Manual de configuración de Adobe Reader para validar la firma

Dirección de Ingeniería de Aplicaciones y Sistemas

Agencia de Informática y Comunicaciones de la Comunidad de Madrid

VICEPRESIDENCIA, CONSEJERÍA DE CULTURA Y DEPORTE Y PORTAVOCÍA DEL GOBIERNO
Comunidad de Madrid

ÍNDICE:

INTRODUCCIÓN

Para poder **validar la firma de los documentos en formato PDF**, que el BOCM pone a disposición de los ciudadanos en la sede electrónica, es necesario configurar la aplicación Adobe Reader como se describe en este manual.

Este manual está diseñado para la versión 9.0 de Adobe Reader, aunque también se puede utilizar para versiones anteriores tanto de Adobe Reader, como de Adobe Acrobat

La firma puede ser validada de **forma manual o automática**, como veremos a lo largo de este documento. Para ambos casos, los primeros pasos para la validación de la firma son:

1) **Instalar los certificados del prestador, en este caso Camerfirma.**

2) **Configurar la aplicación para que confíe en el certificado raíz del certificado de firma.**

1. INSTALAR LOS CERTIFICADOS DEL PRESTADOR.

Para poder verificar correctamente la firma electrónica de los documentos PDF, debe registrar en su navegador los certificados de Camerfirma.

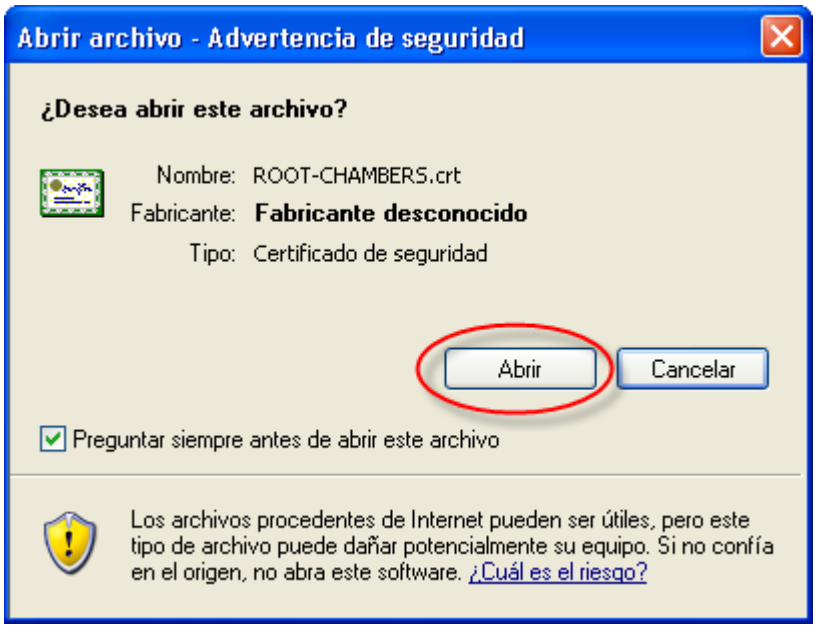
Estos certificados están disponibles en http://www.bocm.es/, y son:

1. El certificado de la Autoridad de Certificación raíz (ROOT-CHAMBERS)
2. El certificado de la Autoridad intermedia (ac_camerfirma_cc)

