Uso de Certificados - Aplicación de firma
Práctica 6C

1. Objetivo

En esta práctica el alumno debe utilizar certificados y un programa de firma para firmar digitalmente documentos y añadirles un sello de tiempo. Posteriormente debe verificar tanto la firma como el sello. **Esta práctica debe realizarse en la Máquina Virtual**.

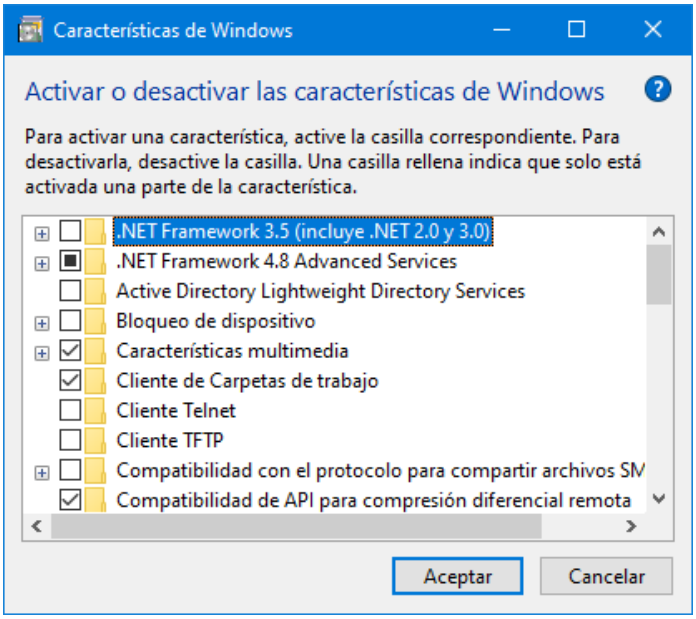
2. Instalación del programa

Se utilizará el programa XolidoSign versión Desktop, que es gratuito para los usuarios particulares. Se puede descargar de la página del desarrollador: **https://www.xolido.com/**

Por facilidad lo puedes descargar del CV. El programa necesita que esté instalado .NET Framework 2.0. Si no está instalado, descarga e instala .NET 3.5 (que incluye .NET 2.0 y 3.0).

Aunque esté instalado .NET 4.8 el programa requiera la version .NET 2.0 y una forma sencilla de instalarlo es así: Panel de control > Activar o desactivar las características de Windows

Aparece la ventana siguiente:

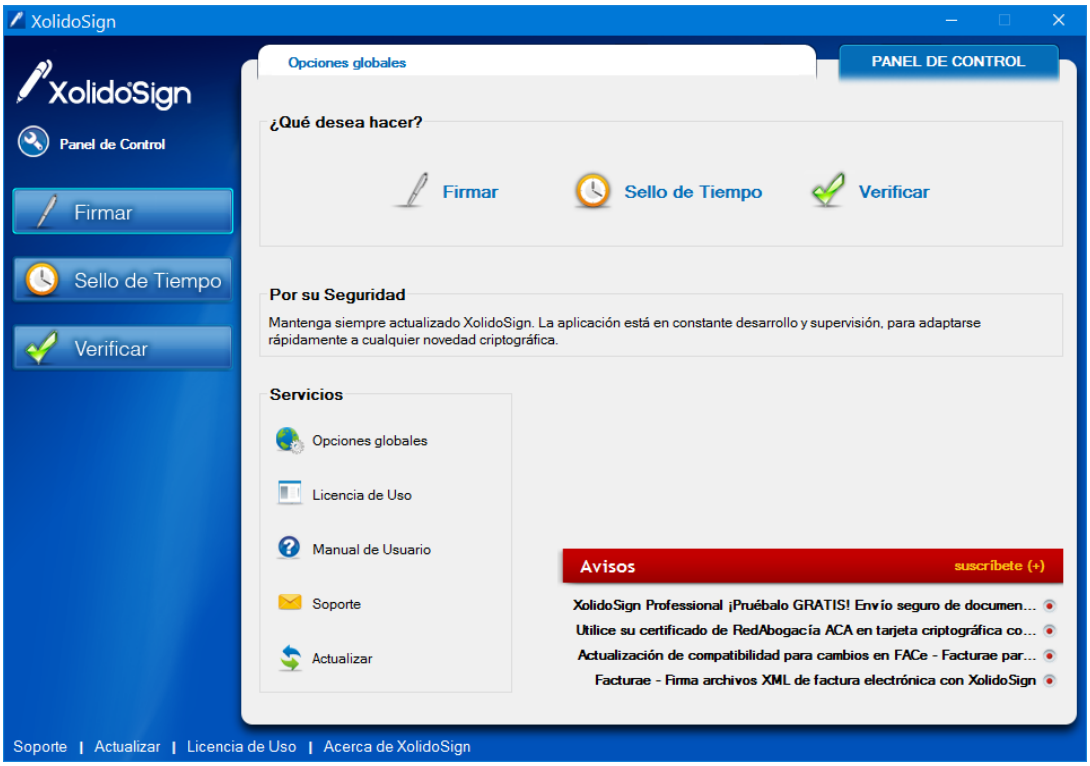


Selecciona la opción .NET Framework 3.5 (Incluye .NET 2.0 y 3.0) y pulsa Aceptar.

Instala el programa en la máquina virtual usada en las prácticas. En la instalación crea una carpeta en el menú inicio y un icono en el escritorio para acceder al programa.

Si la instalación se ha efectuado correctamente se puede acceder al manual de uso del programa en el directorio: C:\Program Files\XolidoSystems\XolidoSign\DOC

Al arrancar el programa aparece la pantalla siguiente que muestra las tres tareas básicas que se pueden realizar. En esta práctica se utilizarán dos: Firmar y Verificar.



3. Firma de ficheros

Prepara un fichero con un editor de textos. Puedes llamarlo hola.txt y contener simplemente la palabra hola.

