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

1. Objetivo

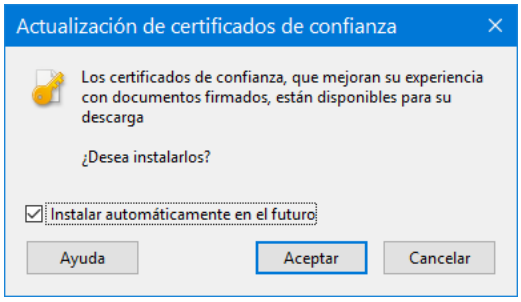
En esta práctica el alumno debe utilizar certificados para verificar firmas digitales de documentos en formato PDF. Además debe gestionar el almacén de certificados de Adobe. Para ello, descargar e instalar Adobe Reader DC en la Máquina Virtual de prácticas.

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

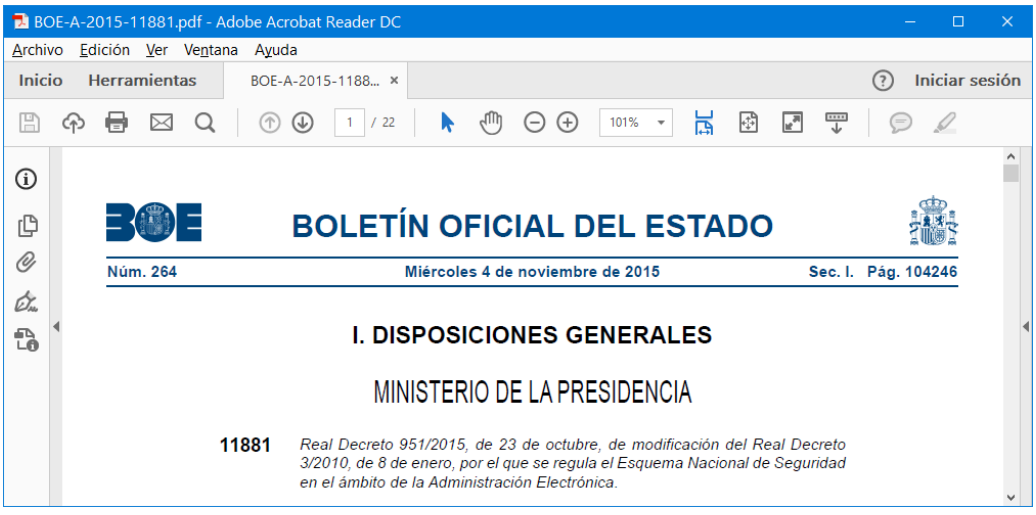
El objetivo es aprender a verificar la firma digital de un documento (fichero) con formato PDF. Para ello se utilizará el fichero de un BOE (Boletín Oficial del Estado) que está en formato PDF y ha sido firmado digitalmente. Accede a la web del BOE y descarga un boletín (PDF) de hoy.

FASE.-1 Confiar en el certificado raíz del certificado usado para firmar el boletín

Abre un boletín. Adobe Reader DC muestra el cuadro de diálogo siguiente:

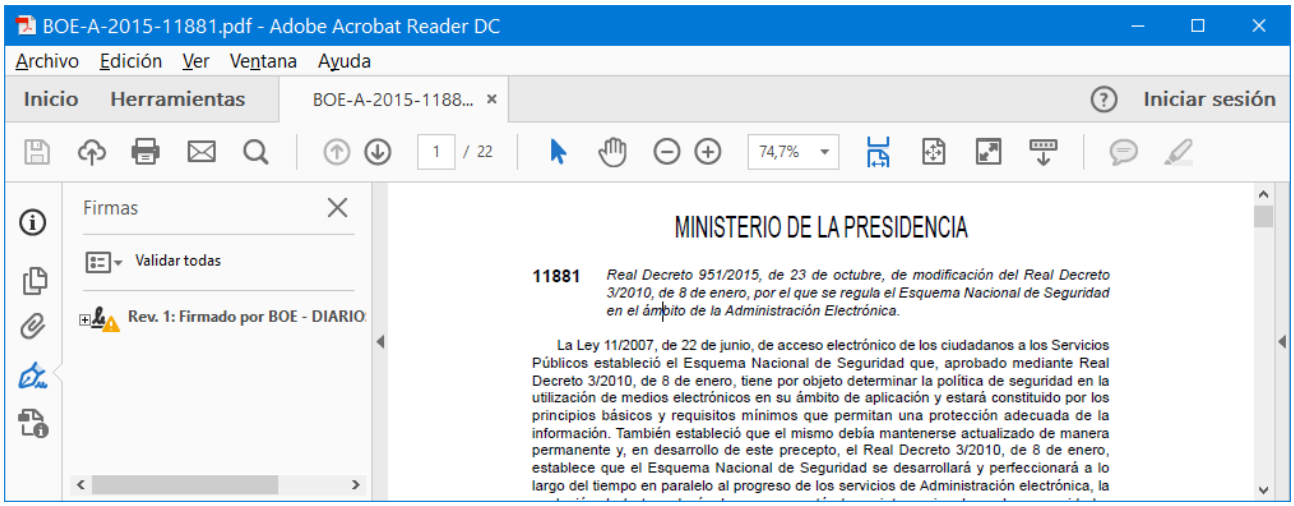


Desmarca el checkbox “Instalar automáticamente en el futuro” y pulsa el botón cancelar.

