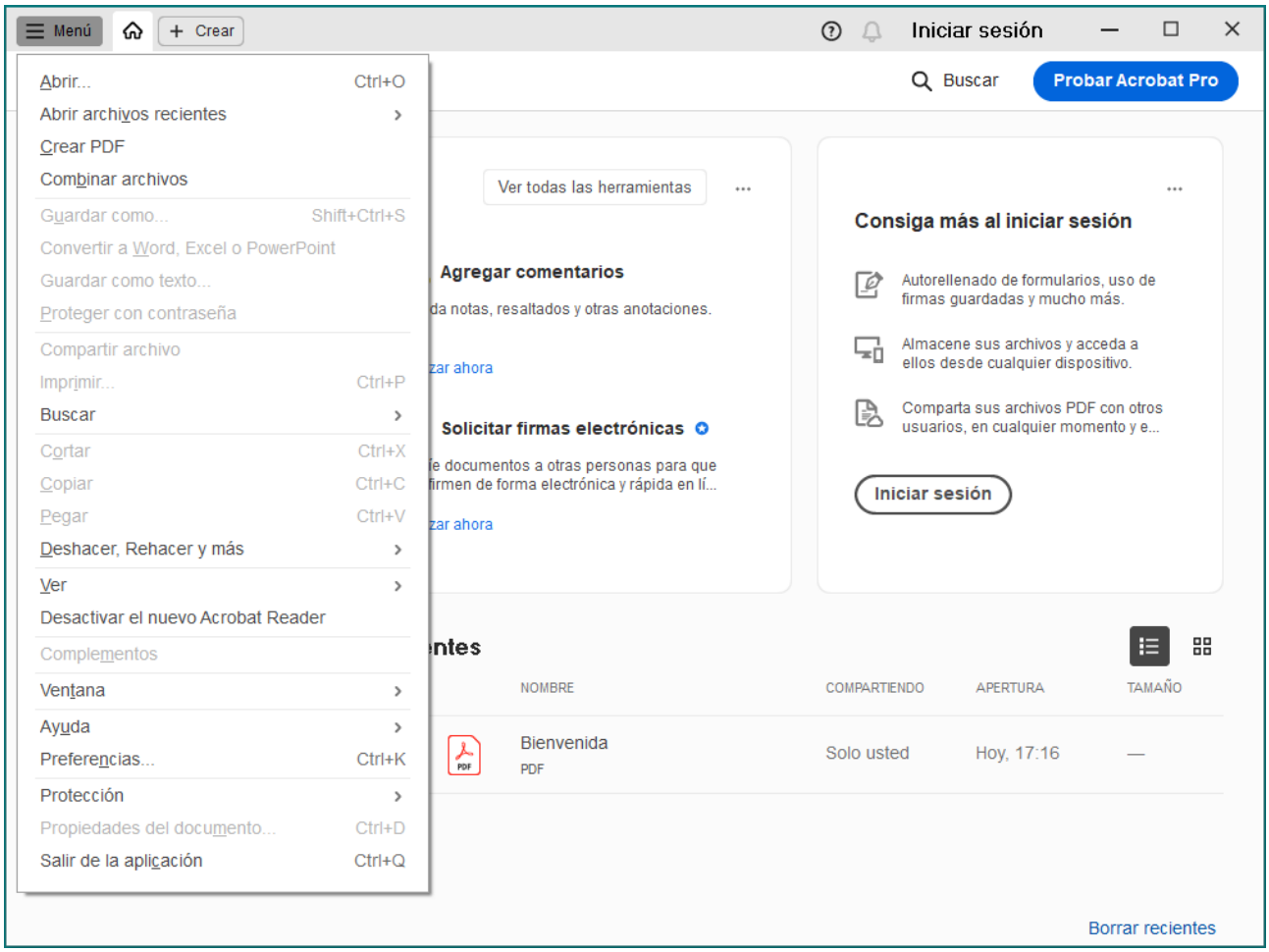
Uso de Certificados - Firmas en PDFs (Realizar con Adobe Reader)
Práctica 6B

1. Objetivo

En esta práctica el alumno debe utilizar certificados para verificar firmas digitales de documentos en formato PDF. Además debe gestionar el almacén de certificados de Adobe y realizar firmas. Para ello, descargar e instalar Adobe Reader en la Máquina Virtual de prácticas.

Al ejecutar Adobe Reader se muestra el nuevo interface.



Desplegar el menú y seleccionar “Desactivar el nuevo Acrobat Reader” para usar la interfaz clásica de Reader, que es la que se usa en esta práctica.

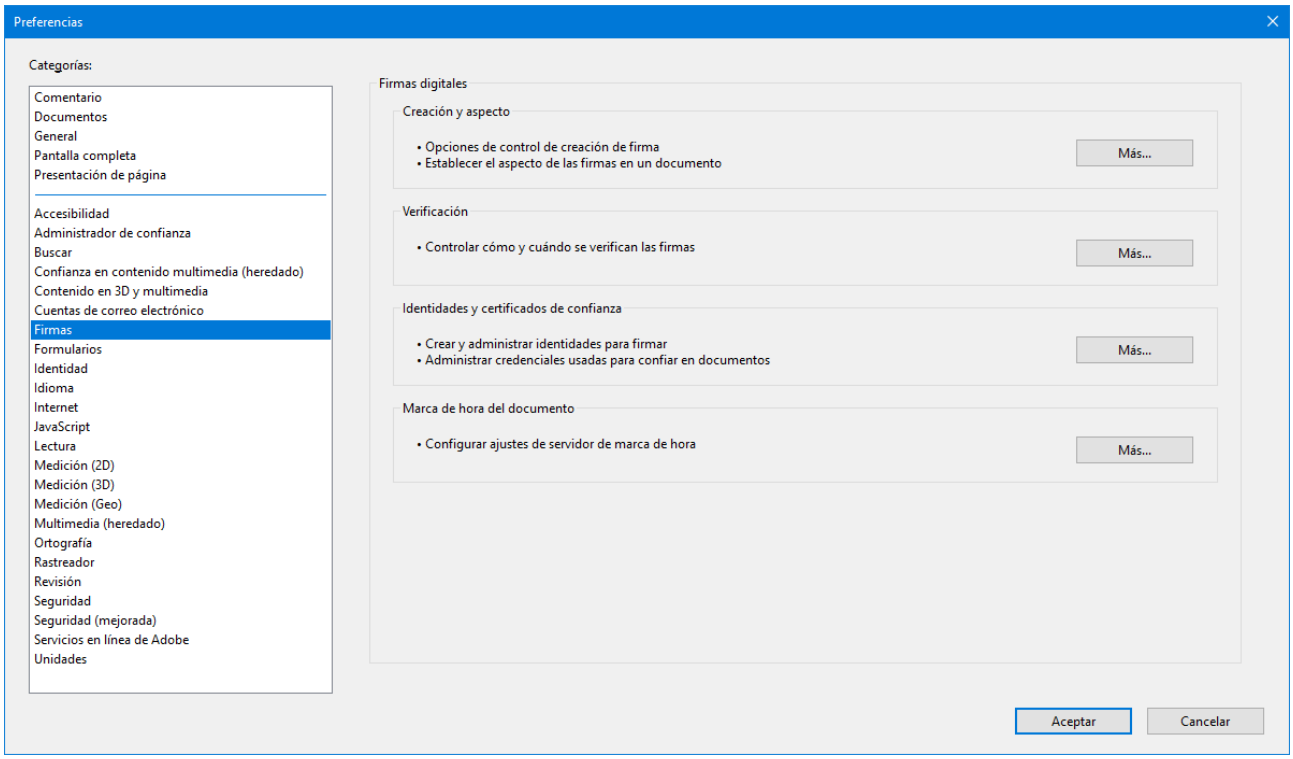
2. Gestión de los certificados de Adobe

Las aplicaciones de Adobe, incluyendo Reader, utilizan un almacén de certificados propio e independiente del almacén de certificados del sistema operativo.

Nada más terminar la instalación de Adobe Reader, el almacén de certificados de confianza de Adobe contendrá solamente dos certificados raíz de Adobe.

Accede a los almacenes de certificados de Adobe para comprobarlo del modo siguiente:

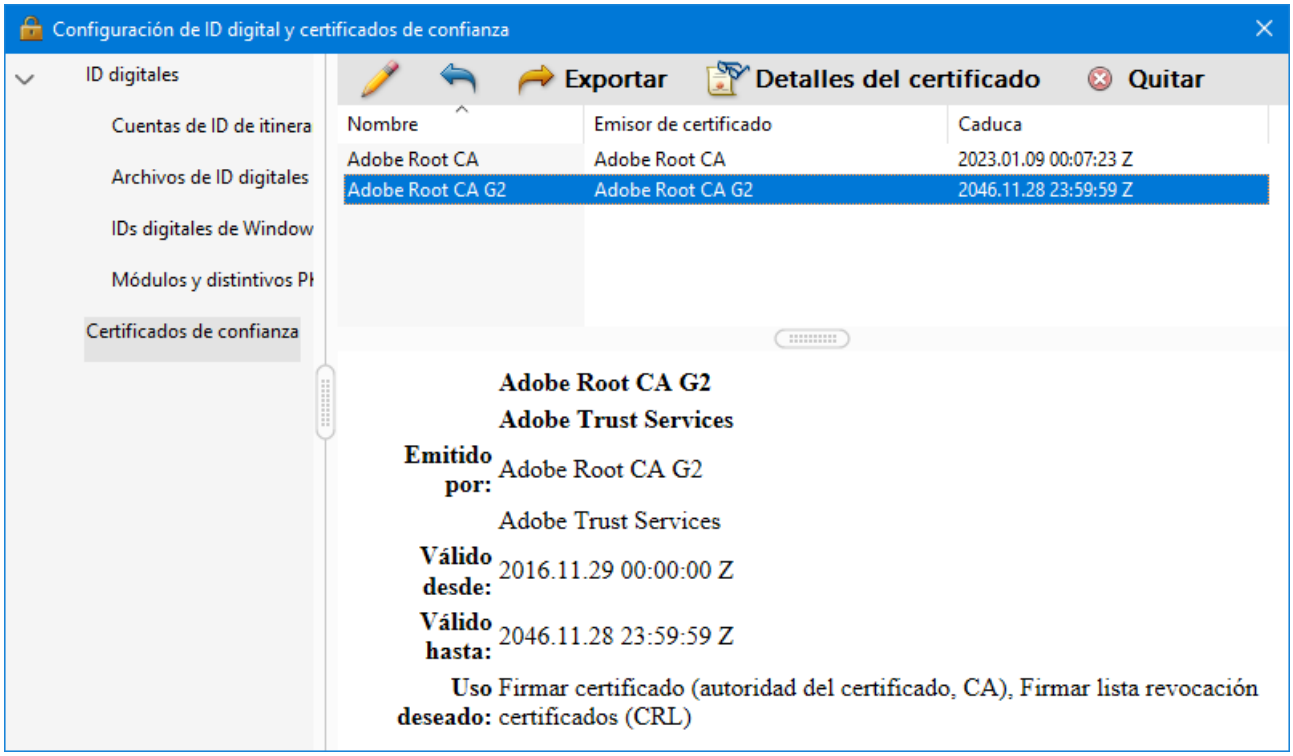
En la barra horizontal de menús de Adobe Reader, selecciona "Edición", y en el desplegable que aparece elige la última opción, "**Preferencias...**". Se muestra la ventana Preferencias. Selecciona Firmas en el panel izquierdo, tal como se muestra en la ventana siguiente:



En el tercer cuadro, Identidades y certificados de confianza, pulsa el botón "Más...".

Aparece la ventana siguiente:

En esta ventana selecciona la última opción del panel izquierdo "Certificados de confianza" y observa los certificados raíz de Adobe que aparecen en el panel derecho:



El almacén de certificados raíz de confianza de Adobe está prácticamente vacío en comparación con el almacén de certificados raíz de confianza del SO Windows.

Hay que realizar la pesada tarea de integrar manualmente cada certificado raíz de confianza que se necesite. Pero esta tarea ¡NO SERÁ NECESARIA! …

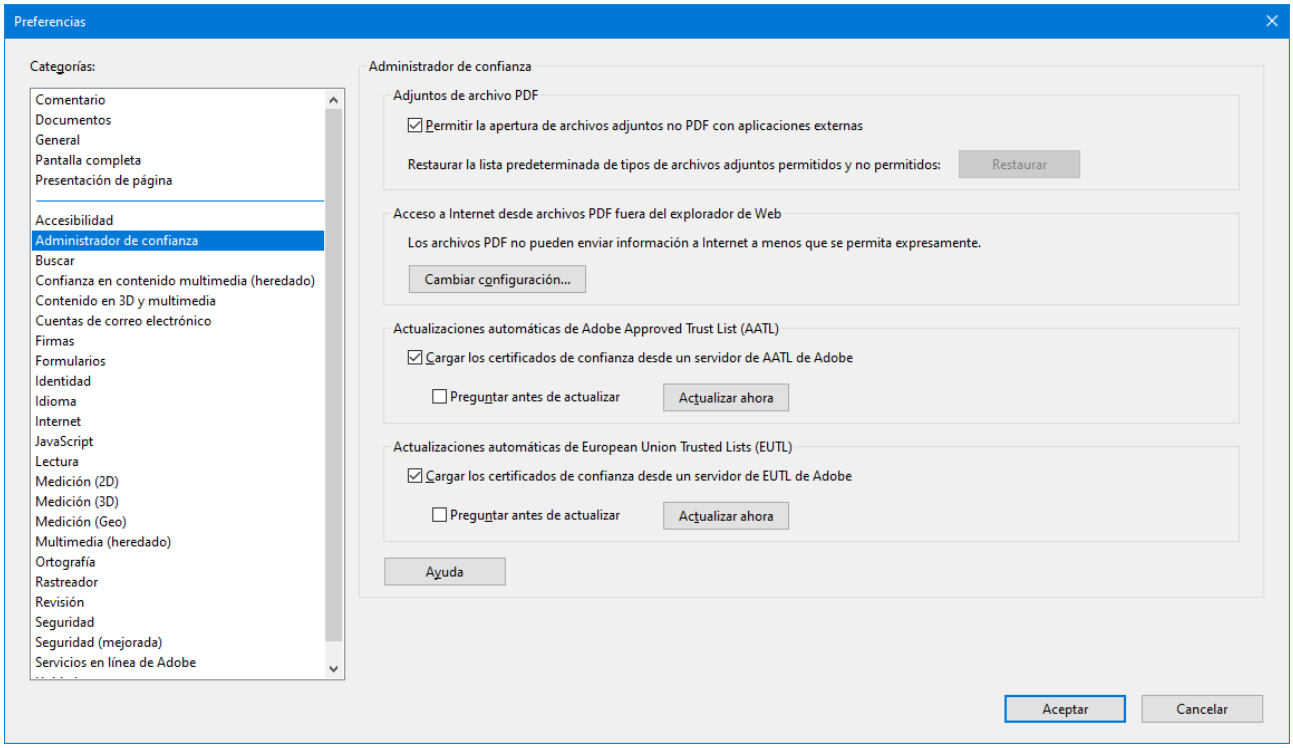
La Lista de certificados raíz de confianza aprobados por Adobe

Adobe mantiene la **AATL** (*Adobe Approved Trust List*). Es una lista de certificados raíz de confianza que muchas Autoridades Certificadoras (ACs) han enviado a Adobe y han sido técnicamente aprobados por Adobe.

