en formato XML firmado tipo XADES. Dicho formato, al mostrar los datos estructurados y con información de metadatos, permite además búsquedas avanzadas sobre los documentos y procesos automatizados sobre las mismas, sin perder las funcionalidades de la firma digital avanzada.

La plataforma es Multi-PKI lo cual permite utilizar cualquier tipo de certificado electrónico X509 v3 emitido por entidades proveedoras de servicios de certificación que se consideren, ahora o en el futuro, de confianza, pero tiene un gran enfoque en el DNI Electrónico, cubriendo todo lo necesario para trabajar con él de manera cómoda y sencilla.



El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior. Goza de la protección que las leyes otorgan a documentos públicos y oficiales. Su titular estará obligado a la custodia y conservación del mismo.

Con la llegada de la Sociedad de la Información y la generalización del uso de Internet se hace necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que operamos cada día en el mundo físico y que, esencialmente, son:

- **Acreditar electrónicamente y de forma indubitada la identidad de la persona**
- **Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita**

[illegible]

La firma digital de documentos XML según el estándar XADES es tratada por este módulo con el apoyo de las librerías Apache XML Security, que permiten un tratamiento muy pormenorizado de las mismas. Si bien estas librerías se crearon para tratar el estándar XMLDSig las extensiones a la misma desarrolladas permitirán adaptarse a cualquier estándar XADES actual o futuro.

## 2. Requisitos

Los requisitos técnicos de la aplicación son los siguientes:

1. Sistemas operativos:

- Windows XP / Vista / 7
- Linux (Kernel 2.6.x o superior)
- Mac OS X (Leopard, Snow Leopard, Tiger)

2. Navegadores:

- Internet Explorer 6 o superior.
- Google Chrome
- Mozilla Firefox 6.0 o superior

Navegadores				
Sistemas Operativos			Internet Explorer	Mozilla
	Windows	XP	✓	✓
		Vista Win 7	✓	✓
	Linux		-	✓*
	Mac OS (KeyStore Mac)		-	-

\* En el caso de uso del DNle, se ha detectado una incompatibilidad entre el navegador Mozilla y la aplicación. Mientras el navegador está lanzado, el DNle queda bloqueado para su uso en la aplicación. Como solución alternativa se recomienda cerrar el navegador una vez lanzada la aplicación antes de insertar el DNle en el lector.

## 3. Vista rápida de la utilidad

Para iniciar la aplicación pulsaremos en el icono correspondiente a la misma que nos aparecerá tras el proceso de instalación, dándonos paso a una sencilla pantalla donde podremos observar tres opciones principales y un menú superior.



Las opciones principales de la utilidad son “Firmar documento original”, “Validar firma” y “Añadir nueva firma” y se tiene acceso directo a ellas desde la pantalla principal. Estas opciones se explicarán con más detalle a lo largo de este documento en los [puntos 5.1 Uso de la utilidad, firma electrónica de un archivo](#), [5.2 Uso de la utilidad, validación de una firma](#) y [5.7 Firma múltiple y contrafirma](#) respectivamente.

Además de las tres opciones principales la utilidad consta de un menú superior con las opciones “Menú”, “Configuración” y “Ayuda”. A continuación se muestran desplegadas las 3 opciones.

Desde la opción “Menú” podemos acceder a todas las funcionalidades de la aplicación, tanto a las tres principales que aparecen en la pantalla inicial como al resto de ellas. El funcionamiento de las opciones se explica a lo largo de este documento.

Menú	Configuración	Ayuda
Ir al menú principal		
Firmar un fichero		Alt-F
Validar una firma		Alt-V
Añadir nueva firma		Alt-K
Validar y generar Log (Recursivo)		Alt-Y
Esteganografía		Alt-Q
Encriptar		Alt-W
Desencriptar		Alt-J
Calculadora de huellas		Alt-G
Salir		Alt-S

Opción	Descripción	Detalle
Firmar un fichero	Realiza la firma electrónica XAdES de uno o varios documentos.	Ver punto 5.1
Validar una firma	Valida una firma electrónica XAdES o PAdES.	Ver punto 5.2
Añadir nueva firma	Firma una firma preexistente.	Ver punto 5.7
Validar y generar Log (Recursivo)”	Valida todas las firmas incluídas en un directorio.	Ver punto 5.3
Esteganografía	Oculta la firma de una imagen dentro de la propia imagen y permite ocultar ficheros dentro de imágenes.	Ver punto 5.4
Encriptar	Encriptar un documento con contraseña o con la parte pública	Ver punto



	de un certificado.	5.5.1
Desencriptar	Desencriptar un documento que ha sido cifrado con contraseña o con certificado.	Ver punto 5.5.2
Calculador de Huellas	Calcula las huellas digitales de un fichero en diferentes formatos y con distintas codificaciones.	Ver punto 5.6

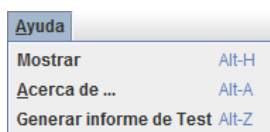
Desde la opción “Configuración” se puede configurar y personalizar la aplicación.

Configuración	Ayuda
Asistente de configuración	
Conexión	Alt-N
Firma	Alt-M
Almacén de certificados	Alt-O
Rol de Firma	Alt-B
Directorios	Alt-D
Firma de múltiples documentos	Alt-T
Esquemas	Alt-E
Apariencia de la aplicación	Alt-X
Administrador de la confianza	Alt-U
Validadores OCSP	Alt-R
Conversor PDF	Alt-I
PDF con datos de firma	Alt-P

Opción	Descripción	Detalle
Asistente de configuración	Lanza el asistente de configuración.	Ver punto 4.1
Conexión	Configuración del proxy.	Ver punto 4.2
Firma	Configuración del nivel de firma y registro para realizar firmas XAdES-T o XAdES-XL.	Ver puntos 4.2 y 4.2.4
Almacén de certificados	Elección y configuración del almacén a utilizar.	Ver punto 4.2

Rol de firma	Permite seleccionar el rol de firma.	Ver punto 4.2
Directorios	Directorios por defecto para selección de certificados, documentos y firmas.	Ver punto 4.2
Firma de múltiples documentos	Configurar si generar una firma independiente por documento o una firma de todos los documentos.	Ver punto 4.2
Esquemas	Versión de XAdES y algoritmo de Hash .	Ver puntos 4.2 y 4.2.5
Apariencia de la aplicación.	Configuración del Look&Feel de la aplicación. Permite elegir la apariencia del sistema para que mantenga su configuración de Accesibilidad.	Ver punto 4.2
Administrador de confianza	Repositorio de certificados declarados por el usuario como de confianza.	Ver puntos 4.2 y 4.2.6
Conversor PDF	Configuración para introducir imágenes dentro de pdfs.	Ver puntos 4.2 y 4.2.2
PDF con datos de firma	Configuración para visualizar pdfs con una zona informativa que contenga datos sobre la firma electrónica asociada	Ver puntos 4.2 y 4.2.3

La última opción del menú superior es “Ayuda”, desde aquí se pueden acceder a las siguientes opciones:



Pulsando en “Mostrar” se obtiene el manual en pdf de la aplicación. “Acerca de...” muestra la versión de la utilidad y permite ver la lista de cambios de esta versión y la opción “Generar informe de Test” se detalla en el 6 de este documento.

## 4. Configuración de la utilidad

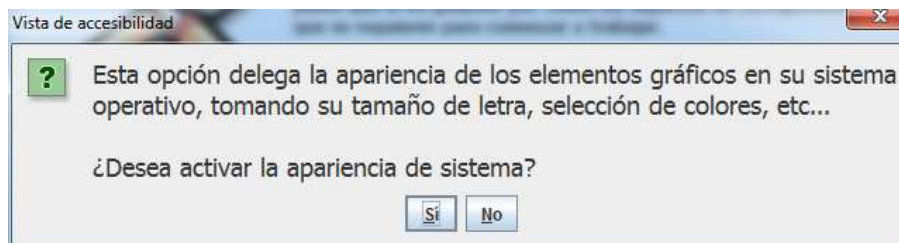
Este cliente permite firmar ficheros, de cualquier tipo, siguiendo el estándar de firma digital XADES. Dichas firmas se realizan mediante el uso de algoritmos RSA, utilizando como claves certificados digitales como el que se encuentra en el DNI electrónico. Para el uso del aplicativo, en su opción de firmar, deberemos estar en posesión de, al menos, un certificado digital válido y en vigor.

### 4.1. Configuración de la utilidad mediante asistente de configuración

La primera vez que se instala la aplicación le aparecerá el asistente de configuración. Una vez instalada la aplicación se podrá volver a acceder al mismo desde la opción “Configuración/Asistente de configuración”. Este asistente tiene el siguiente aspecto:



A lo largo de varios pasos el asistente irá guiando al usuario en la configuración de la aplicación. La primera opción que muestra el Asistente es la de activar la vista de accesibilidad, pulsando en esta opción aparecerá la siguiente pregunta:



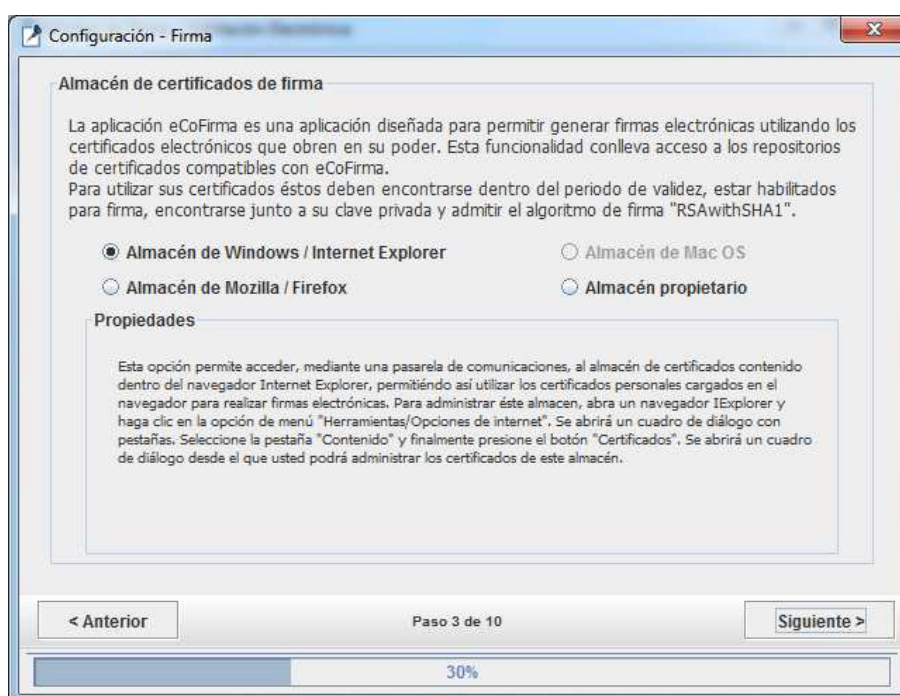
Si se pulsa “Si” se activará la vista de accesibilidad, delegándose la apariencia en el Sistema Operativo. Pulsando en “Siguiente” se avanza al siguiente paso del asistente:



En esta pantalla el usuario puede introducir si lo desea una contraseña para proteger la configuración de la utilidad. De esta forma nadie podrá modificar en el futuro la configuración si no se conoce la contraseña. Si se quiere no introducir ninguna contraseña se debe marcar la casilla “No deseo establecer ninguna contraseña”. Pulsando en “Siguiente” aparece el siguiente punto del asistente de configuración:

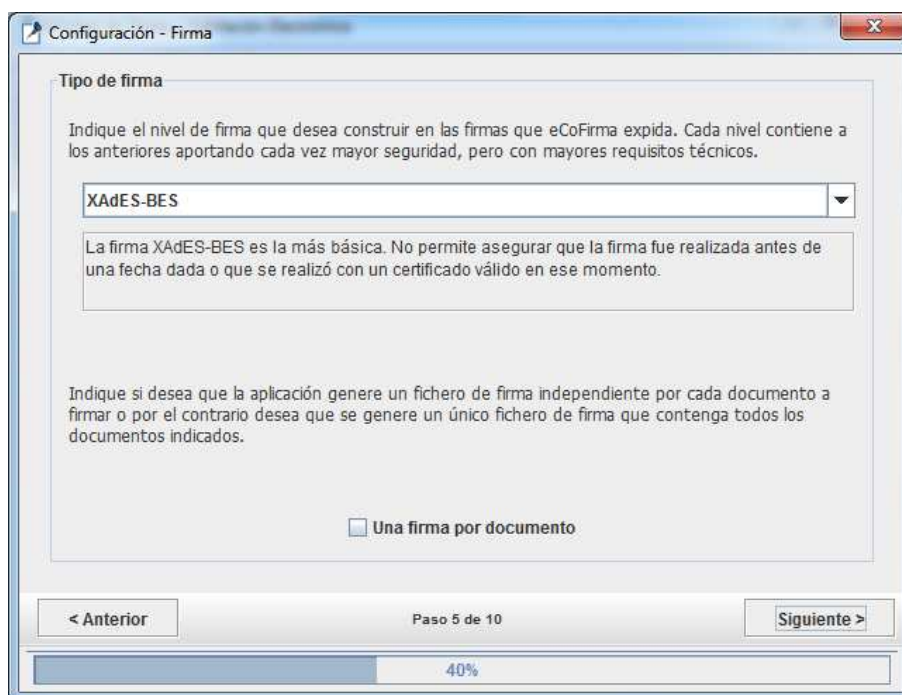


Se nos presenta una pantalla para configurar la conexión a Internet. Esto está explicado en el [punto 4.2](#) de este documento. Si se pulsa “Siguiete” se nos da la opción de configurar el almacén de certificados de firma:



Esta pantalla está explicada en el [punto 4.2](#) de este documento y si se quiere obtener información específica sobre el “Almacén propietario” está recogida en el [punto 4.2.7](#).

La siguiente pantalla del asistente sirve para configurar el nivel de firma XAdES de la utilidad:



La configuración del nivel de firma está explicada en el [punto 4.2.4](#) de este documento.

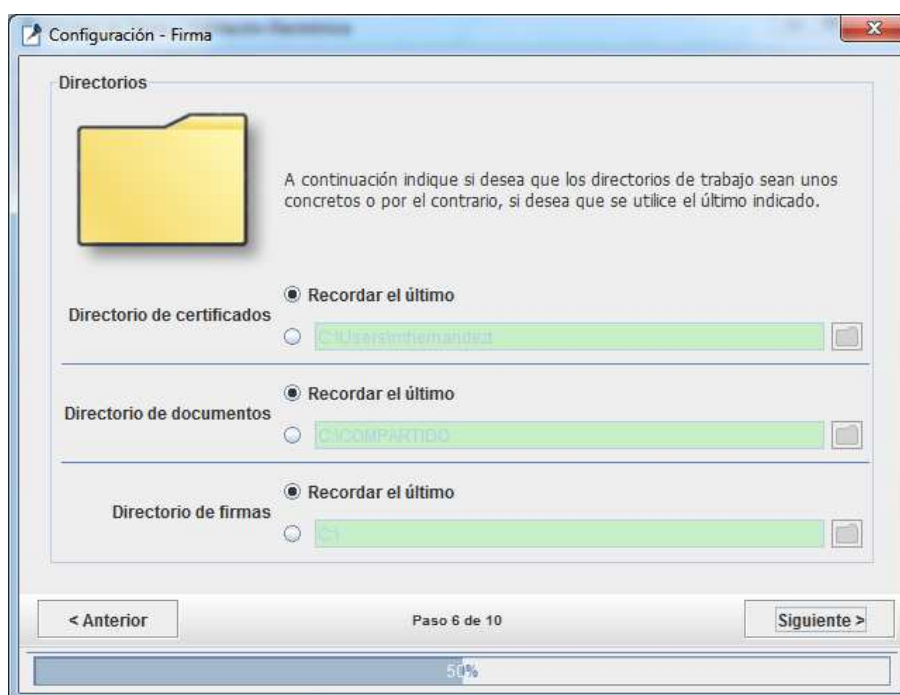
En la siguiente pantalla se puede configurar la lista de validadores OCSP:





La configuración de validadores OCSP está explicada en [el punto 4.2.1](#) de este documento.

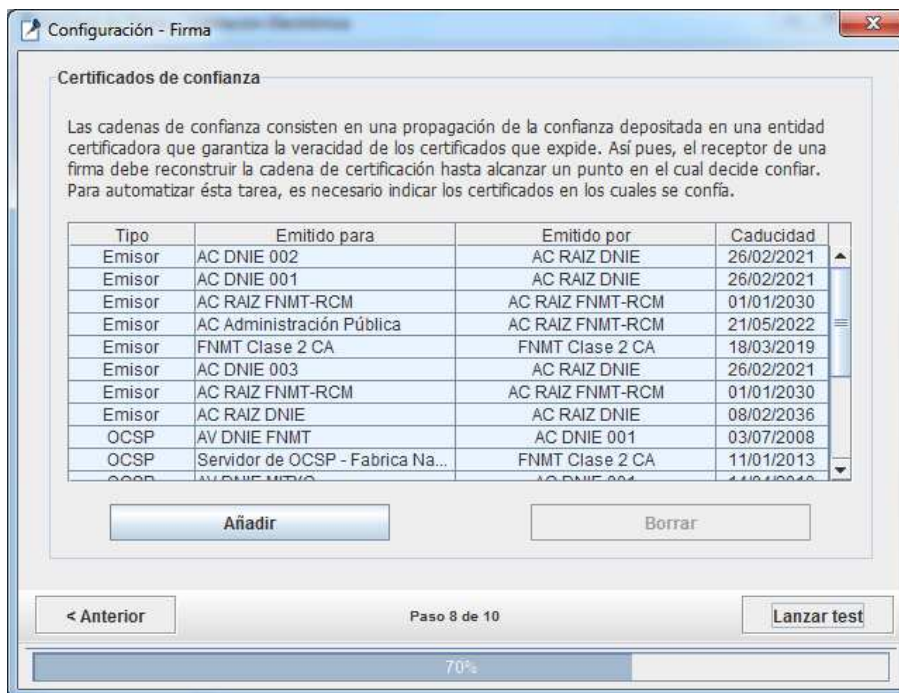
En la siguiente pantalla del asistente se pueden configurar los distintos directorios que utiliza la aplicación:





La configuración de Directorios está detallada en el [punto 4.2](#).