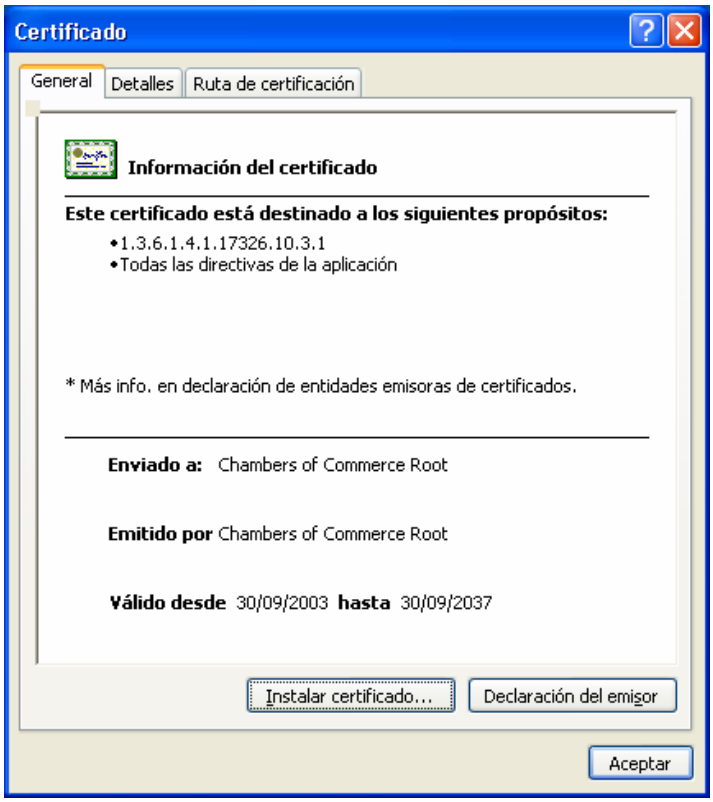
Aunque el proceso de instalación que se describe a continuación se ha elaborado para Internet Explorer, puede servir de guía para otros navegadores.

1) Pulse el enlace “Certificado RAIZ Camerfirma” que encontrará en http://www.bocm.es/.

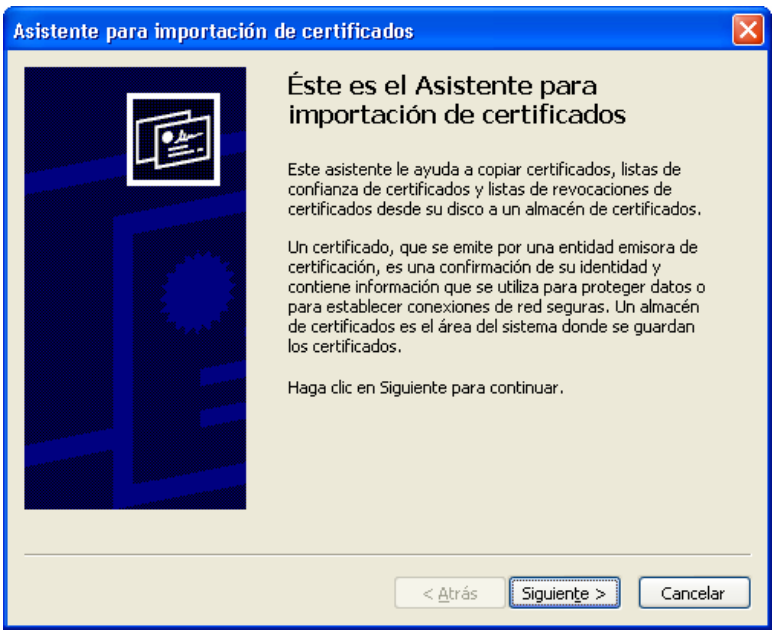
2) Se abrirá una ventana similar a la que se muestra a continuación, preguntando si desea abrir el archivo o guardarlo en su equipo, pulse el botón **“Abrir”.**



3. A continuación, se mostrará una ventana con los datos del certificado, seleccione la pestaña **“General”** y pulse el botón **“Instalar certificado** ...”



4) Se abrirá una nueva ventana con el ***"Asistente para importación de certificados"***, pulse el botón "***Siguiente"*** en este paso y en el paso posterior, y finalmente el botón ***"Finalizar".*** Tras este último paso se mostrará un mensaje indicando que la importación se realizó correctamente.



5) Pulse el botón "***Aceptar"*** de la ventana que muestra la información del certificado para cerrarla.

6) Pulse el enlace **"Certificado ac_camerfirma_cc**" que encontrará en http://www.bocm.es/ y repita los pasos del 2 al 5 para instalar este nuevo certificado.

7) En caso de haber optado por guardar los certificados en su disco, seleccione primero el certificado Raíz "*ROOT-CHAMBERS*" haga doble click sobre el archivo y se mostrará la ventana del paso 4, pudiendo seguir con el resto de pasos hasta importar el certificado.

Posteriormente seleccione el certificado **"AC_CAMERFIRMA_CC**" y repita los pasos.