Periódicamente, la AATL es actualizada, firmada digitalmente por Adobe y puesta a disposición de las aplicaciones en un servidor AATL de Adobe.

Cualquier aplicación Adobe de un usuario puede conectarse al servidor AATL de Adobe para descargar e instalar automáticamente los certificados raíz de confianza.

Comprueba que la actualización automática de los certificados de confianza de Adobe está activada. En la ventana Preferencias de Adobe Reader selecciona “Administrador de confianza” en el panel izquierdo, tal como se muestra en la ventana siguiente:



Observa el tercer cuadro del panel derecho. La opción “Cargar los certificados de confianza desde un servidor AATL de Adobe” esta preseleccionada. No la modifiques.

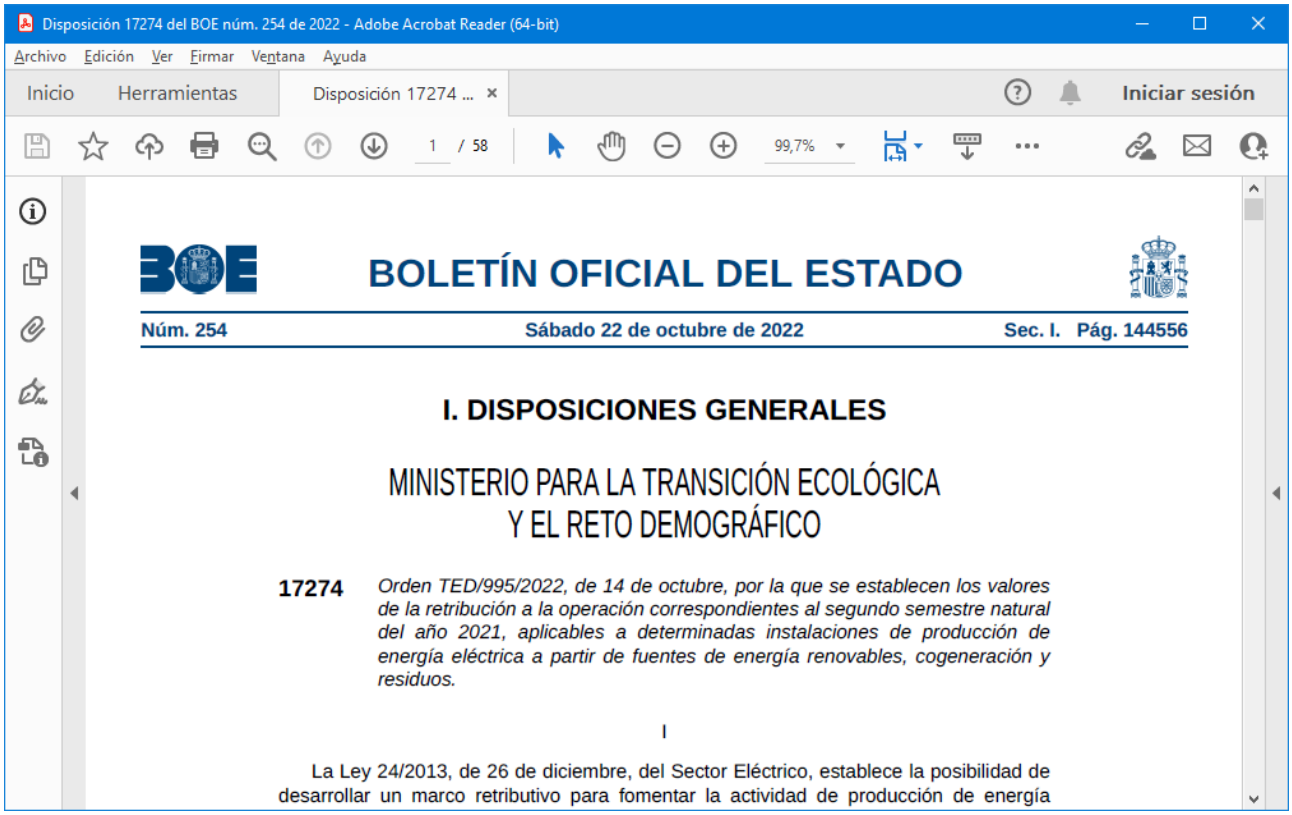
Observa que se dispone del botón “Actualizar ahora” pero no lo utilices.

Observa el cuarto cuadro del panel derecho. La misma técnica de actualización automática se usa para los certificados de confianza que están en las listas de confianza de la Unión Europea, EUTL (*European Union Trusted Lists*). La opción “Cargar los certificados de confianza desde un servidor EUTL de Adobe está preseleccionada. No la modifiques.

Observa que se dispone del botón “Actualizar ahora” pero no lo utilices.

3. Verificar la firma digital de un PDF (Usando el almacén de certificados de Adobe)

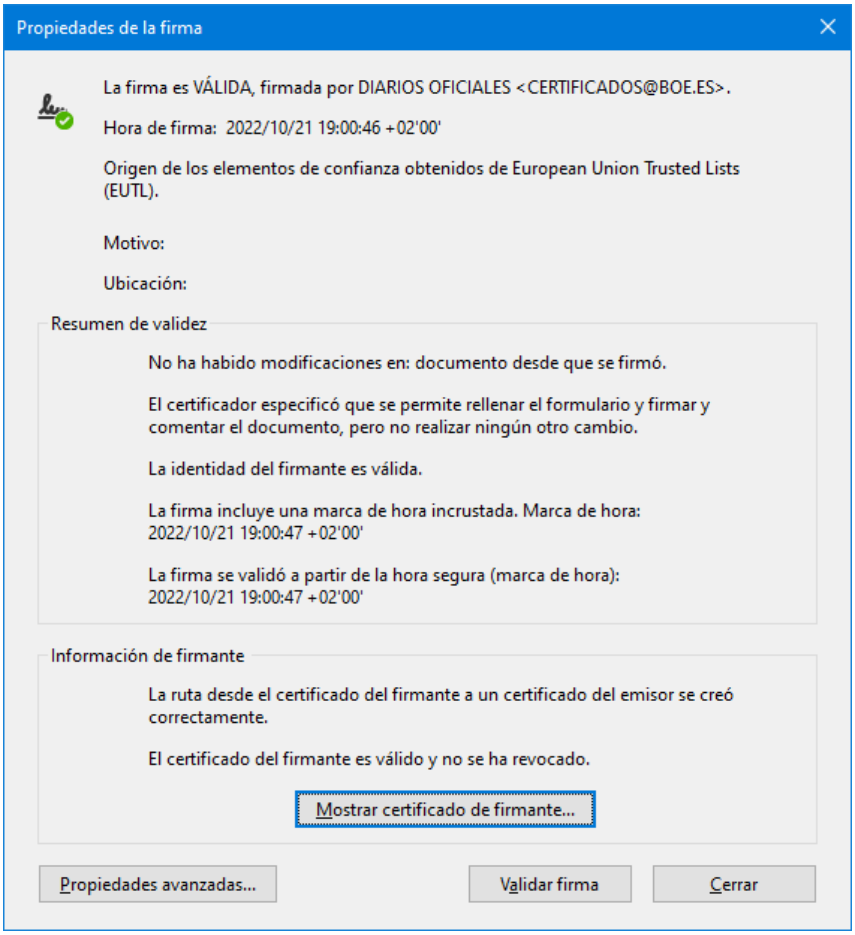
El objetivo es aprender a verificar la firma digital de un documento (fichero) con formato PDF. Para ello se utilizará el fichero de un BOE (Boletín Oficial del Estado) que está en formato PDF y ha sido firmado digitalmente. Accede a la web del BOE y descarga un boletín (PDF) de hoy. Abre el documento con Reader que mostrará el BOE del siguiente modo:



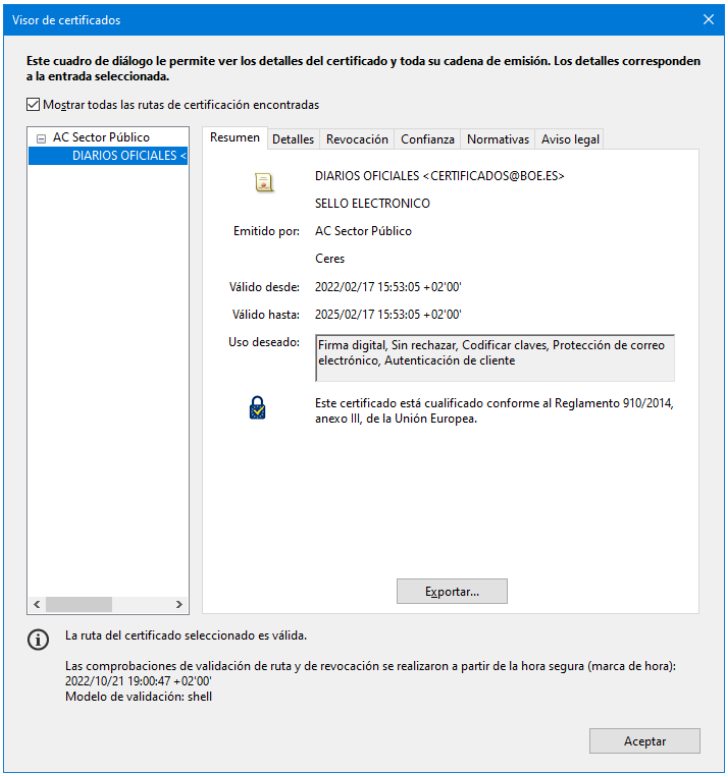
Observa que en la barra de botones izquierda, aparece el símbolo con una pluma (cuarto empezando por arriba) que indica que el documento contiene una firma.

Pulsa en el símbolo para que se despliegue el panel de firmas. Observa que en el icono de firma aparece un circulo verde, que indica que Reader a validado la firma.

Coloca el puntero del ratón sobre la etiqueta de la firma y pulsa el botón derecho del ratón. En el menú contextual que aparece selecciona "Mostrar propiedades de firma..." y aparece la ventana informativa siguiente:



Pulsa el botón "Mostrar certificado del firmante..." y aparece la ventana "Visor de certificados".

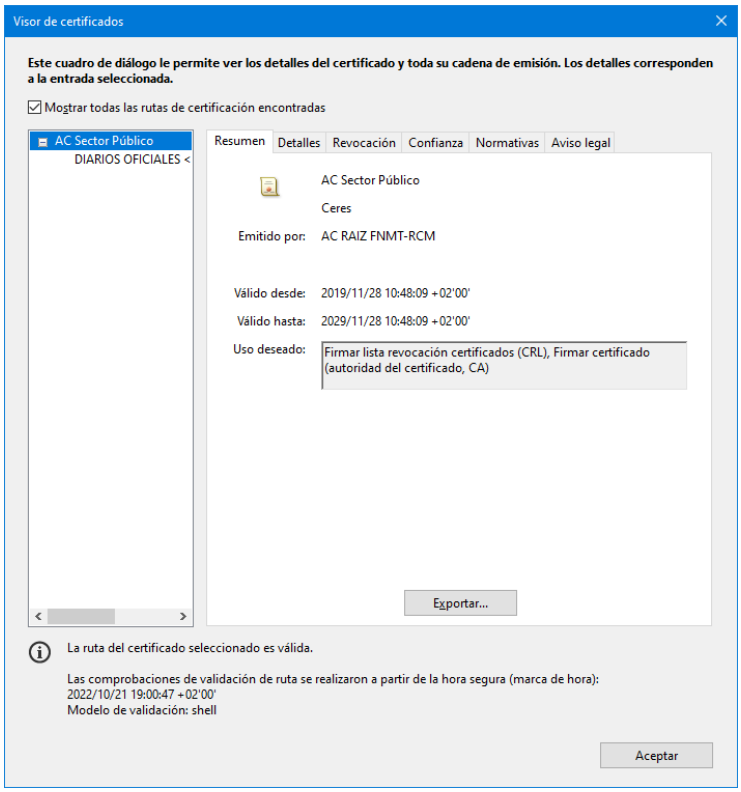


Comprobar la cadena de certificados utilizada para la firma

Observa que el documento PDF integra no solo la firma, sino también el certificado correspondiente a la clave privada usada para firmar el documento PDF y todos los certificados de la cadena hasta llegar al certificado raíz.

En la figura siguiente aparece la ficha "Resumen". Comprueba que al cambiar el certificado seleccionado en el panel de la izquierda, la ficha Resumen muestra los datos del certificado seleccionado. De esta forma podemos comprobar visualmente cada certificado de la cadena de certificados.

Selecciona el certificado raíz de la cadena, que está en la parte superior.



Selecciona la **pestaña "Resumen"**. Observa que el sujeto del certificado (AC Sector público) y su emisor (AC RAIZ FNMT-RCM) no son el mismo, pero se está usando el certificado como un anclaje de confianza.

Este es un ejemplo de que una autoridad certificadora principal puede crear una autoridad certificadora subordinada, que funcionará como anclaje de confianza de una PKI, en este caso una PKI para todo el "Sector público" español.

Selecciona la **pestaña "Detalles"**. Observa el gran periodo de validez del certificado, de 10 años, y comprueba la gran longitud de la clave RSA utilizada, de 4096 bits. Observa la huella digital o Compendio SAH1 del certificado: 95 F6 ··· FF F9.

Selecciona la **pestaña "Revocación"**. Observa que los certificados que funcionan como como anclaje de confianza, se consideran inherentemente de confianza y no se comprueba su revocación.

