INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

COMPONENTES DE FIRMA BASADOS EN EL USO DEL DNI-E

MANUAL DE USUARIO DEL COMPONENTE DE ESCRITORIO V 1.0

ÍNDICE

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 **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.

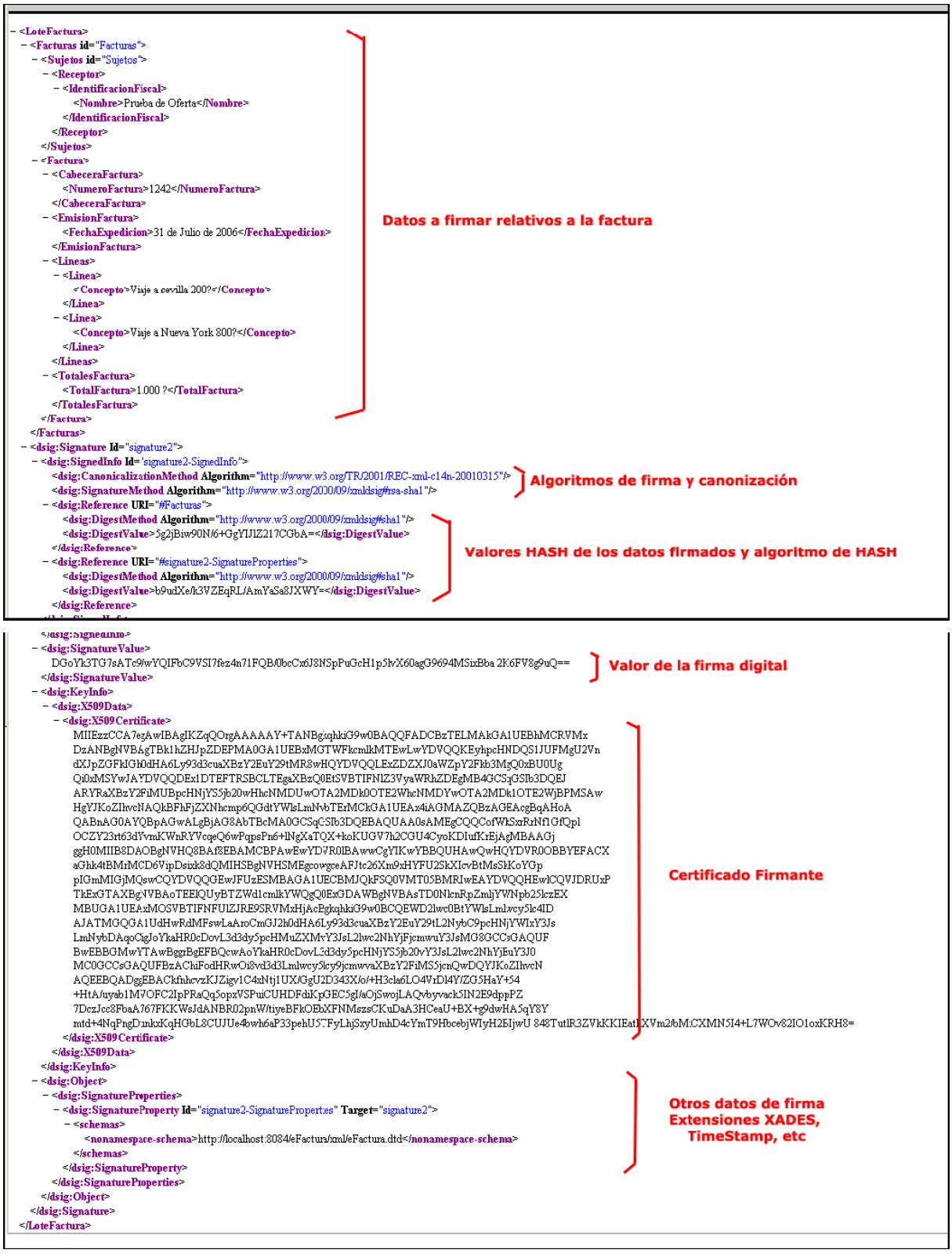
La plataforma es Multi-PKI lo cual permite utilizar cualquier tipo de certificado electrónico X509 v3 emitido por entidades proveedoras de servicios de certificación que se consideren, ahora o en el futuro, de confianza, pero tiene un gran enfoque en el DNI Electrónico, cubriendo todo lo necesario para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

El formato de firma **XMLDSign** y **XADES** se divide en diversas partes, como se refleja en la siguiente imagen:



En ella podemos ver una firma digital y las distintas partes técnicas en las que se divide.