2. CONFIGURAR ADOBE READER PARA CONFIAR EN LOS CERTIFICADOS RAÍZ.

Tras haber instalado los certificados de Camerfirma, hay varias formas de configurar las identidades en las que Adobe Reader confía, sólo es necesario utilizar **uno** de los métodos indicados a continuación.

En todos ellos hay que configurar la aplicación para:

- **Confiar en el certificado raíz del certificado de firma**
- **Confiar en el certificado raíz del certificado de la Autoridad de Sellado de Tiempo**

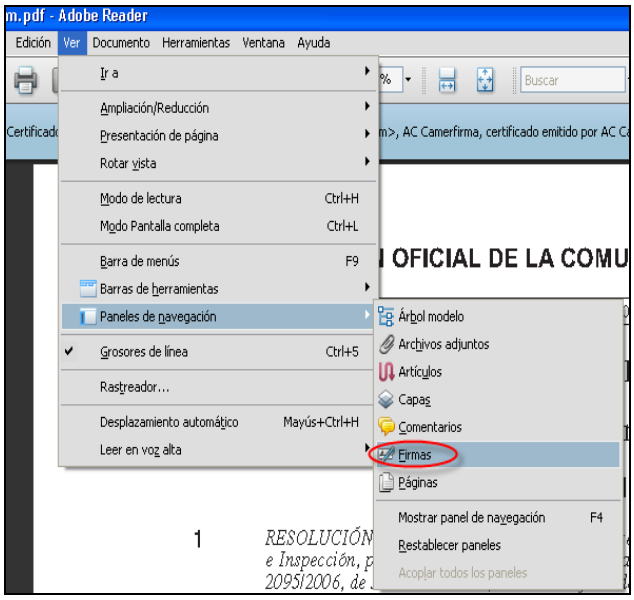
Salvo en el tercer método, en el cual se supone que dichos certificados están en el almacén de Windows.

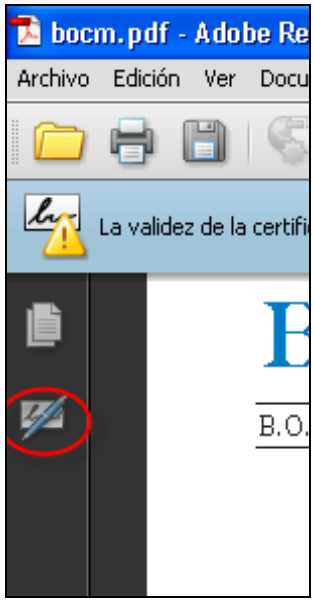
2.1 Primer método

2.1.1 Confiar en el certificado raíz del certificado de firma

Al abrir por primera vez un PDF firmado por el BOCM, se puede añadir el certificado raíz del certificado de firma a las identidades de confianza, de la siguiente manera:

1. Abrir el documento. Seleccionar la ficha de firmas, bien eligiendo del menú principal ***"Ver"*** > ***"Paneles de navegación"*** > ***"Firmas"*****,** o bien seleccionando la ficha **"Firmas"** que se muestra en la parte izquierda del documento.