Selecciona la **pestaña "Confianza"**. Observa que el certificado está incluido en la Lista Europea de Confianza (EUTL) para dos propósitos.

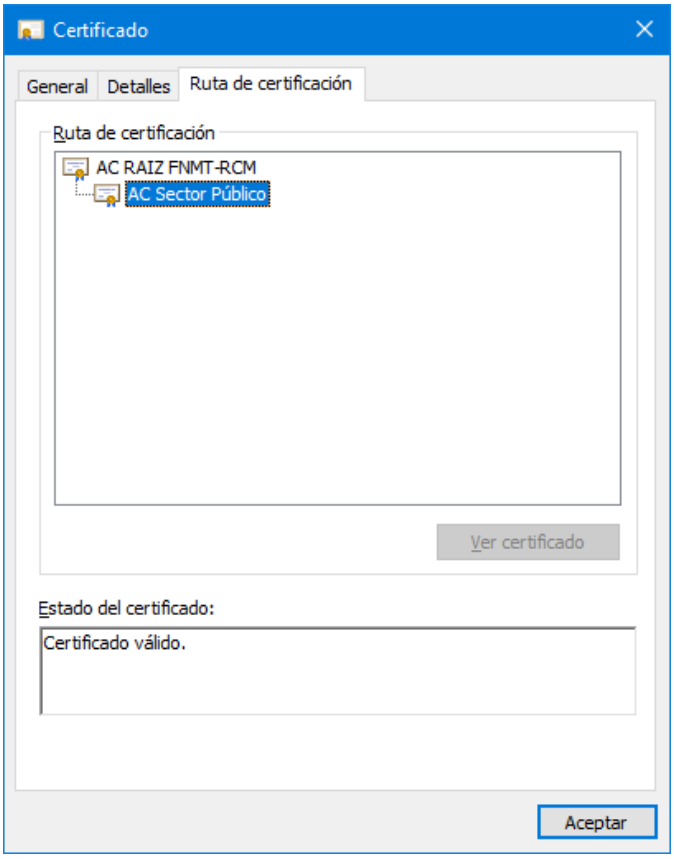
Comprueba la cadena de certificación del certificado AC Sector Público

Busca el certificado de "AC Sector Público" en:

https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

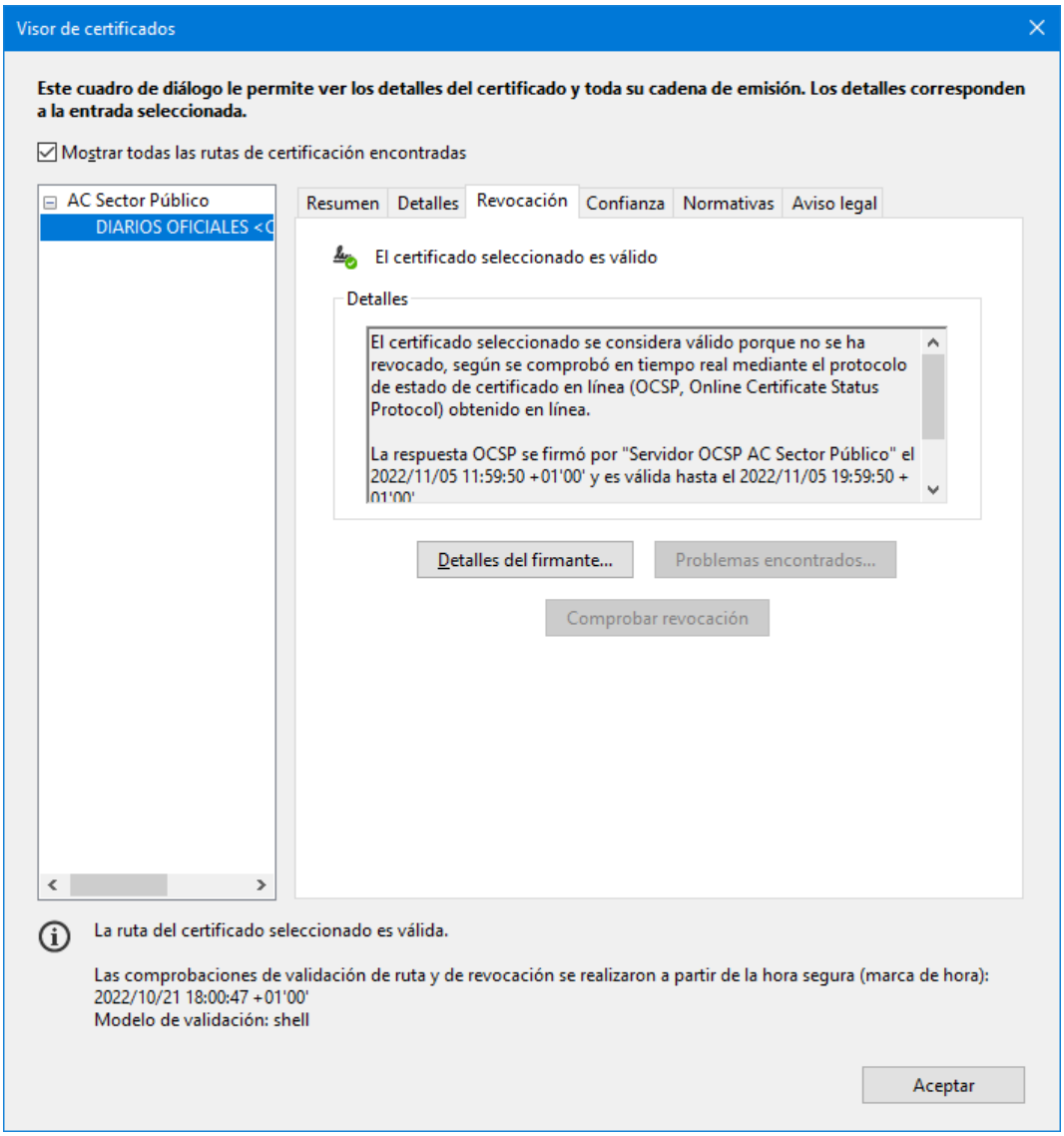
Es muy interesante que visites esta página para que veas cómo una Autoridad Certificadora importante, como la FNMT, publica sus certificados y otra información relevante.

La huella SHA1 del certificado (95 F6 ⋯ FF F9) te permitirá localizarlo de forma inequívoca. Descárgalo y ábrelo haciendo doble clic sobre el propio certificado. Observa la cadena:



Comprobar el estado de revocación del certificado del firmante

En le ventana “Visor de certificados” selecciona el certificado del firmante del boletín en panel izquierdo y selecciona la pestaña “Revocación” en el panel derecho.

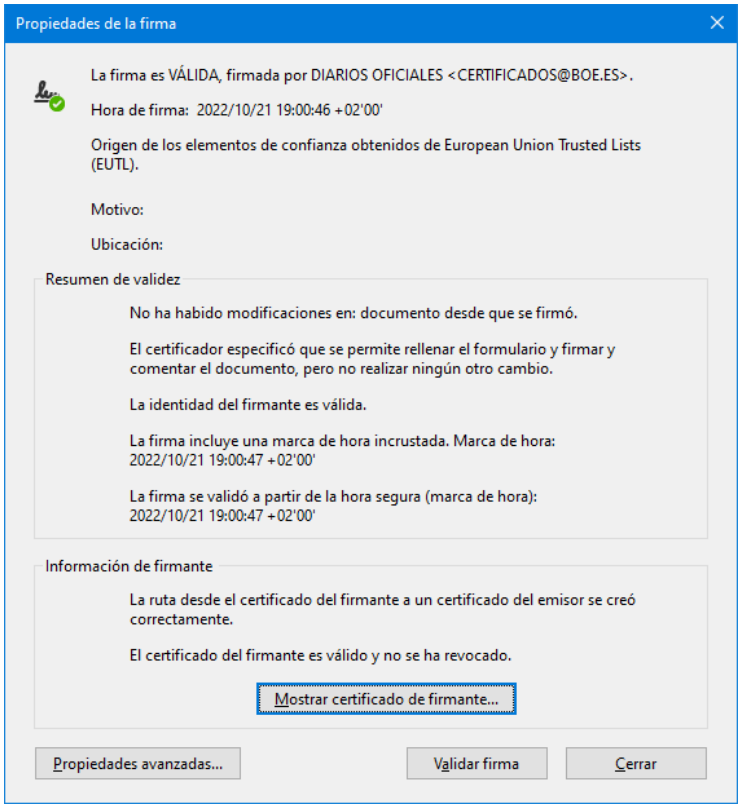


Como puedes comprobar Adobe Reader utiliza el protocolo OCSP para comprobar la validez de los certificados. Lee el contenido del cuadro de texto “Detalles” para ver la respuesta del servidor OCSP.

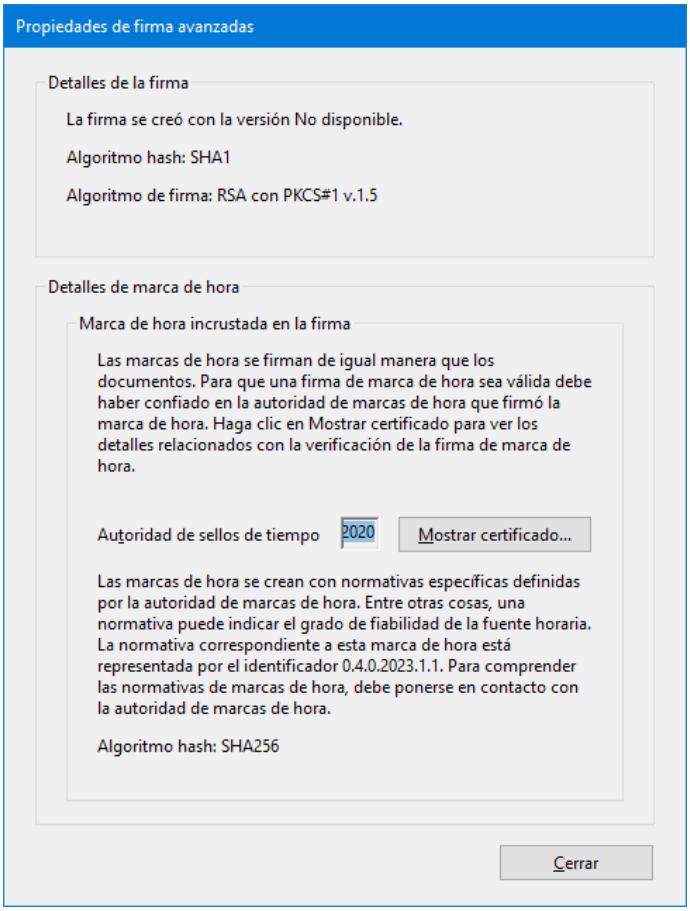
Pulsa el botón "Detalles del firmante..." para ver el certificado de la entidad que ha firmado digitalmente la respuesta recibida del servidor OCSP.

Comprobar el sello de tiempo de la firma

Vuelve a la ventana “Propiedades de la firma”.



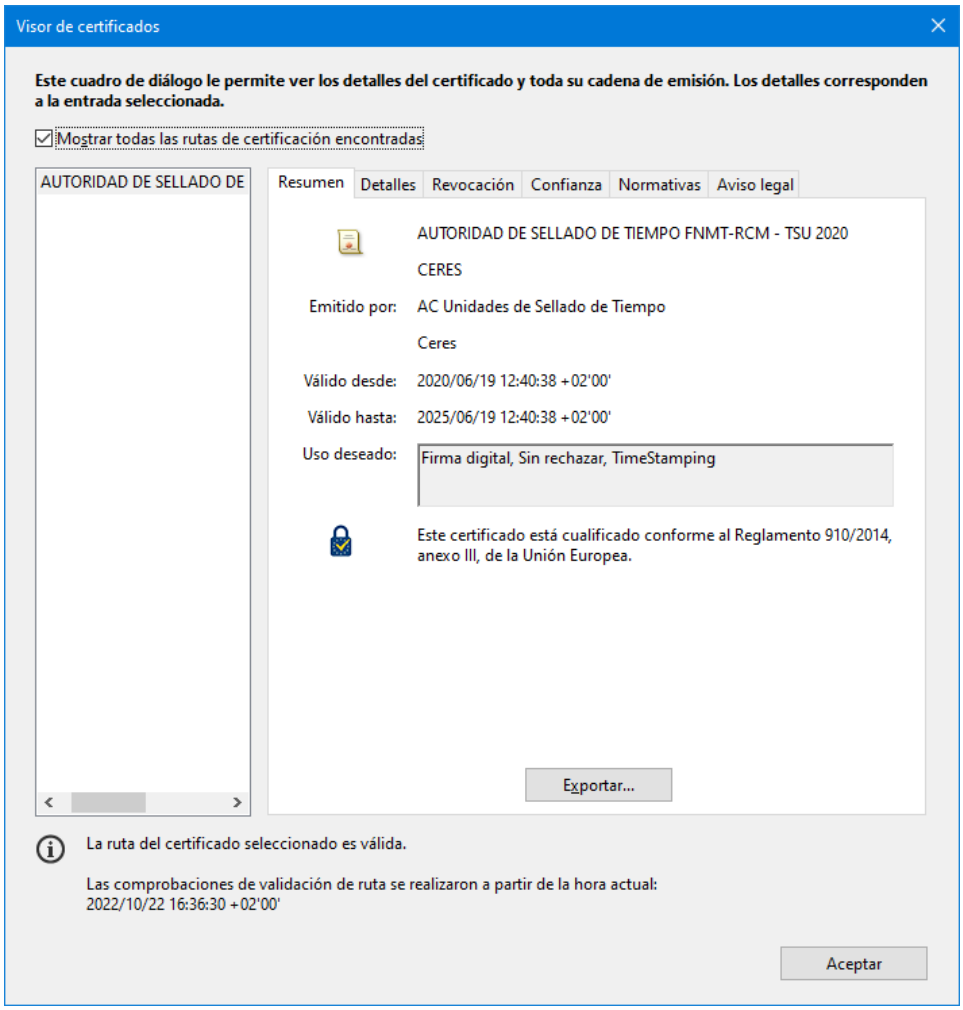
Pulsa el botón "Propiedades avanzadas..." y aparece la ventana "Propiedades de firma avanzadas".