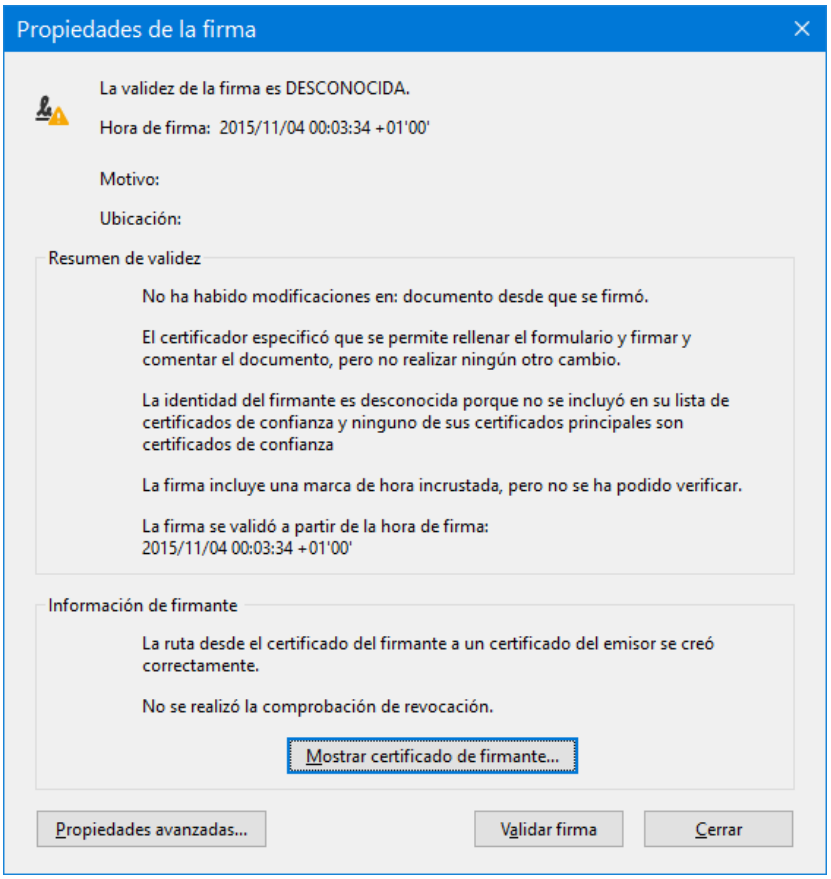


Observa que en el panel de navegación izquierdo, aparece el símbolo con una pluma (cuarto empezando por arriba) que indica que el documento tiene una firma.

Pulsa en el símbolo para que se despliegue el panel de firma. Observa que en el icono de firma aparece un triangulo amarillo, que indica que Reader desconoce la validez de la firma.

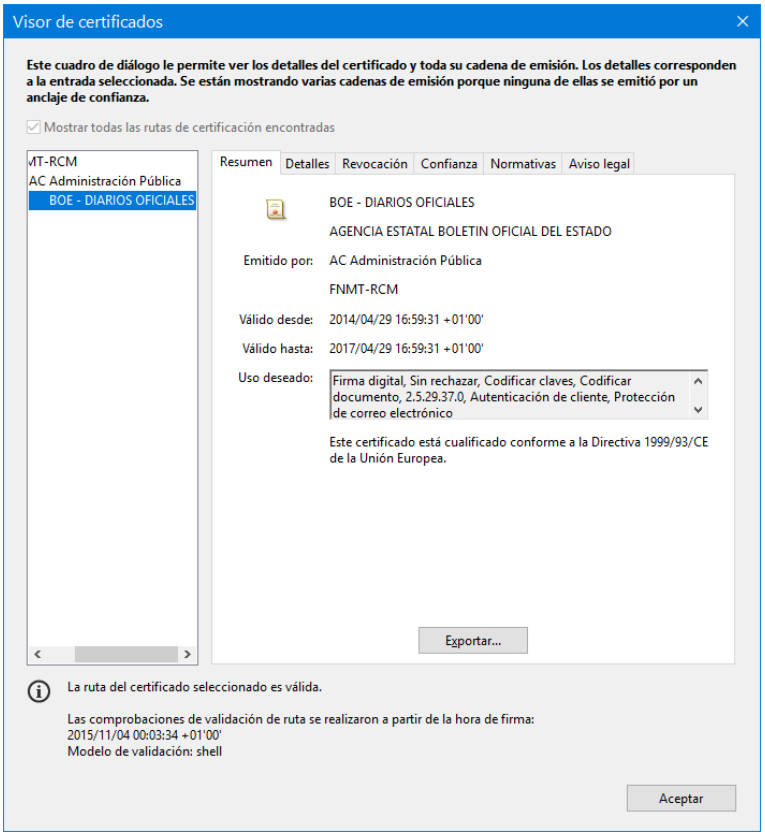


Coloca el puntero del ratón sobre la etiqueta de la firma y pulsa el botón derecho del ratón. En el menú contextual que aparece selecciona "Mostrar propiedades de firma..." y aparece la ventana informativa siguiente:



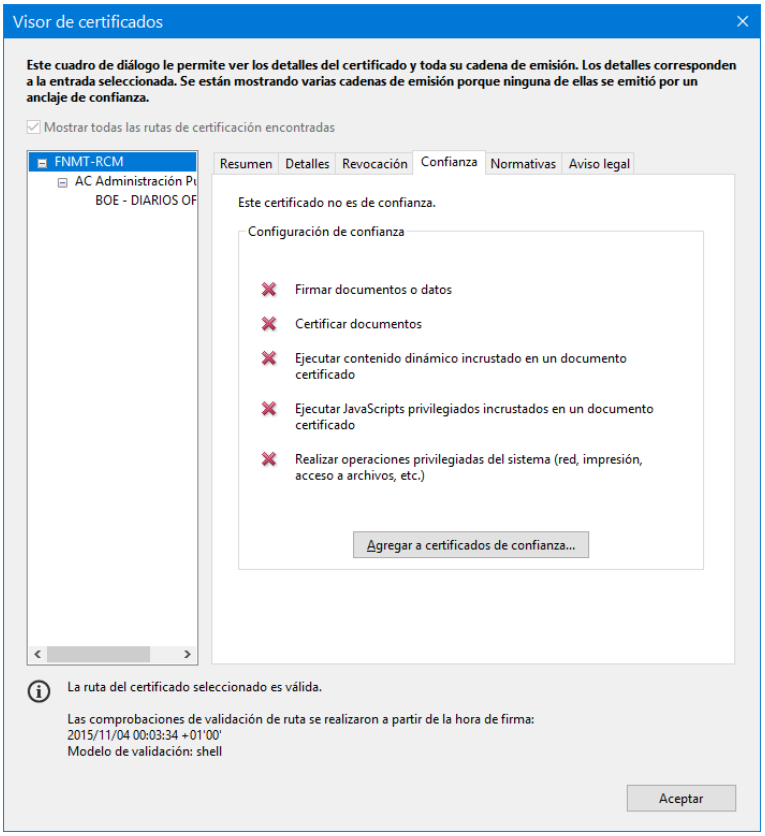
Pulsar el botón "Mostrar certificado del firmante..." y aparece la ventana "Visor de certificados".