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 por este equipo permitirán adaptarse a cualquier estándar XADES actual o futuro. El estándar cubierto es:

XADES (BES): Firma básica de documentos XML acorde con directiva europea de firma digital avanzada "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures", esta firma permitirá que cualquier tipo de contenido sea firmado, con posibilidad de auto-contener el documento firmado. Si dicho documento ya se encuentra en formato XML la firma se realizara sobre el mismo. La firma en XML permite además firmar solamente aquellos elementos o nodos del documento XML que quieran certificarse, y permitir que partes del documento se encuentren sin firmar y se puedan modificar sin invalidar la firma, lo cual se podrá indicar en la configuración de la firma electrónica o a través de directivas de configuración.

2. CONFIGURACIÓN DE LA APLICACIÓN

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.

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

La opción “Configuración” nos permitirá configurar el acceso a través de Internet de servidores externos, para validar el estado de los certificados o acceder a través de un servidor Proxy, y escoger entre varios almacenes de certificados. La ventana que aparece al elegir esta opción muestra las siguientes opciones:

Proxy

Esta opción presenta una ventana para activar la salida a Internet a través de un servidor Proxy. Está opción nos permitirá conectarnos al servidor OCSP a través de una dirección y un puerto Proxy. Si se selecciona esta opción ambos datos son obligatorios. Si se tratara de un puerto autenticado, deberemos seleccionar dicha opción en el cuadro de diálogo indicando un usuario y una contraseña.

Validación OCSP

Validar certificado firmante (OCSP). Esta opción nos permitirá validar el certificado, contra una dirección de Internet donde se encuentre ubicado un servidor de validación de certificados en línea (OCSP). De esta manera podremos comprobar que el certificado no se encuentra revocado. Si se selecciona esta opción la dirección en Internet del servidor OCSP es un dato obligatorio.

Almacén de certificados

Esta opción presenta una ventana en la que se no posibilita la elección entre dos almacenes de certificados: el almacén de Windows (almacén del navegador Internet Explorer) o el almacén de Mozilla/Firefox. En el caso de seleccionar esta última opción debemos indicar la ruta al perfil. Si a priori no la conocemos, podemos pulsar sobre el botón “Ayuda para obtener ruta del perfil” 

tras lo que se abrirá una ventana del navegador con las indicaciones necesarias para obtener dicha ruta.

Para aceptar los cambios introducidos en la configuración de las distintas opciones hay que pulsar el botón “Aceptar” 

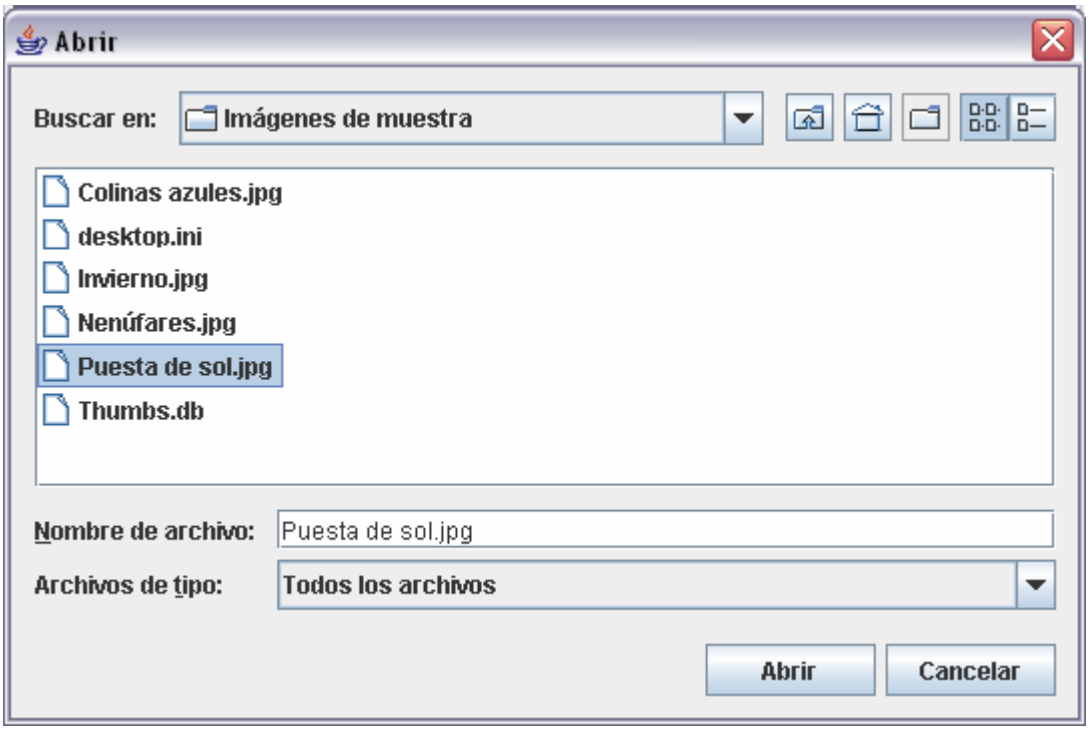
o, en caso contrario, el botón “Cancelar” 