En el cuadro “Detalles de la firma” se pueden comprobar detalles de la generación. El resumen se hace con SHA1 (no muy moderno, pues sería mejor SHA256 o SHA512) y el algoritmo de firma es RSA con relleno determinista PKCS#1 v1.5 (no muy moderno, pues sería mejor usar OAEP).

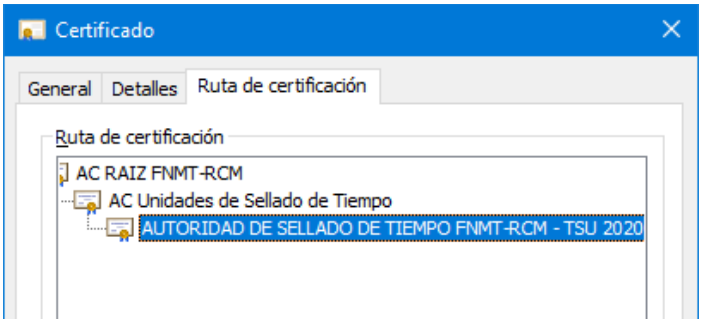
En el cuadro “Detalles de marca de hora” observar la autoridad de sellado de tiempos: AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM - TSU 2020. Para ver todo este nombre hay que desplazarse en el cuadro de diálogo seleccionado que contiene solo el final del nombre, esto es, 2020.

Pulsa el botón "Mostrar certificado..." para ver el certificado de la autoridad de sellado de tiempos.



La “AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM – TSU 2020” opera como un anclaje de confianza en Adobe, pero realmente es una autoridad subordinada de otras dos autoridades.

Busca la huella o compendio SHA1 del certificado en la pestaña “Detalles”. Luego descarga el certificado de la web de la FNMT y ábrelo. Observa la cadena:



4. Revisión de los certificados de confianza de Adobe

Antes de comprobar la firma del PDF del BOE solo había 2 certificados raíz de Adobe en el almacén de certificados de confianza.

PERO… se ha comprobado que Reader confía en:

- El certificado del firmante porque ha sido emitido por una autoridad certificadora, cuyo certificado Adobe considera de confianza.
- El certificado de la autoridad de sellado de tiempos, cuyo certificado Adobe considera directamente de confianza.

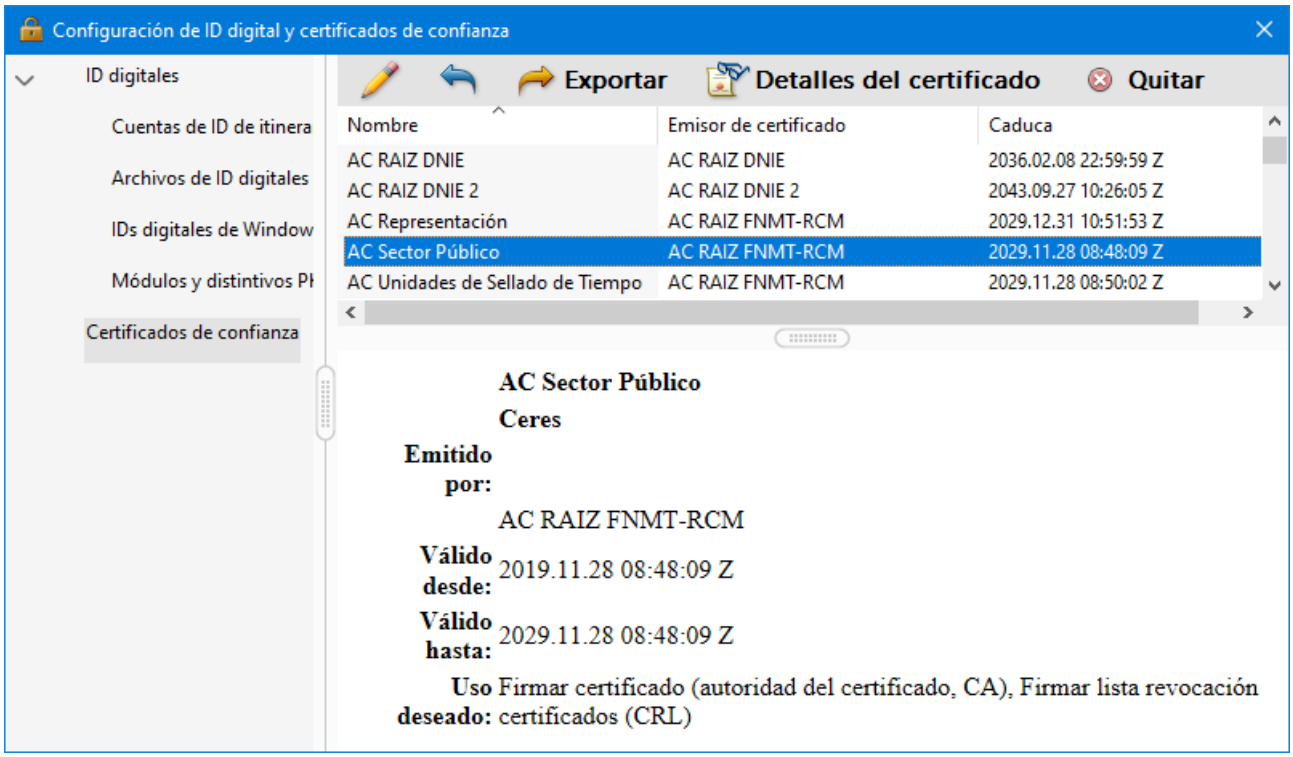
Estos dos certificados tienen que estar integrados en el almacén de certificados de confianza de Adobe. ¡COMPRUÉBALO!

Para comprobarlo, abre nuevamente el almacén de certificados de Adobe. Aparece esta ventana:

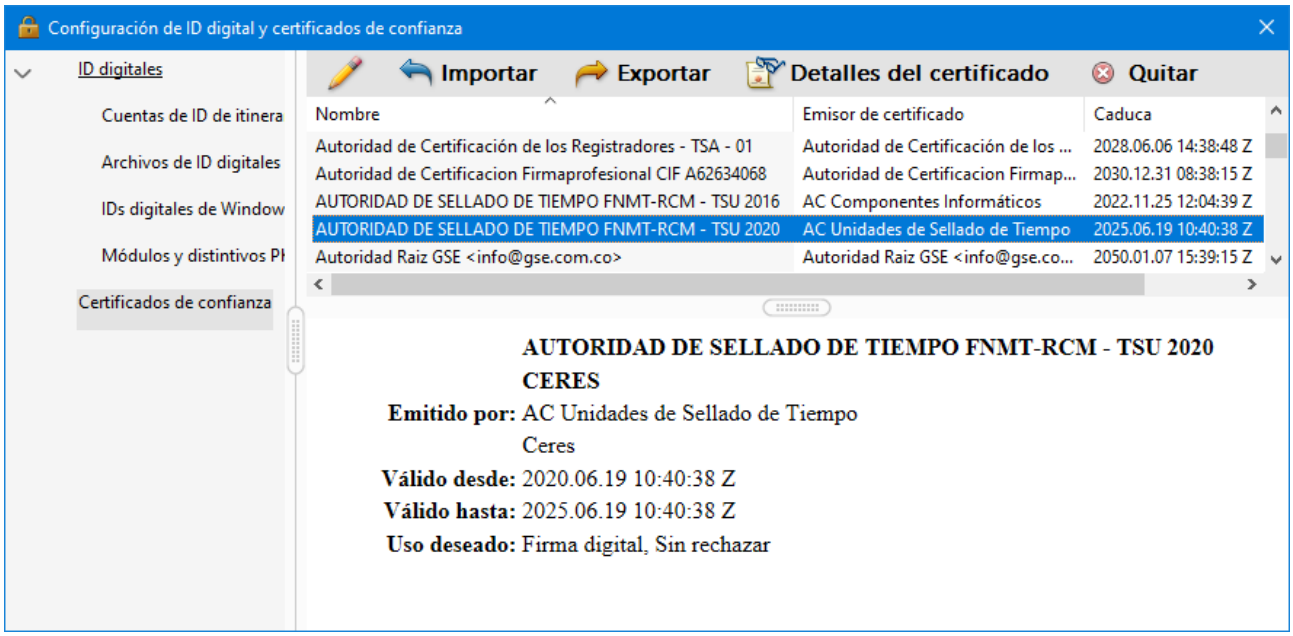
Desplaza el cursor en el panel derecho observando los certificados: HAY MUCHOS.

Reader, para verificar el PDF del BOE, ha cargado los certificados de las listas AATL y EUTL.

En la ventana siguiente se muestra el certificado de "AC Sector Púbico", pero también se pueden ver los certificados raíz del DNIE y certificados de autoridades subordinadas de la FNMT.



Continuando la visualización se llega al certificado de la autoridad de sellado de tiempos.



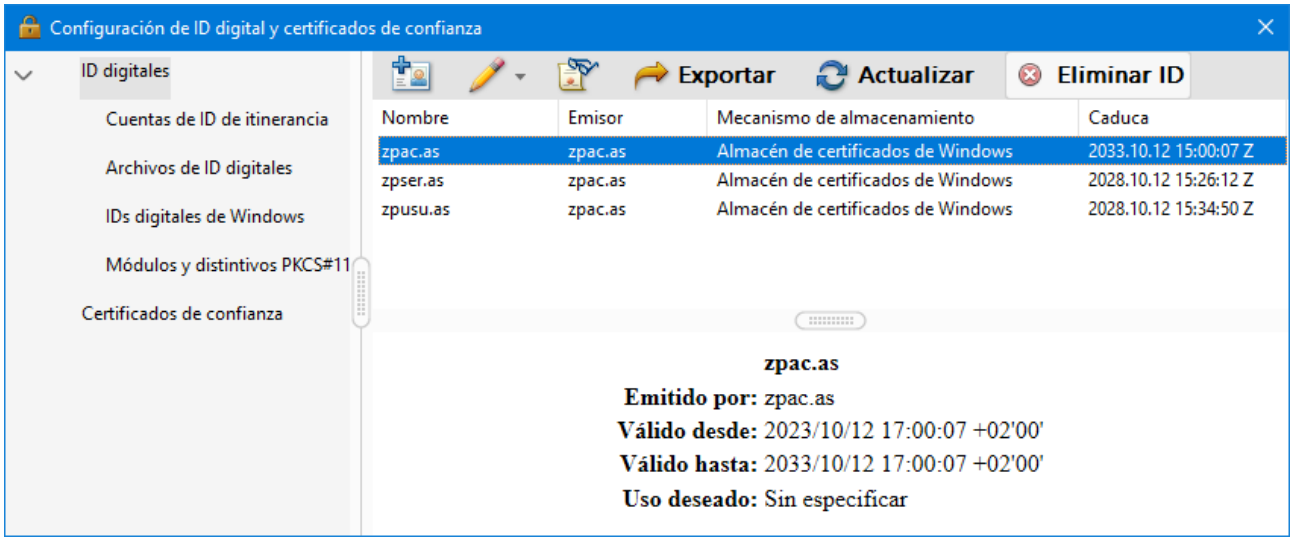
5. Firmar y verificar firmas con Reader (Usando el almacén de certificados de Adobe)

En esta sección se estudia como firmar y verificar firmas con Reader, pero antes hay que cargar el certificado del usuario y su certificado raíz correspondiente en el almacén de Adobe.

PROBLEMA:

Si estas realizando esta práctica en la misma MV que has usado para generar los certificados de zpac.as, zpser.as y zpusu.as, al abrir la ventana "Configuración de ID digital y certificados de confianza" ya aparecen estos ID digitales como disponibles en Adobe.

En Reader: Edición > Preferencias > Firmas > Identidades y certificados de confianza > Más…

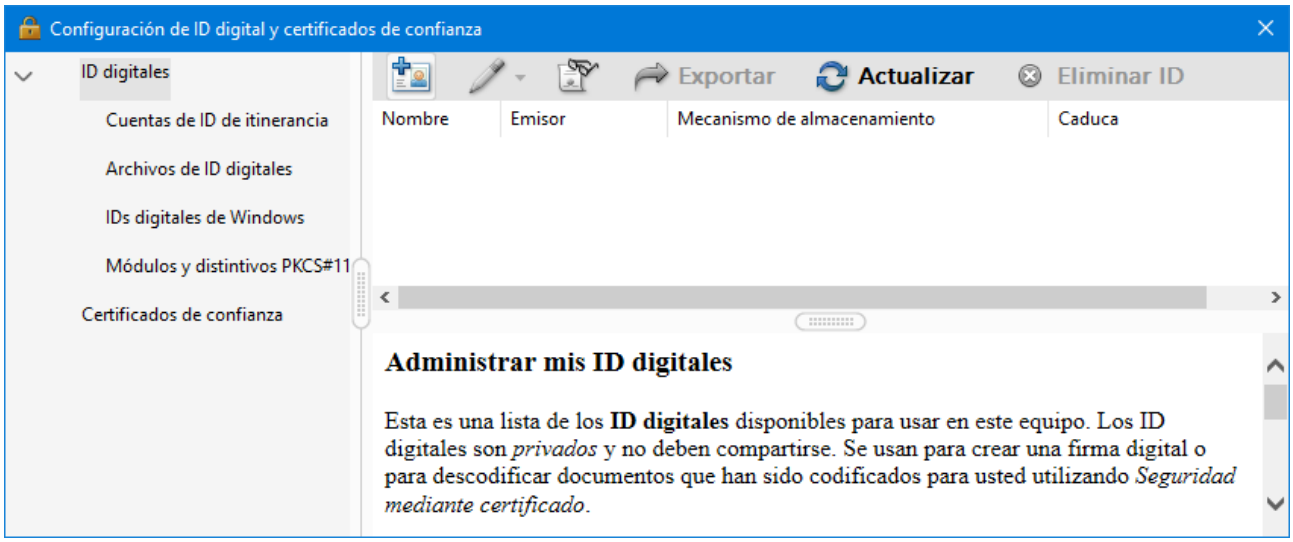


Al pulsar el botón "Eliminar ID" (esquina superior-derecha) Adobe indica que la eliminación de esta ID se debe hacer en el sistema operativo Windows.

SOLUCIÓN:

Para continuar el desarrollo de la práctica es necesario eliminar estos certificados. Pero antes de eliminarlos es necesario tener disponibles los ficheros en los que están almacenados, esto es zpACas.cer, zpACas.pfx, zpSERas.pfx, zpUSUas.pfx.