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

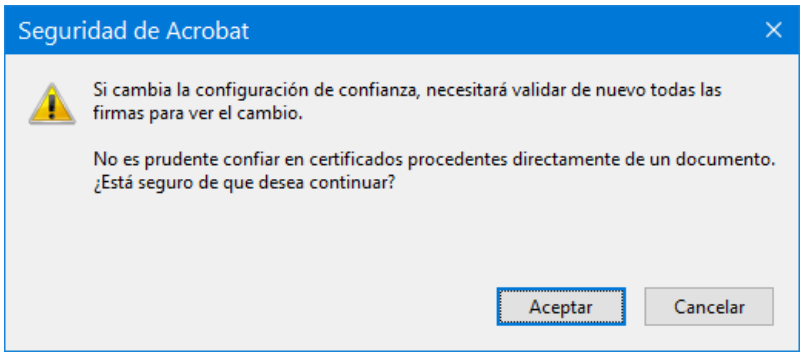


En la figura aparece la ficha "Resumen". Comprobar que al cambiar el certificado seleccionado en el panel de la izquierda, la ficha Resumen muestra los datos del certificado seleccionado. De esta forma podemos comprobar visualmente la cadena de certificados.

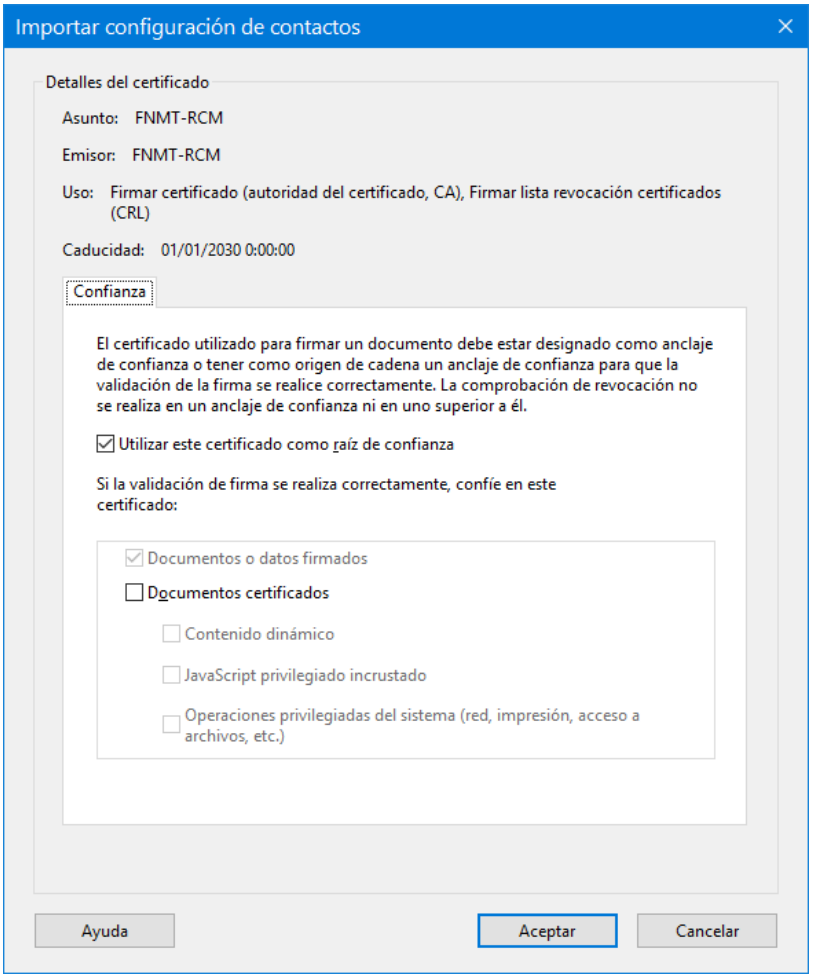
Selecciona el certificado raíz de la FNMT, que está en la parte superior y luego selecciona la pestaña "Confianza". Tenemos la ventana siguiente:



Pulsa el botón "Agregar a certificados de confianza..." y pulsa "Aceptar" en el cuadro de diálogo que muestra Adobe para advertir que es peligroso fiarse de ciertos certificados.



Se abre la ventana "Importar configuración de contactos". Comprueba que tiene seleccionada la opción "Utilizar este certificado como raíz de confianza" y pulsa el botón Aceptar.



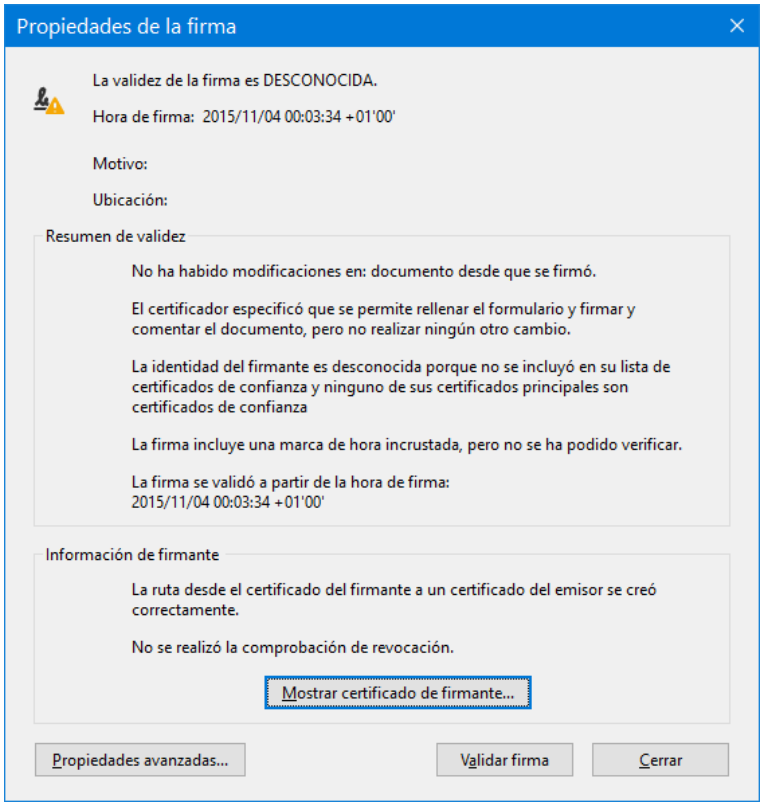
Hemos agregado el certificado al almacén de certificados de Adobe, que es un almacén independiente del almacén de certificados de Windows.