La siguiente pantalla del asistente de configuración hace referencia a los Certificados de confianza:



**Configuración - Firma**

**Certificados de confianza**

Las cadenas de confianza consisten en una propagación de la confianza depositada en una entidad certificadora que garantiza la veracidad de los certificados que expide. Así pues, el receptor de una firma debe reconstruir la cadena de certificación hasta alcanzar un punto en el cual decide confiar. Para automatizar ésta tarea, es necesario indicar los certificados en los cuales se confía.

Tipo	Emitido para	Emitido por	Caducidad
Emisor	AC DNIE 002	AC RAIZ DNIE	26/02/2021
Emisor	AC DNIE 001	AC RAIZ DNIE	26/02/2021
Emisor	AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01/01/2030
Emisor	AC Administración Pública	AC RAIZ FNMT-RCM	21/05/2022
Emisor	FNMT Clase 2 CA	FNMT Clase 2 CA	18/03/2019
Emisor	AC DNIE 003	AC RAIZ DNIE	26/02/2021
Emisor	AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01/01/2030
Emisor	AC RAIZ DNIE	AC RAIZ DNIE	08/02/2036
OCSP	AV DNIE FNMT	AC DNIE 001	03/07/2008
OCSP	Servidor de OCSP - Fabrica Na...	FNMT Clase 2 CA	11/01/2013
OCSP	AV DNIE FNMT	AC DNIE 001	03/07/2008

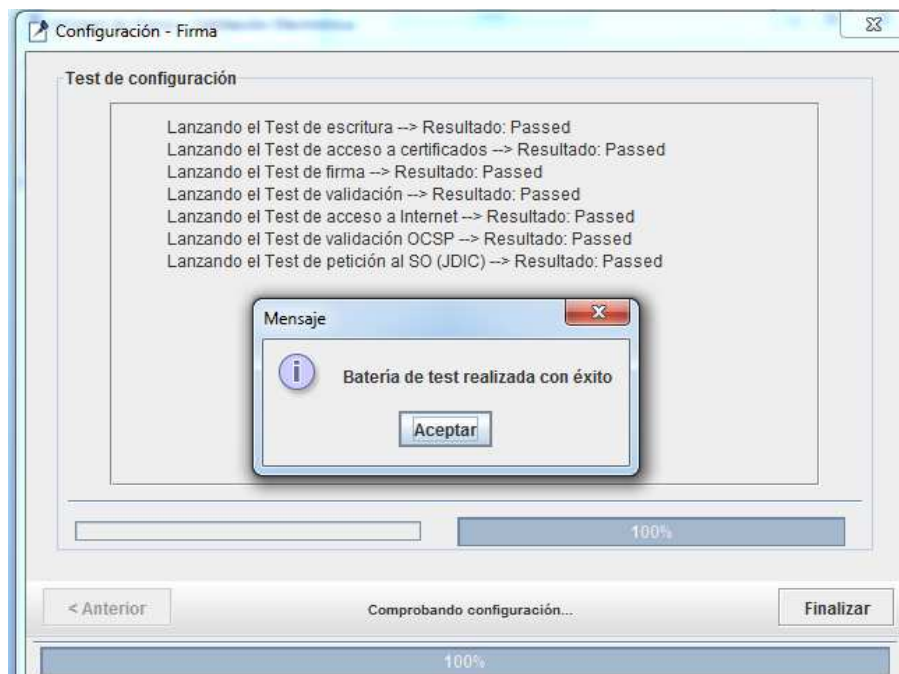
**Añadir** **Borrar**

**< Anterior** **Paso 8 de 10** **Lanzar test**

70%

La configuración de los Certificados de confianza se encuentra en el [punto 4.2.6](#) de este manual.

Para finalizar con el asistente de configuración se debe pulsar en el botón “Lanzar test”



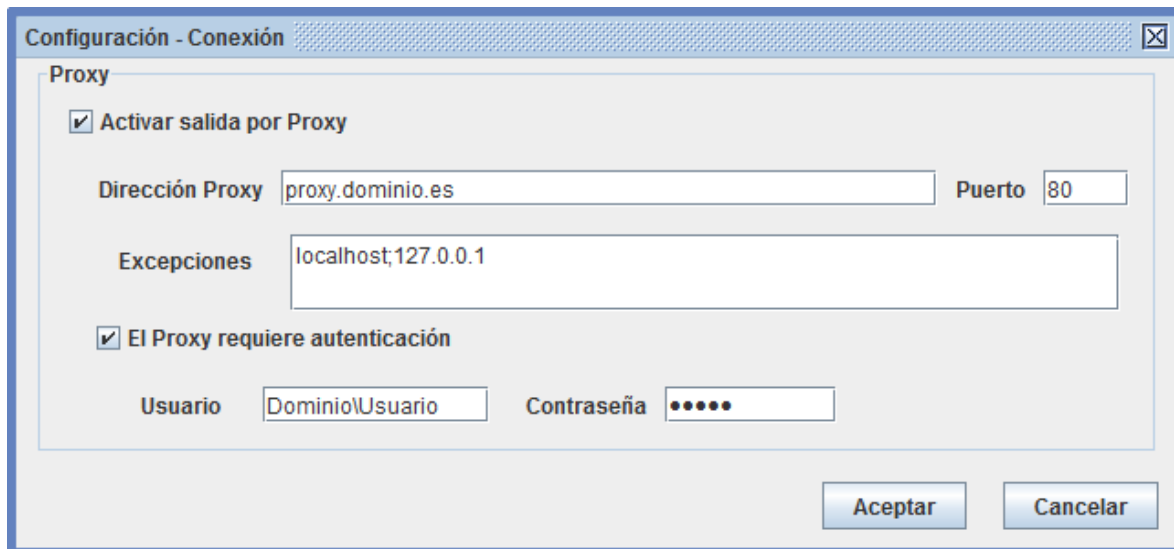
Se iniciarán una serie de test para comprobar el correcto funcionamiento de la aplicación y se abrirá el manual de usuario. En caso de que algo falle se indicará dónde se encuentra el problema para poder solucionarlo. Pulsando en el botón “Finalizar” se terminará con el asistente de configuración.

## 4.2. Configuración de la aplicación de forma manual

<u>C</u> onfiguración	<u>A</u> yuda
<b>Asistente de configuración</b>	
Conexión	Alt-N
Firma	Alt-M
Almacén de certificados	Alt-O
Rol de Firma	Alt-B
Directorios	Alt-D
Firma de múltiples documentos	Alt-T
Esquemas	Alt-E
Apariencia de la aplicación	Alt-X
Administrador de la confianza	Alt-U
Validadores OCSP	Alt-R
Conversor PDF	Alt-I
PDF con datos de firma	Alt-P

La opción “Configuración” nos permitirá lanzar de nuevo el Asistente de Configuración si queremos reconfigurar varias opciones de la aplicación.

La ventana que aparece al escoger la opción de configuración llamada “Conexión” permite indicar la URL de un servidor Proxy, opcionalmente autenticado, que permita al programa eCoFirma acceder a Internet si el usuario navega a través de un Proxy. La ventana tiene el siguiente aspecto:



**Configuración - Conexión** [X]

**Proxy**

☒ Activar salida por Proxy

Dirección Proxy  Puerto

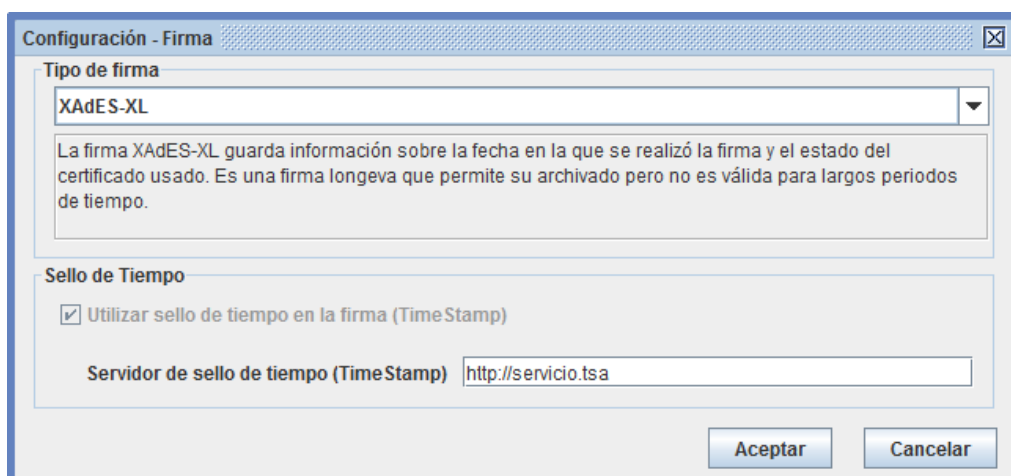
Excepciones

☒ El Proxy requiere autenticación

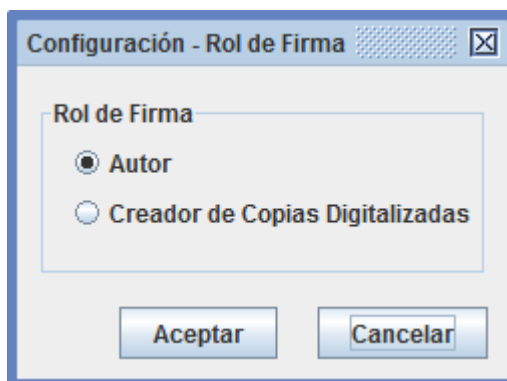
Usuario  Contraseña

**Aceptar** **Cancelar**

La ventana que aparece al escoger la opción de configuración llamada “Firma” permite indicar el nivel de firma XAdES que generará la aplicación. Por cada nivel seleccionable existe una descripción pormenorizada y una serie de requisitos. Puede encontrar más información en el [punto 4.2.4](#) del presente manual. La ventana tiene el siguiente aspecto:



La ventana que aparece al elegir la opción de “Rol de Firma” en el menú es la siguiente:

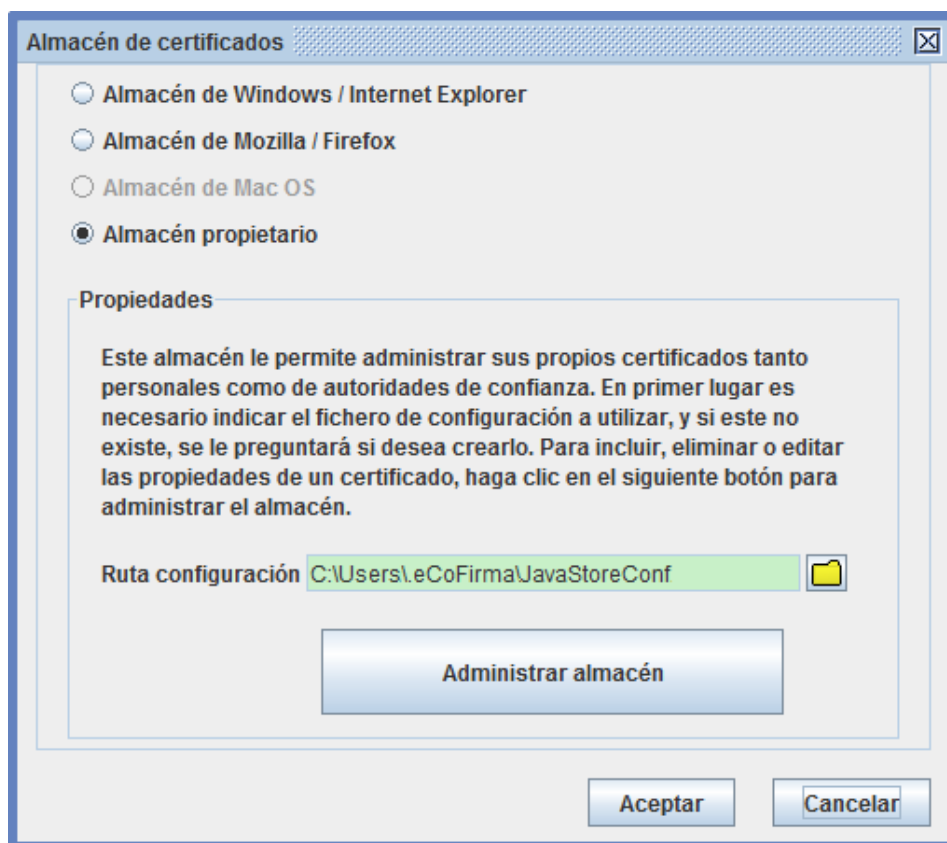


En esta ventana tendremos la posibilidad de seleccionar entre dos opciones de firma, excluyentes entre sí:

1. Firmar con el rol de firma *Autor* (opción por defecto).
2. Firmar con el rol de firma *Creador de Copias Digitalizadas*.

Estas opciones indican el rol o papel que asume el firmante al generar una firma electrónica XAdES, indicando si es el autor del contenido firmado o se trata de una copia/compulsa.

La ventana que aparece al elegir la opción de “Almacén de certificados” en el menú es la siguiente:



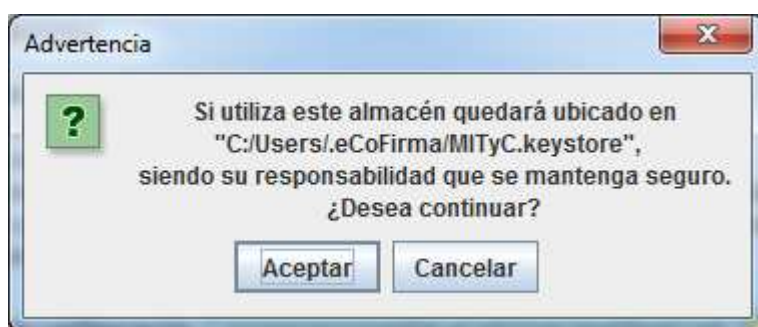
En esta ventana podemos escoger entre el repositorio de certificados contenidos en Internet Explorer, el almacén de certificados contenido en el navegador Mozilla Firefox, el almacén de certificados del sistema operativo Mac OS X o un cuarto almacén propietario. En el caso de seleccionar el almacén de Firefox, es preciso indicar la ruta a su perfil. Para ello, utilice el botón de ayuda que abrirá una página en su navegador Firefox (en otro navegador no funcionaría) con la información de la ruta al perfil.

Para utilizar el almacén propietario, es necesario indicar un fichero donde se puedan encontrar las propiedades de configuración de este tipo de almacén, es decir, donde se encuentra el fichero físico que compone el almacén propiamente dicho, y en caso de que existan, las rutas a los drivers de acceso vía PKCS#11 a otros dispositivos, como tarjetas inteligentes.

En caso de que utilice el almacén por primera vez, presione el botón que contiene el icono de una carpeta e indique la ruta donde desea que este fichero se auto-genera. Se le propondrá un

valor por defecto. Finalmente, una vez que se ha creado el fichero de configuración, presione el botón “Administrar almacén” para que el nuevo almacén de certificados se auto genere. Durante éste proceso, se le pedirá que indique las contraseñas que serán necesario indicar para poder acceder a éste almacén.

Al finalizar, si se seleccionó el almacén propietario, se mostrará una advertencia de seguridad. Puede encontrar más información en el [punto 4.2.7](#) de este manual.

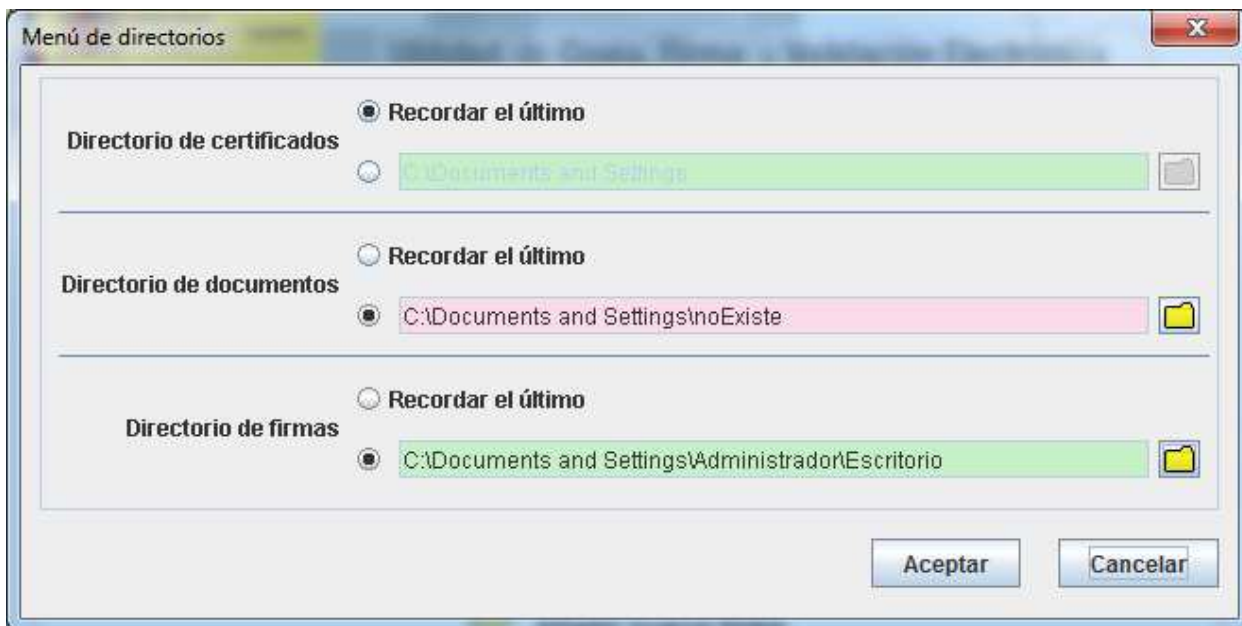


La ventana que aparece al escoger la opción de configuración llamada “Esquemas” permite configurar los algoritmos que se van a emplear en las firmas y cálculo de huellas. Puede encontrar más información en el [punto 4.2.5](#) del presente manual. La ventana tiene el siguiente aspecto:






La ventana que aparece al elegir la opción de “Directorios” en el menú es la siguiente:

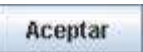



En esta ventana podemos escoger los directorios en los que se situará cada uno de los diálogos de cargar/salvar ficheros al lanzarse.