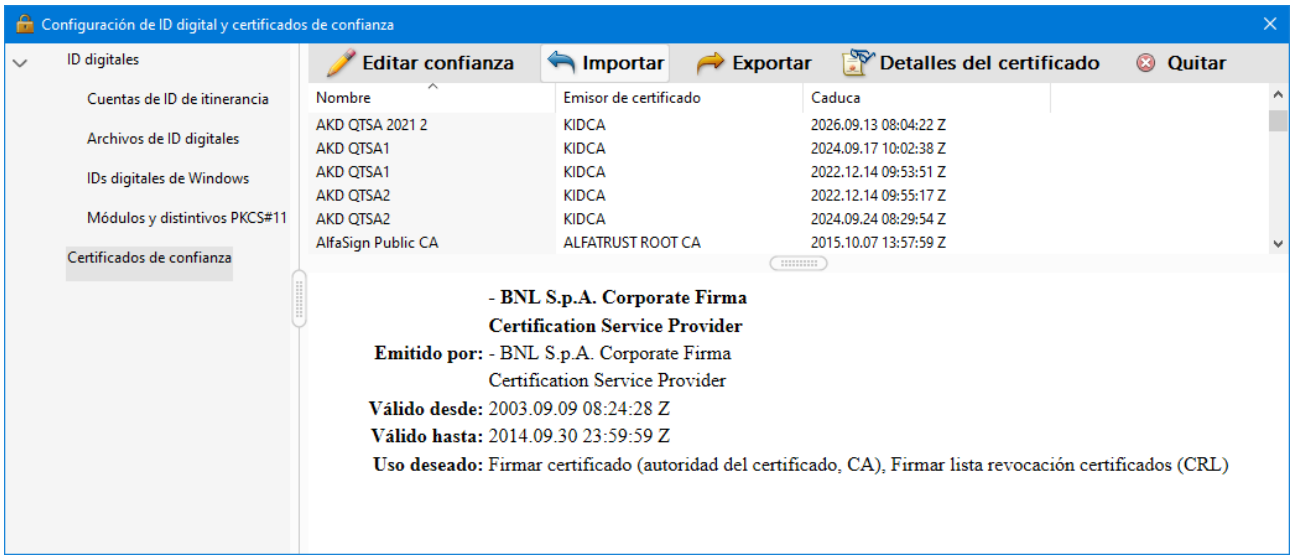
Una vez borrados, se continua la realización de la práctica sin ID digitales disponibles.



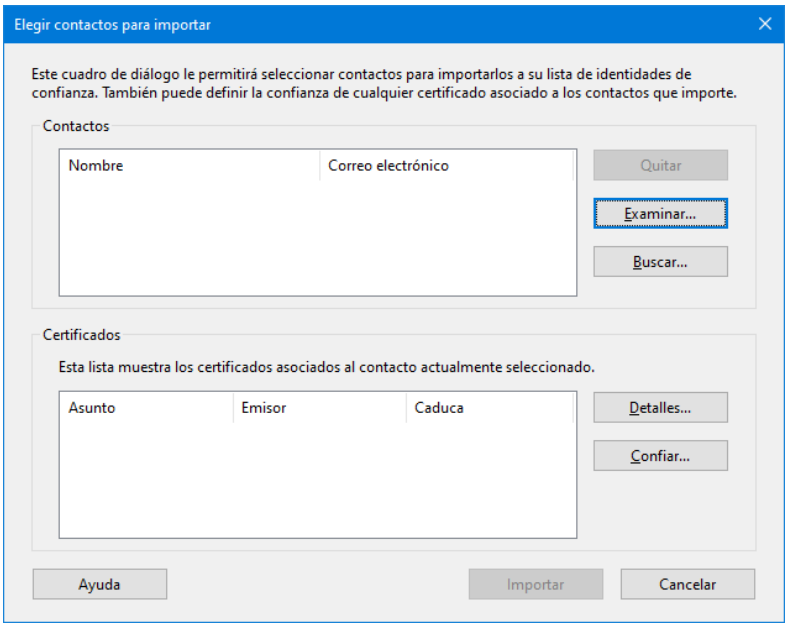
Cargar el certificado de una autoridad certificadora en el almacén de Adobe

Abre la ventana “Configuración de ID digital y certificados de confianza”:

En Reader: Edición > Preferencias > Firmas > Identidades y certificados de confianza > Más…

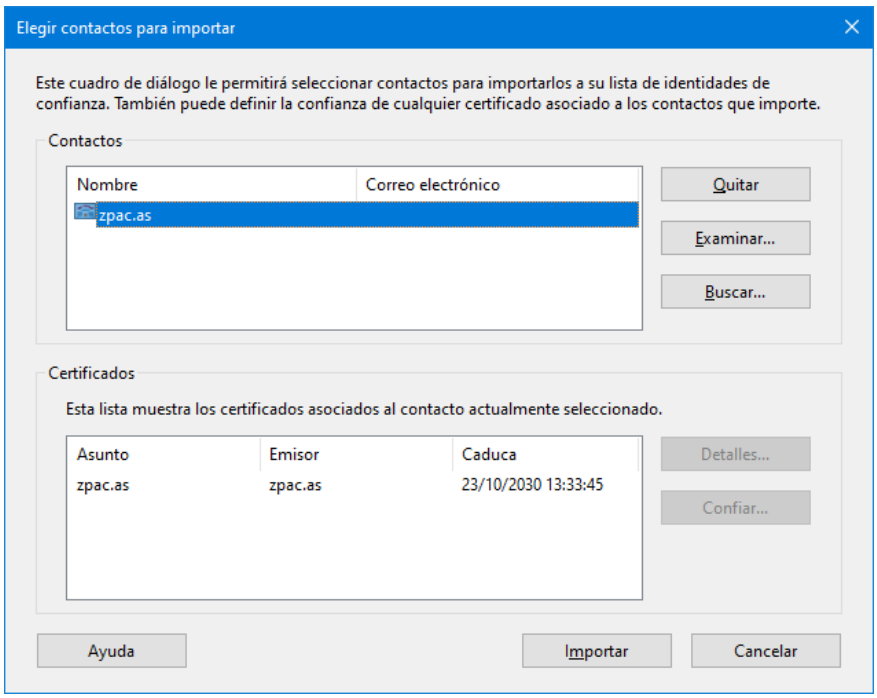


AL pulsar el botón “Importar” aparece la ventana “Elegir contactos para importar”:

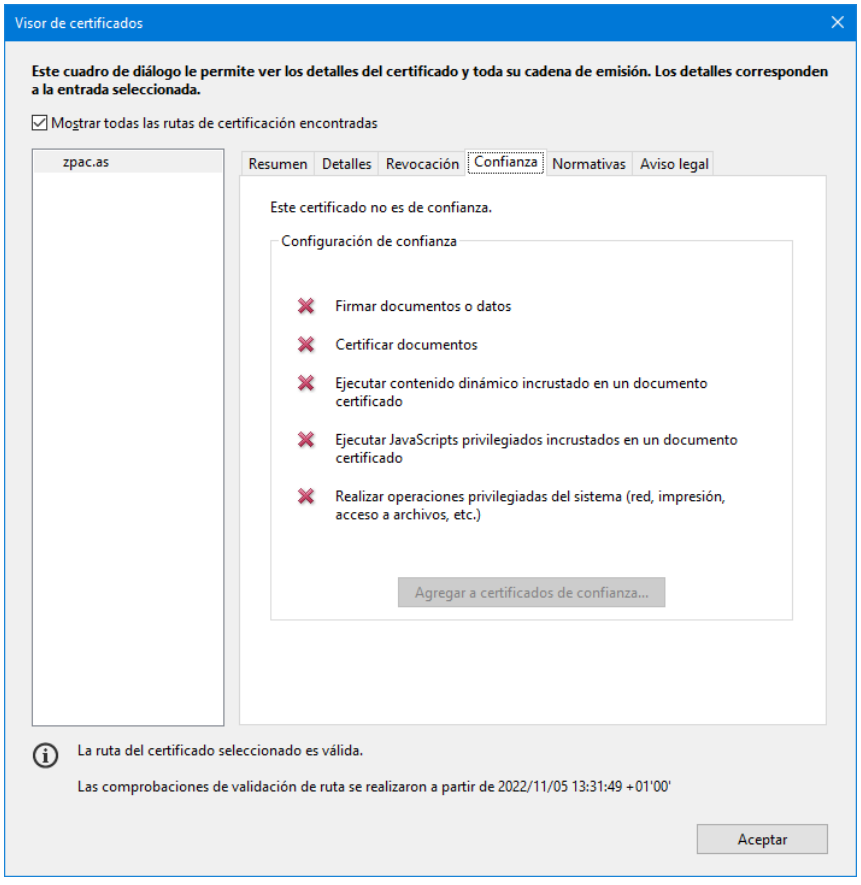


Pulsa el botón examinar y en la ventana “Buscar archivos de certificados” selecciona el fichero de la autoridad certificadora zpACas.cer.

Tras la carga, se puede observar el nombre de autoridad certificadora en el cuadro “Contactos”. Al seleccionar un contacto, en el cuadro “Certificados” aparecen los certificados asociados al contacto.

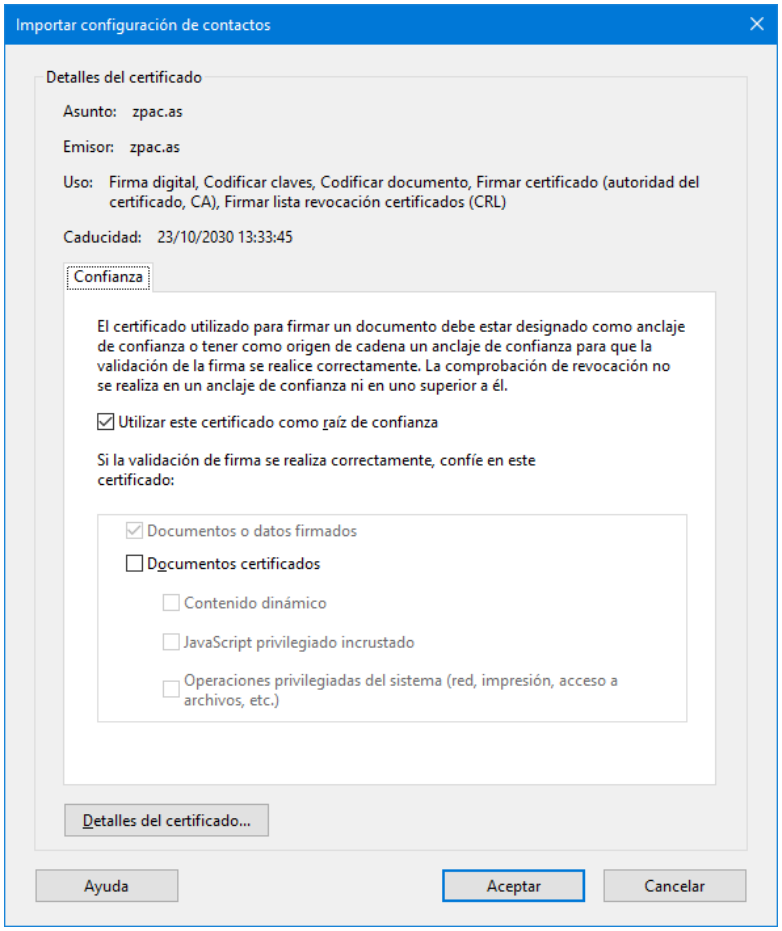


Selecciona el certificado disponible. Los botones "Detalles…" y "Confiar…" se activan. Pulsa el botón "Detalles…" y en la ventana que aparece selecciona la pestaña "Confianza".

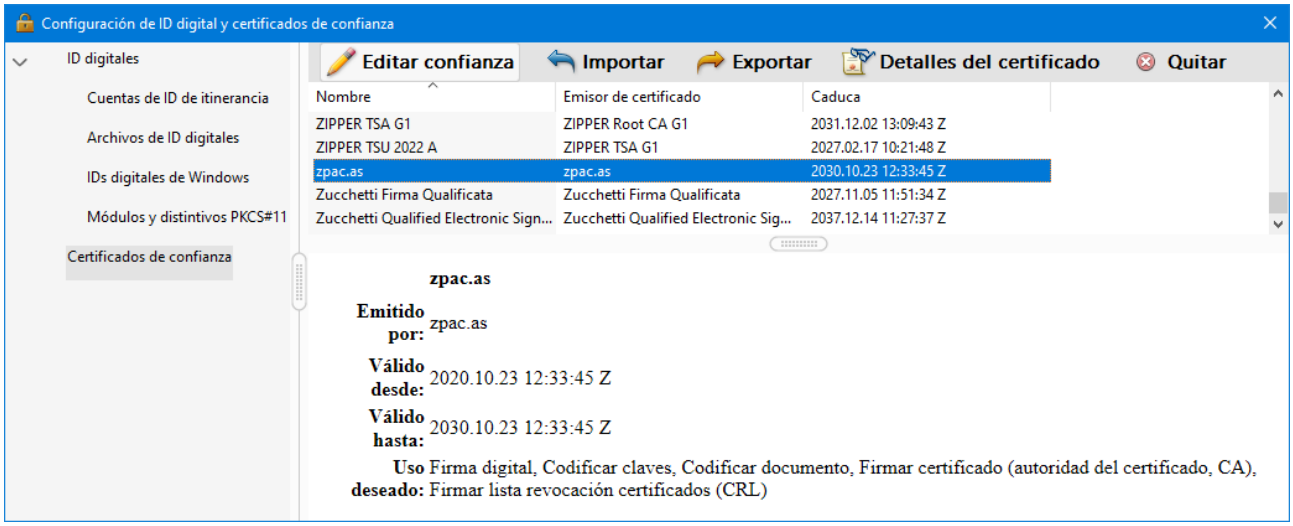


Tal y como está el certificado no proporciona confianza para ningún tipo de operación. Pulsa el botón "Aceptar" para salir de esta ventana, y volver a la ventana "Elegir contactos para importar".