Cierra todas las ventanas abiertas hasta llegar nuevamente al boletín en PDF.

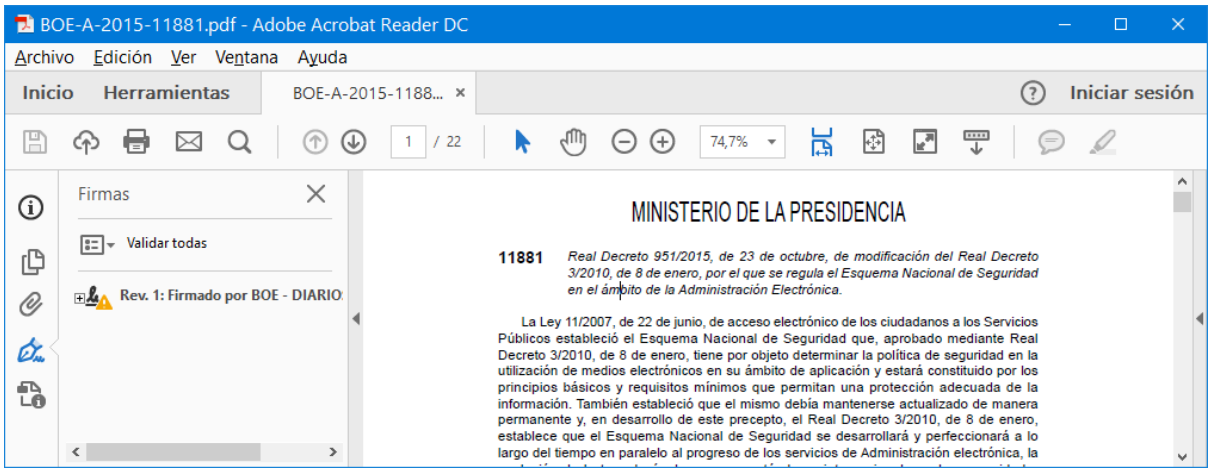
Ahora, en el panel de firmas, despliega el menú contextual y solicita validar (verificar) la firma. Se obtiene: La firma es VÁLIDA, firmada por BOE - DIARIO OFICIAL.

FASE.-2 Confiar en el certificado raíz del certificado de la autoridad de sellado de tiempos

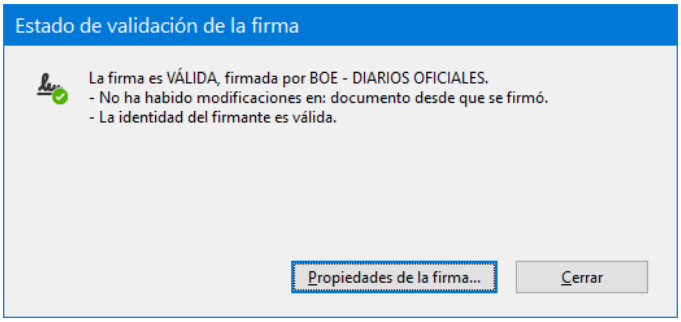
En la ventana "Propiedades de firma" se pudo comprobar anteriormente que "la firma incluye una marca de hora incrustada, pero no se ha podido verificar" tal como muestra la ventana siguiente:



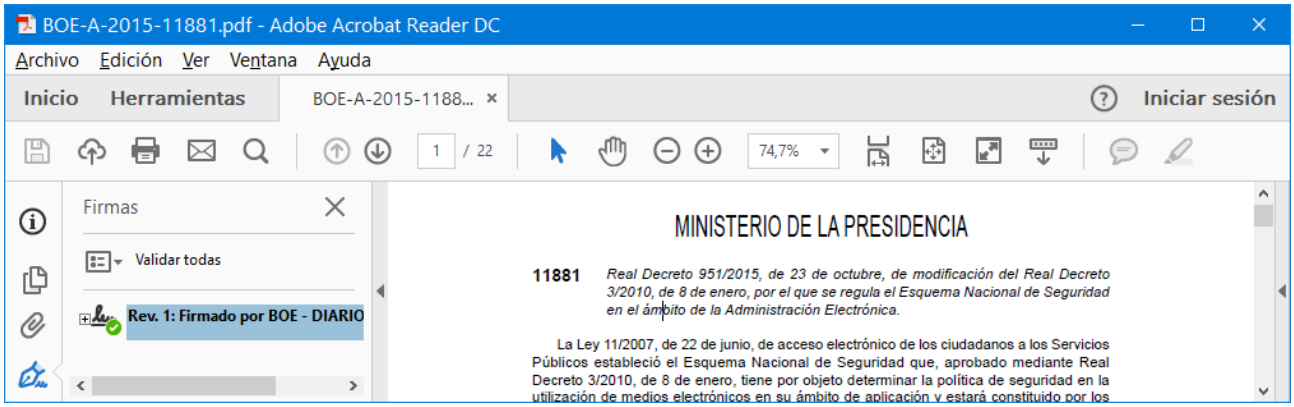
En la ventana de Adobe, mostrada debajo, coloca el puntero ratón sobre el icono de firma con el triángulo en color amarillo y pulsa el botón derecho del ratón.