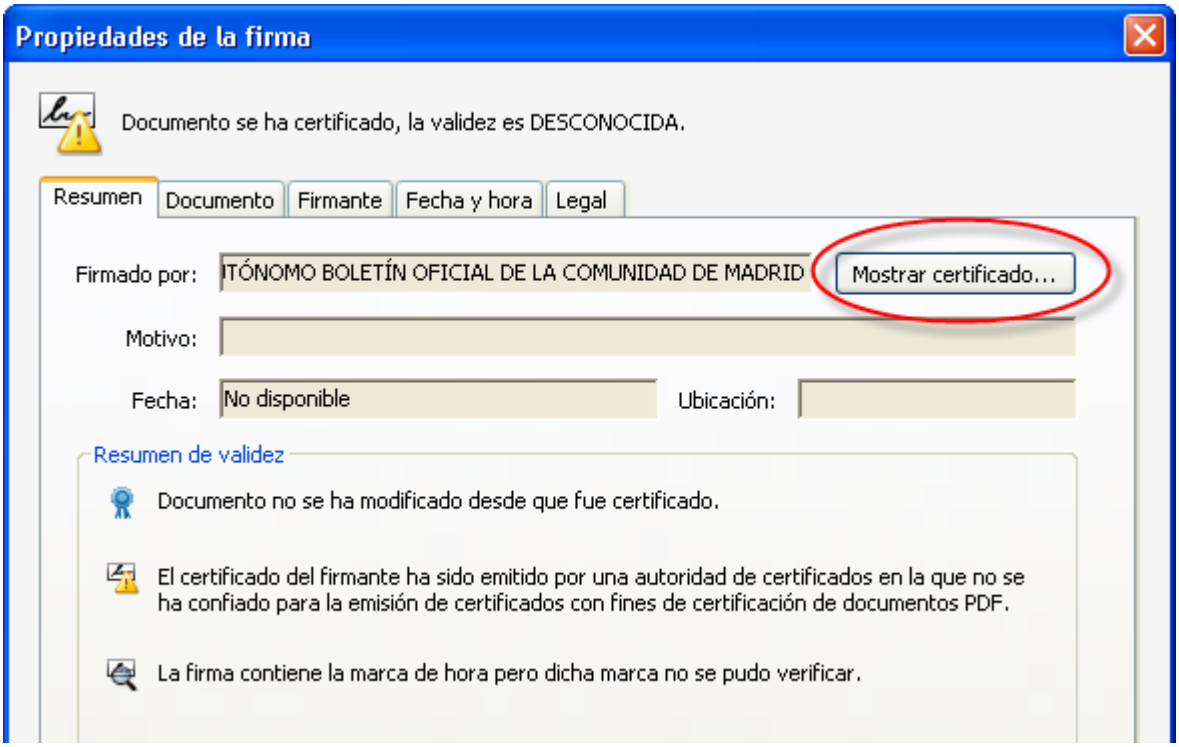




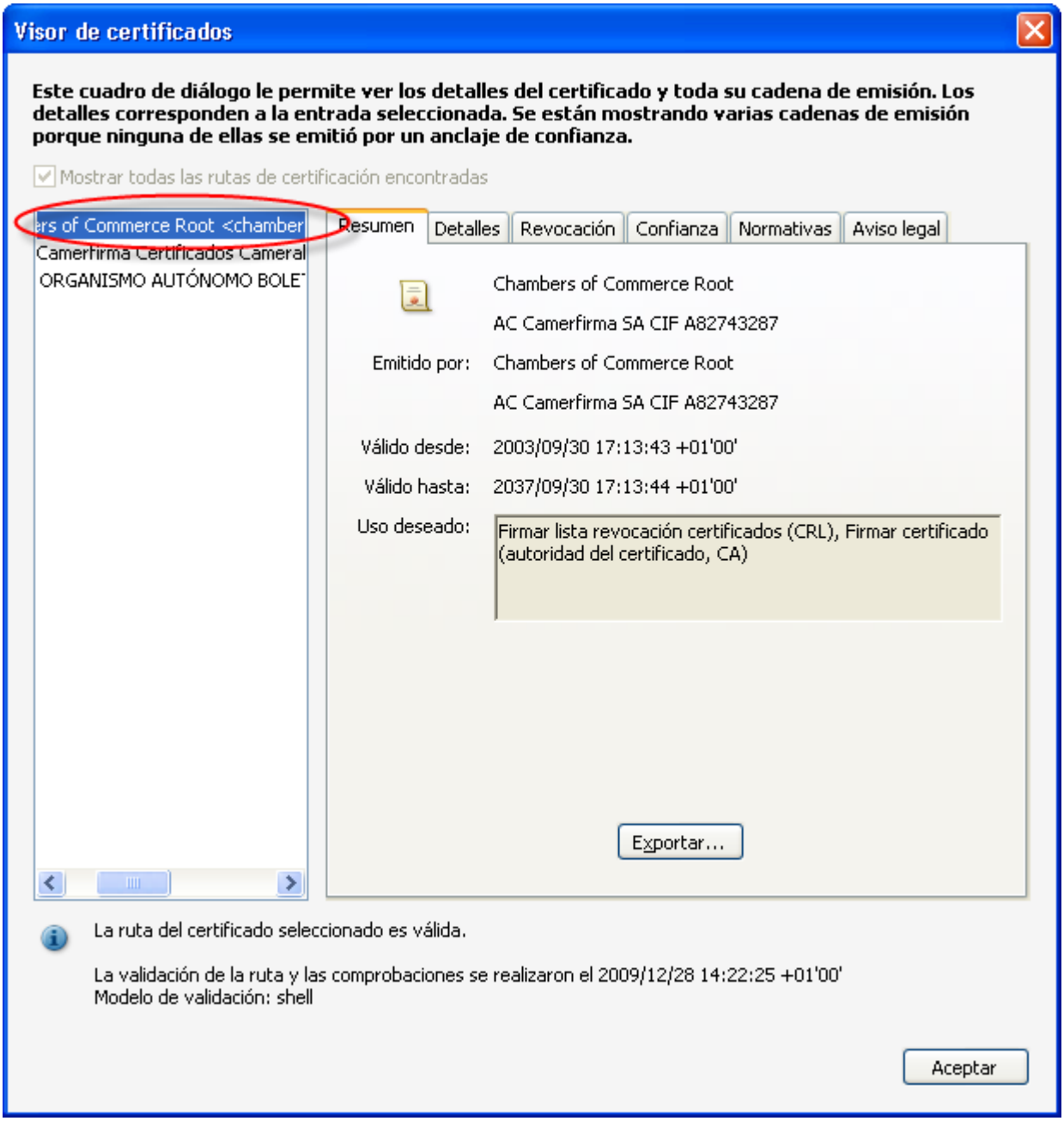
2. Seleccionar la firma (se mostrará el icono  o uno similar, junto a la firma para indicar que la identidad del firmante es desconocida porque no se ha incluido en la lista de identidades de confianza y ninguno de sus certificados principales es una identidad de confianza) .