para deshacer las modificaciones realizadas en la configuración.

3. USO DE LA APLICACIÓN, FIRMA ELECTRÓNICA DE UN ARCHIVO

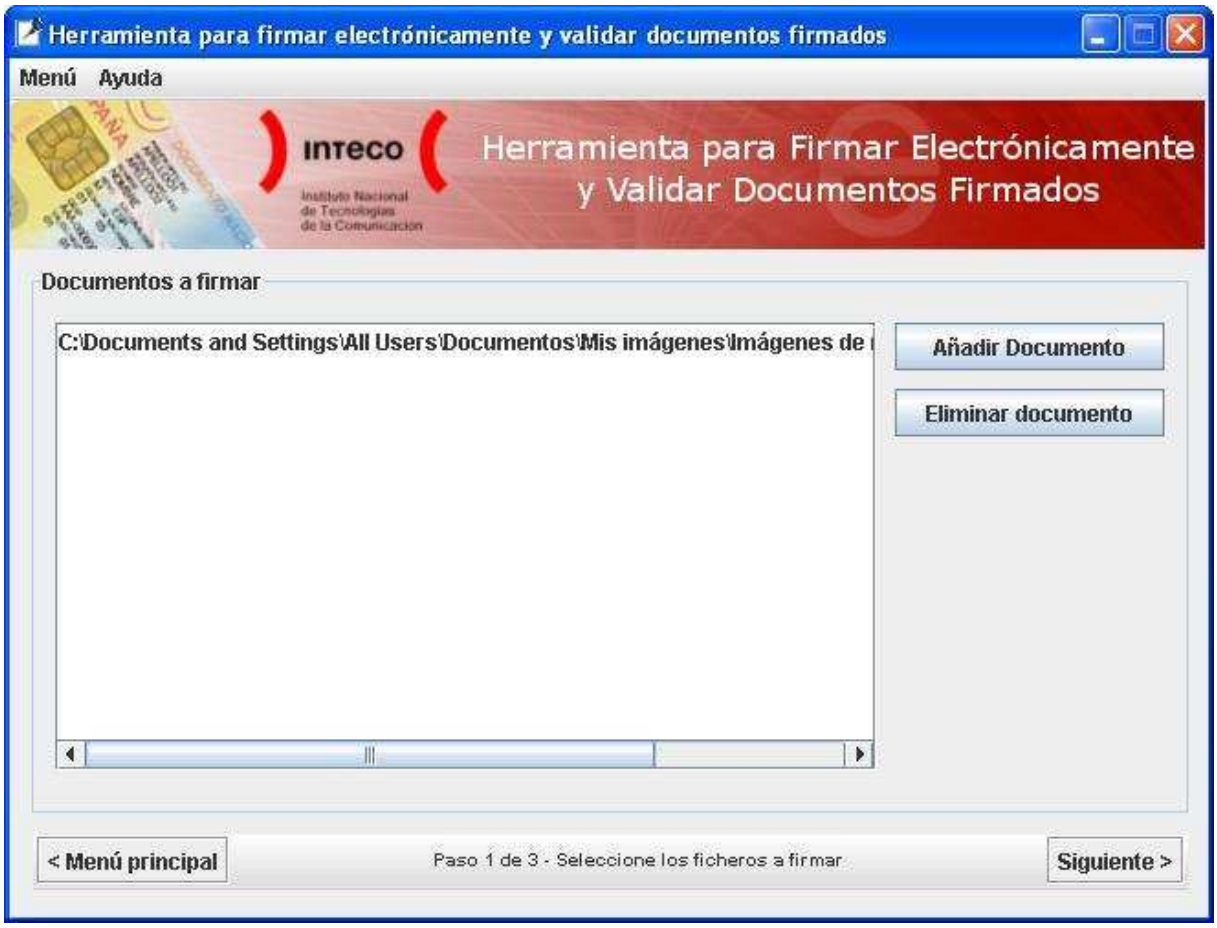
La firma electrónica XADES de un documento se realiza desde el menú principal de la aplicación pulsando en el botón “Firmar Documentos”.