En la ventana “Elegir contactos para importar”, con el certificado de zpac.as seleccionado, pulsa el botón “Confiar…”. En la ventana que aparece “Importar configuración de contactos” marca la casilla “Utilizar este certificado como raíz de confianza”, tal como se muestra en la figura siguiente:



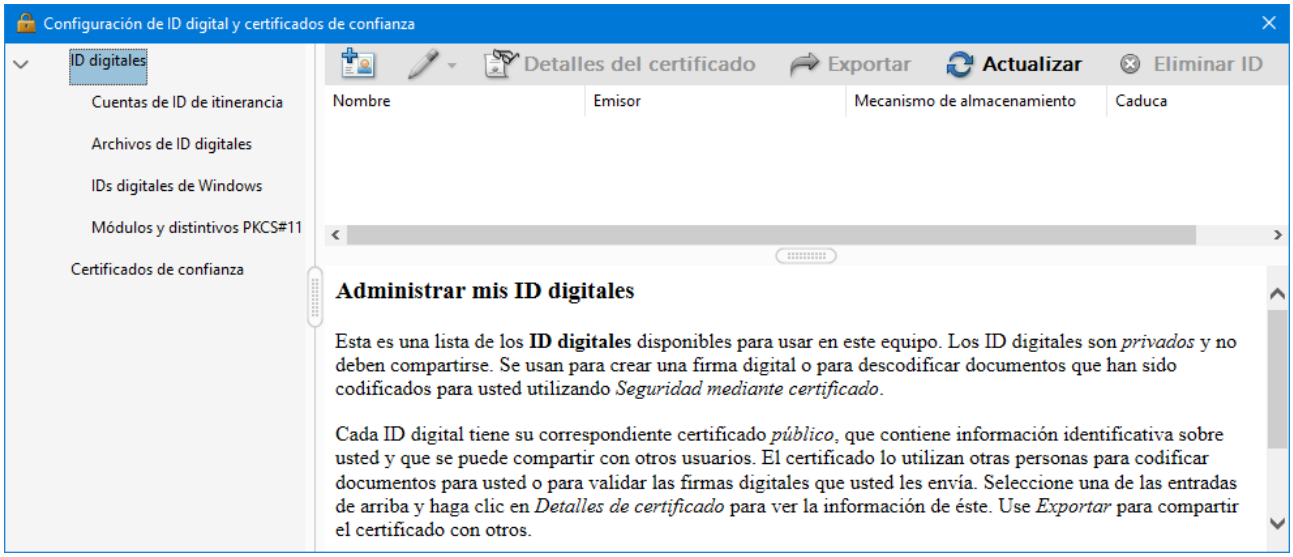
Ahora, en la ventana “Elegir contactos para importar”, pulsa el botón “Importar”. Comprueba que el certificado aparece en la lista de certificados de confianza.



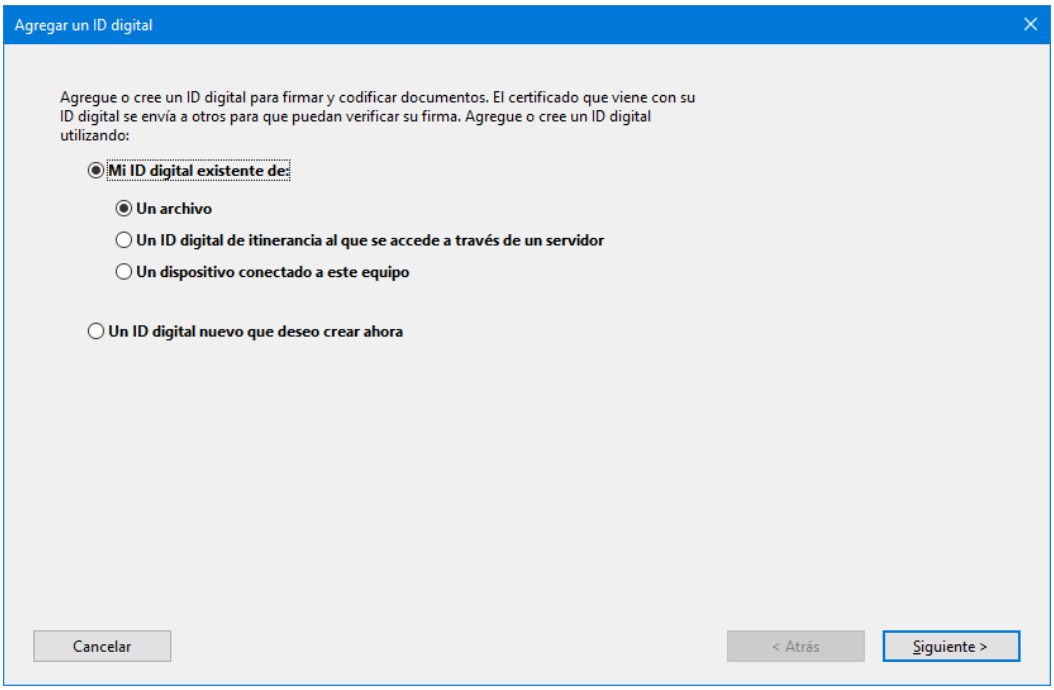
Haz doble clic sobre el certificado seleccionado para que se habrá el “Visor de certificados”. En la pestaña “Confianza” comprueba que el certificado es ahora un anclaje de confianza para la firma de documentos o datos.

Cargar el certificado y la clave privada de un usuario en el almacén de Adobe

Abre la ventana “Configuración de ID digital y certificados de confianza”:

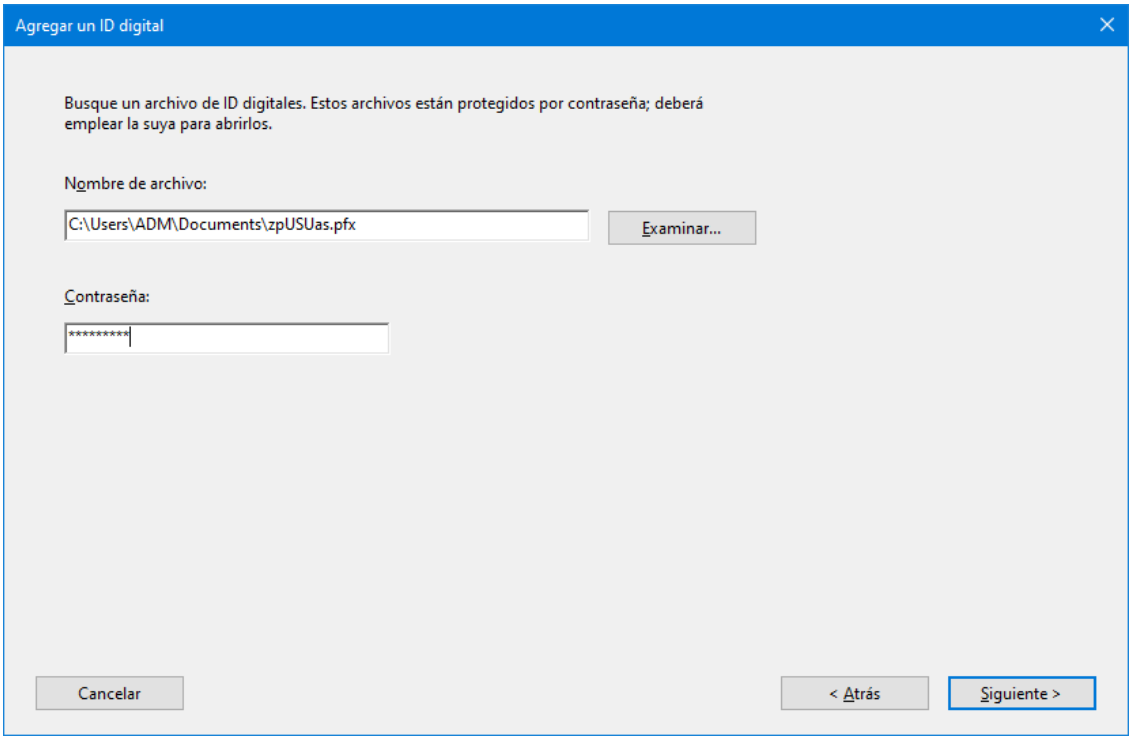


Pulsa el botón Nombre y aparece la ventana “Agregar un ID digital”:

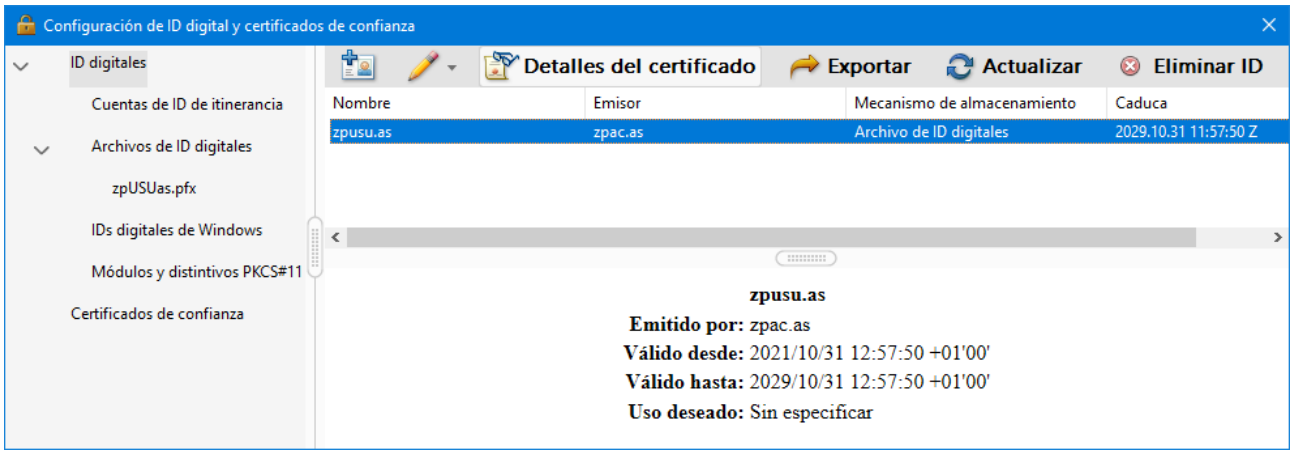


Usa la selección indicada de crear la ID desde un archivo. Seleccionar el archivo y proporciona la contraseña: **conusupfx**.

En la nueva ventana, usa el botón “Examinar…” para busca el fichero .pfx del usuario.



Al finalizar, en la ventana “Configuración de ID digital y certificados de confianza” se puede observar la nueva ID digital añadida:



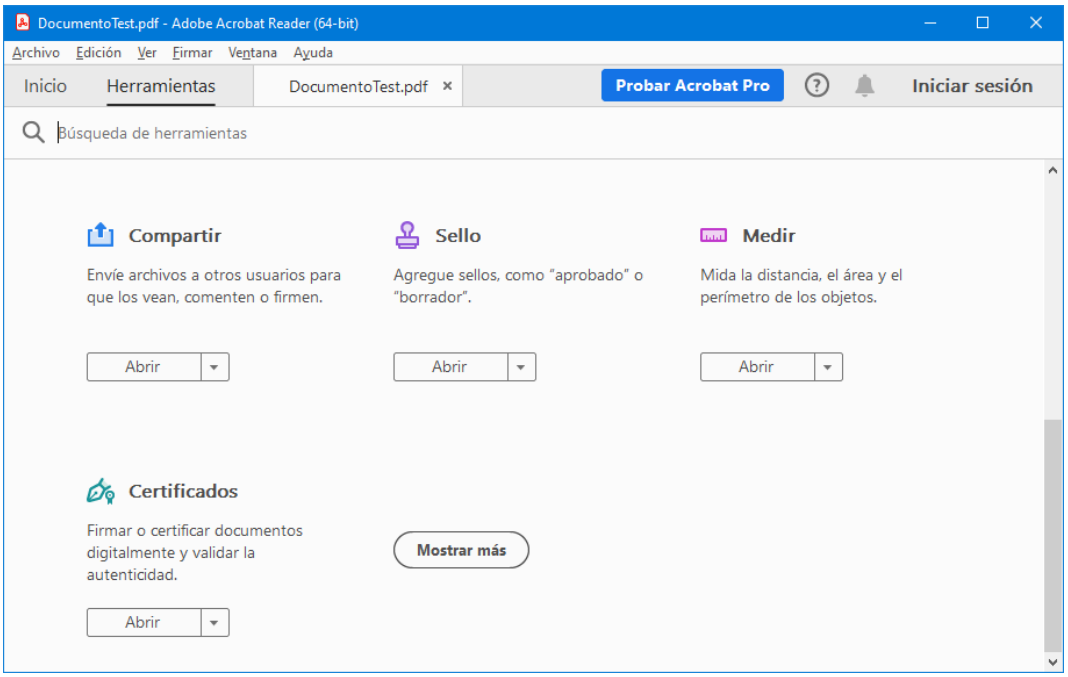
Pulsa el botón “Detalles del certificado” (o haz doble clic sobre el certificado) y revisa la información que se muestra en la pestaña “Resumen” (cadena de certificación), en la pestaña “Confianza” (confianza para firmar) y en la pestaña “Revocación” (no se puede determinar).

COMPRUEBA que el certificado de la autoridad certificadora zpac.as y el certificado del usuario zpusu.as NO aparecen el almacén de certificados de Windows. Se han cargado en el almacén de certificados de Adobe, que es independiente del almacén de certificados se Windows.

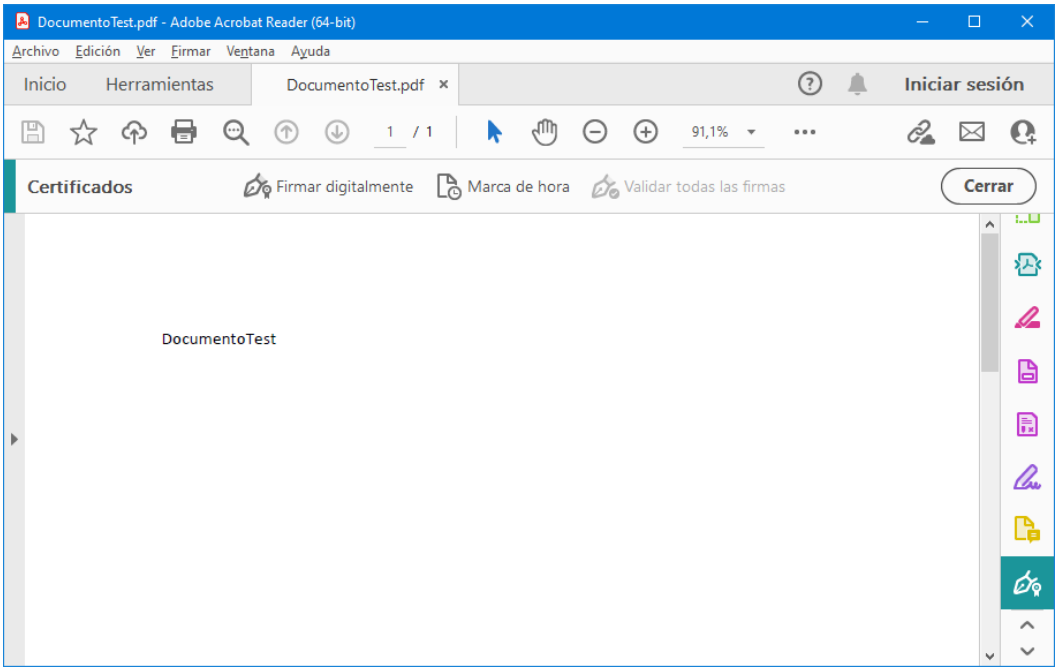
Firmar y verificar la firma de un fichero PDF con Reader

Crea el fichero DocumentoTest.pdf a partir de un documento Word. El documento contiene solo una línea con el nombre: DocumentoTest.