3. Una vez seleccionada la firma, pulsar el botón derecho del ratón y elegir la opción ***"Mostrar propiedades de la firma ..."*** del menú que se despliega.

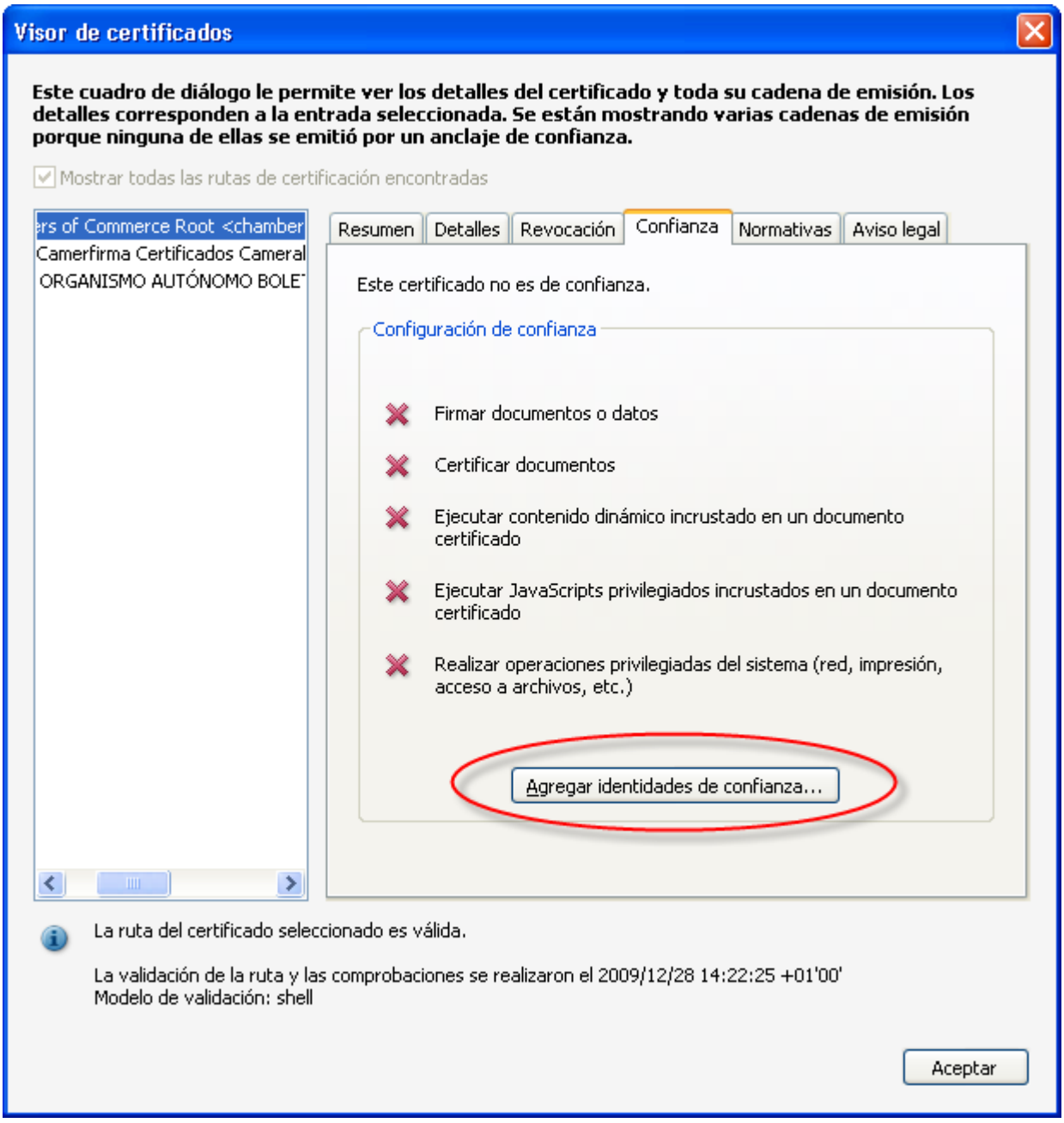
4. Se abrirá la ventana "Propiedades de la firma", en la que se muestran varias pestañas. Elegir la primera ("Resumen") y pulsar el botón "Mostrar certificado.