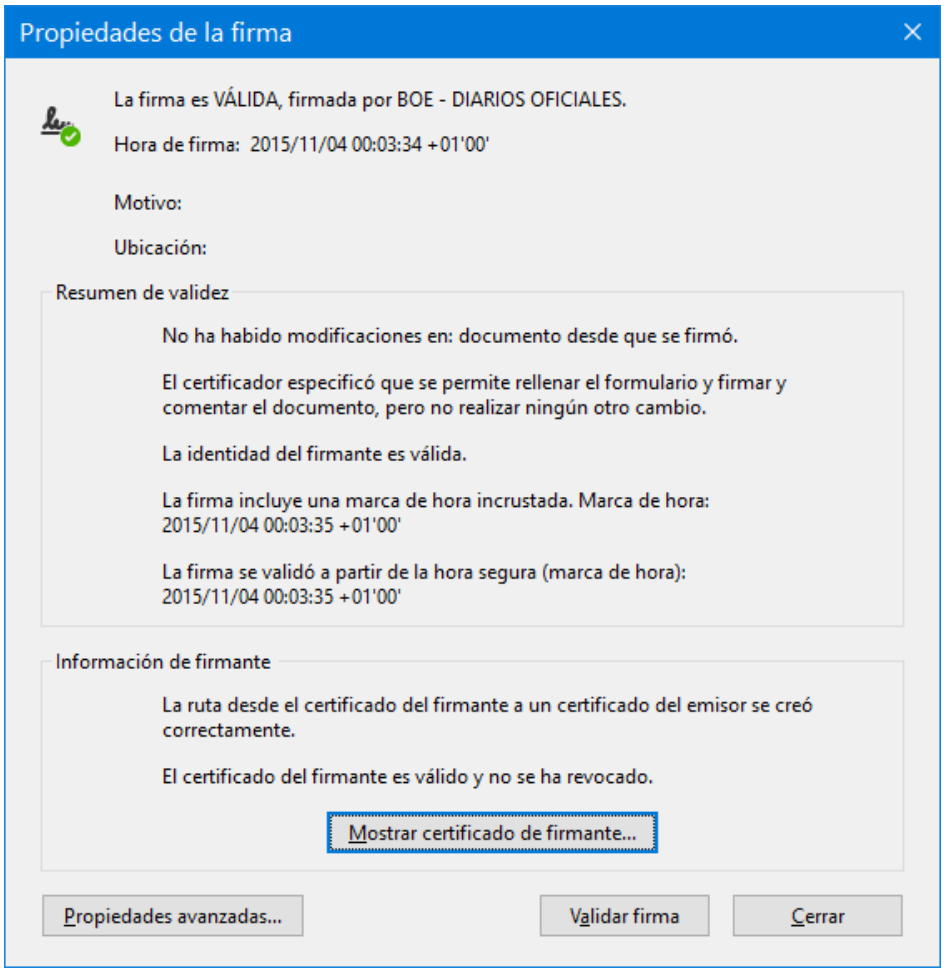
En el menú emergente selecciona la opción “Validar firma”. Se muestra el cuadro siguiente:



La ventana de adobe se muestra de la siguiente forma:



Ahora, si se vuelve a mostrar las propiedades de la firma obtenemos esta ventana:

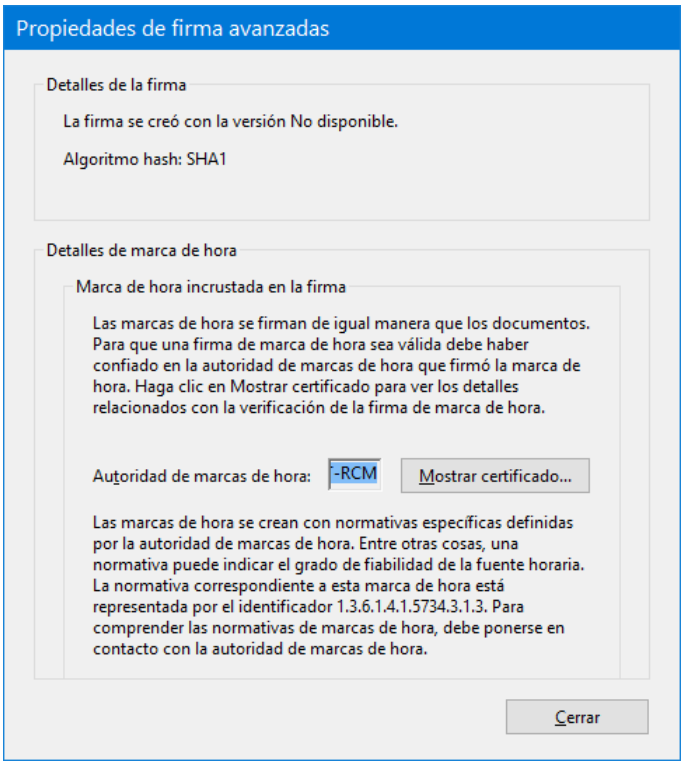


Además de validar la firma, también se ha podido validar el sello de tiempo incluido en el documento.

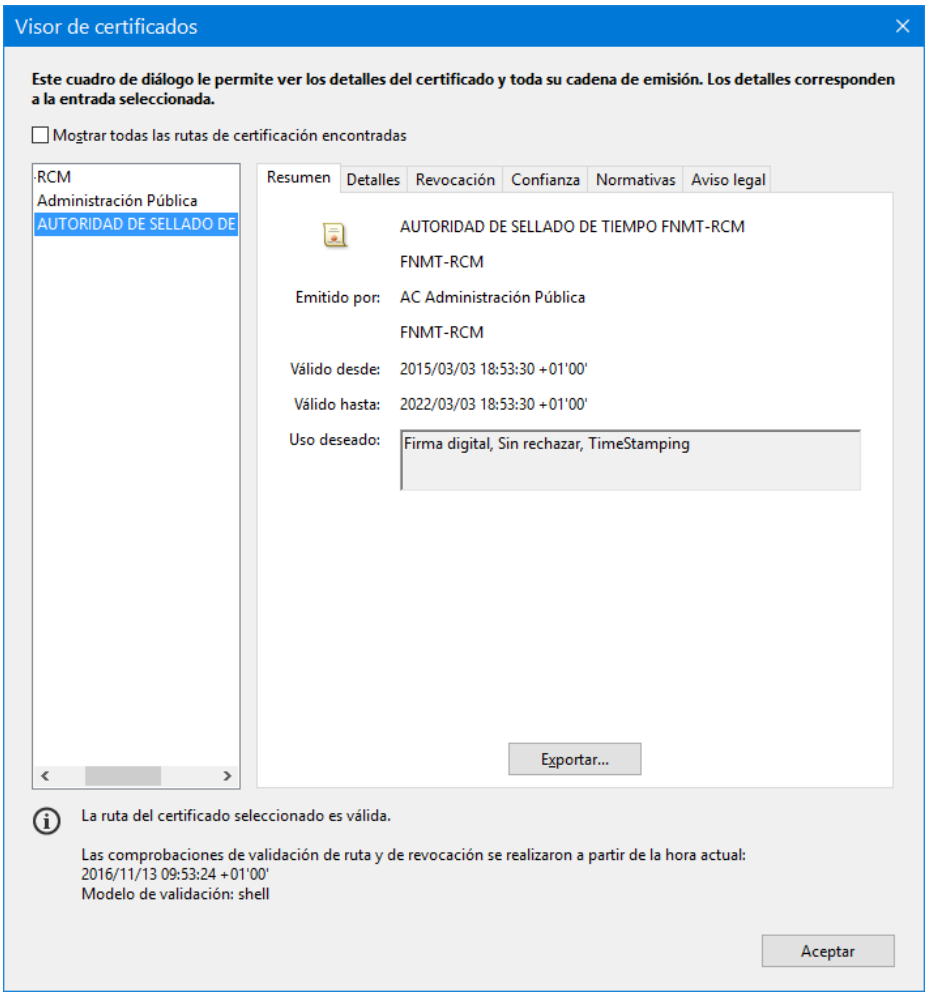
Esto se debe a que, en este caso, el certificado raíz del certificado de la autoridad de sellado de tiempos es el mismo que el del certificado usado para firmar el boletín.