Se distingue entre tres tipos de diálogos en función del tipo de archivo a cargar/salvar: el directorio para certificados, el directorio para documentos y finalmente, el directorio que se mostrará para cargar/salvar firmas.

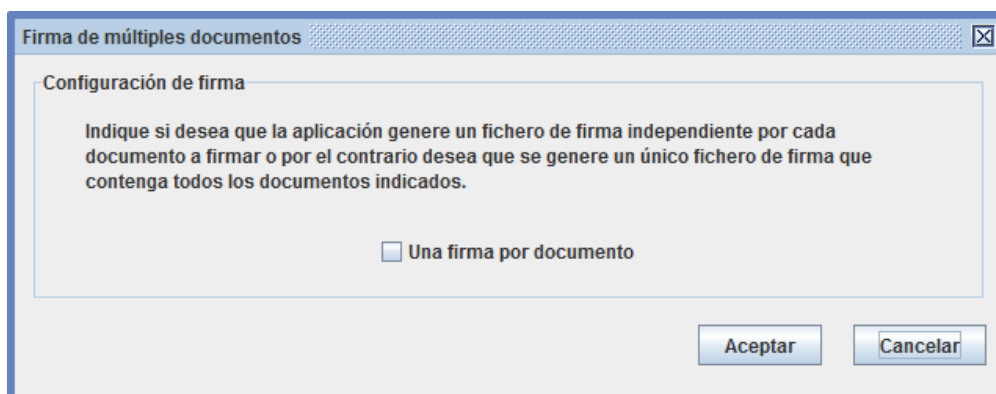
El diálogo le ofrece la posibilidad de escoger entre dos opciones. La primera opción consiste en que la aplicación salve el directorio seleccionado cada vez que se realice una operación de cargar/salvar. De ésta forma, la próxima vez que lance una operación de este tipo, el diálogo que se muestre se ubicará en la misma ruta que se utilizó por última vez. La segunda opción da la posibilidad de que se indique directamente la ruta sobre la que se desea que se ubique el diálogo en la próxima operación de cargar/salvar, de manera fija.

Para cambiar el directorio en la segunda opción es necesario presionar en el botón a la derecha del cuadro de texto () . Se mostrará un cuadro de diálogo para que seleccione o escriba el directorio deseado. El propio diálogo muestra, mediante el color de fondo del área de texto que contiene al directorio, si la ruta indicada existe o no.

Finalmente, para aceptar los cambios introducidos en la configuración de las distintas opciones hay que pulsar el botón “Aceptar”  o, en caso contrario, el botón “Cancelar”  para deshacer las modificaciones realizadas en la configuración.



La ventana que aparece al escoger la opción de configuración llamada “Firma de múltiples documentos” permite parametrizar el comportamiento de la aplicación cuando se va a firmar más de un documento. En caso de seleccionar una firma por documento, se generará un fichero XSIG por cada documento, en procesos sucesivos de firma. La ventana tiene el siguiente aspecto:

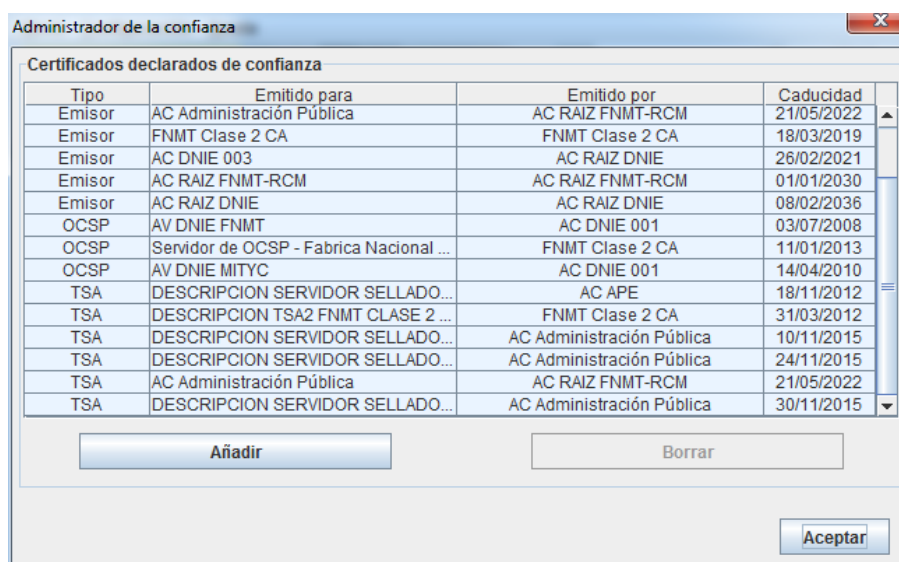


La ventana que aparece al escoger la opción de configuración llamada “Apariencia de la aplicación” permite escoger entre diferentes aspectos gráficos. También es posible utilizar el aspecto por defecto que tenga definido la plataforma de ejecución. La ventana tiene el siguiente aspecto:



La ventana que aparece al escoger la opción de configuración llamada “Administrador de la confianza (Alt+U)” permite administrar el repositorio de confianza automática.

Si se hace clic sobre esta opción de menú, se mostrará un cuadro de diálogo que contiene los certificados públicos incluidos por el usuario en el sistema de confianza y un par de botones que permiten incluir nuevos certificados o borrarlos. Puede encontrar más información en el [punto 4.2.6](#) del presente manual. La ventana tiene el siguiente aspecto:



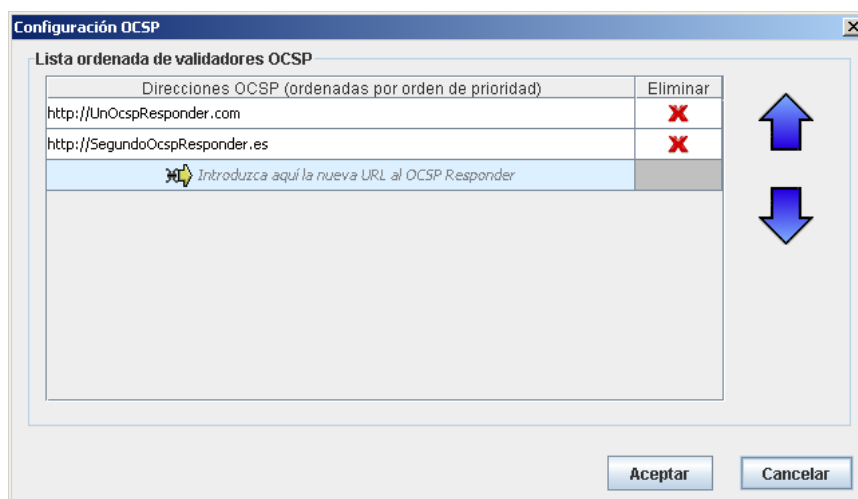
## 4.2.1. Validadores OCSP

Cuando una autoridad de certificación (CA) emite un certificado, le asigna automáticamente un periodo de validez, y un estado de revocación. El periodo de validez es un plazo de tiempo definido durante el cual el uso del certificado está habilitado. El estado de revocación es un estado de validez que la CA asigna al certificado, y que puede cambiar de valor en cualquier momento. Dicha validez puede tener dos estados diferentes, “certificado válido” o “certificado revocado”. La utilidad de éste sistema de estados consiste en definir un mecanismo con el cual deshabilitar el uso indebido del certificado en caso de que éste quede comprometido, ya sea por robo, pérdida, deterioro, etc...

Para que el estado de un certificado pueda ser consultado, las CAs publican unos servicios Web que bajo un protocolo dado, el protocolo OCSP (Online Certificate Status Protocol) que permite realizar una consulta sobre un certificado en concreto. El servicio Web responderá a la consulta de tres maneras distintas, “Certificado válido” cuando el uso del certificado está declarado como legítimo, “Certificado revocado” cuando el certificado ha sido deshabilitado y “Certificado desconocido” en caso de que la CA no disponga de datos sobre el certificado consultado.

La aplicación eCoFirma permite realizar consultas sobre el estado de un certificado siguiendo éste mecanismo de validación. Para ello, se ha de configurar la aplicación para que realice las consultas OCSP a una URL en concreto.

La opción de configuración que permite configurar las URLs de los validadores OCSP se encuentra en “Configuración/Validadores OCSP”. Al hacer clic sobre dicha opción, aparecerá un diálogo con el siguiente aspecto.



Como se puede observar, se trata de una lista ordenada con las direcciones donde se encuentran ubicados los servicios de validación. El estado de revocación de un certificado se irá consultando contra las URL configuradas empezando por la primera en adelante, hasta que se obtenga una respuesta relevante para conocer el estado del certificado.

Para agregar una nueva URL, haga clic sobre la última fila de la tabla e introduzca la dirección.

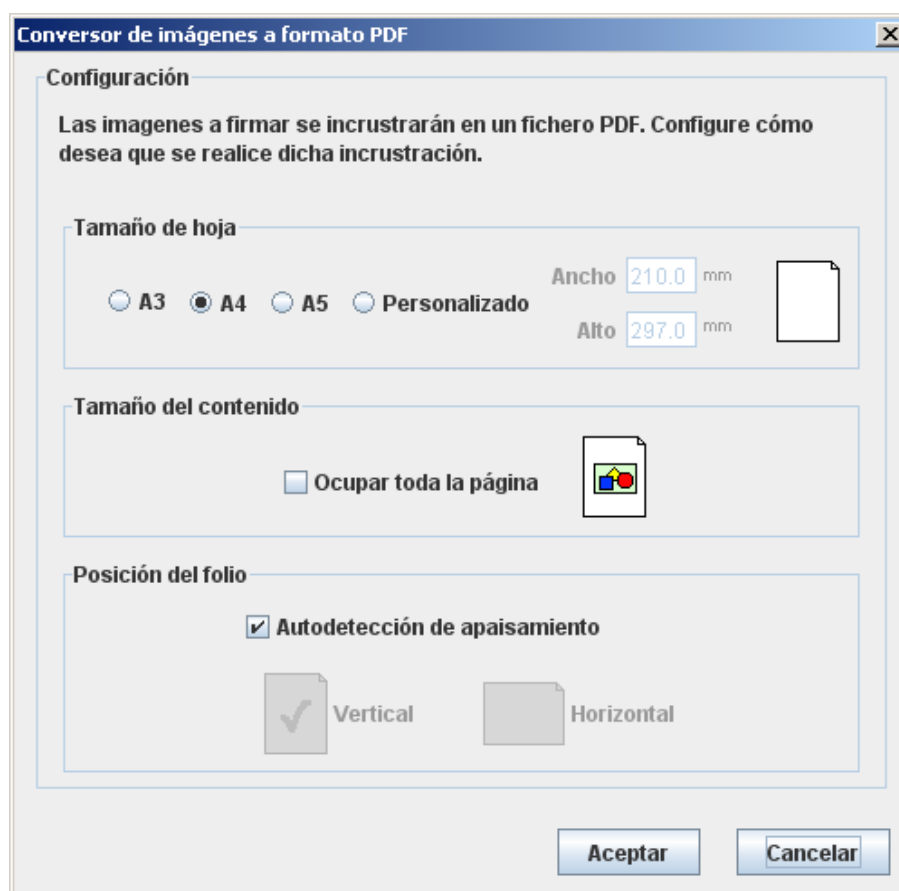
Para eliminar una URL, haga clic sobre el aspa que aparece a su derecha.

Para modificar una URL, haga doble clic sobre la fila en cuestión e introduzca las modificaciones. Finalmente, presione *Intro* o haga clic fuera de la línea para fijar los cambios.

Para modificar el orden de una URL, haga clic sobre la fila para seleccionarla y muévala libremente utilizando las flechas que aparecen en la derecha del diálogo.

## 4.2.2. Conversión de imágenes a PDF

El programa eCoFirma implementa la posibilidad de que, en caso de que se firmen imágenes, éstas sean introducidas dentro de un único fichero PDF, siguiendo una configuración parametrizable:



Esta conversión se realizará en función de la configuración de usuario, en la cual se puede especificar el tamaño que tendrá la hoja sobre la que se incrustará la imagen. También se puede especificar si se desea que se conserven los tamaños de imagen originales o se desea que las imágenes se reescalen hasta ocupar todo el espacio disponible en la página. Finalmente, en el tercer apartado, se puede especificar la posición de la página, o dejar que se detecte automáticamente qué posición es más conveniente, en función de las proporciones de la/s imagen/es a incrustar.

Para introducir imágenes en un fichero PDF que será firmado, y de esta forma poder explotar las ventajas que ofrecen los ficheros PDF, tan solo hay que seguir el proceso normal de firma.

Si todos los ficheros introducidos en el momento de agregar documentos a firmar, son ficheros de tipo imagen, al pulsar el botón “Siguiente” automáticamente se introducirán la/s imagen/es en un fichero PDF.

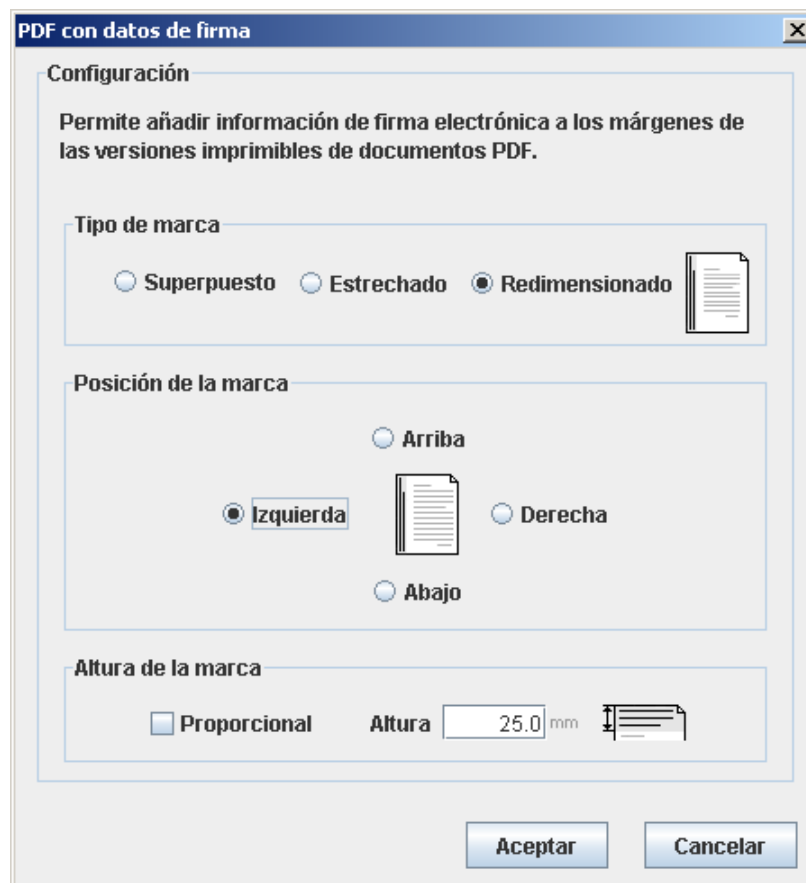
### 4.2.3. Visualización con datos de firma

El programa eCoFirma implementa la posibilidad de que se visualicen ficheros PDF (o imágenes, dado que es posible convertirlas a PDF, como se explica en el apartado anterior), con una zona informativa que contenga datos sobre la firma electrónica asociada, de manera que se pueda visualizar los datos firmados junto con los datos de su firma. Esta área de información también está denominada como “marca de agua”. Para poder acceder a ella, es necesario lanzar un proceso de validación completo sobre una firma, e ir al apartado de ficheros firmados. Si el tipo de fichero firmado lo permite, se habilitará un botón (una gota de agua) que permite abrir el PDF con información de firma en una marca de agua. Del mismo modo, si se hace clic con el botón derecho del ratón sobre la fila correspondiente, aparecerá una opción habilitada para ver el documento con marca de agua.



La marca de agua mostrada es configurable. Para configurar cómo se muestra la marca de agua haga clic en la opción de menú llamada "Configuración/PDF con datos de firma" o presione a la vez las teclas Alt y P.