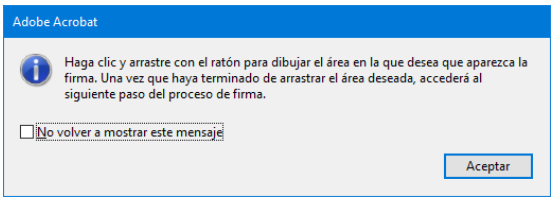
Abre el documento y selecciona la pestaña "Herramientas" como se muestra en la figura:



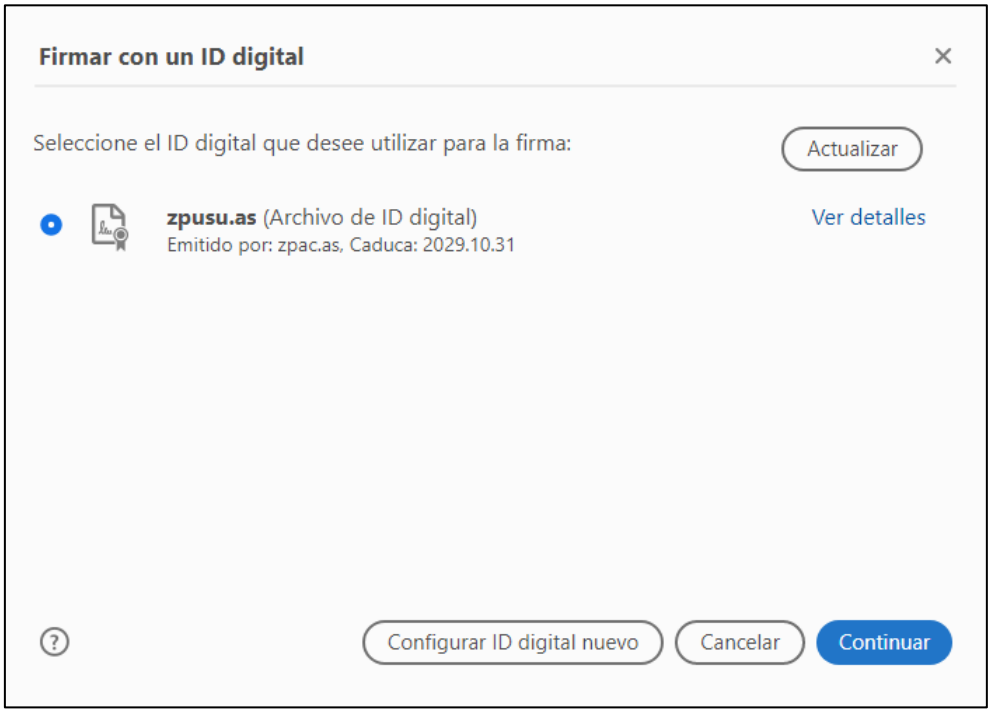
La última de las herramientas mostradas es "Certificados". Haz clic sobre ella.



Aparece la barra de herramientas "Certificados" con tres opciones. Pulsa la primera opción "Firmar digitalmente". Aparece una ventana que indica que se seleccione el área de firma:

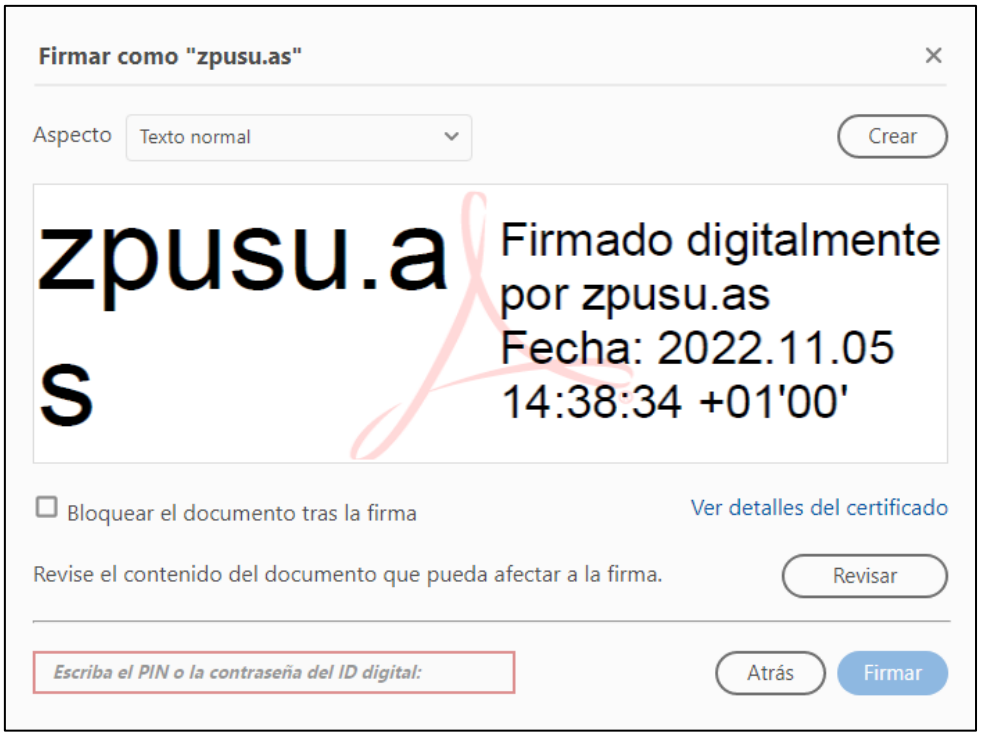


Se abre una ventana para seleccionar el certificado con el que se desea firmar el PDF:



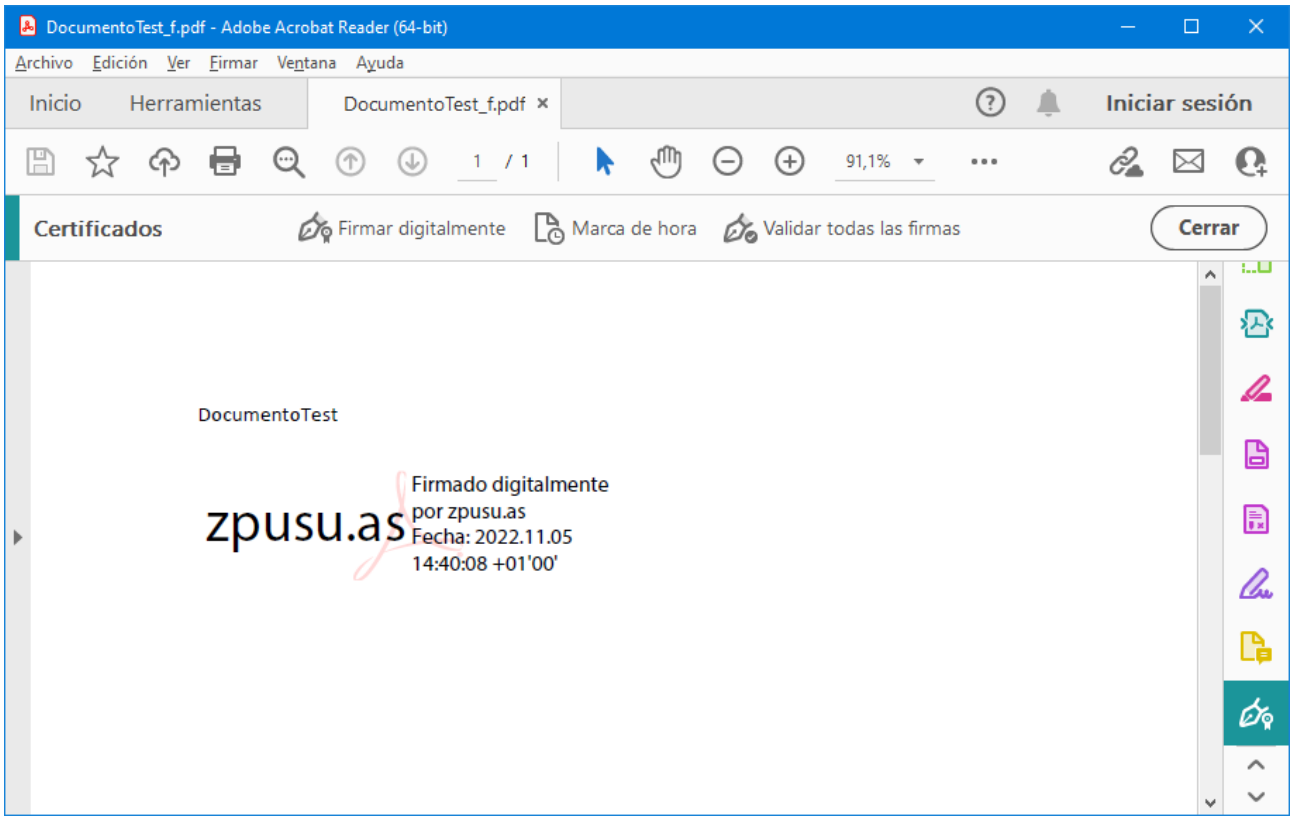
Seleccionar el certificado de zpusu.as y pulsa el botón continuar.

Ahora hay que proporcionar la contraseña: conusupfx.

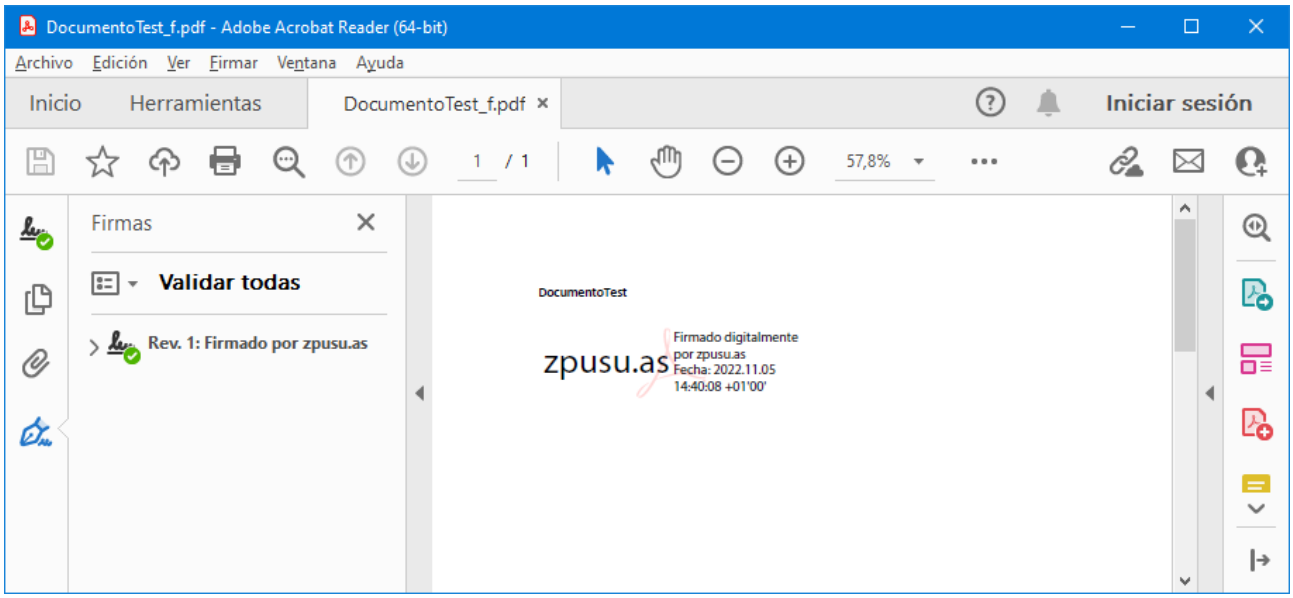


Una vez proporcionada, pulsa el botón Firmar.

Finalmente se obtiene un nuevo fichero PDF firmado. Lo denominamos igual que el original pero con el sufijo _f.

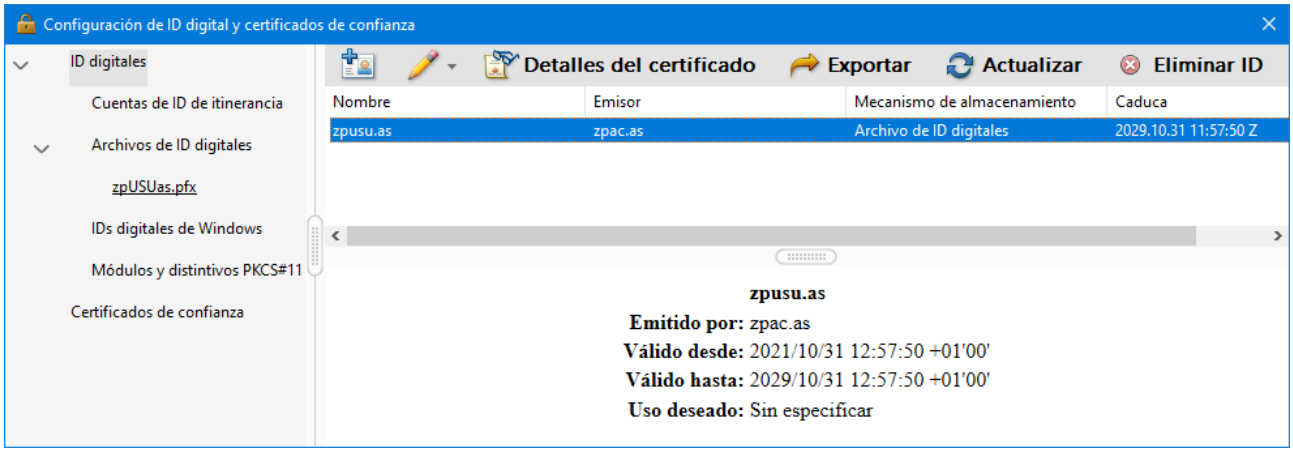


Cierra el documento y vuelve a abrirlo. Justo al abrirlo, Reader valida las firmas:

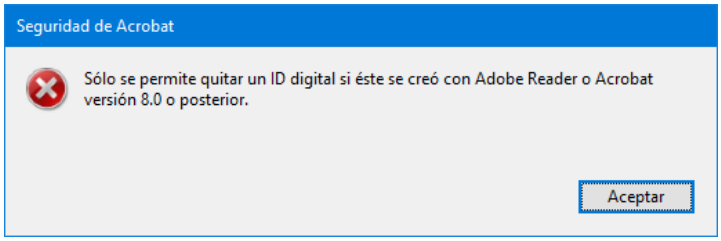


Elimina el certificado de la autoridad certificadora zpac.as y verifica la firma. Comprueba que la validez de la firma es “desconocida”.