Propiedades de la firma
Documento se ha certificado, la validez es DESCONOCIDA.
Resumen
Documento
Firmante
Fecha y hora
Legal
Firmado por:
ITÓNOMO BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID
Mostrar certificado...
Motivo:
Fecha:
No disponible
Ubicación:
Resumen de validez
Documento no se ha modificado desde que fue certificado.
El certificado del firmante ha sido emitido por una autoridad de certificados en la que no se ha confiado para la emisión de certificados con fines de certificación de documentos PDF.
La firma contiene la marca de hora pero dicha marca no se pudo verificar.

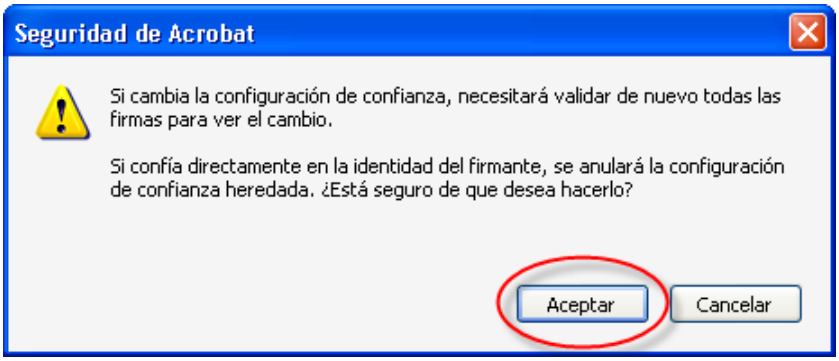
5) Se abrirá una nueva ventana, ***"Visor de certificados"***, en la que se muestra en el panel de la izquierda la lista de certificados que componen la ruta de certificación completa. Seleccionar el certificado raíz (el primero en la jerarquía).