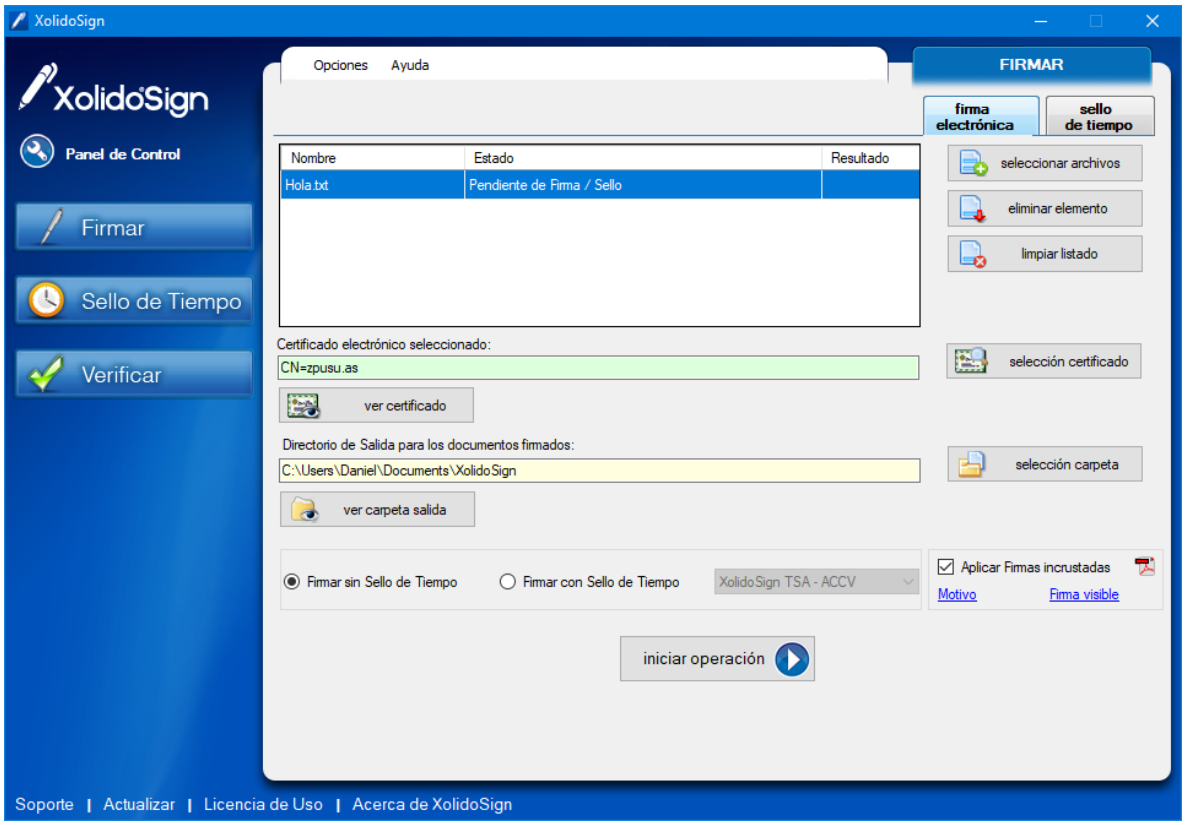
Carga en los almacenes de certificados de Windows, los certificados zpusu.as y zpac.as si es que no están cargados ya.

El certificado de la autoridad certificadora se debe cargar desde el fichero zpACas.cer en el almacén lógico "Entidades de certificación raíz de confianza". Esto es lo normal, pues el usuario nunca tendrá acceso al fichero zpACas.pfx que tiene la clave privada de la autoridad certificadora.

Pero no cargues ahora el certificado de la autoridad certificadora. Cárgalo posteriormente. Si ya estuviese cargado en el almacén de certificados, bórralo.

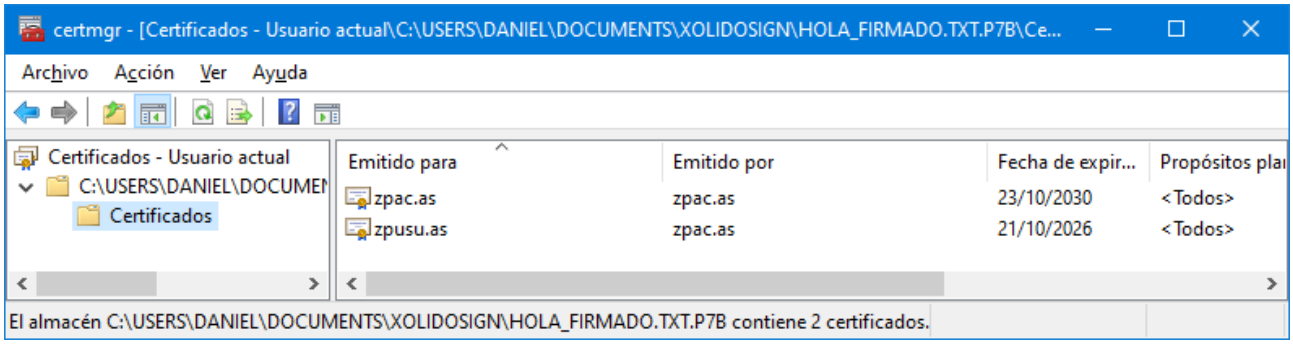
El certificado de zpusu.as se debe cargar desde el fichero zpUSUas.pfx, pues este fichero tiene la clave pública y también tiene asociada la clave privada del usuario, en el almacén lógico "Personal". La clave privada es necesaria para firmar (cifrar) el resumen del documento, cuya firma digital se desea crear.

Arranca el programa y pulsa el botón Firmar. En la ventana que aparece selecciona el archivo a firmar y después selecciona el certificado de usuario, que debe tener una clave privada asociada para poder firmar documentos. Omite las dos advertencias del programa. Finalmente, selecciona también el directorio de salida para los ficheros firmados. Una vez seleccionado todo, tal como se puede ver en la figura siguiente, inicia la operación de firma.



Usando el Explorador de Ficheros, comprueba que en el directorio de salida, en este ejemplo en el directorio C:\Users\Daniel\Documents\XolidoSign\, aparece una copia del fichero firmado con el mismo nombre, pero al que se le ha añadido el sufijo "_firmado". Además aparece un fichero con el mismo nombre y extensión que el anterior al que se le ha añadido una nueva extensión: ".p7b".

El fichero .p7b es un contenedor, que sigue el formato PKCS#7, y contiene la firma digital y la cadena de certificados necesaria para verificarla. En este caso la cadena puede ser zpac.as y zpusu.as. Si se hace clic sobre el fichero .p7b se abre automáticamente la aplicación certmgr, para visualizar los certificados que contiene el fichero, tal como se muestra en la figura siguiente:



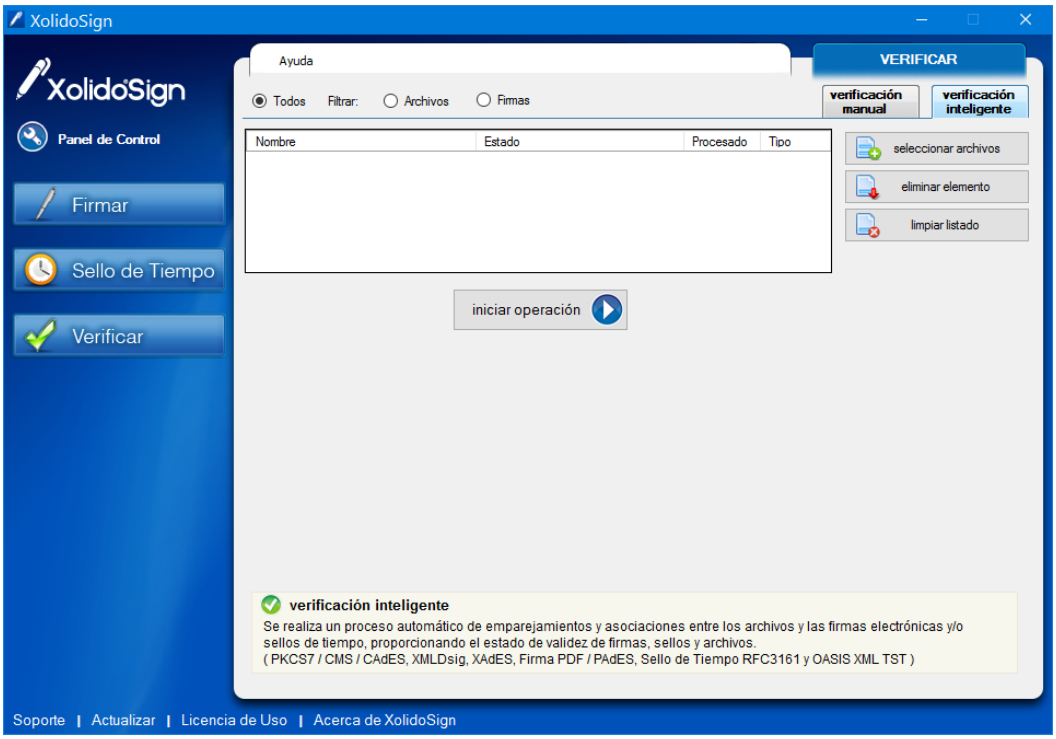
Comprobar también que el programa XolidoSign genera un listado de las firmas que se han realizado en el fichero XolidoSign.csv, que se puede importar en Excel, como registro de los documentos firmados. Estudiar el significado de cada línea del fichero en el manual del programa.