Ahora elimina el certificado del usuario zpusu.as antes de verificar nuevamente la firma. Para ello abre la ventana "Configuración de ID digital y certificados de confianza" y con el certificado de zpusu.as pulsa el botón "Eliminar ID".

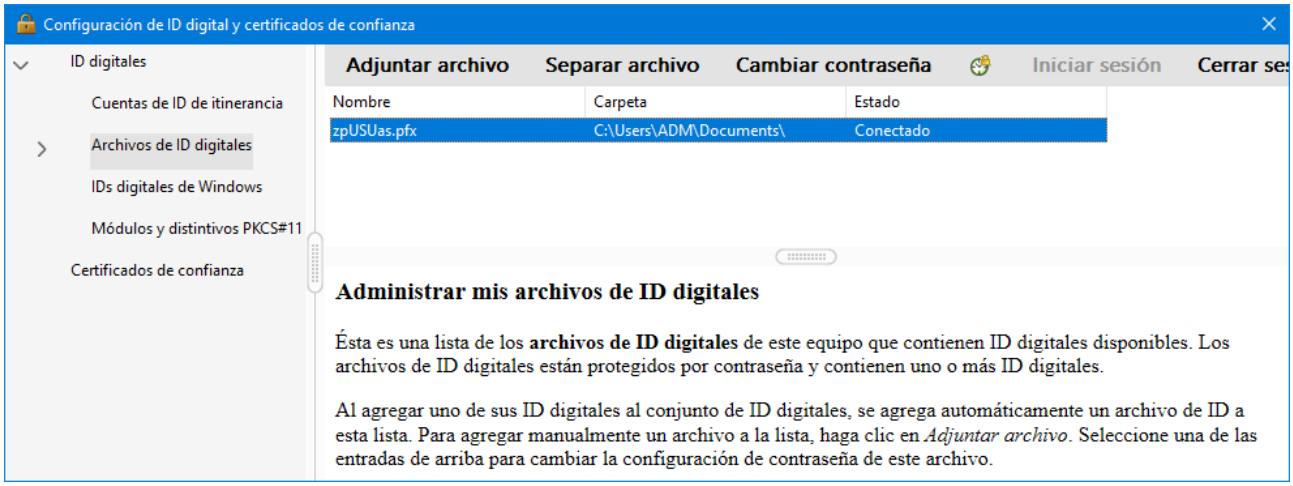


Se abre una ventana indicando un error:



Se puede usar un método alternativo para eliminar el certificado del usuario.

En la ventana "Configuración de ID digital y certificados de confianza" selecciona en el panel izquierdo "Archivos de ID digitales" y en el derecho el archivo de nombre zpUSUas.pfx:



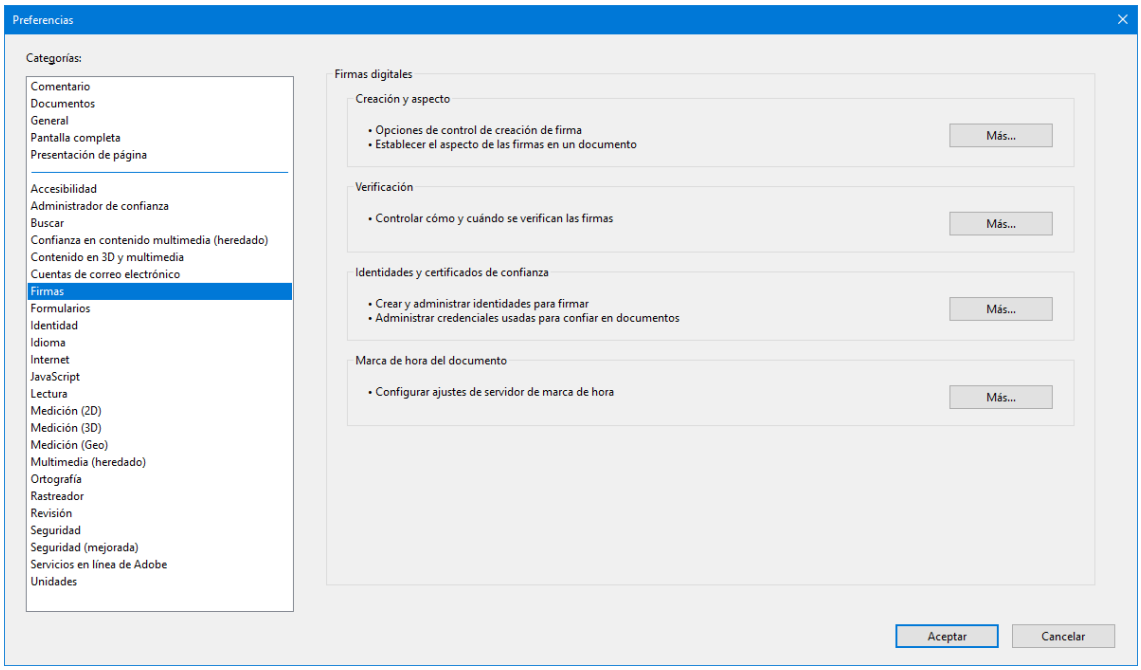
Pulsa el botón "Separar archivo" y la ID digital desaparece. Comprueba también que el archivo no ha sido borrado del directorio del sistema operativo.

Abre nuevamente el documento PDF y comprueba que la firma es "desconocida".

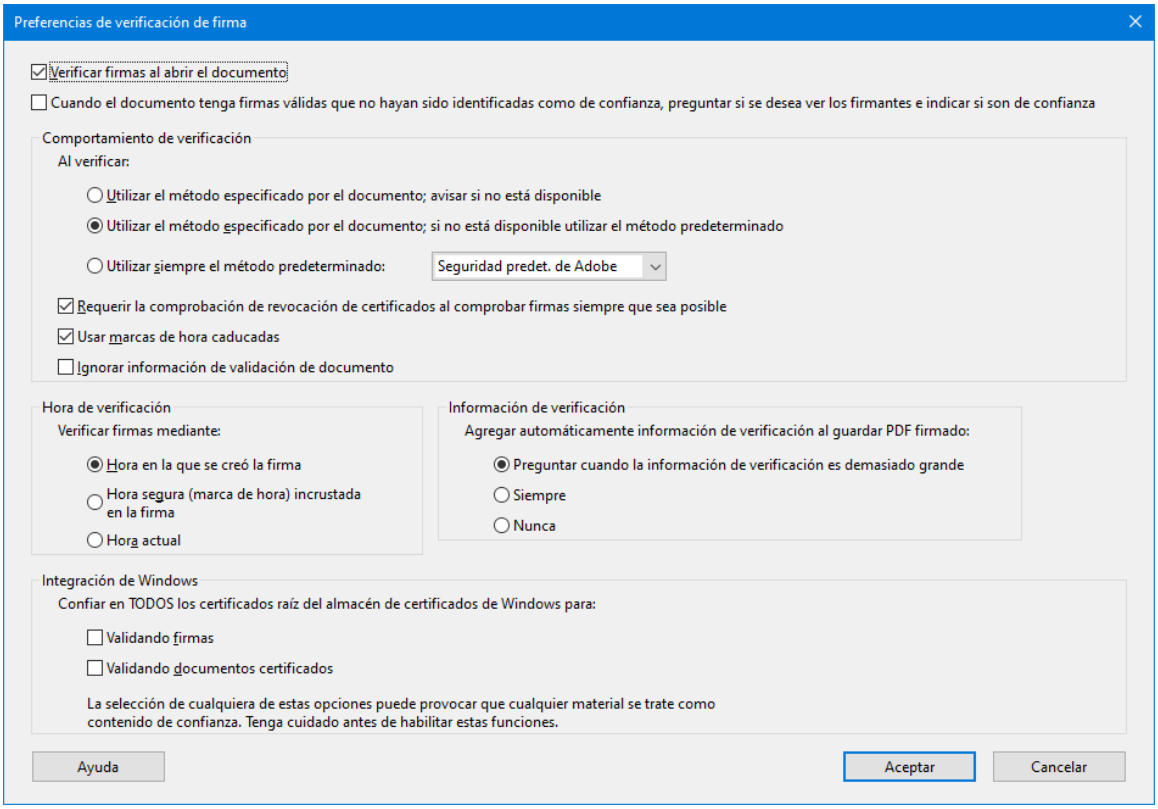
IMPORTANTE: La eliminación del certificado de zpusu.as del almacén de Adobe no afecta a la verificación de la firma. Comprueba que si ahora se carga nuevamente el certificado de zpac.as en el almacén de Adobe, Reader verifica la firma como válida. Elimina el certificado de zpac.as del almacén de certificados de confianza de Adobe, antes de seguir con la práctica.

6. Verificar firmas con Reader (Usando el almacén de certificados de Windows)

En esta sección se estudia como verificar firmas con Reader, pero permitiendo que Adobe confíe en todos los certificados raíz que hay en el almacén "Entidades de certificación raíz de confianza" de Windows. Abre la ventana Preferencias de Reader y selecciona Firmas en el panel izquierdo.



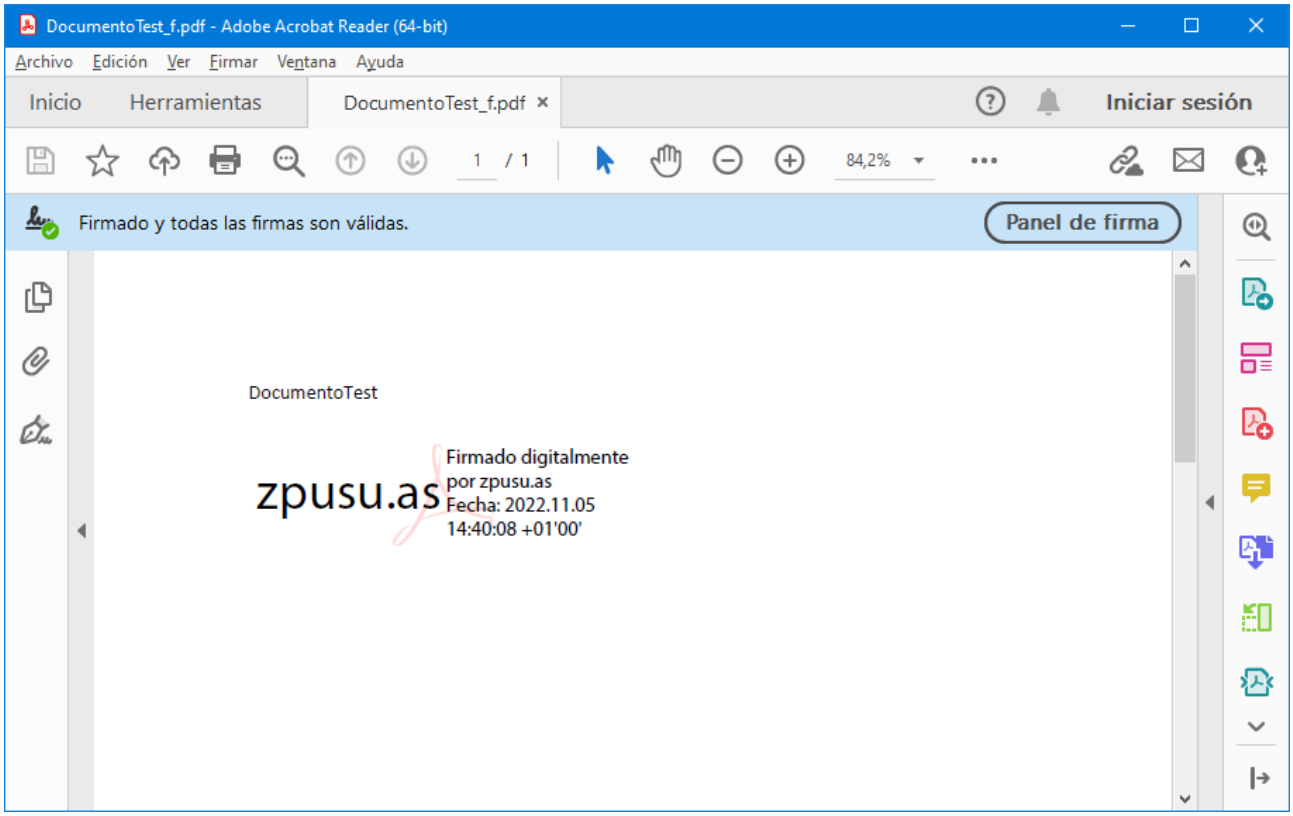
En el cuadro "Verificación - Controlar cómo y cuándo se verifican las firmas" pulsar el botón "Más...". Aparece la ventana siguiente:



Observa el cuadro inferior "Integración de Windows". Selecciona la opción "Validando firmas" para indicarle a Adobe que también utilice los certificados raíz de confianza de Windows.

Ahora hay que cargar el certificado raíz zpac.as en el almacén "Entidades de certificación raíz de confianza" de Windows.

Abre el nuevamente el documento PDF firmado con Reader. Se obtiene el resultado esperado:



Reflexiona: El certificado de zpusu.as NI está cargado en el almacén de certificados de Adobe, NI en el almacén de certificados de Windows.

Para verificar la firma realizada con zpusu.as (con su clave privada asociada) solo ha sido necesario el certificado raíz de zpusu.as que es el origen de confianza de ese certificado.

El certificado y su clave privada asociada son necesarios para firmar, pero no para verificar.