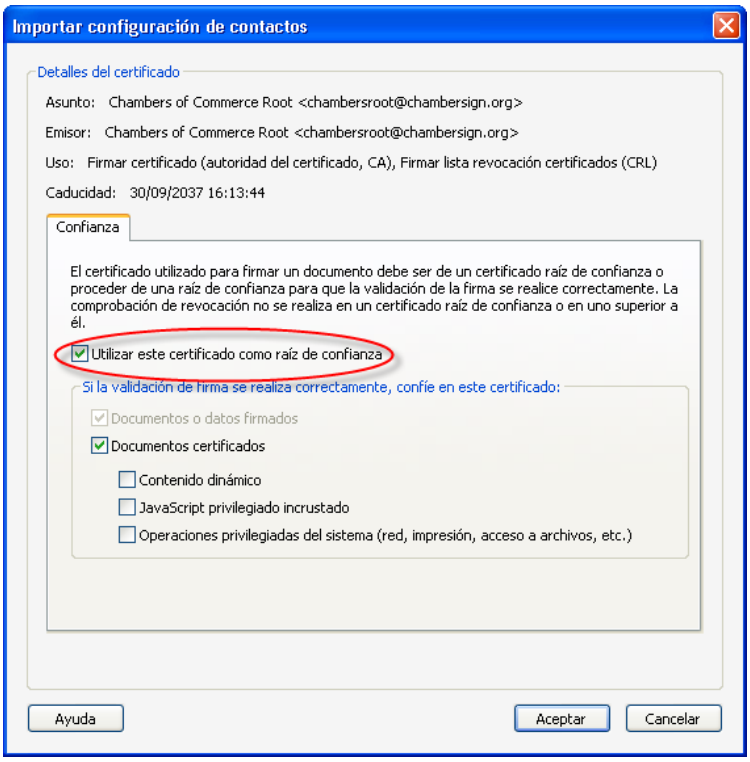
6) Seleccionar la pestaña **“Confianza**” y pulsar el botón “**Agregar identidades de confianza...”**



7) Pulsar "**Aceptar**" de la ventana de seguridad de Acrobat.



8) Se abre una nueva ventana, "**Importar configuración de contactos**", en ella, seleccionar el check "**utilizar este certificado como raíz de confianza**"



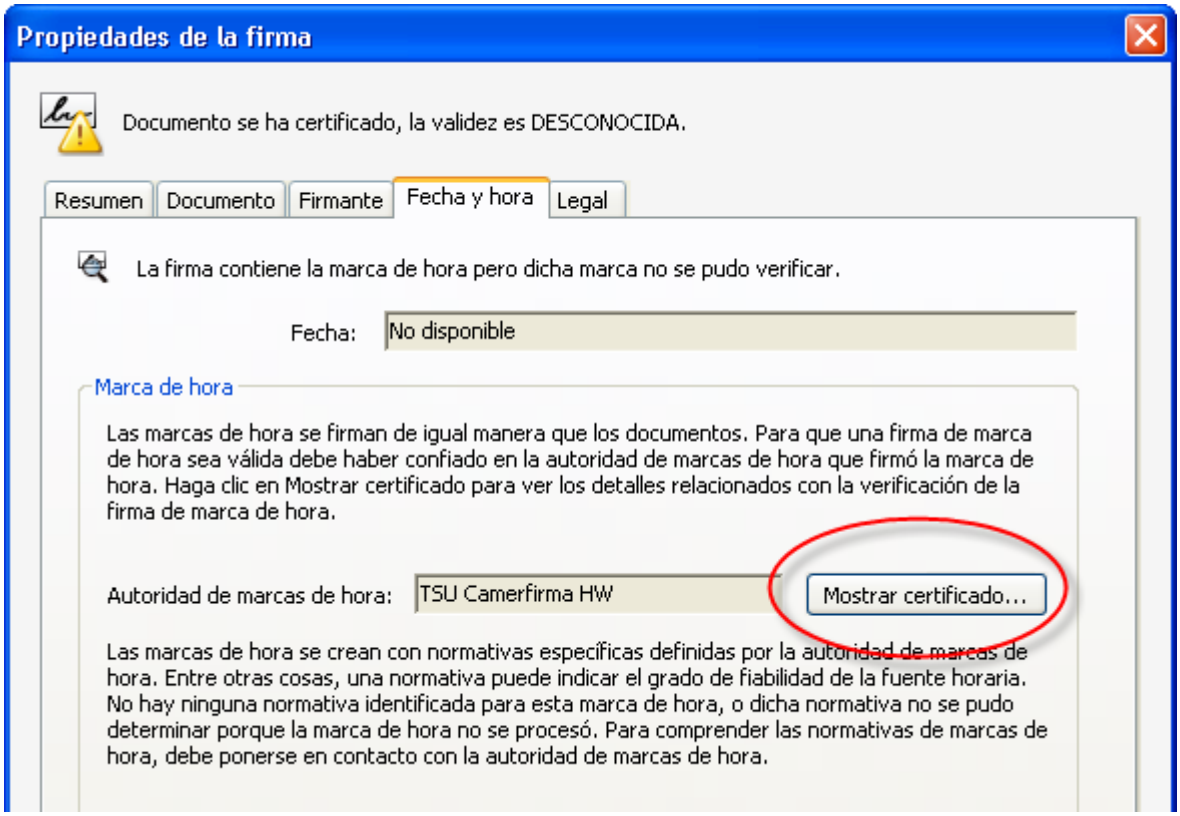
9) Pulsar **"Aceptar"** para cerrar la ventana "**Importar configuración de contactos"** y de nuevo **"Aceptar"** en la ventana "**Visor de certificados**".