Observar que en la ventana Firmar hay un menú de Opciones (F5) que abre una ventana de configuración. Analiza las opciones que soporta el programa. Como ejemplo, abre Firma electrónica y Opciones avanzadas y comprueba cómo se puede seleccionar el algoritmo usado para resumir el contenido del fichero. Recuerda que el cifrado del resumen es la firma digital.

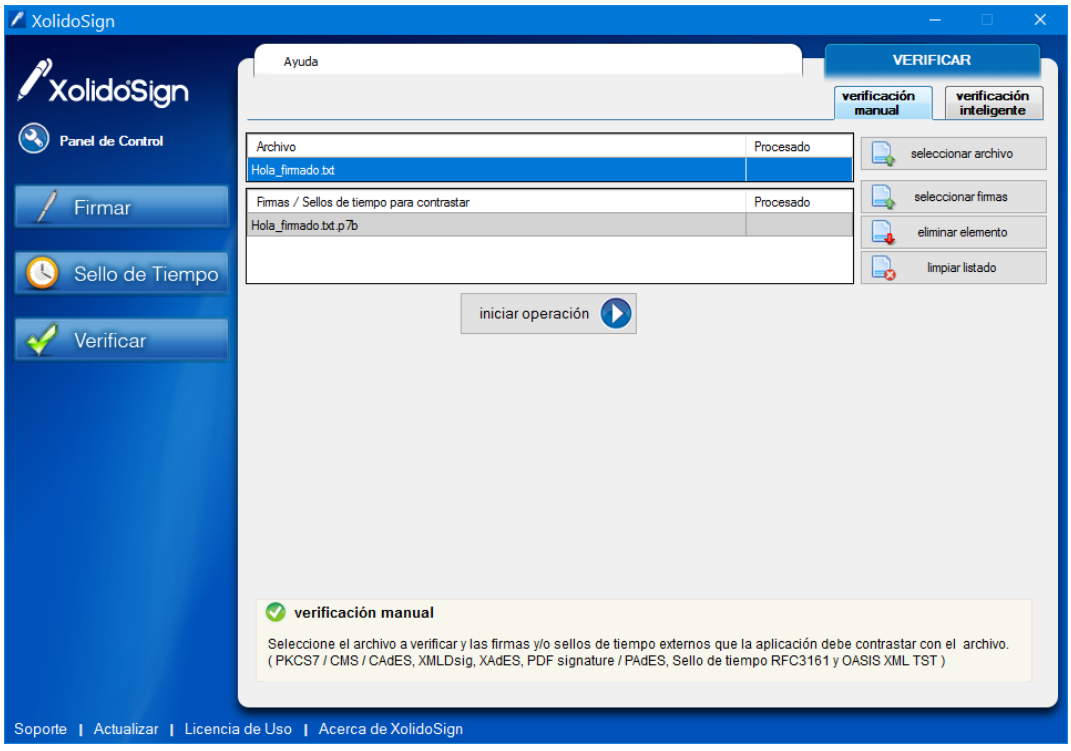
4. Verificación de firmas

Se supone que el fichero firmado junto con su firma digital se envía a otro usuario. El usuario receptor debe verificar la firma para asegurarse de que el contenido del fichero no ha sido modificado y el autor es el propietario del certificado usado para firmar el fichero.

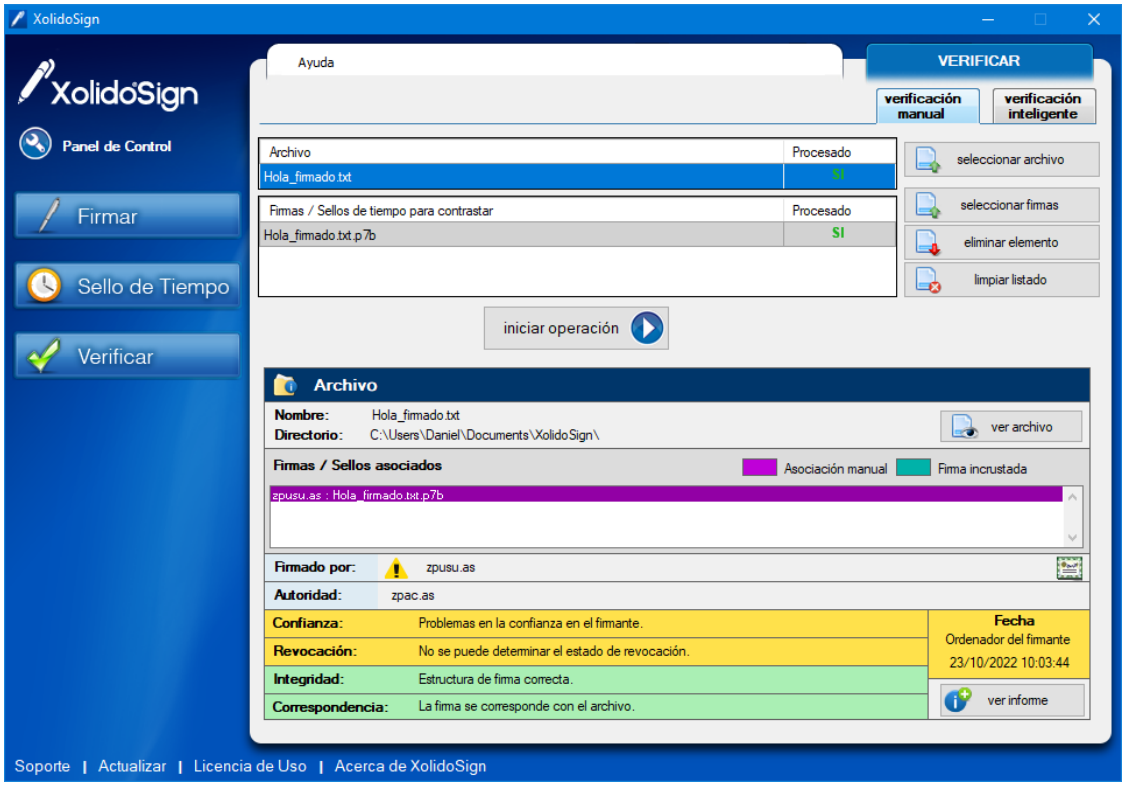
Al pulsar el botón Verificar, el programa XolidoSign muestra la pantalla siguiente:



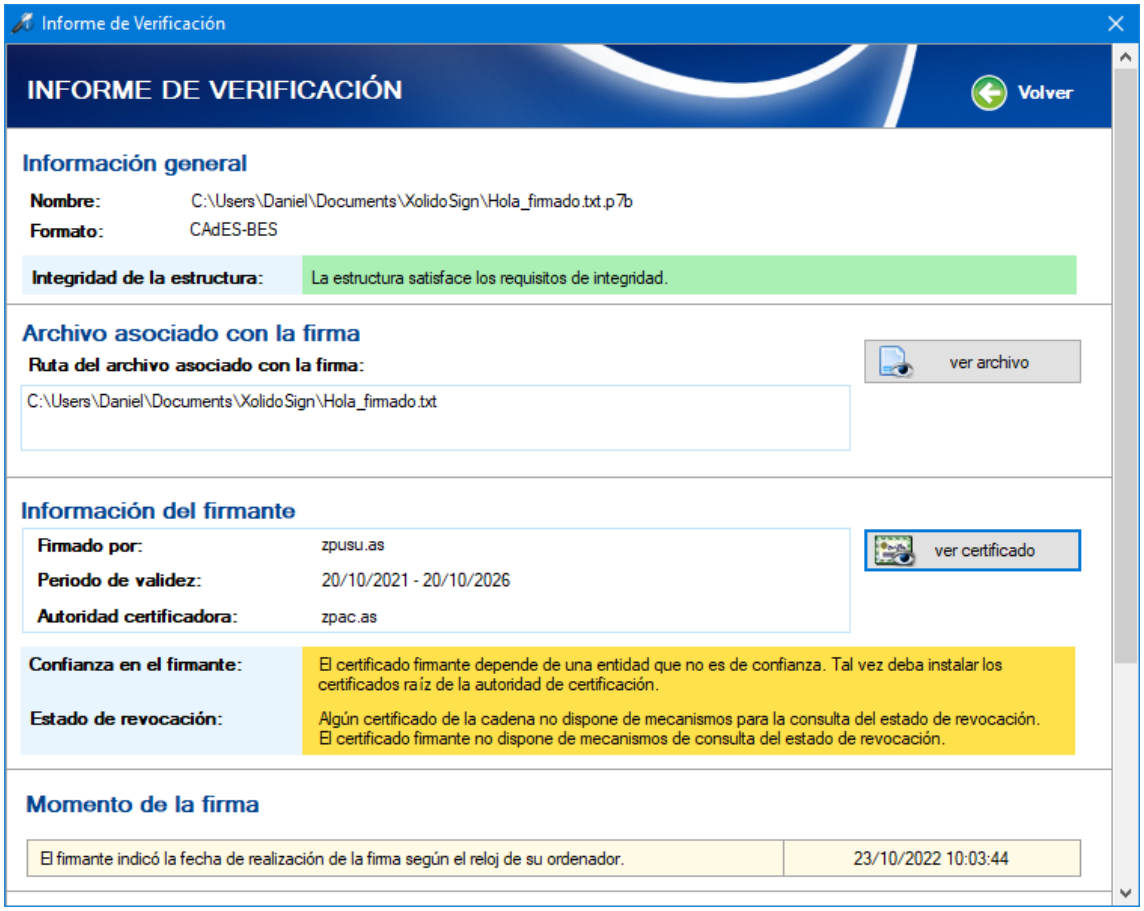
Está seleccionada la Verificación inteligente, que no debemos usar inicialmente. Selecciona en la parte superior derecha de la ventana, la pestaña "verificación manual". Selecciona el archivo a verificar y la firma a usar en la verificación. La pantalla mostrará lo que se indica a continuación.



Finalmente, pulsa el botón "iniciar operación".



Como se puede comprobar en la ventana, aparecen dos líneas amarillas en la parte inferior de la pantalla. Pulsar el botón "ver informe" ubicado en la esquina inferior derecha de la ventana.



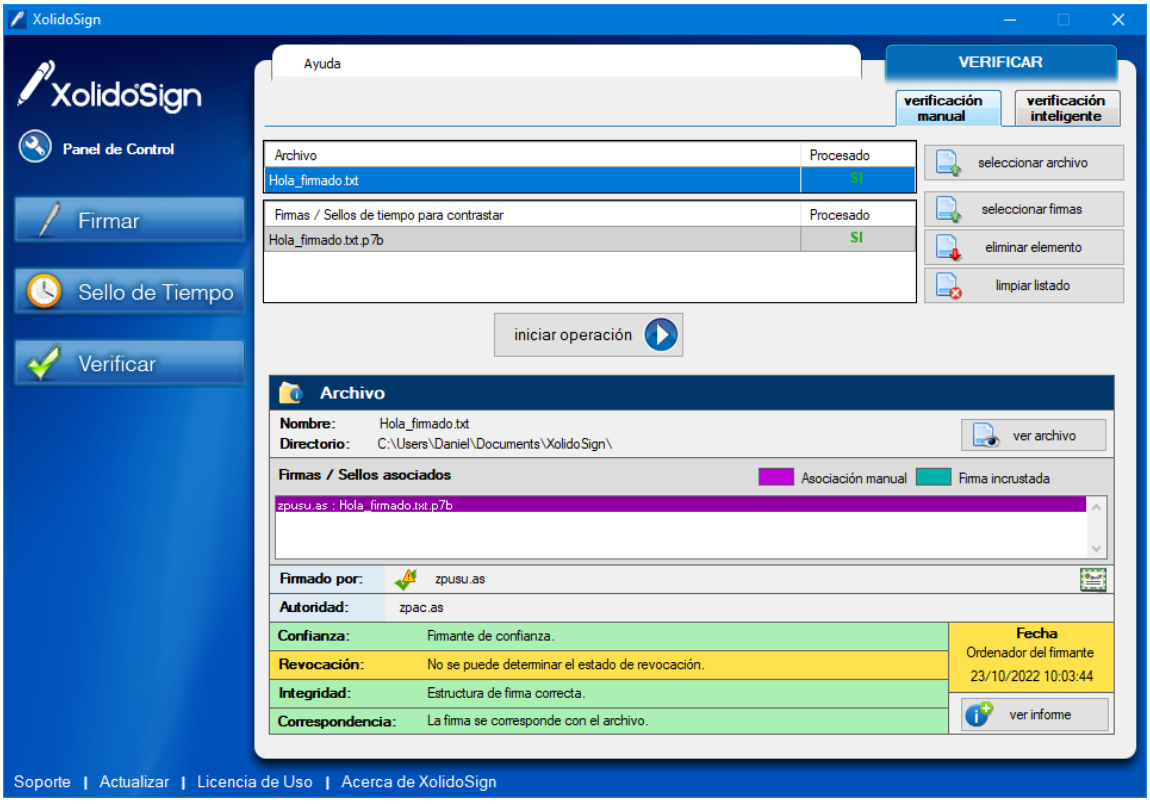
El primer problema es la falta de confianza en el firmante. Para resolverlo hay que instalar el certificado de la autoridad certificadora que ha emitido el certificado utilizado para firmar el fichero en el almacén lógico de certificados denominado "Entidades de certificación raíz de confianza".