Se abrirá un cuadro de diálogo en el que podrá definir la posición de la marca de agua en el documento, su relación con el contenido del PDF, y su altura. Si se marca la altura "proporcional", el tamaño de la marca de agua se calculará automáticamente en función del texto a mostrar en la marca de agua y el tamaño del documento sobre el que se va a situar.



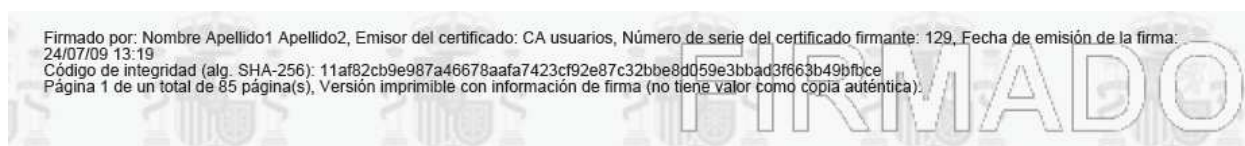
El estilo de marca superpuesta mantiene el documento PDF sin cambios y coloca encima la marca de agua, que es semitransparente. El estilo estrechado, hace el contenido más estrecho, sin mantener las proporciones originales del mismo. En cambio, el estilo redimensionado reescala el contenido manteniendo las proporciones originales.



La marca de agua consiste en una imagen de fondo que muestra el escudo de España en mosaico, junto con la palabra FIRMADO, todo ello con una opacidad semitransparente, y que contiene información sobre todas las firmas que directa o indirectamente hayan firmado el documento a mostrar. Dicha información estará formada por el nombre del actor firmante, extraído de su certificado, el nombre de la autoridad de certificación que lo expidió, el número de serie asignado por la CA al certificado firmante, y en caso de estar disponible, los sellos de tiempo incluidos en la misma. En caso de no disponer de sellos de tiempo, se mostrará la fecha de emisión de la firma.

Seguidamente, se recoge un código de integridad del documento original para que sea posible comprobar que los datos recogidos no fueron modificados. Dicho valor es el resultado hexadecimal de aplicar el algoritmo de Digest indicado entre paréntesis al documento original.

Finalmente, se muestra información sobre el número de página actual de un total de páginas también definido, y un mensaje informativo que ilustra que la marca de agua tiene un valor informativo, sin vinculación legal que asegure que lo que se está mostrando es auténtico.



#### 4.2.4. Selección del nivel de firma

La aplicación eValFirma, por defecto, realiza firmas de tipo XAdES-BES, que son el tipo de firma extendida de menor nivel, en la cual se toman los datos a firmar, se firman y se incluyen datos sobre el certificado firmante y la fecha y hora tomadas del sistema sobre el que se calculó la firma. Cada nivel de firma extiende del nivel anterior, formando un orden jerárquico, en el cual, el nivel mayor de firma XAdES lo engloba todo.

Dicha ventana de diálogo se encuentra accesible haciendo clic sobre la opción de menú llamada “Configuración/Firma (Alt+M)”.

Las firmas XAdES tienen sus raíces en la especificación XMLDSig y a partir de ella extienden el formato. Las firmas XMLDSig (<http://www.w3.org/TR/xmlsig-core/>) son un tipo de firmas basadas en el metalenguaje XML que reciben como parámetros de entrada un contenedor XML sobre el cual se va incluir la firma calculada.

Opcionalmente, la aplicación permite seleccionar entre diferentes niveles de firma XAdES a escoger entre:



- XAdES-BES.- La firma XAdES-BES es la más básica. No permite asegurar que la firma fue realizada antes de una fecha dada o que se realizó con un certificado válido en ese momento.
- XAdES-T.- La firma XAdES-T es similar a XAdES-BES, pero incluye un sello de tiempo que permite asegurar la existencia de la firma antes de una fecha de tiempo. Esta firma no asegura que el certificado usado fuera válido en ese momento.
- XAdES-XL.- La firma XAdES-XL guarda información sobre la fecha en la que se realizó la firma y el estado del certificado usado. Es una firma longeva que permite su archivado pero no es válida para largos periodos de tiempo.



**Configuración - Firma**

**Tipo de firma**

XAdES-XL

La firma XAdES-XL guarda información sobre la fecha en la que se realizó la firma y el estado del certificado usado. Es una firma longeva que permite su archivado pero no es válida para largos periodos de tiempo.

**Sello de Tiempo**

Servidor de sello de tiempo (TimeStamp)

**Aceptar** **Cancelar**

Para aquellas firmas que requieran un servidor de sellado de tiempo, se habilita una campo de texto donde el usuario debe indicar la URL que corresponda.

#### 4.2.5. Selección de esquemas

Con la aplicación eCoFirma es posible seleccionar el tipo de esquema de firma que se va a emplear en las firmas que se expidan a través de una ventana de diálogo.

Dicha ventana de diálogo se encuentra accesible haciendo clic sobre la opción de menú llamada "Configuración/Esquemas (Alt+E)". En el cuadro de diálogo podrá:

- Seleccionar el esquema de firma XAdES a emplear, a escoger entre los esquemas XAdES 1.2.2 y XAdES 1.3.2.
- Seleccionar el algoritmo de Digest a emplear en la firma, a escoger entre SHA-256 y SHA-512.

- Próximamente se podrá emplear también para escoger el algoritmo de Digest de los sellos de tiempo.



Esquemas y algoritmos de Hash

Esquema XAdES de firma <http://uri.etsi.org/01903/v1.3.2#>

Hash de firma <http://www.w3.org/2001/04/xmlenc#sha256>

Hash de sello de tiempo <http://www.w3.org/2000/09/xmldsig#sha1>

Aceptar Cancelar

#### 4.2.6. Administrar el repositorio de confianza

En los procesos de firma electrónica se emplean certificados que contienen datos relativos a la identidad del propietario, que lo identifican unívocamente. Sin un mecanismo que asegure la veracidad de esta información, cabría la posibilidad de que el certificado contenga unos datos falseados o que no se corresponden con la verdadera identidad de aquel que posee la clave privada. Es ahí donde entran en juego las cadenas de confianza.

Las cadenas de confianza consisten en una propagación de la confianza depositada en una entidad oficial (la FNMT, la DGP, etc...) que garantiza la veracidad de los datos firmados que expide. De esta forma, cualquier usuario puede comprobar sin lugar a dudas que el certificado que eventualmente ha recibido fue expedido por una autoridad que es de confianza.

Así pues, el receptor de un documento firmado debe utilizar la clave pública del firmante para comprobar que la firma es válida, y adicionalmente, reconstruir la cadena de certificación (validando las firmas de cada punto de la cadena de certificados utilizando para ello la clave pública del emisor. Es una cadena de firmas) hasta alcanzar un certificado oficial en el cual el receptor *decide* confiar.

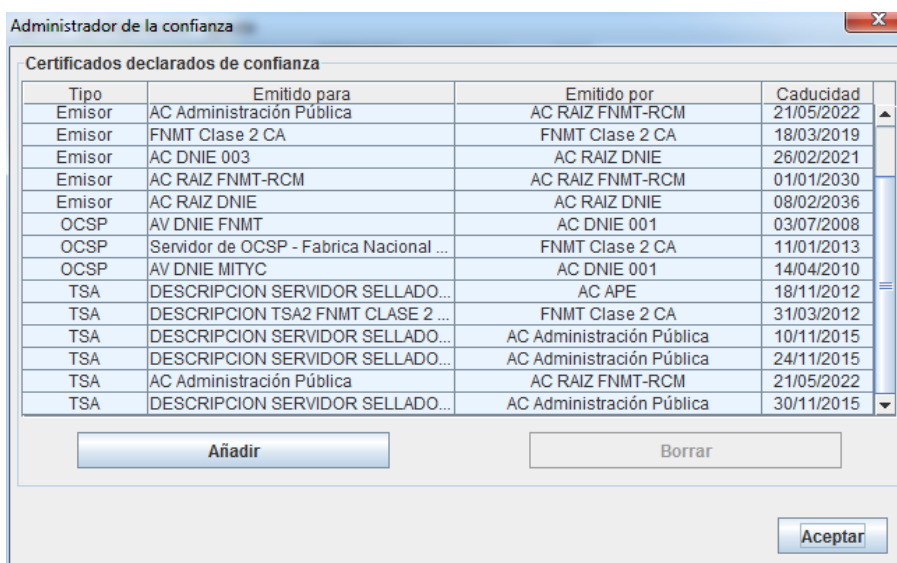
Por lo tanto, los componentes de firma implementan un mecanismo que realiza estas comprobaciones de manera automática. Es decir, cuando se valida una firma electrónica, se valida también cada uno de sus componentes para comprobar que fueron expedidos por una autoridad declarada de confianza.

Para ello, la aplicación eCoFirma contiene un repositorio de certificados declarados por el usuario como de confianza, que debe gestionar el propio usuario ya que es su responsabilidad. De esta manera, la firma que acompaña a los certificados, los sellos de tiempo, respuestas OCSP, etc..., pueden ser validadas para comprobar que fueron expedidas por una entidad que, según el usuario, garantiza la veracidad de lo que expide, y en caso de que esto no sea así, muestre un aviso para que el validador compruebe personalmente si los emisores no recogidos en el sistema son merecedores de confianza o no.

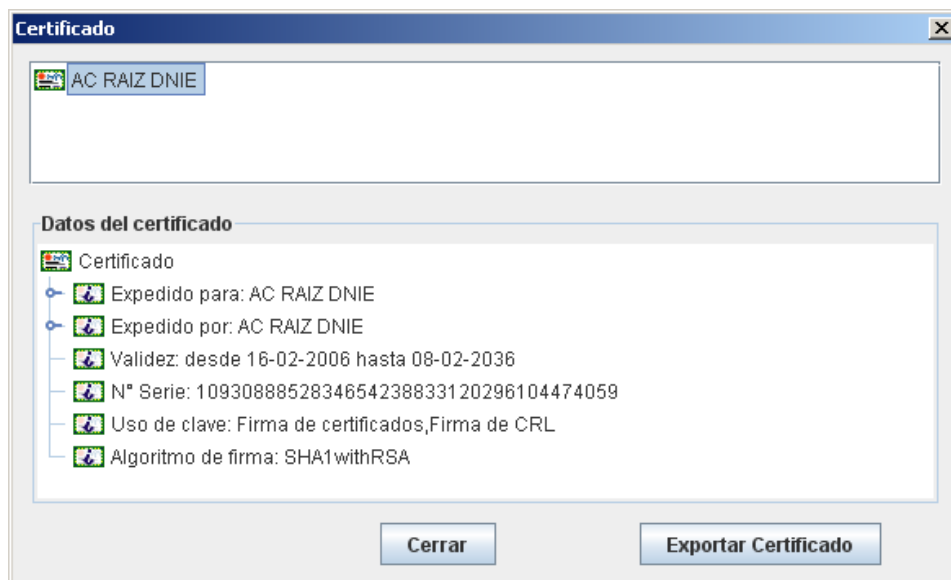
Por defecto, la aplicación eCoFirma asigna como “de confianza” cualquier elemento emitido por la Fabrica Nacional de la Moneda y Timbre, y por los certificados raíz del DNI electrónico. Es responsabilidad del usuario indicar en este repositorio aquellos certificados de otras entidades en las cuales el usuario confía.

La aplicación eCoFirma implementa un administrador para este repositorio de confianza, accesible desde la opción de menú “Configuración/Administrador de la confianza (Alt+U)”.

Si se hace clic sobre esta opción de menú, se mostrará un cuadro de diálogo que contiene los certificados públicos incluidos por el usuario en el sistema de confianza y un par de botones que permiten incluir nuevos certificados o borrarlos



Si se hace doble clic sobre alguno de los certificados se mostrará una ventana flotante que contiene toda la información contenida en el certificado, junto a un botón que permite exportar el certificado mostrado.



Para incluir un nuevo certificado se debe hacer clic sobre el botón “Añadir”. Se mostrará un cuadro de diálogo para que se indique el fichero donde se encuentra el certificado público a agregar al repositorio, y posteriormente, se mostrará un cuadro de diálogo cuya finalidad consiste en que se indique qué tipo de certificado es



- **Certificado de firma de usuario:** Sirve para indicar que el certificado de confianza es de una persona o entidad, únicamente.
- **Certificado emisor de certificados de firma:** Sirve para indicar que se confía en cualquier certificado expedido por el certificado incluido.

- **Certificado OCSP de entidad:** Sirve para indicar que se confía en cualquier respuesta OCSP firmada con el certificado añadido.
- **Certificado emisor de certificados OCSP:** Sirve para indicar que se confía en cualquier certificado firmante de respuestas OCSP que haya sido expedido por el añadido.
- **Certificado emisor de listas de revocación:** Sirve para indicar que se confía en cualquier CRL (lista de certificados revocados) firmada por el certificado incluido.
- **Certificado TSA de entidad:** Sirve para indicar que se confía en cualquier sello de tiempo firmado por el certificado incluido.
- **Certificado emisor de certificados de TSA:** Sirve para indicar que se confía en cualquier sello de tiempo firmado por un certificado que haya sido expedido por el certificado añadido.

Para borrar un certificado del repositorio de certificados de confianza, simplemente seleccione de la lista el certificado que desea borrar y haga uso del botón “Borrar”.

#### 4.2.7. Administrar el almacén propietario de Java

Un almacén de certificados (o Key Store, en inglés) es un recipiente software que almacena certificados y sus claves asociadas, entre otras posibilidades, es decir, es un fichero que hace las veces de repositorio de certificados y claves.

Este almacén se localiza en un único archivo (aunque es posible tener varios archivos o almacenes) y cada archivo se puede editar de tal manera que se pueden introducir nuevos certificados y eliminar o exportar los ya existentes.

La ruta, *path* o ubicación del almacén se llama usualmente “almacén de certificados”. Un almacén tendrá, a menudo, muchos certificados, posiblemente emitidos por varias entidades emisoras distintas.

La información que compone dicho almacén, por lo tanto, consiste en certificados software asociados a una clave criptográfica pública, y opcionalmente, a una clave privada. Los accesos a esa información están protegidos mediante encriptación, haciendo especial hincapié en la protección de las claves privadas.

De ésta forma, en el momento en el que se requiere una autenticación, o se va a realizar una firma electrónica, se accede al almacén de certificados para emplear las capacidades de

los certificados ahí recogidos, que se encuentran clasificados atendiendo a criterios de uso, y protegidos de usos indebidos mediante criptografía.

Generalmente, los usos más comunes de un certificado dependen de si éste tiene una clave privada asociada o no. En caso de tener asociada una clave privada, el certificado será empleado normalmente para realizar labores de firma y autenticación frente a terceros. En cambio, si el certificado sólo contiene su clave pública, será empleado para realizar labores de validación de autenticidad, dado que con la clave pública, se puede comprobar si unos datos fueron firmados empleando la clave privada simétrica. En caso de que dicha validación se cumpliera, los datos estarían firmados por una autoridad de *confianza* y serían aceptables.

Para realizar todas estas validaciones y con el fin de proporcionar una navegación más segura, los navegadores Explorer y Firefox tienen sus propios almacenes de certificados, en los cuales ya se encuentran precargadas unas autoridades de confianza reconocidas, y en los cuales un usuario puede importar sus propios certificados. Se puede acceder al almacén de Explorer haciendo clic en la opción de menú "Herramientas/Opciones de Internet". A continuación vaya a la pestaña "Contenido", y haga clic en "Certificados". Para Firefox, el camino a seguir sería ir a "Herramientas/Opciones". En la pestaña "Cifrado", haga clic en "Certificados" para acceder.

Existen diversas utilidades para manejar toda esta información, aunque mencionaremos solamente y por ejemplo, la utilidad "keytool.exe" (por línea de comandos, incluido en Java JDK o JRE) que es una colección de herramientas que permiten realizar diversas tareas sobre almacenes de certificados. También puede utilizar una aplicación gráfica basada en la utilidad llamada "KeyTool GUI". Es un útil de administración con su propio almacén.

La implementación que el Ministerio de Industria ha escogido para su almacén de certificados se apoya en el estándar PKCS #12, el cual se explica más adelante.

## Un vistazo a los estándares PKCS

PKCS se refiere a un grupo de estándares de criptografía de clave pública, que fueron concebidos y publicados por los laboratorios RSA en California. Dichos estándares fueron evolucionando con el tiempo, por lo que existen estándares obsoletos que ya no se utilizan, y existen estándares que sustituyen a otros o se apoyan en ellos.

En general, se puede decir que estos estándares definen una manera de emplear algoritmos criptográficos para implementar los distintos usos que se pueden conseguir con éstos. Es decir, establecen una manera uniforme de organizar la información para realizar una firma, o para realizar una petición de certificado, etc... Cada uno de estos estándares tiene un ámbito de aplicación acotado, y están diseñados para usos bien definidos. Los principales estándares, y sus principales usos son los siguientes:

Nombre	Ver.	Comentario
PCKS#1	2.1	<a href="#">RFC 3447</a> . Define el formato del cifrado RSA.
PKCS#3	1.4	Estándar de intercambio de claves Diffie-Hellman.
PKCS#7	1.5	<a href="#">RFC 2315</a> Estándar sobre la sintaxis del mensaje criptográfico. Usado para firmar y/o cifrar mensajes en <a href="#">PKI</a> .
PKCS#8	1.2	Estándar sobre la sintaxis de la información de clave privada.
PKCS#11	2.2	Interfaz de dispositivo criptográfico (" <a href="#">Cryptographic Token Interface</a> "). Define un API genérico de acceso a dispositivos criptográficos.
PKCS#12	1.0	<a href="#">Estándar</a> de sintaxis de intercambio de información personal. Define un formato de fichero usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.