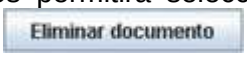
Al pulsarlo se nos abrirá una ventana que nos permitirá seleccionar el documento que queremos firmar.



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).

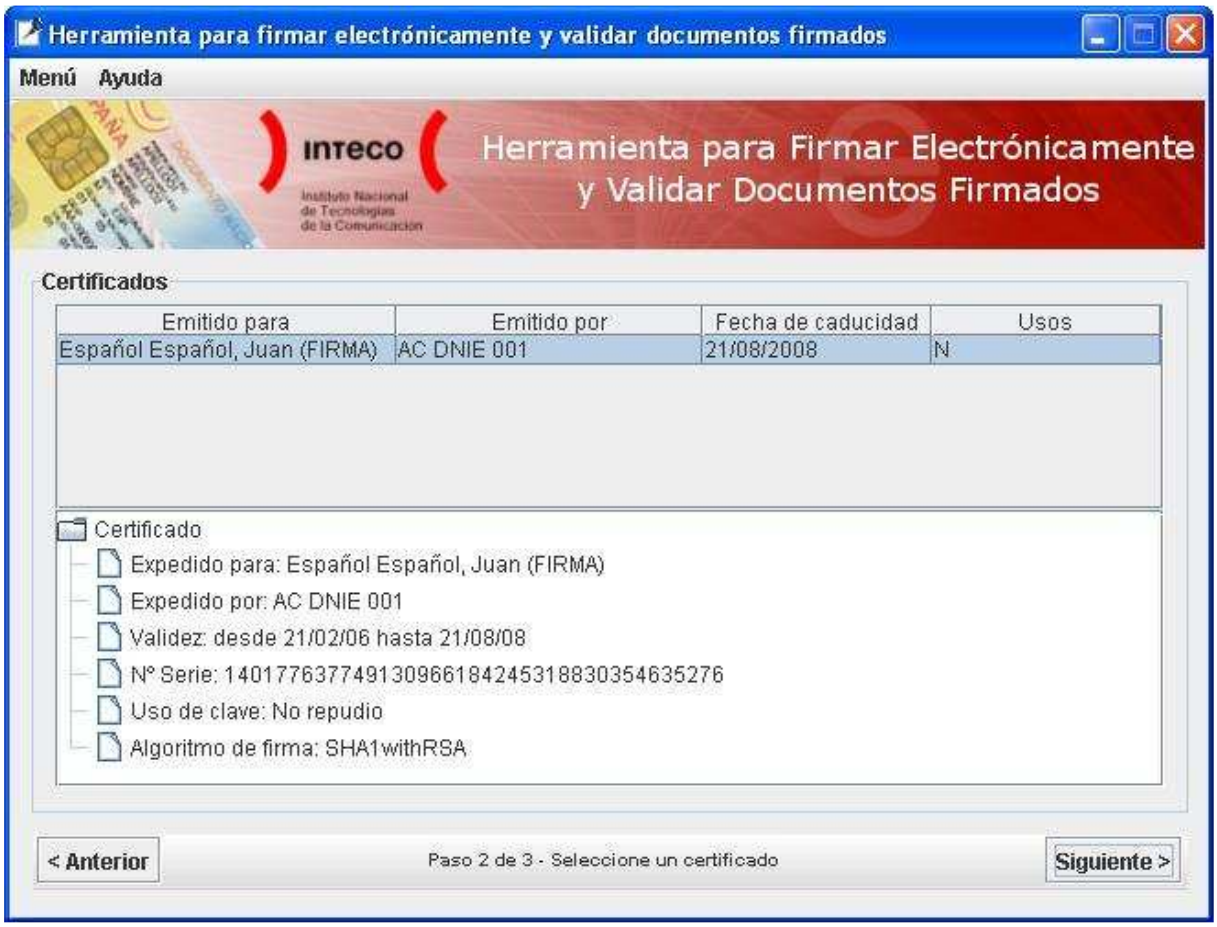


Pulsando el botón “Añadir documento”  nos permitirá seleccionar otro fichero para firmar, mientras que el botón “Eliminar documento”  nos permitirá borrar el fichero que aparezca seleccionado en la lista de Documentos a firmar.