El segundo problema se deriva de la imposibilidad de comprobar el estado de revocación de todos los certificados de la cadena. Para ello sería necesario proporcionar al programa XolidoSign acceso a las listas de revocación de certificados necesarias o utilizar el protocolo OCSP. Esto excede el tiempo disponible en esta práctica y no se tratará.

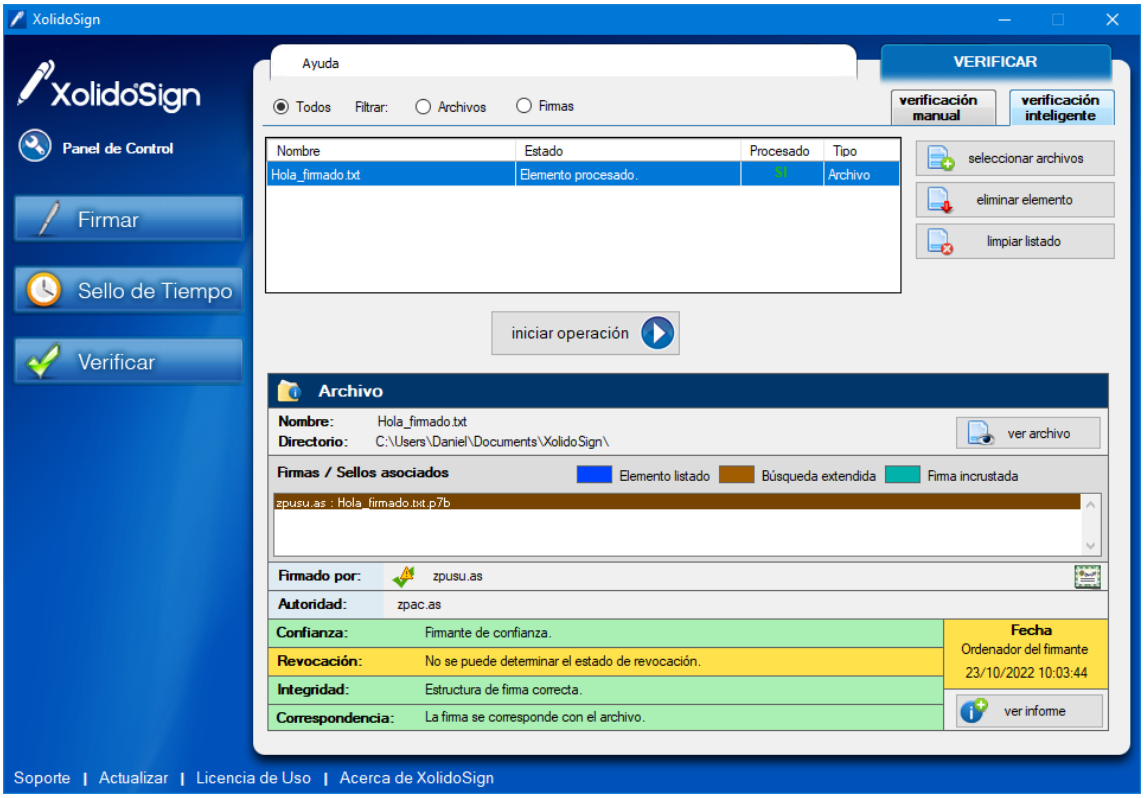
Una vez instalado el certificado zpac.as en el almacén lógico de certificados denominado "Entidades de certificación raíz de confianza" se puede volver a pulsar el botón "iniciar operación".

IMPORTANTE: El certificado zpac.as instalado debe ser el utilizado para generar (firmar) el certificado del Usuario utilizado para obtener la firma de fichero. Puede que haya otro certificado zpac.as instalado en el almacén de certificados del computador generado previamente. Este certificado no es válido, pues aunque se denomina igual, la clave pública que contiene es distinta. Se puede comprobar utilizando certmgr.

Una vez instalado el certificado raíz apropiado la nueva verificación genera el resultado que se puede ver en la ventana siguiente:



Probar el proceso de verificación inteligente, en el que solo se proporciona el nombre de los archivos para los que se ha generado su firma digital. El programa busca los archivos con las firmas de forma automática, tal como se muestra en la figura siguiente.

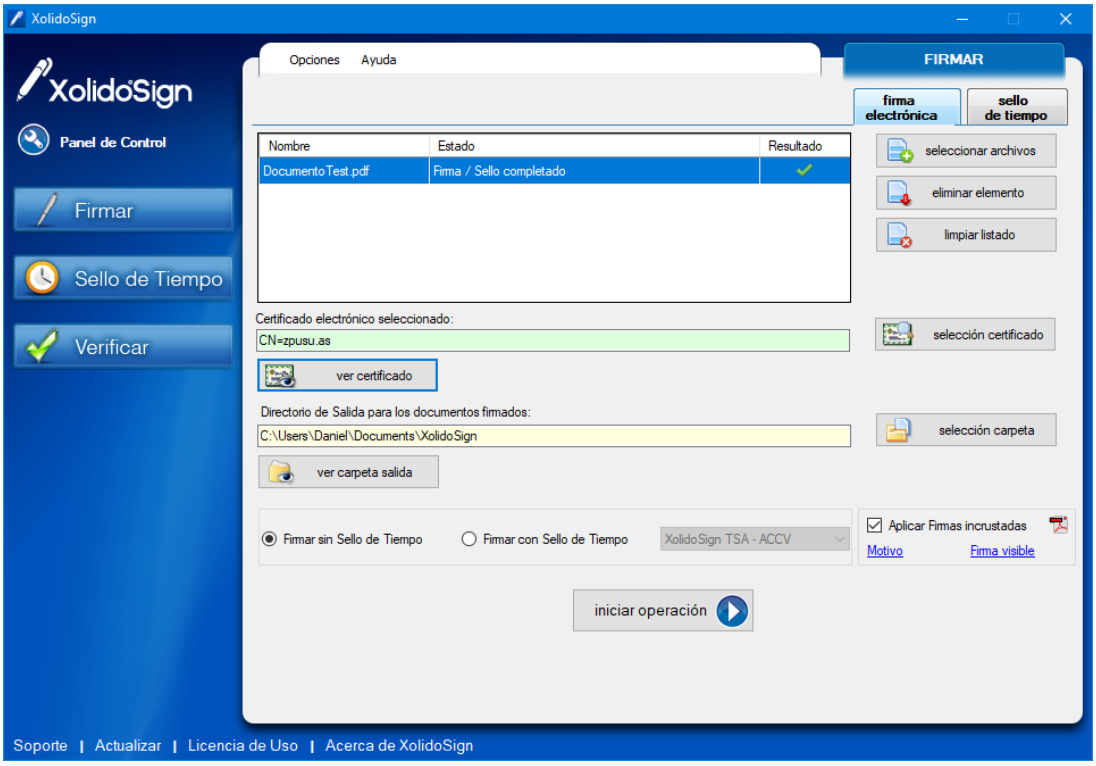


5. Firmas incrustadas

Hay formatos de documentos que disponen de espacio interno para almacenar la firma del propio documento, y por tanto no hay que almacenar la firma en un fichero separado. Los documentos más comunes de este tipo son los de Microsoft Office (Word, Excel, etc.) y los PDF de Adobe.