## El estándar PKCS 12

Este estándar define un medio de almacenaje de información que será compartida y debe estar protegida. En la arquitectura PKCS12, existen dos formas diferenciadas de compartir la información, el modo privado y el modo público.

Hay cuatro combinaciones de modos privados y modos de integridad según se utilicen políticas de llave pública o de contraseña. Los modos privados utilizan el cifrado para dar **protección** a la información personal frente a una posible exposición pública y los modos de **integridad** protegen la información personal de la falsificación o modificación indebida de ésta. Adicionalmente, el estándar contiene un campo que sigue el estándar PKCS 7, utilizado para firmar el contenido y así asegurar la **autenticación**.

## El estándar PKCS 11

El estándar PKCS 11 es un estándar que define los accesos a dispositivos criptográficos basados en hardware, es decir, se trata del acceso a tarjetas inteligentes, que generan, almacenan y protegen claves criptográficas. Suelen aportar aceleración hardware para operaciones criptográficas de clave pública, que se efectúan dentro del propio hardware.

Es decir, que las labores criptográficas se realizan dentro del propio chip, de manera que las claves implicadas en el proceso no salgan de éste entorno seguro. El protocolo establece vías de comunicación para hacer peticiones a la tarjeta.

Para un correcto funcionamiento de una pasarela de comunicación PKCS#11 con un recurso criptográfico alojado en una tarjeta inteligente, es preciso que el fabricante del *token* (de la tarjeta) provea del *driver* de comunicaciones específico que implementa éste protocolo estándar de comunicación, que normalmente, viajará a través de un lector de tarjetas (el cual también requerirá su *driver* específico).

## El almacén Propietario

El almacén de certificados desarrollado por el ministerio de industria, energía y turismo, es un almacén basado en el estándar PKCS#12, que es un estándar para el almacenamiento de claves privadas, certificados, información secreta y extensiones. La utilidad del uso de un estándar es que cualquier máquina que soporte esta norma puede importar, exportar y emplear un conjunto de informaciones, protegidas con un identificador personal.

El almacén, además, contempla el acceso adicional y configurable a pasarelas PKCS#11 para la comunicación con tarjetas inteligentes, indicando cual es el *driver* de comunicación para el *token* deseado (la tarjeta).

Este almacén consiste en un único fichero, que puede estar ubicado en cualquier soporte físico, cuyo acceso puede estar protegido con contraseña, u opcionalmente, puede dejarse abierto a cualquiera que pueda acceder al mismo.

Los accesos a claves privadas están protegidos adicionalmente. Dicha protección es configurable por el usuario, que puede escoger entre:

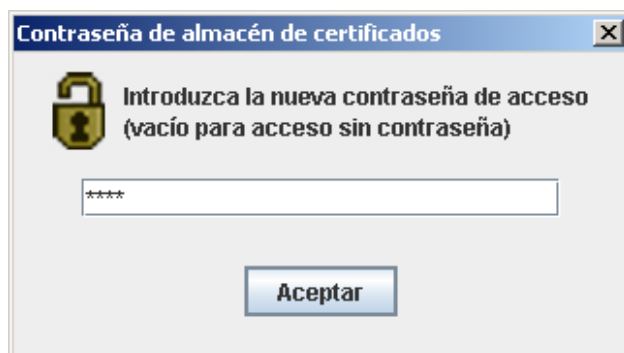
- Acceso con contraseña adicional.- Se pide la contraseña en cada petición de acceso.
- Acceso con contraseña adicional cacheada.- Se pide la contraseña sólo en el primer acceso.
- Acceso con aviso.- Se muestra un aviso en cada acceso, dando la posibilidad al usuario de que cancele.
- Acceso transparente.- Se accede al recurso sin que medie ninguna protección.

## Funcionamiento del administrador

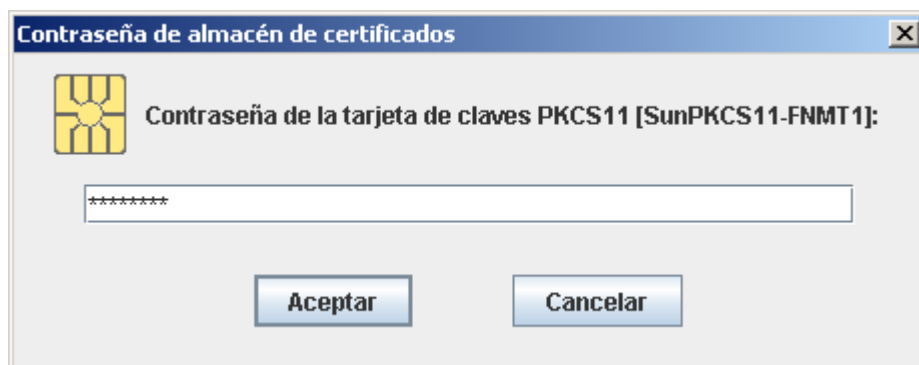
El administrador del almacén es una interfaz que haciendo uso de la interfaz de escritura del almacén, permite importar, exportar, actualizar o borrar certificados, así como configurar la protección que se desea. Su funcionamiento es el siguiente:

En primer lugar, es preciso levantar la instancia del almacén. Para ello se debe proveer de un fichero de configuración. Dicho almacén emplea internamente el proveedor propio de SUN para la clase *KeyStore*, llamado “JCEKS”. Puede consultar la información sobre dicha clase en el API de Java.

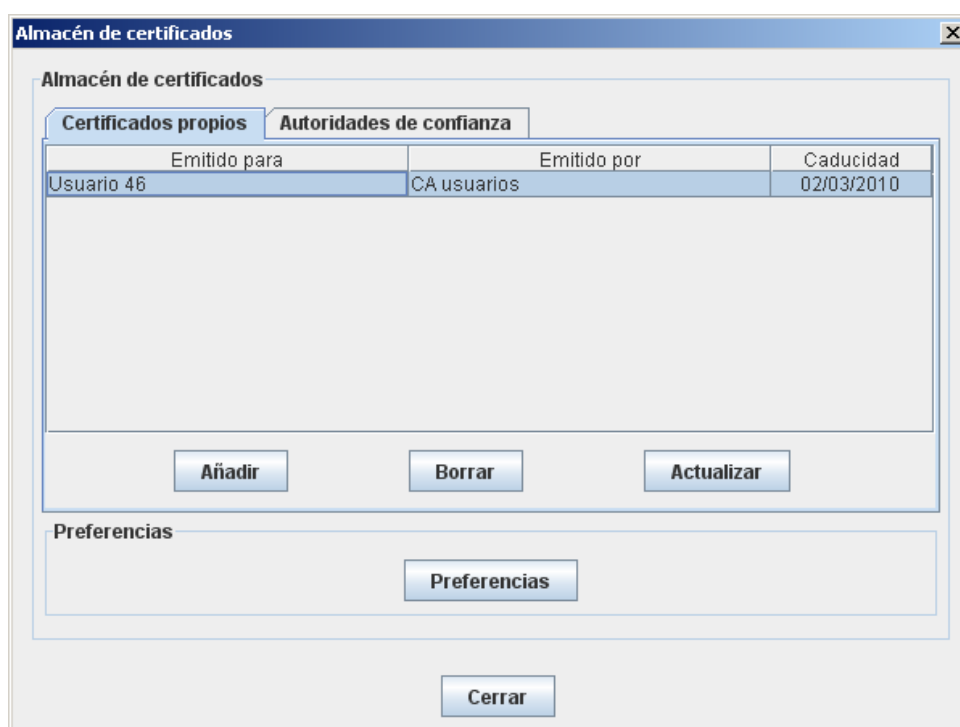
Si el almacén no existe y se autogenera, se pedirá al usuario que introduzca la contraseña de protección que se pedirá en los futuros accesos al almacén.



Si la configuración del almacén incluye *drivers* para accesos PKCS 11 a tarjetas inteligentes, y se detecta que existe una introducida en el *slot* del lector, se accederá automáticamente a ella, pidiendo, en caso de que sea necesario, el PIN.



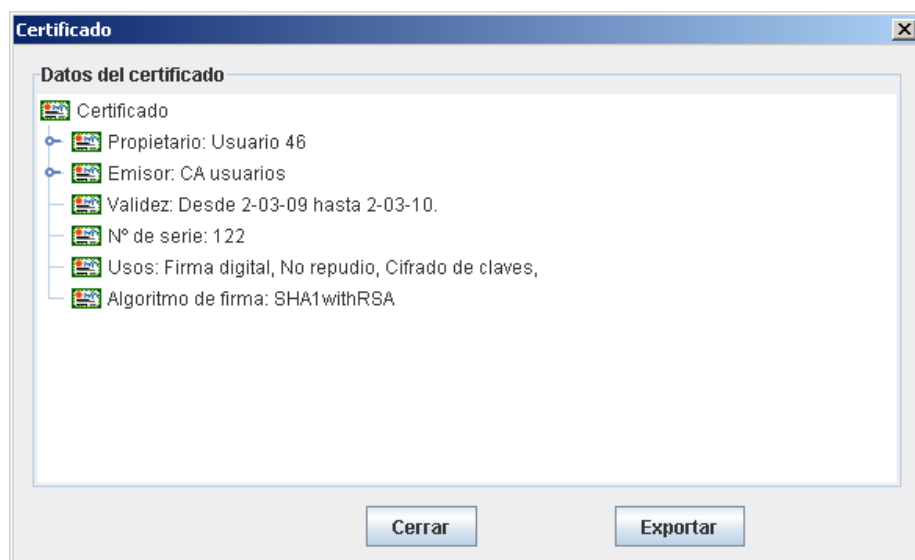
Una vez que se ha accedido al almacén, se muestra su contenido en dos tablas. Está la tabla de certificados propios, que son certificados de firma, con clave privada asociada, y las autoridades de confianza, solo con clave pública. Cada tabla tiene tres botones asociados para realizar las tareas comunes, es decir, hay un botón para importar un certificado, borrarlo o actualizarlo.



En el caso de las autoridades de confianza, no se permite actualizar certificados.

Cada tabla muestra tres tipos de datos sobre los certificados que contiene. El primero de los datos indica quién es el propietario del mismo, la segunda columna de la tabla muestra que fue el emisor que lo expidió y la tercera cabecera indica cual es su fecha de caducidad.

Si se hace doble clic sobre cualquiera de los certificados, se mostrará una ventana de información con los datos pormenorizados más relevantes de dicho certificado. Además, dicha ventana permite exportar el certificado *X509Certificate*. En ningún caso se permite exportar la clave privada asociada, en caso de que exista.



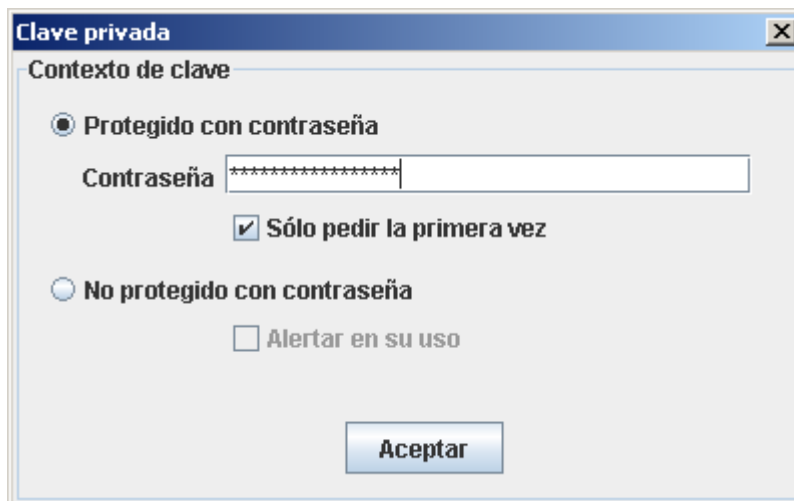
Si se desea borrar un certificado del almacén, haga clic en el botón "Borrar". El borrado será automático para el caso de los certificados de autenticación. En el caso de los certificados de firma, el borrado incluye también el borrado del par de claves asociadas al mismo, por lo que se requiere un acceso a la clave privada. En caso de que la clave privada a borrar está protegida, se seguirá el mismo protocolo de seguridad que se sigue en los accesos a claves privadas.

A continuación se explica el funcionamiento de una importación de certificado. En el siguiente apartado podrá ver cómo es el sistema que permite indicar el contexto de seguridad a aplicar para los accesos a las claves privadas.

Si se desea añadir un certificado al almacén, haga clic en el botón “Añadir”. Se mostrará un diálogo para que indique la ruta del fichero que contiene el certificado, que podrá ser un fichero “.p12” (para certificados con clave privada, según PKCS 12) o un “.cer”.

Si el contenedor del certificado está protegido con contraseña, se pedirá que la indique. Es posible que el acceso a la clave privada también esté protegido por contraseña.

A continuación, se muestra el diálogo que le permite indicar cual es el contexto de seguridad a aplicar en los futuros accesos a claves privadas. En él puede establecer que el acceso se proteja mediante una contraseña, o que no se proteja de ningún modo.. También puede simplemente indicar que se avise en su uso.



Cada cambio en el almacén de certificados es automáticamente salvado, por lo que cada acción realizada será irreversible, por políticas de seguridad. Tenga cuidado con las acciones que realiza en el administrador para no perder información.

## El fichero de configuración

El fichero de configuración indica dónde se encuentra situado físicamente el almacén de certificados a cargar, es decir, el *path* donde se encuentra el fichero PKCS 12.

Además, el archivo de configuración indica dónde se encuentran los *drivers* para la comunicación con tarjetas inteligentes. Habrá una entrada para cada uno de los prestadores que se soportarán, indicando nombre y ruta al *driver*.

```
##### Almacén de certificados #####  
  
# Uso: KeyStoreName=./.keystore  
  
##### Rutas a librerías PKCS#11 #####  
  
# Uso: <prefijo>.name =  
#      <prefijo>.library =
```

## Incluir un driver para el acceso PKCS#11

La interfaz gráfica de administración del almacén dispone de un botón, llamado “Preferencias”, que al ser pulsado permite realizar dos acciones, cambiar la contraseña de acceso al propio almacén y enlazar con un *driver* de acceso a tarjetas inteligentes.



Para enlazar un *driver*, simplemente pulse el botón añadir e indique la ruta al *driver*.



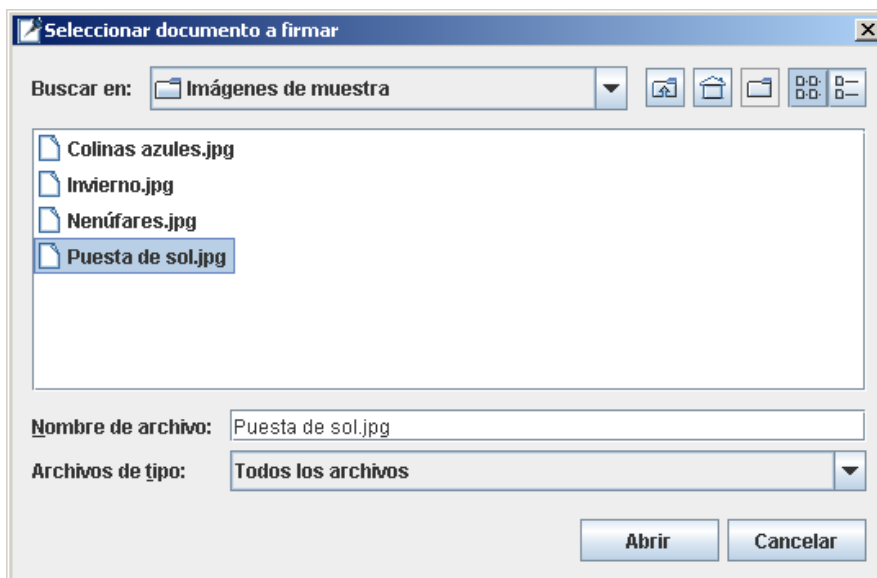
## 5. Uso de la utilidad

### 5.1. Firma electrónica de un archivo

La firma electrónica XADES de un documento se realiza desde el menú principal de la aplicación pulsando en el botón “Firmar documento original”.



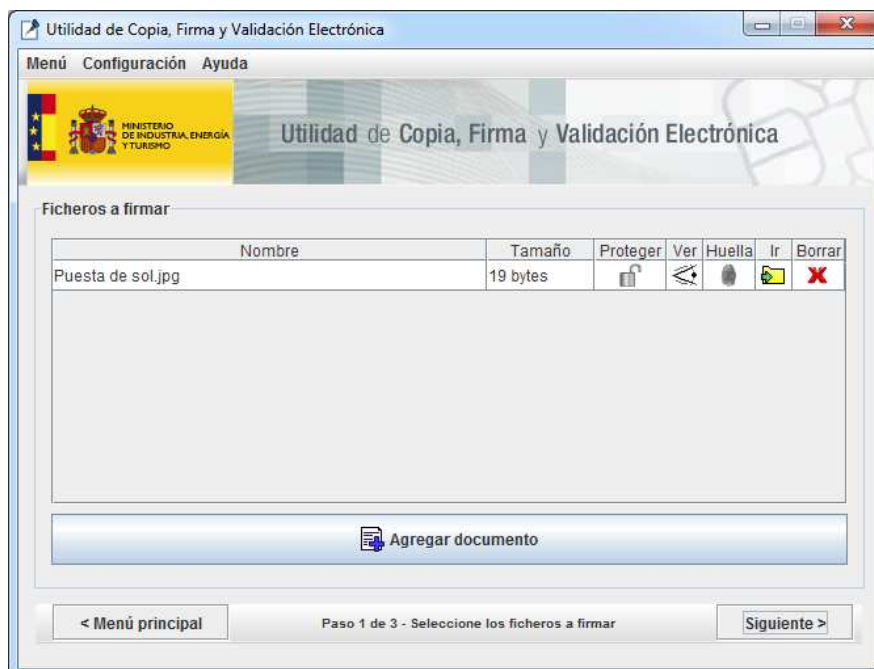
Al pulsarlo se nos abrirá una ventana que nos permitirá seleccionar el documento que queremos firmar.