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 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 demorase en leer el contenido de la tarjeta, por lo tanto debería hacerse un nuevo intento luego de aguardar un tiempo. Con los certificados digitales cargados la aplicación presente 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.

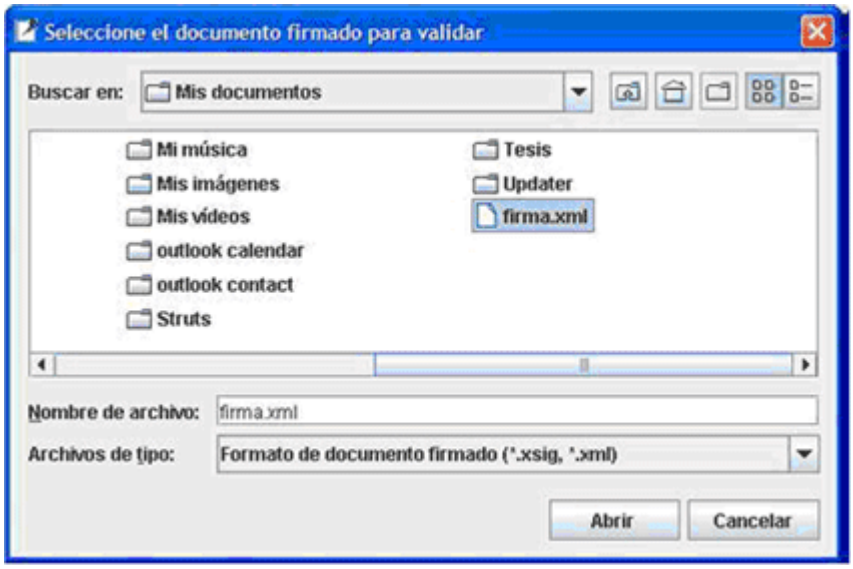
Una vez que se selecciona el certificado deseado se continúa el proceso pulsando en el botón “Siguiente”. Para escoger otro documento distinto al que ya se ha seleccionado, o para agregar nuevos documentos a la firma, se pulsa el botón “Anterior” y se vuelve al primer paso en donde es posible cambiar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

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. Para poder firmar el documento se le requerirá en algún momento que introduzca en PIN de seguridad correspondiente al certificado seleccionado.

4. USO DE LA APLICACIÓN, VALIDACIÓN DE UNA FIRMA

La validación de una firma electrónica XADES se realiza desde la aplicación pulsando en el botón “Validar Documentos Firmados” 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 firmo el documento.