El certificado raíz de la FNMT es raíz para ambas firmas, la del documento y la de tiempo. Al establecer la confianza en el certificado raíz de la FNMT, Adobe Reader confía en el certificado "BOE - DIARIOS OFICIALES", y también confía automáticamente, en el certificado "AUTORIDAD DE SELLADO DE TIEMPO FNMT-RCM" como se puede analizar a continuación.

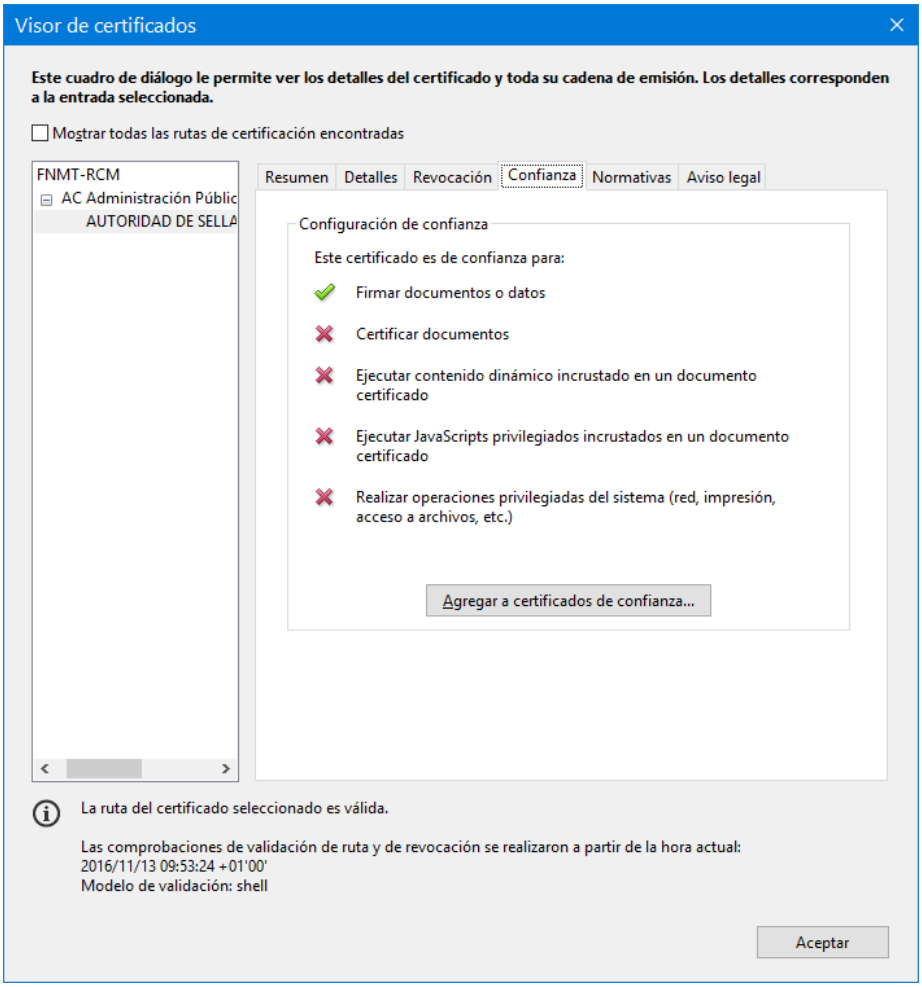
En la ventana anterior pulsa el botón "Propiedades avanzadas..." y aparece la ventana "Propiedades de firma avanzadas".



Pulsa el botón "Mostrar certificado". Aparece la ventana siguiente:



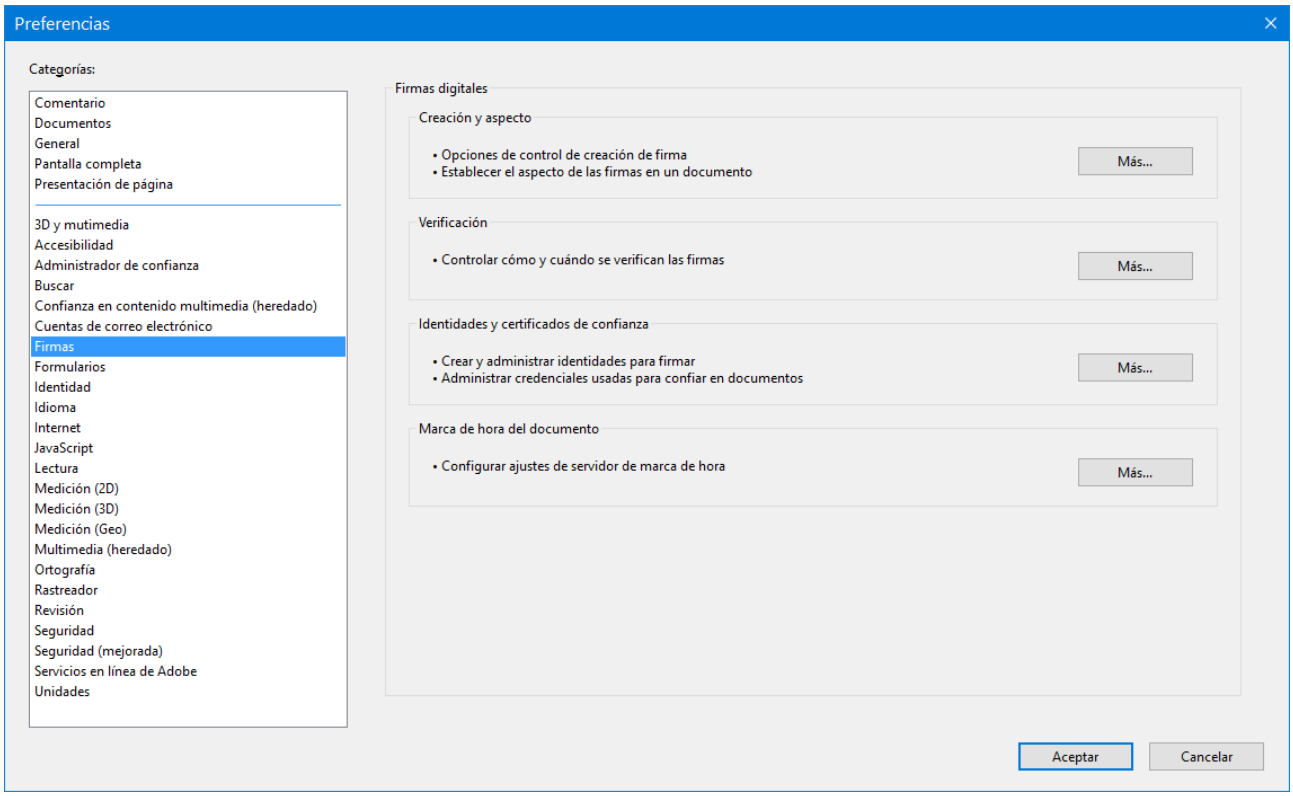
Si se selecciona la pestaña Confianza se puede comprobar la configuración de confianza:



NOTA: Si el certificado raíz del certificado de la autoridad de sellado de tiempos es DISTINTO que el del certificado usado para firmar el boletín, también hay que agregarlo a los certificados de confianza en los que confía Adobe Reader. Si no se agregase, no se podría validar la estampa de tiempo del documento.

3. Gestión de los certificados de Adobe

En la barra horizontal de menús de Adobe Reader DC, 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 cuadro Identidades y certificados de confianza pulsa el botón "Más...". En la ventana que aparece selecciona Certificados de confianza en el panel izquierdo y se obtiene:

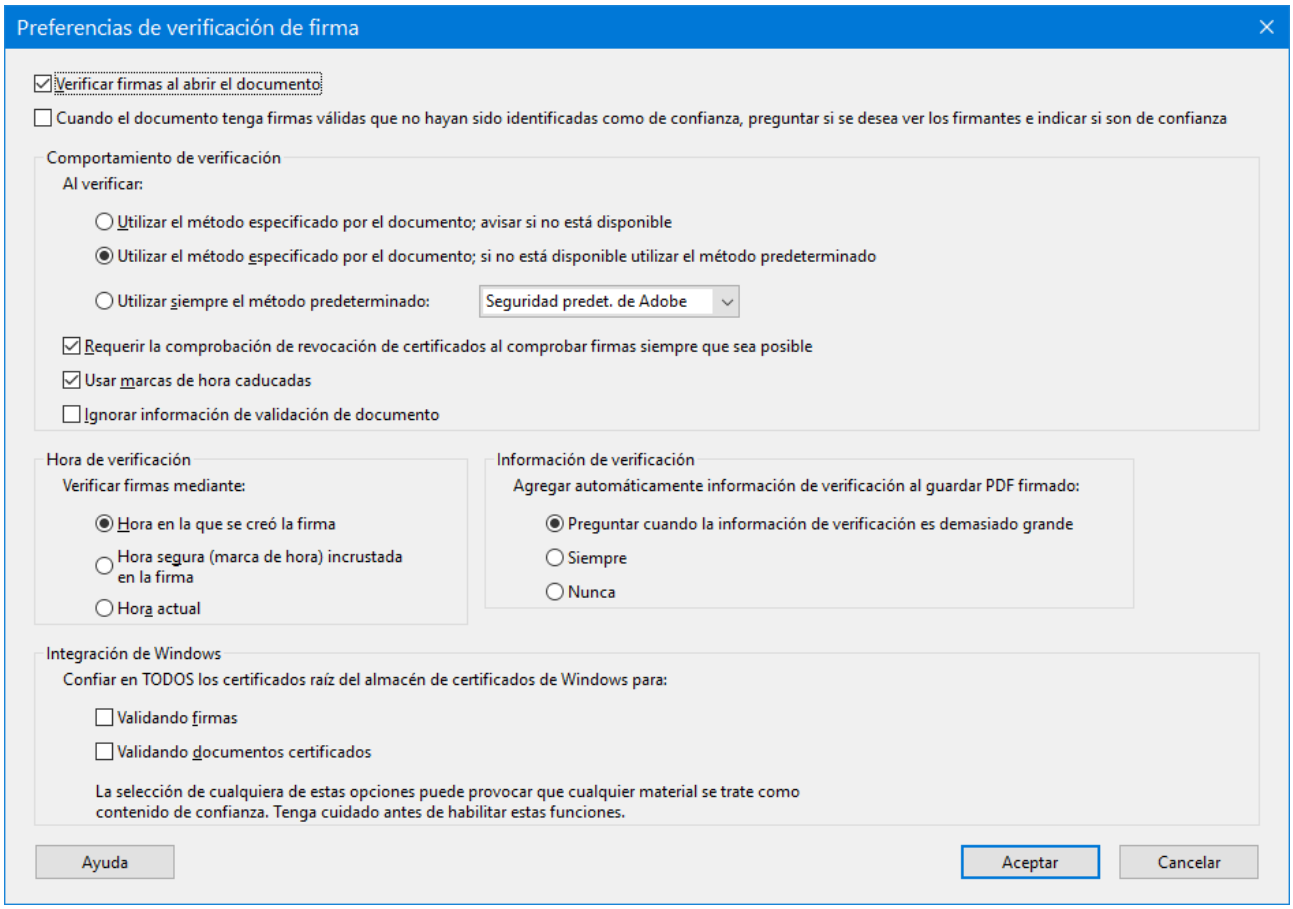
Comprueba las operaciones (botones superiores) que se pueden hacer con este certificado.

Quita el certificado del almacén de certificados de confianza de Adobe y vuelve a verificar la firma del boletín. Comprueba como ahora no se puede verificar la firma ni el sello de tiempos.

Todo este comportamiento es independiente del almacén de certificados de Windows. Se supone que en el almacén "Entidades de certificación raíz de confianza" de Windows no está cargado el certificado raíz de la FNMT. Si lo estuviera, podrías borrarlo y comprobar que el comportamiento es independiente de que esté o no esté.