Genera un documento Word denominado DocumentoTest.docx que contenga la palabra hola y guárdalo como PDF en el directorio compartido entre la máquina virtual y la máquina física.

Inicia una operación de firma electrónica con el programa XolidoSign. Selecciona la opción "Aplicar firmas incrustadas" en la parte inferior derecha. Selecciona un motivo y solicita que se incluya una marca de firma visible en la parte superior derecha de la primera página.



Abre el fichero DocumentoTest_firmado.pdf con Adobe Reader DC y comprueba cómo indica que está firmado.

Verifica la firma del fichero PDF con el programa XolidoSign.

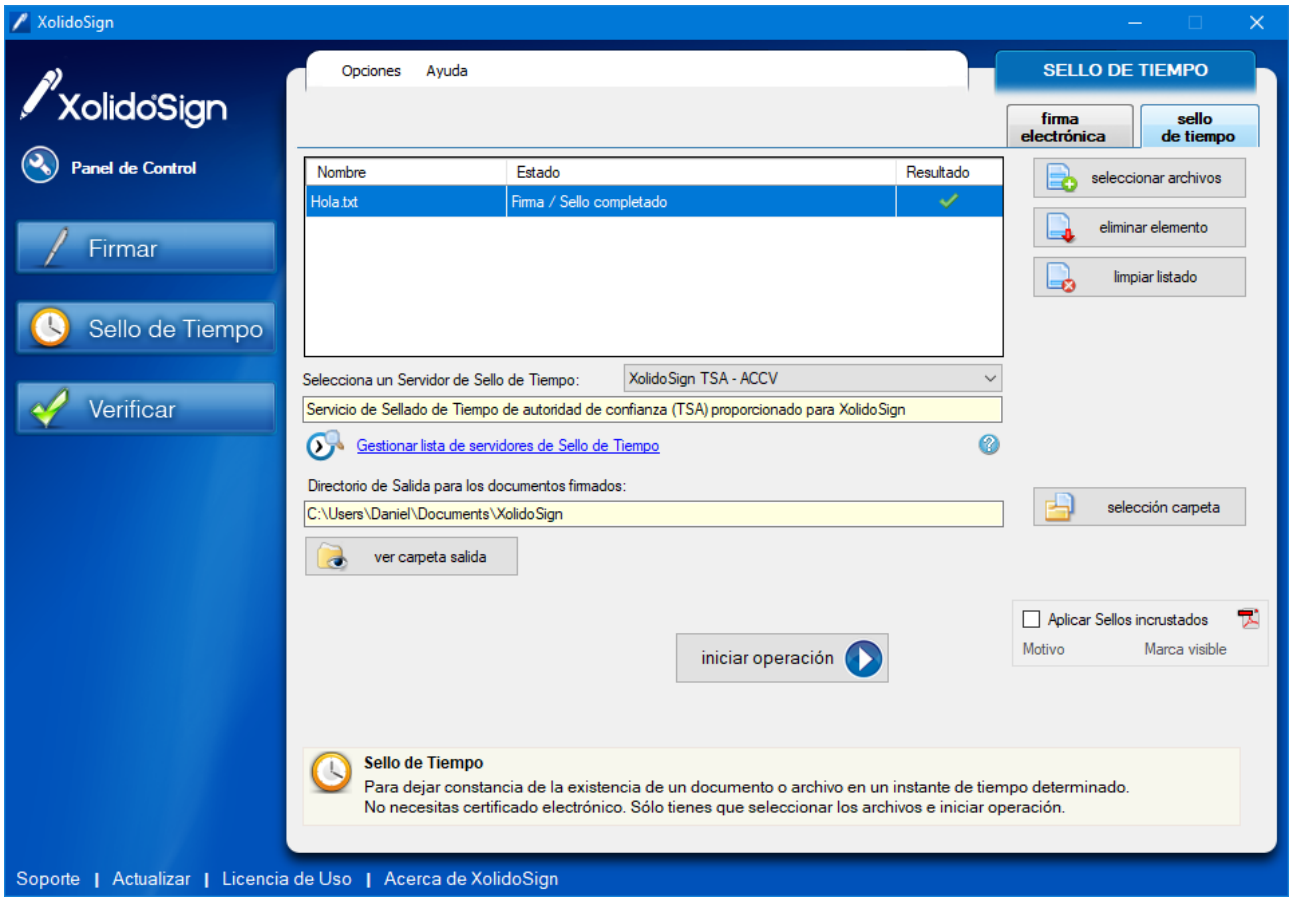
Si tienes tiempo suficiente haz la tarea siguiente. En caso contrario prescinde de ella, pues el certificado de la FNMT se usa obligatoriamente en la última sección de esta práctica.

Carga tu certificado personal emitido por la FNMT en el almacén de certificados del usuario y comprueba si el certificado raíz de la FNMT está disponible en el almacén de certificados de las Entidades raíz de confianza.

Repite alguna de las tareas anteriores usando el certificado de la FNMT. Determina si plantea los mismos problemas que el certificado de pruebas.