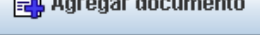


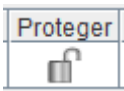




Seleccionamos el fichero deseado y finalizamos pulsaremos el botón “Abrir”.




El fichero seleccionado aparecerá cargado, con toda su ruta, en la siguiente ventana (si hemos cancelado la selección no aparecerá ningún fichero cargado).



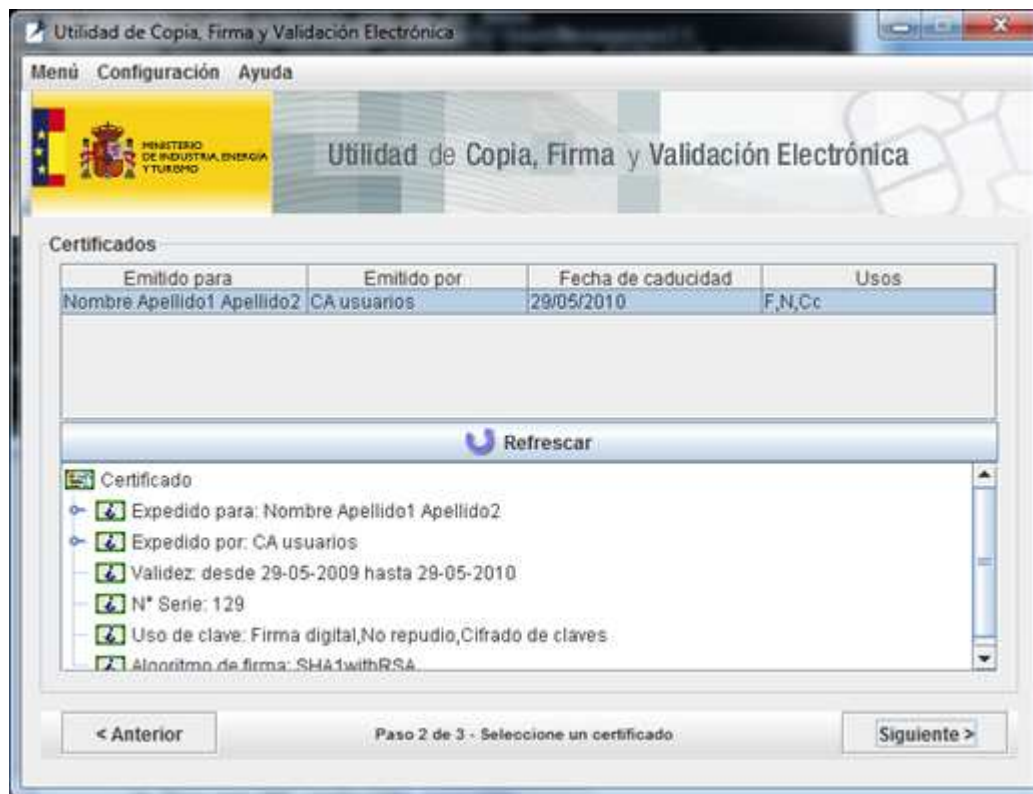
Pulsando el botón “Agregar documento”  se nos permitirá seleccionar otro fichero para firmar. En la parte derecha de la tabla aparece un conjunto de botones para realizar distintas acciones. Estos botones son:

- El botón “Proteger” , permite codificar los datos previamente para protegerlos de accesos no autorizados. Puede ver más información en el [punto 5.5.1](#).
- El botón “Ver” , realiza una petición al sistema operativo para abrir el fichero.
- El botón “Huella” , permite calcular la huella de un fichero mediante distintos algoritmos. Puede encontrar más información en el [punto 5.6](#).
- El botón “Ir” , abre la carpeta contenedora del documento,
- El botón “Borrar” , permite borrar el fichero de la lista de documentos a firmar.

Tras agregar el/los fichero/s pulsaremos en “Siguiente”  con lo que se nos mostrará el paso 2 del asistente de firma. En dicho apartado seleccionaremos el certificado con el que deseamos realizar la firma digital. El certificado debe estar ubicado en el almacén de certificados de Windows o Mozilla de manera que sea accesible para las aplicaciones de firma electrónica. La aplicación buscará de forma automática los certificados almacenados. Si no encontrara ningún certificado, la aplicación nos daría una advertencia y volvería al paso anterior.



Si los certificados estuviesen almacenados en una tarjeta criptográfica, es posible que el sistema operativo se demorase en leer el contenido de la tarjeta, por lo tanto, debería hacerse un nuevo intento tras aguardar un momento. Con los certificados digitales cargados la aplicación presenta una nueva ventana.





El cuadro superior presenta una lista de certificados cuyo uso permite la firma de documentos. Se selecciona el primero de ellos por defecto. El cuadro inferior muestra en un modo de presentación tipo árbol los datos del certificado seleccionado: para quién y por quién fue expedido, su validez, su número de serie, los usos permitidos para el certificado y el algoritmo que utiliza para la firma.

Una vez que se selecciona el certificado deseado se continúa el proceso pulsando en el botón "Siguiete". **Siguiete >** Para escoger otro documento distinto al que ya se ha seleccionado, o para agregar nuevos documentos a la firma, se pulsa el botón "Anterior" **< Anterior** y se vuelve al primer paso en donde es posible cambiar la selección de ficheros.

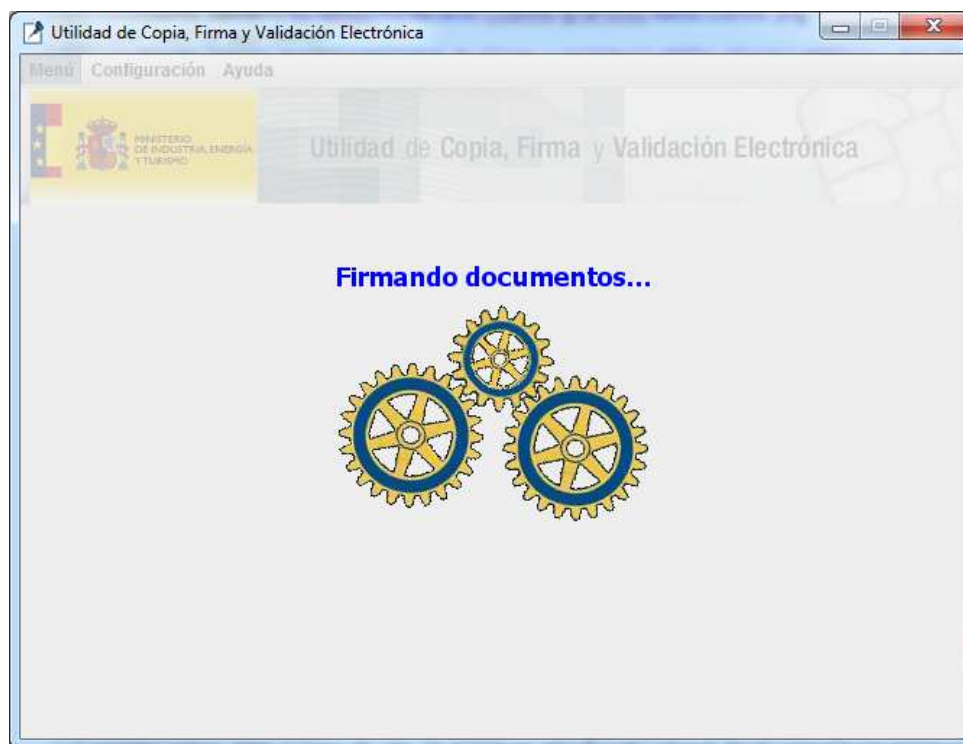
A continuación se abrirá una ventana para indicar dónde guardar el fichero XML de firma.



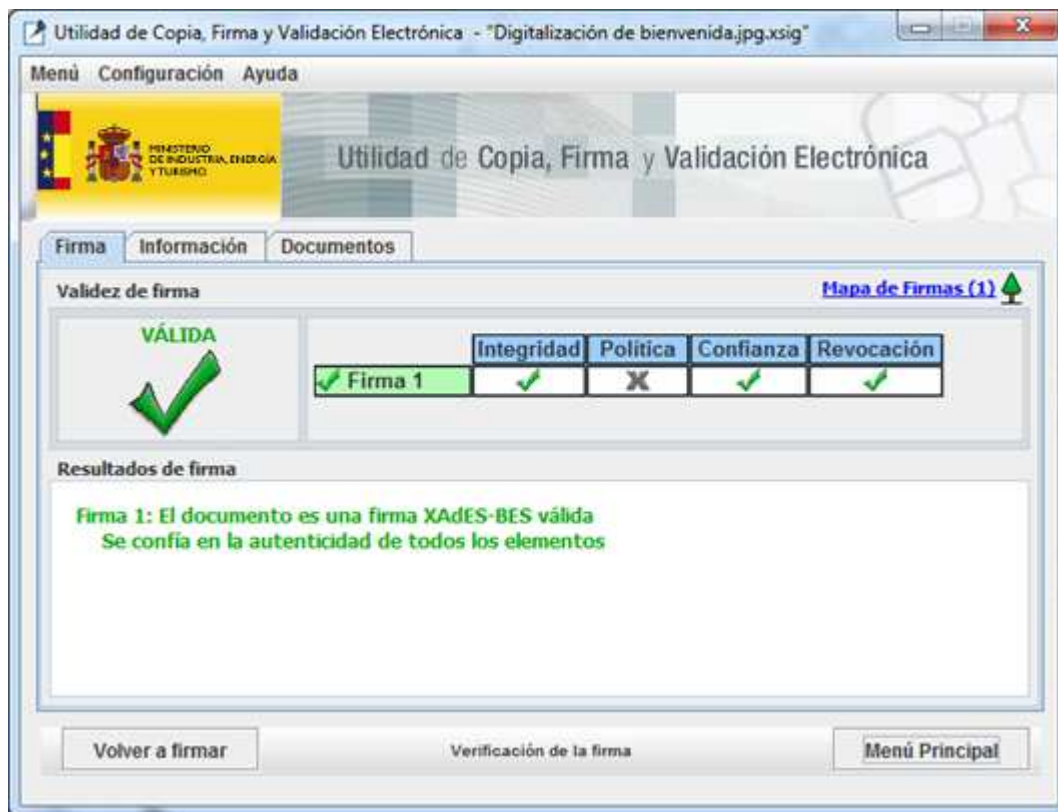
Para guardar el fichero XML, escriba un nombre (por defecto utiliza la extensión xml), escoja la ruta dónde quiere almacenarlo y luego pulse el botón “Guardar”.  Si escoge pulsar el botón “Cancelar”  el proceso se perderá y deberá volver a generarlo para poder guardarlo.

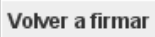


En el tercer y último paso se genera la firma digital XADES. El tiempo en que se tarde en firmar el documento depende del tamaño del/de los fichero/s y de las claves criptográficas utilizadas (por ejemplo, la clave del DNle es una clave larga, y por lo tanto, es un dispositivo lento en firmar). Para poder firmar el documento se le requerirá en algún momento que introduzca en PIN de seguridad correspondiente al certificado seleccionado, en caso de que se encuentre protegido.



Una vez finalizada la firma, la aplicación automáticamente presentará una ventana de validación con el documento firmado.



Los detalles sobre esta ventana serán explicados en el apartado siguiente. Baste decir que si se pulsa sobre el botón “Volver a firmar”  se iniciará un proceso de contrafirmado (Véase el [punto 5.7](#) del presente manual), es decir, permitirá añadir otra firma en cadena al fichero de firma que se acaba de generar.

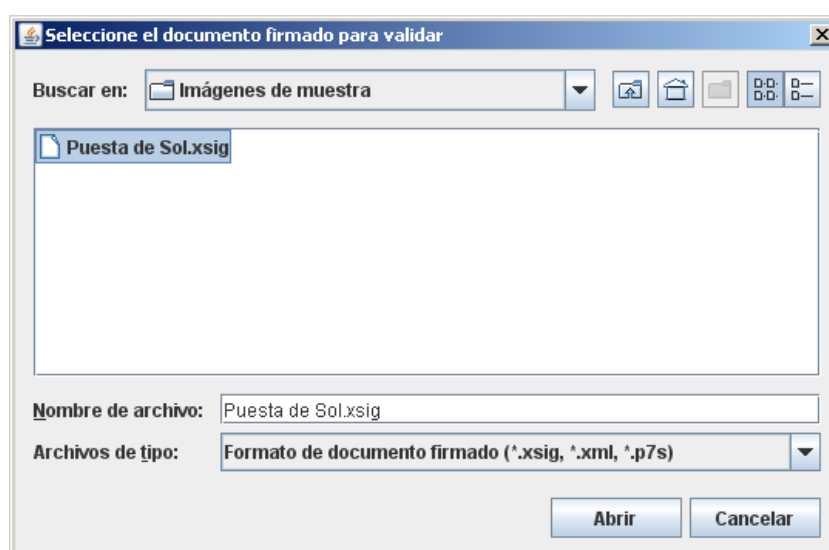
## 5.2. Validación de una firma


La validación de una firma electrónica XADES se realiza desde la aplicación pulsando en el botón “Validar firma” del menú principal. La validación incluye la validación de los campos firmados en el documento XML, la garantía de que los ficheros firmados no se han modificado y el “no repudio” del documento por el poseedor del certificado electrónico que firmó el documento.





Tras pulsar el botón se nos muestra una ventana emergente en dónde deberemos escoger el fichero firmado que deseamos validar.



Una vez seleccionado el fichero correspondiente pulsamos en el botón “Abrir”  para proceder con la validación o “Cancelar”  para volver al Menú principal.

Los resultados de validación de la aplicación eCoFirma tratan de ofrecer en un rápido vistazo la información recogida sobre los resultados obtenidos. Tras validar una firma electrónica, se obtiene un resultado desglosado en tres partes fundamentales:

- **Resúmenes:** Se trata de la ventana de resumen donde se indica rápidamente la valoración que se ha realizado sobre la validez de la firma y en caso de error, cuál es el problema que se ha detectado.
- **Información:** En esta pestaña se muestra desglosado cada uno de los extraídos de la/s firma/s validada/s. Se puede así observar la fecha de firma, el certificado firmante, si se incluyen sellos de tiempo, etc...
- **Documentos:** En esta pestaña se muestran los contenidos firmados. Cada línea contiene el nombre del documento, el tamaño, la firma que lo asegura y un color de fondo que indica el resultado de validación. En la parte derecha se muestran iconos para visualizar el documento firmado, visualizar el documento con información de firma (sólo en ficheros con formato PDF) y una tercera opción para exportar el documento.

La ventana de resúmenes muestra un cuadro con un resumen general que informa del resultado de todo el proceso de validación, seguido de una tabla donde se desglosan por firma los criterios de integridad, políticas si las hubiera, estado de confianza de los elementos presentes y estado de revocación.



Los iconos de resultado pueden ser de cuatro tipos.



Un resultado correcto se indica mediante el icono verde. En caso contrario, se marcará con el icono rojo. Si no se dispone de información suficiente como para asegurar nada, se utiliza el icono amarillo. El icono gris se emplea cuando el criterio no se aplica en la firma actual.

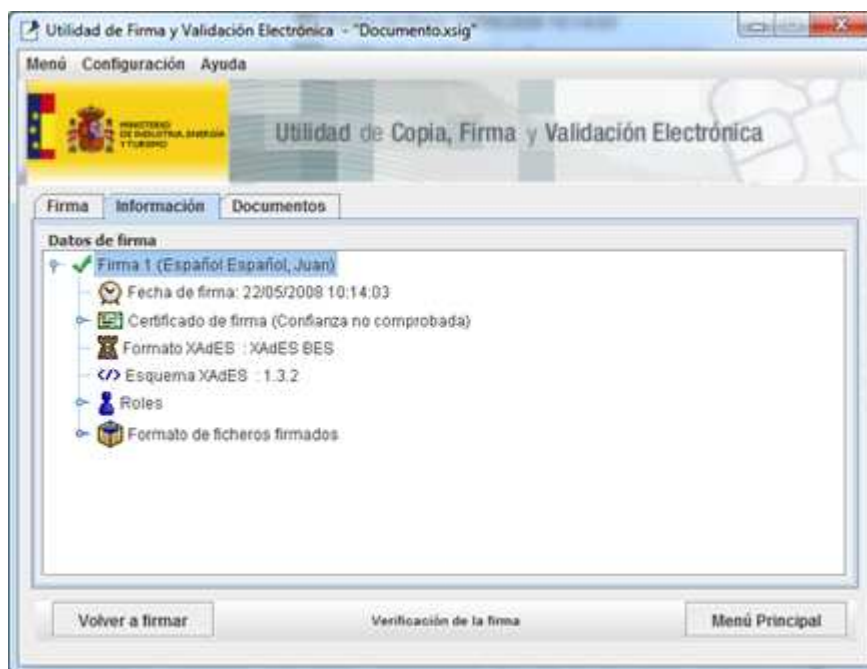
Adicionalmente, si se pulsa con el ratón sobre alguno de los valores en la tabla de resultados se abrirán diálogos explicativos que indican pormenorizadamente cuál es el problema detectado, por qué es un problema de seguridad y algunas sugerencias sobre cómo resolverlo.