Pero se puede hacer que Adobe utilice el almacén de certificados de Windows.

En la ventana "Preferencias", en la categoría “Firmas”, y 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”. La idea es que ahora se le indica a Adobe que también utilice los certificados raíz de confianza de Windows.

Ahora hay que introducir el certificado raíz de la FNMT en el almacén de certificados raíz de Windows. Y comprobar que el certificado raíz de la FNMT no está el almacén de certificados de confianza de Adobe Reader.

Vuelve a validar la firma del BOE. Debería ser correcta.

Con este modo de funcionamiento, es necesario que estén instalados en el computador los certificados de la entidad que ha firmado el boletín.

Como se puede ver, la entidad que firma los boletines es la FNMT (Fabrica Nacional de Moneda y Timbre). Se pueden descargar los certificados raíz de la FNMT de su página web:

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,.

Carga los certificados en el almacén de certificados de Windows. Es posible que el certificado raíz de la FNMT ya este cargado en el almacén denominado "Entidades de certificación raíz de confianza". Comprueba si ya está cargado antes de volver a cargarlo.

Importa el otro certificado y deja que el asistente elija el almacén. Comprueba que lo coloca correctamente en el almacén denominado "Entidades de certificación intermedias".

NOTA: En realidad solo necesitamos importar el certificado raíz de la FNMT.

Comprueba que se puede validar la firma y el sello de tiempos correctamente a partir del certificado raíz instalado en el almacén de certificados de Windows.

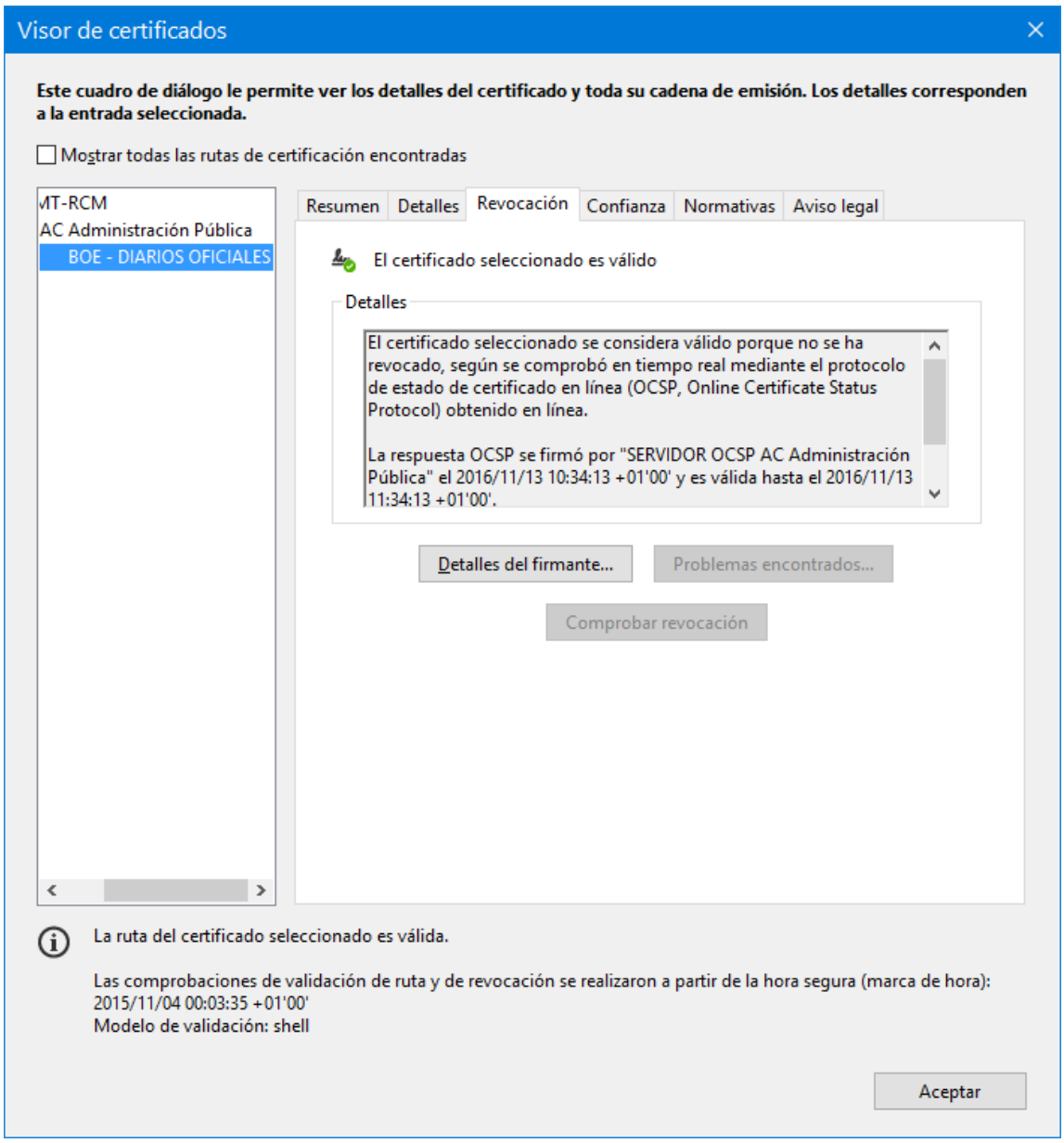
COMPROBACIÓN DE LA VALIDEZ DE LOS CERTIFICADOS

Todo el proceso descrito de verificación de firmas y sellos de tiempo es correcto si los certificados utilizados son válidos. Adobe comprueba la validez de los certificados y podemos analizar la comprobación realizada por Adobe.

Con el documento PDF abierto, despliega el panel de firmas y colocando el puntero del ratón sobre la firma pulsa el botón derecho. En el menú contextual que aparece selecciona la opción mostrar propiedades de la firma.

En la ventana "Propiedades de la firma" pulsa el botón "Mostar certificado de firmante..." para que se visualice la ventana "Visor de certificados".

En la ventana "Visor de certificados" selecciona el certificado usado para firmar el boletín y selecciona la pestaña "**Revocación**". Se visualiza la ventana siguiente:



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.

El mismo proceso se puede realizar para comprobar la validez del certificado de la entidad que ha generado el sello de tiempo.