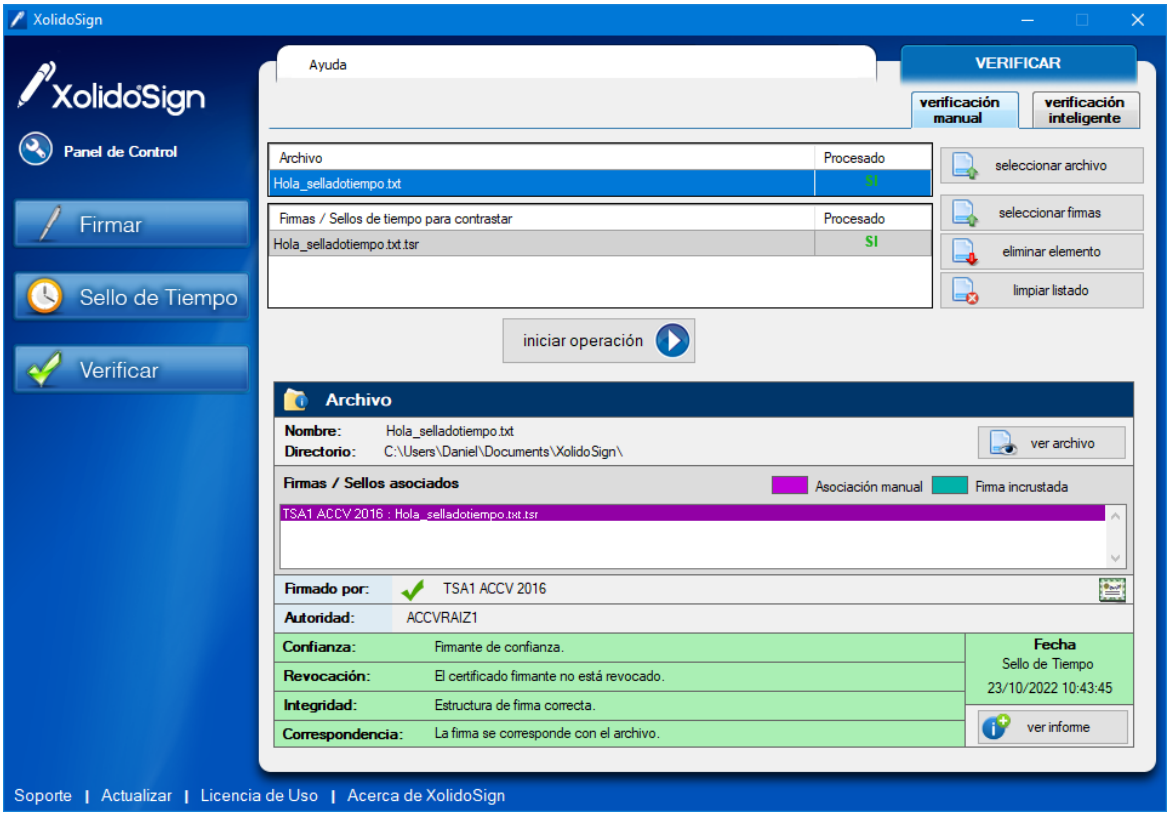
6. Sellos de tiempo

Crea una estampa de tiempo para el fichero hola.txt Comprueba, revisando las diapositivas de teoría, que el usuario no necesita un certificado/clave privada para crear un sello de tiempo para un documento. En la interfaz del programa pulsa el botón "Sello de Tiempo". Selecciona el fichero de entrada, un servidor de sellos de tiempo y el directorio de salida, como se muestra en la figura siguiente. Inicia la operación de generación del sello de tiempos. Se obtiene el resultado siguiente:

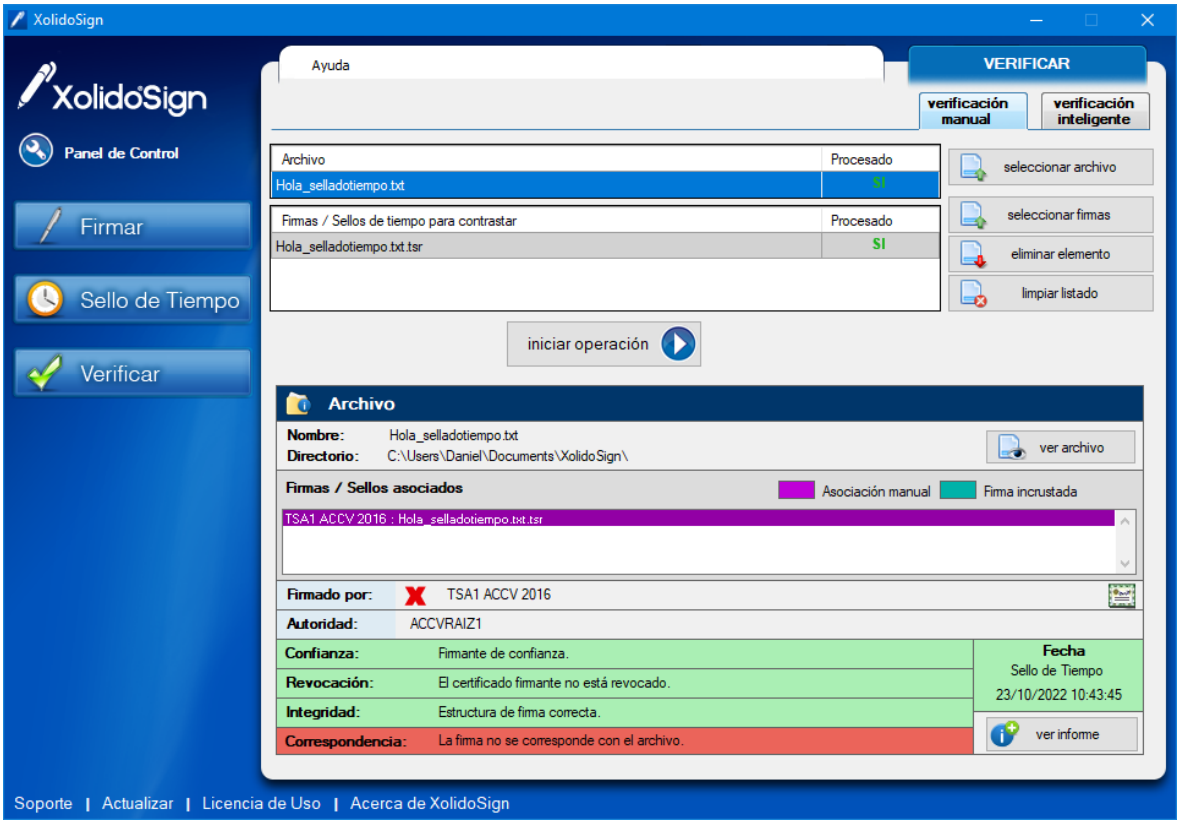


Usando el explorador de ficheros, comprueba que en el directorio de salida, en este ejemplo en el directorio C:\Users\Daniel\Documents\XolidoSign\, aparece una copia del fichero con el mismo nombre, pero al que se ha añadido el sufijo "_selladotiempo". Además aparece un fichero con el mismo nombre y extensión que el anterior al que se ha añadido una nueva extensión: ".tsr" (**t**ime **s**tamp **r**esponse o **r**eply, según RFC 3161).