Por ejemplo, si se hace clic sobre la cruz roja que aparece en la columna llamada “Confianza”, aparecerá un cuadro flotante que, aparte de la información que anteriormente se mencionaba, contiene un par de botones que permiten llegar a un diagnóstico del problema (visualizar el certificado firmante) o llevar a cabo una tarea que lo resuelva (agregar el certificado de la CA al sistema automático de confianza).

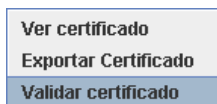


Al final de la pestaña se muestra una descripción rápida del tipo de firma validado y una descripción del problema detectado en caso de que se produzca.

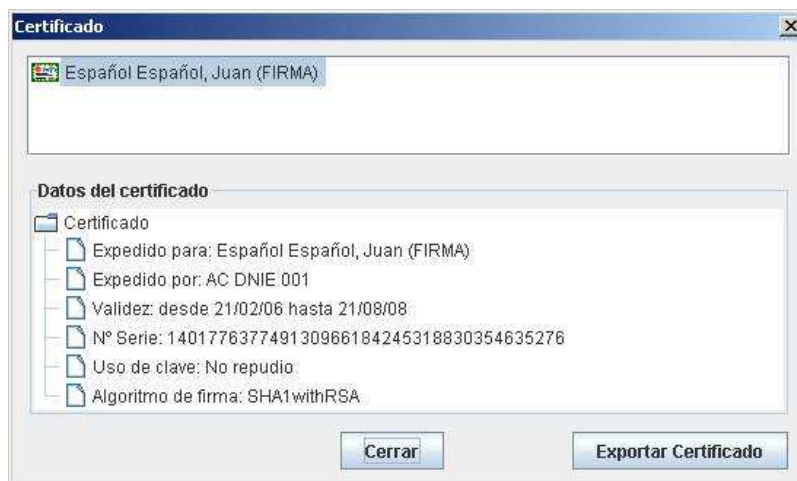
La segunda pestaña, llamada “Información” desglosa los resultados de validación pormenorizadamente dentro de una estructura en árbol.




El primer nodo es el nodo de la firma, que contiene un icono que define su validez, el nombre asignado a la firma según el orden leído del documento y el certificado firmante de la misma entre paréntesis. Los datos de la firma penden de éste nodo. Entre dichos datos, se muestra la fecha en que se firmó el documento. El siguiente nodo muestra los datos de los certificados digitales almacenados en el fichero de firma. Si se hace clic con el botón secundario del ratón sobre el nodo de certificado o alguno de sus hijos se mostrará un menú contextual que permite escoger entre tres opciones, ver los datos del certificado, exportar el certificado y validar el certificado vía OCSP, si esta correctamente configurado un validador OCSP.



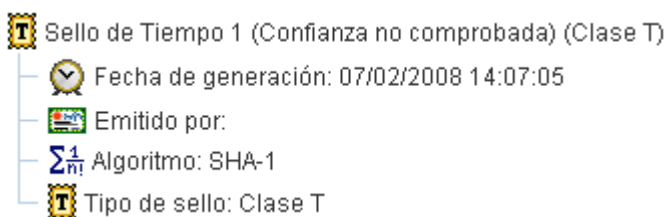
Como muestra el siguiente cuadro, al hacer doble clic sobre cualquiera de los nodos del tipo certificado (o al hacer clic con el botón secundario del ratón y seleccionar la opción de ver certificado) se mostrará información detallada de los mismos con una ventana emergente en un modo de presentación tipo árbol: los datos del certificado seleccionado, para quién y por quién fue expedido, su validez, su número de serie, los usos permitidos para el certificado y el algoritmo que utiliza para la firma. La otra opción disponible en el menú emergente es la de exportar el certificado.



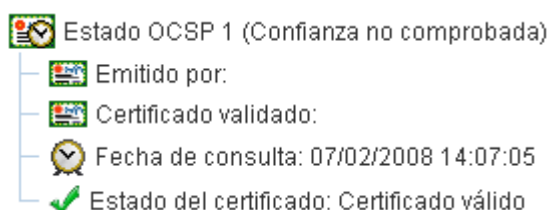
Cualquiera de los certificados mostrados puede ser exportado a un fichero “.cer” mediante el botón exportar .

A continuación se muestra el formato XAdES de la firma, junto con el tipo de esquema XAdES que el documento firmado tiene.

También, en el caso de que la firma poseyera el formato XADES-T en adelante, nos mostraría información sobre los sellos de tiempo contenidos: fecha y hora exacta de generación, el emisor del sello, la precisión si la tuviese, el algoritmo utilizado en su generación y el tipo de sello que es.



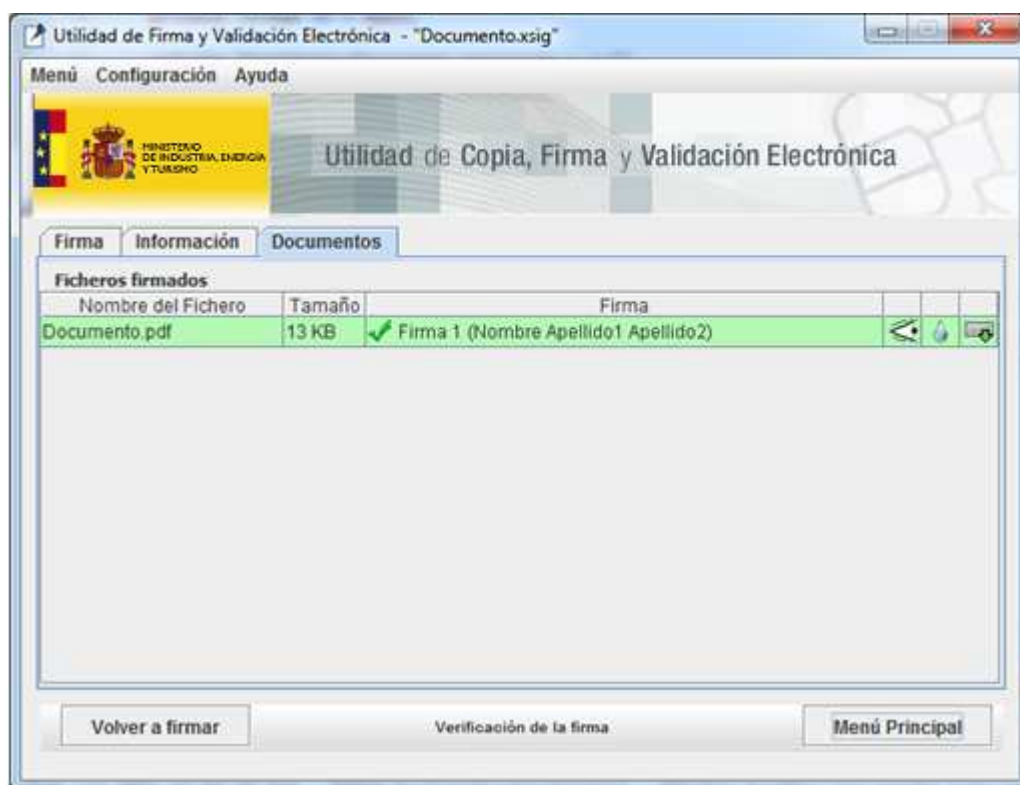
Análogamente, si la firma es de tipo C en adelante, se mostrarían datos sobre las consultas de certificados existentes, ya sean vía OCSP o vía listas de revocación. Los datos son, el emisor de la respuesta, el nombre del certificado validado, la fecha de la consulta y el resultado obtenido sobre el estado del certificado.



En caso de haberlos, también nos mostraría los roles del firmante.

Cada uno de los elementos implicados en los datos de la firma, tienen un estado de confianza asociado, que indica si el elemento es considerado de confianza por la aplicación. Esto quiere decir que se comprueba automáticamente si la entidad es oficial, permitiendo al usuario depositar su confianza en dicho elemento. Para un certificado, se comprobaría si se confía en el emisor del certificado, etc...

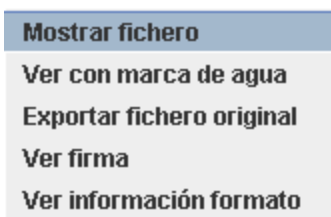
En la siguiente pestaña, llamada "Ficheros firmados", se nos mostrarán los datos originales firmados, contenidos dentro del fichero de firma:

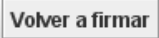




Se muestra el nombre, tamaño y firma asociada, con un color de fondo que es indicativo del resultado de la validación de firma (verde para firmas válidas, rojo para las inválidas). Al hacer doble clic sobre el nombre del documento nos permitirá abrirlos con la aplicación que tengamos asociada a la extensión del documento en nuestro Sistema Operativo. Al hacer doble clic en el tamaño se nos permitirá exportar el documento a la ubicación que se indique mediante un cuadro de diálogo, y finalmente, si se hace doble clic sobre la firma asociada, la utilidad mostrará los datos de dicha firma contenidos en la pestaña de firmas. Adicionalmente, en la parte derecha de la tabla, se encuentran dos botones con la misma funcionalidad que tiene hacer doble clic sobre la primera y segunda columna, es decir, para visualizar o exportar el fichero firmado.

Si en cualquiera de las tres celdas de la tabla se hace clic con el botón secundario del ratón se muestra un menú emergente que muestra las tres opciones anteriormente descritas, mas una cuarta para ver los datos sobre el formato del fichero y otra opción adicional que permite visualizar el documento con marca de agua, en caso de que se trate de un PDF.



Por último, si se pulsa el botón “Volver a firmar”  se iniciará un proceso de contrafirmado (Véase el [punto 5.7](#) del presente manual), es decir, permitirá añadir otra firma en cadena al fichero de firma que se acaba de validar.

### 5.3. Lanzar validaciones recursivas

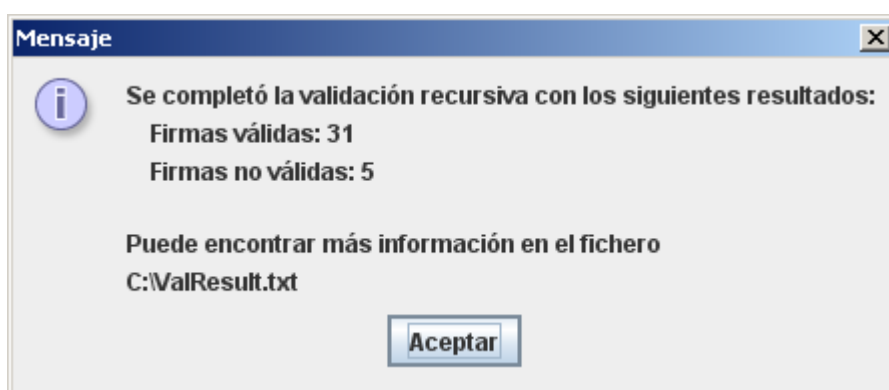
La aplicación eCoFirma implementa un mecanismo que permite validar todas las firmas contenidas dentro de un directorio (y contrafirmas presentes en cada fichero de firma) para generar un fichero donde se recojan todos los resultados de validación obtenidos.

Este mecanismo es accesible desde la opción de menú “Menú/Validar y generar log (recursivo) (Alt + V)”. Si se selecciona esta opción entonces el sistema le pedirá que indique dos datos:



- Ruta al directorio a validar, donde se encuentran las firmas electrónicas
- Destino del fichero de Log a generar

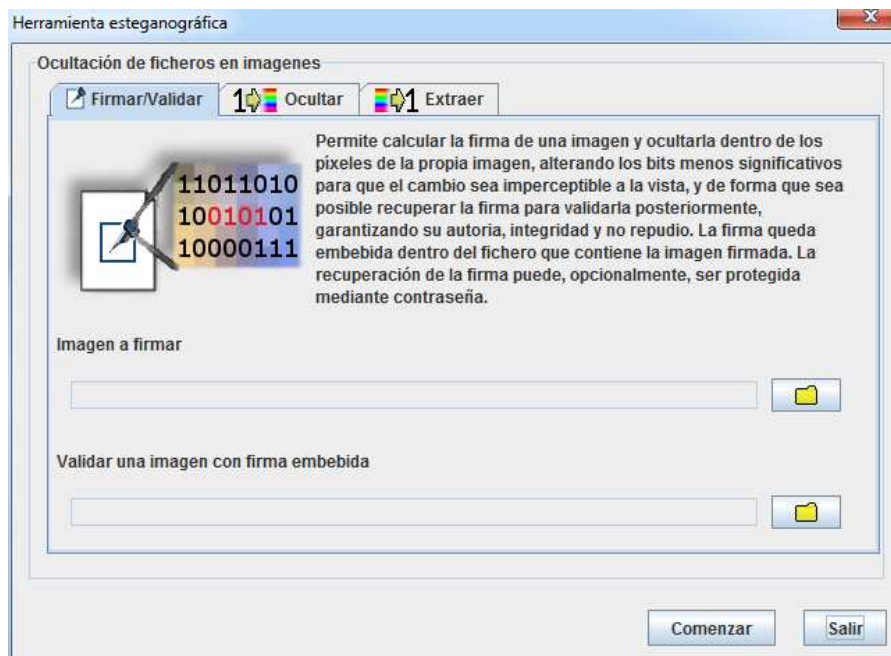
Una vez indicados estos dos parámetros, se lanza el proceso de validación recursiva firma a firma y cuando termine el proceso se mostrará un cuadro emergente mostrando un resumen de los resultados obtenidos.



Adicionalmente, se ha generado un fichero de texto plano donde se pormenorizan los resultados de cada firma.


## 5.4. Herramienta Estenográfica

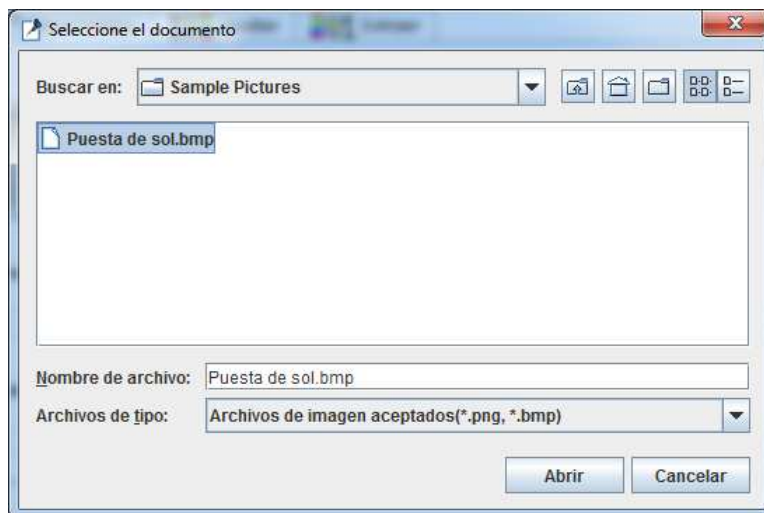
Para acceder a la herramienta esteganográfica hay que entrar dentro de la opción "Menu/Estenografía". La estenografía es la parte de la criptografía que se encarga de ocultar mensajes dentro de otros.



La pantalla de la herramienta esteganográfica se compone de 3 pestañas desde las que se pueden realizar 3 procesos distintos. A continuación se explica cada una de ellas.

Primeramente nos encontramos con la pestaña Firmar/Validar. Desde aquí se puede calcular la firma de una imagen y ocultarla dentro de los píxeles de la propia imagen, alterando los bits menos significativos para que el cambio sea imperceptible a la vista, y de forma que sea posible recuperar la firma para validarla posteriormente, garantizando su autoría, integridad y no repudio. La firma queda embebida dentro del fichero que contiene la imagen firmada.

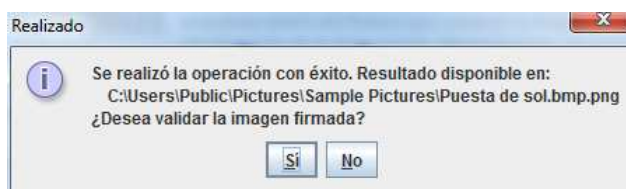
Para firmar una imagen y ocultar su firma en la propia imagen es necesario presionar en el botón a la derecha del cuadro de texto () debajo de la opción "Imagen a firmar". Se mostrará un cuadro de diálogo para que seleccione o escriba la ruta de la imagen a firmar. La imagen podrá ser bmp o png sin mapa de colores.