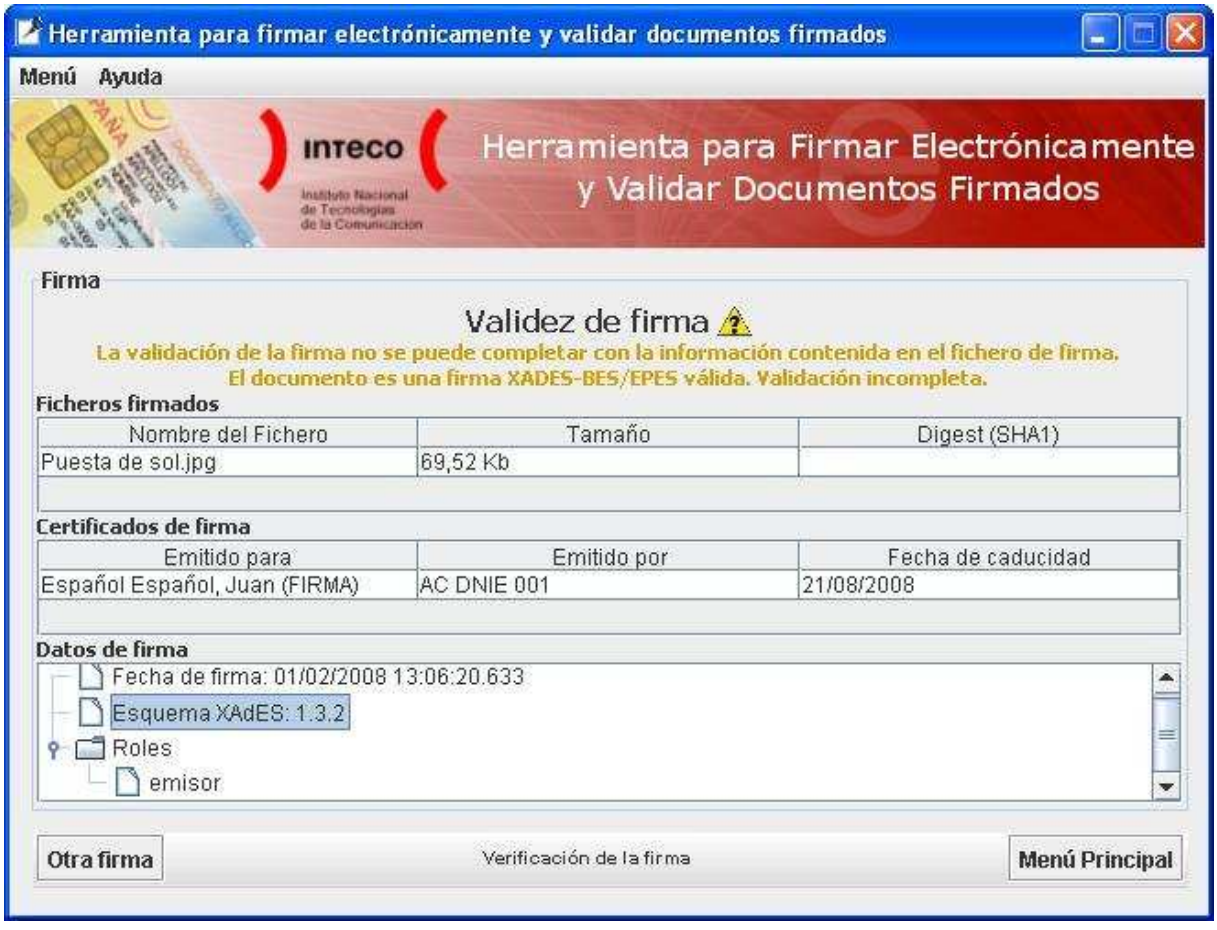
Tras pulsar el botón se nos muestra una ventana emergente en dónde deberemos escoger el fichero firmado que deseamos validar.



Una vez seleccionado el fichero correspondiente pulsamos en el botón “Abrir” 

para proceder con la validación o “Cancelar” 

para volver al Menú principal. El resultado aparecerá en una nueva ventana.



El primer mensaje que aparece nos informará si la firma es válida  o no  El resultado válido de una firma XADES-BES aparece en amarillo a modo de advertencia debido a que este formato, como viene indicado en la especificación, no permite saber el estado del certificado al tiempo de la firma y tampoco hay manera de saber con confianza cuándo fue creada la firma.

En cualquier caso, en los siguientes cuadros nos mostrará los datos almacenados en el fichero de firma. El primer cuadro muestra todos los documentos firmados almacenados en el fichero de firma, indicando su nombre, tamaño y digest. Al hacer doble clic sobre cualquiera ellos nos permitirá abrirlos con la aplicación que tengamos asociada a la extensión del documento en nuestro Sistema Operativo.

El segundo cuadro muestra los datos de los certificados digitales almacenados en el fichero de firma. Al hacer doble clic sobre cualquiera de ellos nos mostrará una información detallada de los mismos en un modo de presentación tipo árbol: 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.

El último cuadro nos muestra también en formato tipo árbol datos de la firma: la fecha en que se firmó el documento y el valor de la firma en el fichero digital. En caso de haberlos, también nos mostraría los roles del firmante.

Por último, si se pulsa el botón “Otra firma” 

nos permitirá seleccionar un nuevo fichero de firma para verificar su validez y los datos que contiene.