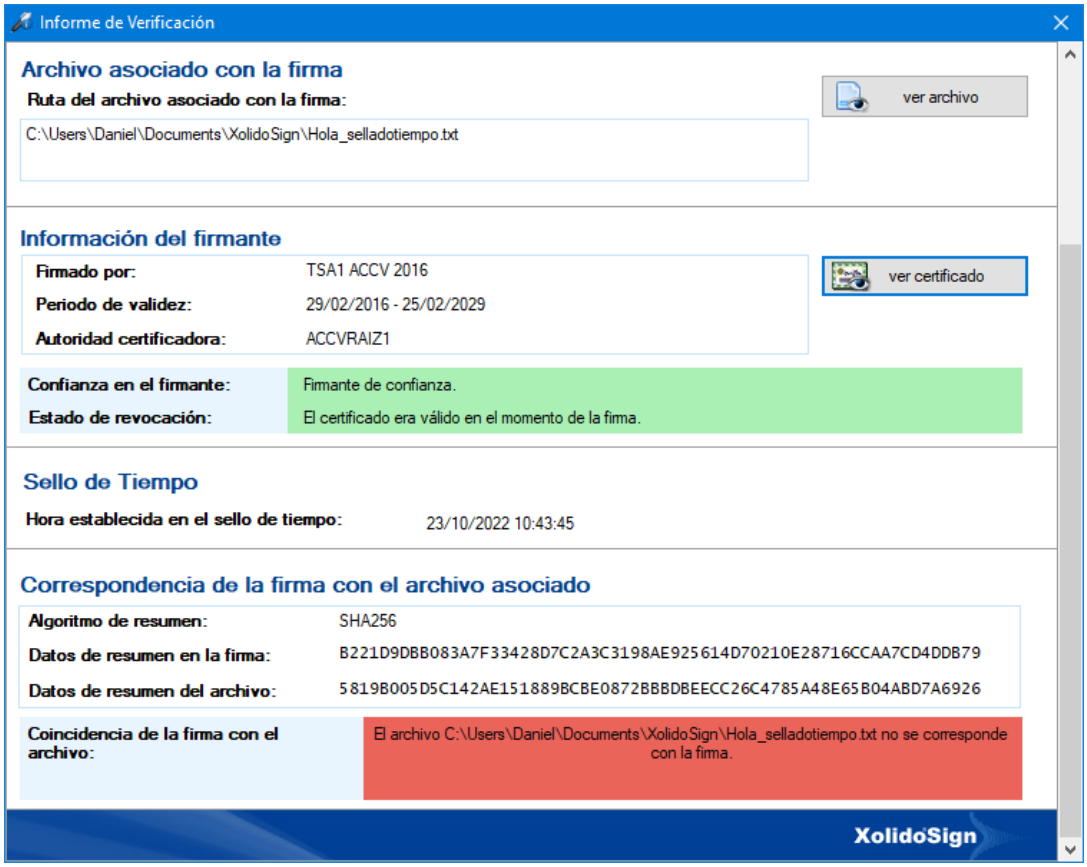
Para verificar un sello de tiempo, pulsar el botón Verificar. Selecciona el fichero a verificar y el fichero con el sello de tiempo. Pulsa el botón "iniciar operación". Los resultados se presentan debajo de este botón, tal como se muestra en la figura siguiente.



Ahora edita el fichero Hola_selladotiempo.txt, añade un segundo hola y guárdalo. Vuelve a verificar el sello de tiempo. Se obtiene el resultado siguiente:



Si se solicita el informe pulsando el botón "ver informe" se obtiene:



REFLEXIONAR:

Observar que la operación Verificar se aplica por igual a Firmas y a Sellos.

- La Firma es el cifrado del hash del documento con la clave privada del usuario.
- El Sello es el cifrado del hash del documento junto con el tiempo de la TSA con la clave privada de la TSA (*Time Stamping Authority*). O sea, el sello es una firma digital con un formato específico.

Observar que para verificar un sello de tiempo creado por una TSA el programa XolidoSign necesita la clave pública (certificado) de esa TSA. Si XolidoSign no ha cargado automáticamente el certificado raíz de la TSA que utiliza en el almacén de certificados de Windows, es posible que haya que hacerlo manualmente. Consultar la web de la TSA usada por XolidoSign:

https://www.accv.es/servicios/sellado-de-tiempo/

7. Combinación de firmas y sellos en PDF

En esta sección de la práctica se utilizará el certificado de usuario de la FNMT.

Para un fichero (documento) se puede crear una firma digital y un sello de tiempo. A continuación se describen posibles formas de realizar esta tarea.

FIRMA NO INCRUSTADA

Por ejemplo para un fichero de texto como hola.txt.

MÉTODO INCORRECTO

Paso1: Generar una firma SIN sello de tiempo. Se crean los ficheros hola_firmado.txt y hola_firmado.txt.p7b. En la ventana de verificación de la firma de XolidoSign, en la esquina inferior derecha pulsa el botón "ver informe" tras la verificación. Observa que el formato de la firma es CAdES-BES.

Paso 2: Genera un sello de tiempo para los dos ficheros previos. XolidoSign genera un sello de tiempo independiente para cada fichero.

MÉTODO CORRECTO

Borra los ficheros del directorio de salida de XolidoSign. Genera una firma CON sello de tiempo. Se crean los ficheros hola_firmado.txt y hola_firmado.txt.p7b. En la ventana de verificación de la firma de XolidoSign, en la esquina inferior derecha pulsa el botón "ver informe" tras la verificación. Observa que el formato de la firma es CAdES-T.

La firma CAdES-T integra un sello de tiempo realizado sobre la firma digital (o quizás sobre toda la firma electrónica CAdES-BES).

FIRMA INCRUSTADA

Por ejemplo para un fichero de tipo PDF como hola.pdf.

MÉTODO INCORRECTO

Paso 1: Generar una firma SIN sello de tiempo. Se crea el fichero hola_firmado.pdf. Reader DC valida la firma correctamente y XolidoSign también.

Paso 2: Genera un sello de tiempo para el fichero hola_firmado.pdf. XolidoSign crea el fichero denominado hola_firmado_selladotiempo.pdf. XolidoSign al verificar este documento encuentra dos elementos y muestra un informe de verificación para cada uno de ellos.

MÉTODO CORRECTO

Genera una firma CON sello de tiempo. En la ventana "Firmar" de XolidoSign selecciona Opciones (en la parte superior junto a la barra de título) o pulsa F5. Se abre la ventana "Configuración".

En el panel izquierdo selecciona "Formato de la firma". Asegúrate de que está seleccionado el formato de "Firmas electrónicas básicas", por ejemplo CAdES-BES.

Después, en el panel izquierdo selecciona "Preferencias de la firma". Asegúrate de que está marcada la opción "Seleccionar firma electrónica incrustada en PDF por defecto" y que no está seleccionada la opción "Firma incrustada PDF en modo PAdES-BES". De este modo se obtendrá una firma PDF elemental. Tras firmar se genera el documento hola_firmado.pdf.

Al abrir el documento hola_firmado.pdf con Reader DC se valida la firma y el sello de tiempo correctamente. Pero para ello, deben estar cargados en el almacén de Certificados Raíz de Confianza de Adobe: el certificado raíz de la FNMT y el certificado raíz de la autoridad de sellado de tiempos, TSA-ACCV.

Otra posibilidad es cargar estos dos certificados en el almacén "Entidades de certificación raíz de confianza de Windows" e indicarle a Adobe:

Confiar en TODOS los certificados raíz del almacén de certificados de Windows para:

Validando firmas

Al verificar el documento hola_firmado.pdf con XolidoSign todo debe ser correcto. Se puede comprobar que solo hay una firma que incluye un sello de tiempo. Al pulsar "ver informe" se refleja en el informe la inclusión del sello y que el formato de la firma es PDF.

Comprobaciones adicionales:

Comprobación 1) Vuelve a generar una firma CON sello de tiempo. Pero en la Configuración (F5) en "Preferencias de la firma" asegúrate de que está marcada la opción "Seleccionar firma electrónica incrustada en PDF por defecto" y que SI está seleccionada la opción "Firma incrustada PDF en modo PAdES-BES". De este modo se obtendrá una firma PDF avanzada.

Comprobación 2) Vuelve a generar una firma CON sello de tiempo. Pero en la Configuración (F5) en "Preferencias de la firma" asegúrate de que está marcada la opción "Seleccionar firma electrónica incrustada en PDF por defecto" y que SI está seleccionada la opción "Firma incrustada PDF en modo PAdES-BES" y también está seleccionada la opción "Incluir valores de longevidad como PAdES-LTV". De este modo se obtendrá una firma PDF avanzada y con validación a largo plazo.