Una vez seleccionada la imagen a firmar se debe pulsar en el botón “Comenzar”

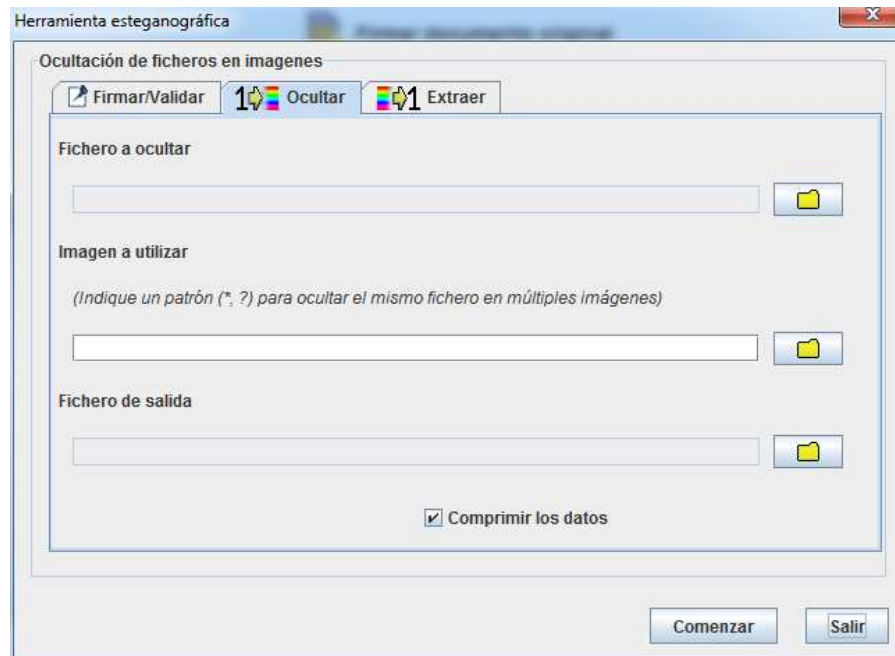
Comenzar

Acto seguido se debe escoger un certificado válido para realizar la firma de la misma forma que se describe en el [punto 5.1](#) (Firma electrónica de un archivo) de este manual. Después de llevarse a cabo la firma si todo va bien la aplicación mostrará la siguiente ventana:



En caso de pulsar “No” volveremos a la pantalla inicial de la herramienta esteganográfica, en caso de pulsar “Si” se procederá a validar la firma de forma similar a como se describe en el [apartado 5.2](#) (Validación de una firma) de este manual.

Desde la pestaña Firmar/Validar también se puede validar la firma embebida en una imagen. Para realizar esta acción es necesario presionar en el botón a la derecha del cuadro de texto (📁) debajo de la opción “Validar una imagen con firma embebida”. Se mostrará un cuadro de diálogo para que seleccione o escriba la ruta de la imagen a validar y se llevará a cabo un proceso similar al descrito en el [punto 5.2](#) (Validación de una firma) de este manual.




La segunda pestaña de la herramienta esteganográfica es la correspondiente a la opción “Ocultar”. Desde aquí podemos ocultar un fichero dentro de una imagen sin alterar esta última de modo significativo permitiendo que pase desapercibida la ocultación.

Para ocultar un fichero es necesario presionar en el botón a la derecha del cuadro de texto (📁) debajo de la opción “Fichero a ocultar”. Se mostrará un cuadro de diálogo para que seleccione el fichero a ocultar.

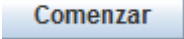


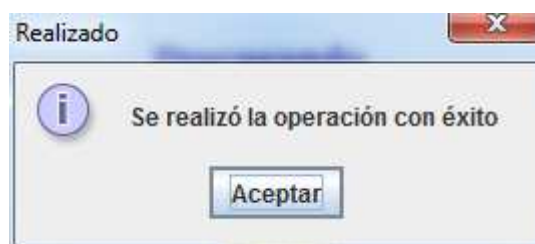
Una vez seleccionado el fichero a ocultar se debe elegir la imagen dónde se ocultará. Para realizar esta acción es necesario presionar en el botón a la derecha del cuadro de texto (📁)

debajo de la opción “Imagen a utilizar”. Se mostrará un cuadro de diálogo similar al anteriormente mostrado para que seleccione la imagen a utilizar.

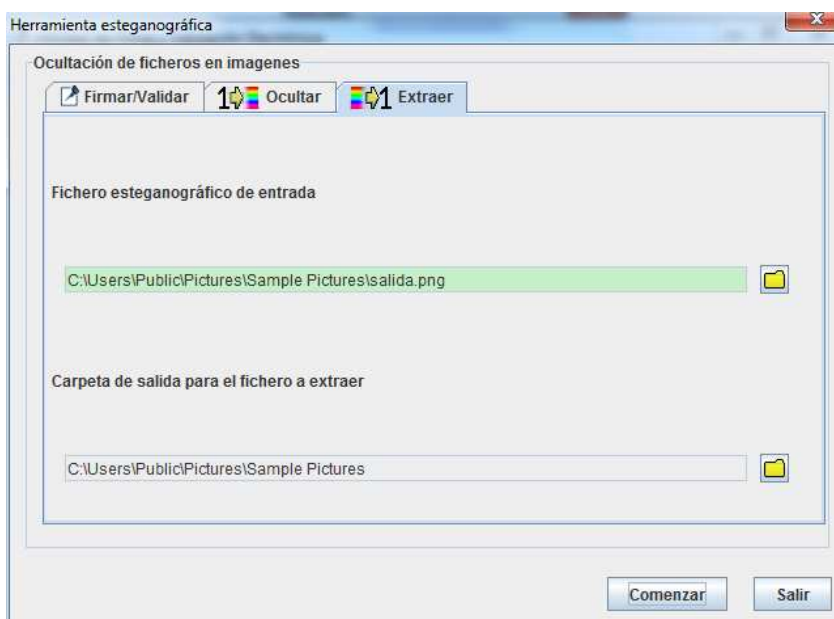
Después de seleccionar el fichero a ocultar y la imagen a utilizar se debe especificar un fichero de salida. . Para realizar esta acción es necesario presionar en el botón a la derecha del cuadro de texto () debajo de la opción “Fichero de salida”. Aparecerá nuevamente un cuadro de diálogo similar a los anteriores donde se podrá escribir la ruta y el nombre que se desee dar al fichero de salida que tendrá la información ocultada.


Finalmente se puede marcar o desmarcar la opción “Comprimir los datos” para que se compriman o no los datos a ocultar.


Una vez hecho todo lo anterior se debe pulsar en el botón “Comenzar”  para llevar a cabo la ocultación del fichero en la imagen. Si todo va bien se obtendrá el siguiente mensaje:

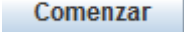


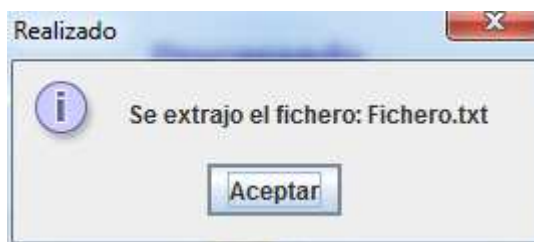
La tercera pestaña de la herramienta esteganográfica se corresponde con la opción “Extraer”. Esta opción realiza la operación contraria a “Ocultar” es decir, permite extraer la información oculta en una imagen en la que previamente se ha ocultado información.



Lo primero que se debe hacer es elegir la imagen con el contenido oculto que queremos extraer. Para realizar esta acción es necesario presionar en el botón a la derecha del cuadro de texto (  ) debajo de la opción “Fichero esteganográfico de entrada”. Se mostrará un cuadro de diálogo similar a los mostrados anteriormente para que seleccione el fichero desde el que se extraerá información.

A continuación se debe seleccionar una carpeta de salida donde se almacenará el fichero con la información extraída de la imagen. Para realizar esta acción es necesario presionar en el botón a la derecha del cuadro de texto (  ) debajo de la opción “Carpeta de salida para el fichero a extraer”. Aparecerá nuevamente un cuadro de diálogo similar a los anteriores donde se podrá seleccionar la ruta dónde se extraerá el fichero oculto en la imagen.

Una vez hecho todo lo anterior se debe pulsar en el botón “Comenzar”  para llevar a cabo la extracción de información. Si todo va bien se obtendrá el siguiente mensaje:

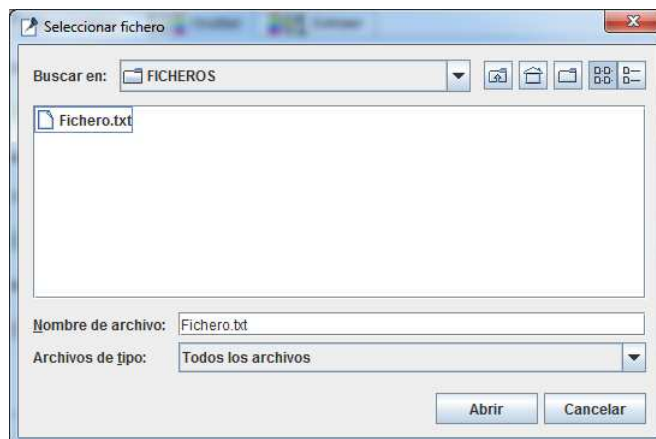


Si miramos en el directorio indicado encontraremos el fichero que se ocultó dentro de la imagen.

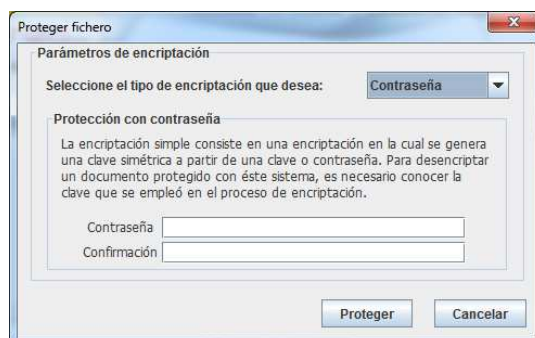
## 5.5. Protección de documentos

### 5.5.1. Encriptar un documento

Para encriptar un documento se debe seleccionar la opción “Menu/Encriptar”. Se mostrará un cuadro de diálogo para que seleccione el fichero a encriptar:



Una vez seleccionado el fichero se debe elegir el tipo de encriptación. Si se elige la encriptación por contraseña lo que se lleva a cabo es una encriptación en la cual se genera una clave simétrica a partir de la contraseña introducida. Será necesario recordar la contraseña para desencriptar el archivo encriptado.



El segundo caso emplea el algoritmo Triple DES para proteger la información mediante una clave aleatoria que se encripta a su vez mediante la clave pública asociada a un certificado electrónico (elegir parte pública del certificado del receptor del fichero encriptado), de forma que para recuperar la información sea necesario disponer de acceso a la clave privada correspondiente.





Para realizar el proceso se le solicitará que mueva el ratón por un área determinada y así generar ruido para obtener la semilla aleatoria y se volverá a la ventana de selección de certificados.

Tanto si se ha elegido cifrar con contraseña como si se ha elegido cifrar con certificado una vez completados los datos requeridos se debe pulsar el botón “Proteger” para llevar a cabo el proceso de cifrado del fichero.

## 5.5.2. Desencriptar un documento

Para desencriptar un documento se debe seleccionar la opción “Menu/Desencriptar”. Se mostrará un cuadro de diálogo para que seleccione el fichero a desencriptar:



Acto seguido aparecerá otro nuevo cuadro de diálogo para elegir el nombre y la ubicación del fichero desencriptado:





### 5.5.3. Encriptar de un documento durante el proceso de firma

Durante el primer paso del proceso de firma se da la opción al usuario de proteger los datos a firmar mediante el uso de sistemas de encriptación simétrica y asimétrica. La encriptación se lleva a cabo de la misma forma que como se explica en el punto 5.5.1. Si el proceso fue realizado con éxito aparecerá el siguiente icono en la tabla:



Al intentar abrir el documento tras validar la firma se solicitará la contraseña con la que se cifró o el certificado con la clave privada para realizar el proceso de desencriptar el documento.

## 5.6. Cálculo de huellas digitales

La aplicación eCoFirma incorpora una calculadora de huellas digitales. A esta opción se puede acceder desde “Menu/Calculadora de huellas” o durante la selección de documentos a firmar, eligiendo la opción “Huella”, que realizará el cálculo mediante diversos algoritmos presentándolos de una manera resumida. Si utiliza el ratón para seleccionar cualquiera de ellos quedarán almacenados automáticamente en el portapapeles.

La huella de un fichero es una transformación que, a partir de unos datos de longitud variable, da lugar a una serie alfanumérica de longitud fija, que es única a partir de los datos de entrada. Es decir, en teoría no existe otra entrada distinta que dé por resultado el mismo hash, huella o Digest.



También se podrá obtener el hash de un documento cuando se va a firmar seleccionando el icono con una huella dactilar que aparecerá junto al fichero a firmar.

## 5.7. Firma múltiple y contrafirma

El programa eCoFirma implementa la validación de ficheros compuestos por múltiples firmas y da la posibilidad de realizar la contrafirma de una de las firmas validadas. La contrafirma es un proceso por el cual una firma preexistente se firma nuevamente.

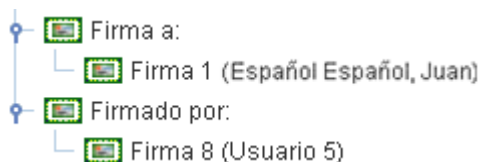
A continuación se explican las peculiaridades de la interfaz de validación con firmas múltiples.



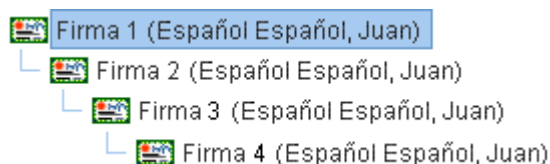
Al validar un documento con una firma compuesta, el resultado de firma mostrado es un resumen de los resultados de todas las firmas implicadas, de forma que si existe una firma inválida, el resultado mostrado será de invalidez total, mostrándose, a la derecha, el desglose de los resultados obtenidos de cada una de las firmas.

Tras validar y mostrar el resultado, se abre de manera automática el mapa de firmas, que ilustra la estructura de firmas interna del documento. Dicha ventana se desvanecerá cuando pierda el foco, pudiendo ser recuperada haciendo clic en el texto azul y subrayado de la esquina superior derecha.

Si se hace doble clic sobre alguna de las firmas mostradas en el mapa de firmas, se mostrarán los datos de dicha firma, que incluirán un nodo adicional indicando si son contrafirma de otra firma y/o si es una firma contrafirmada por otra. Si se hace doble clic sobre la firma contenida en éste nodo, se muestra su información.



Para contrafirmar la última firma validada (en la figura de abajo, se contrafirmaría la Firma 4) presione el botón “Volver a firmar”. La acción realizada es una contrafirma de la última firma, de forma que la estructura de firmas que puede obtenerse de ésta manera es la siguiente:

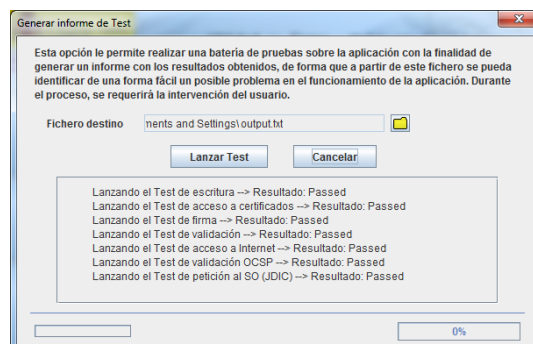


A continuación, se lanza el proceso de contrafirma, que es un proceso análogo al proceso de firma explicado anteriormente, pero sin necesidad de indicar el documento original a firmar.

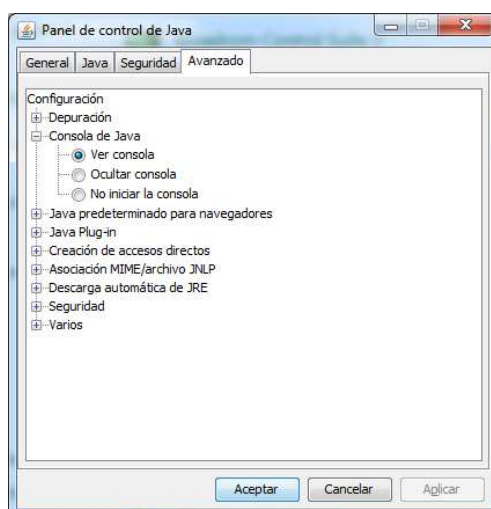
Adicionalmente, es posible realizar una contrafirma haciendo clic sobre el tercer botón del menú principal, titulado “Añadir nueva firma”, que lanzará un proceso completo de contrafirma de la última firma de la cadena, partiendo de la/s firma/s originales, en caso de que superen un proceso completo de validación.

## 6. Manejo de errores

En la opción de configuración “Ayuda/Generar batería de Test Alt+T”, dentro del menú principal, se encuentra un asistente que permite realizar un juego completo de pruebas sobre la configuración actual de forma que se genere un documento de texto que contenga las trazas que permiten seguir el flujo del programa y documente sus eventuales errores.



También es posible visualizar las trazas del flujo del programa en la propia consola de Java. Para que la consola se abra automáticamente cada vez que se abre una aplicación, es necesario dirigirse al administrador de Java. Usualmente se encuentra como una opción más dentro del panel de control que le corresponda al sistema operativo.



En la pestaña “Avanzado” se encuentra la opción llamada “Ver consola”, que determina este comportamiento.



# Manual de usuario de la utilidad de copia y firma electrónica eCoFirma v1.4.0

Puede consultar las preguntas frecuentes en la dirección  
[http://oficinavirtual.mityc.es/javawebstart/soc\\_info/ecofirma/faq.html](http://oficinavirtual.mityc.es/javawebstart/soc_info/ecofirma/faq.html).

## 7. Enlaces de interés

Ley 59/2003 de firma electrónica en España

<http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf>

Sobre XAdES:

<http://www.w3.org/TR/XAdES/>

Aplicación eCoFirma (Componentes de firma del Ministerio)

[http://oficinavirtual.mityc.es/javawebstart/soc\\_info/ecofirma/index.html](http://oficinavirtual.mityc.es/javawebstart/soc_info/ecofirma/index.html)

Código fuente y descargas de los componentes de firma

<http://oficinavirtual.mityc.es/componentes/>

Sobre el DNI electrónico

<http://www.dnielectronico.es/>