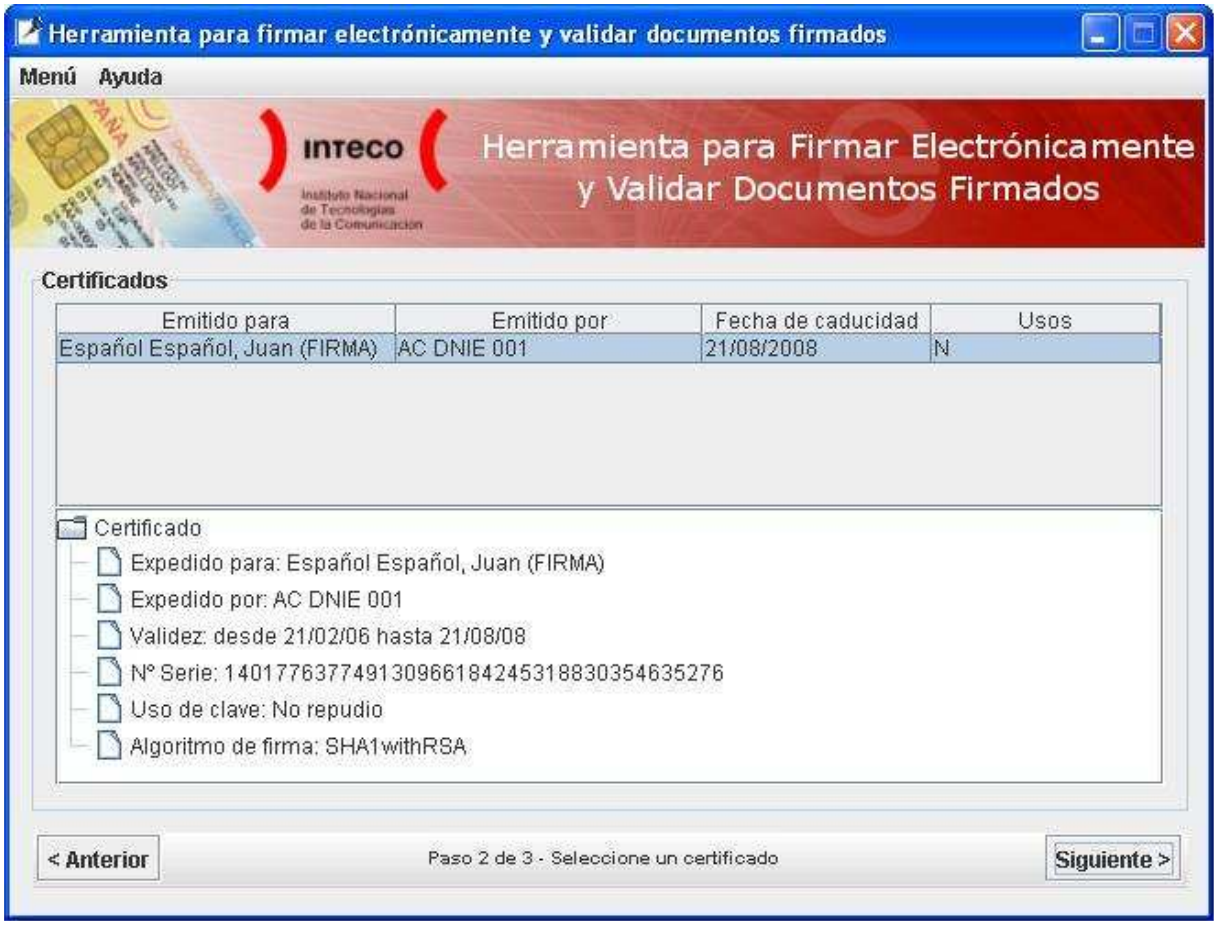
5. USO DE LA APLICACIÓN, VALIDACIÓN DE UN CERTIFICADO

Por último, podremos determinar la validez de los certificados que poseemos en nuestro equipo realizando una validación OCSP de los mismos.
La validación OCSP (Protocolo de estado de certificados “en línea”) es una validación que sigue un estándar internacional y que permite conocer, en un momento dado, si dicho certificado se encuentra activo o revocado.
Para acceder a esta opción pulsaremos en el botón “Validar Certificados Digitales” en el menú principal.

Lo primero que hará la aplicación es verificar que en la configuración se hayan establecidos los datos del servidor OCSP. Si no fuese así, la aplicación nos avisaría con una ventana emergente.

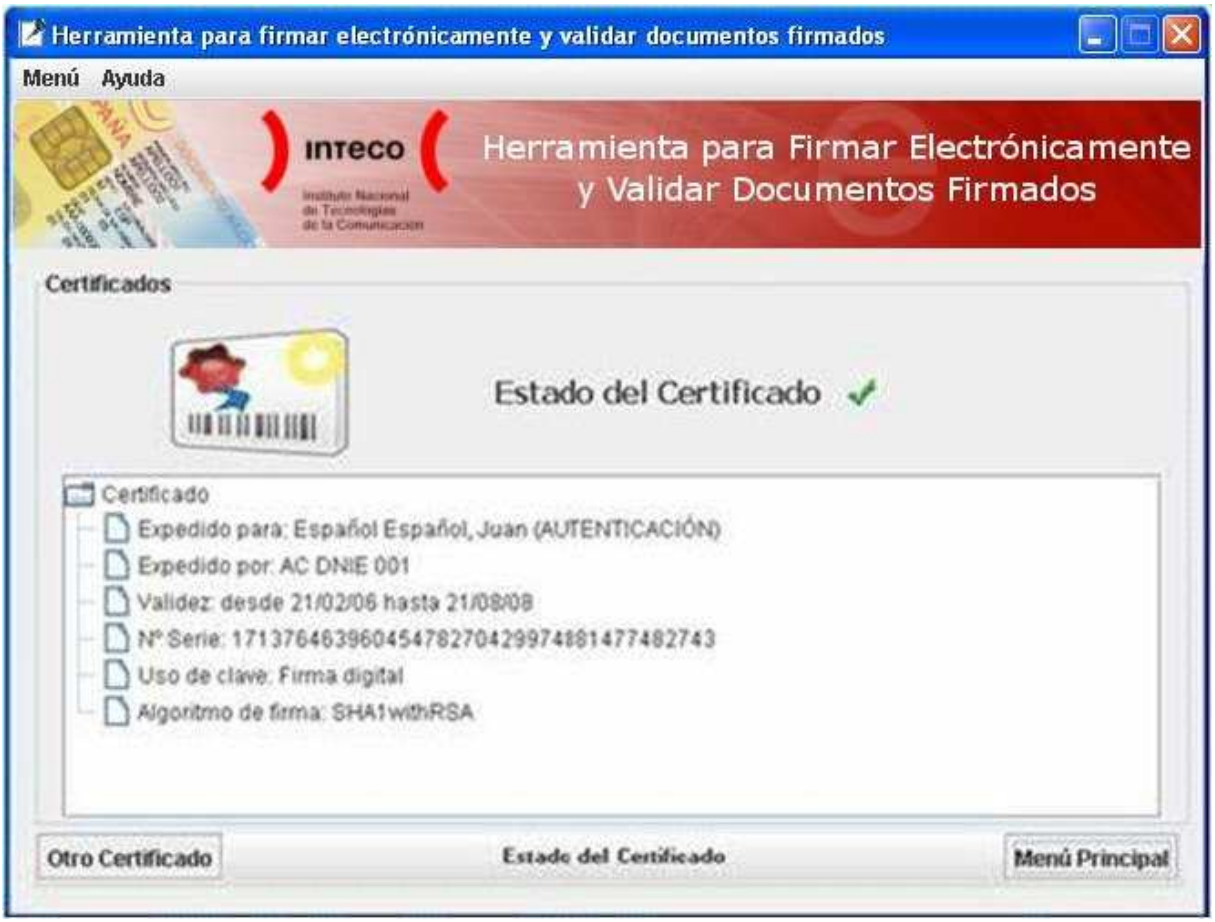
En este caso, se debería seguir las instrucciones del apartado 2 para configurar correctamente el servidor OCSP.

Una vez configurado el servidor, o si éste ya estaba configurado, al pulsar el botón “Validar Certificados Digitales” del Menú principal aparecerá una ventana que nos permitirá seleccionar el certificado. En este caso aparecen *todos* los certificados disponibles en el almacén de certificados.



Seleccionamos el certificado que deseamos validar y pulsamos el botón “Siguiente”

El resultado de la validación aparece en una nueva ventana.



Existen tres resultados para el estado de un certificado: válido, Revocado o Desconocido. Esto último puede deberse a varios factores que la aplicación detalla: la petición no se realizó de forma correcta, hubo un error interno en el servidor OCSP, el servidor estaba ocupado, la petición no estaba firmada, o no se ha podido autorizar la petición.

Pulsando el botón “Otro Certificado” Otro Certificado la aplicación permite seleccionar un nuevo certificado para validar.