2.1.2 Confiar en el certificado raíz del certificado de la Autoridad de Sellado de Tiempo

Si en la ventana ***"Propiedades de la firma"***, en la pestaña ***"Resumen",*** se muestra en la sección ***"Resumen de validez"*** el mensaje *"**La firma contiene la marca de hora**"*, significa que cuando se firmó el documento, se solicitó a una Autoridad de Sellado de Tiempo un sello temporal que garantiza, por esta tercera parte de confianza, que la firma se realizó en la hora indicada.

En estos casos, es necesario confiar también en el certificado raíz del certificado de esta Autoridad de Sellado de Tiempo, si no está ya entre las identidades en las que confía Adobe, para ello.

1. En la ventana ***"Propiedades de la firma"*** seleccionar la pestaña ***"Fecha y hora",*** y en la sección *"**Marca de hora"*** pulsar el botón *"**Mostrar certificado ..."*.**



2. Se abrirá de nuevo la ventana ***"Visor de certificados"***, seguir los mismos pasos indicados en los puntos 5 al 9 de la sección anterior.

3. Una vez que se ha establecido la confianza en los certificados raíz del certificado de firma y del certificado de la Autoridad de Sellado de Tiempo, pulsar ***"Cerrar"*** en la ventana ***"Propiedades de la firma".***

2.2 Segundo método

2.2.1 Confiar en el certificado raíz del certificado de firma.

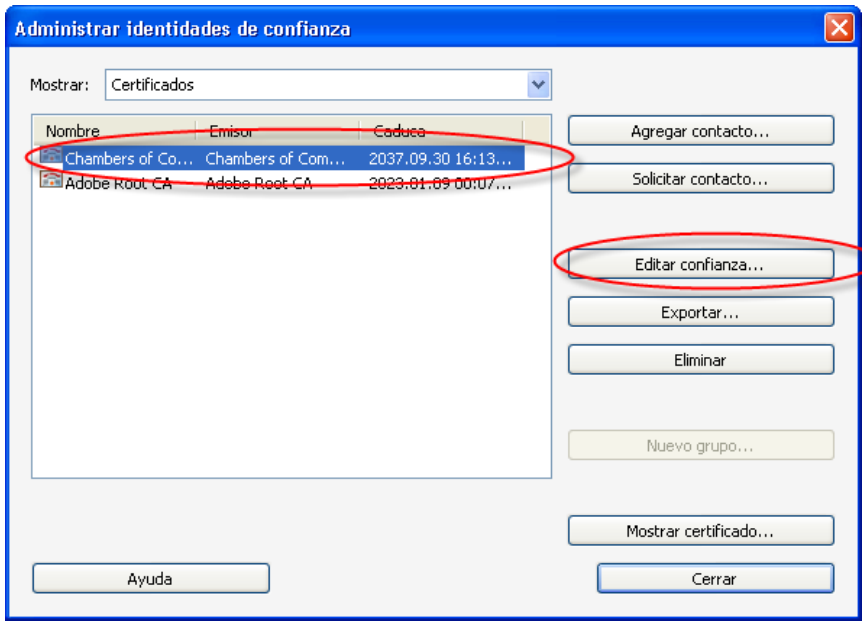
Añadir el certificado raíz del certificado de firma a las identidades de confianza usando el Administrador de identidades de confianza de Adobe Reader, según los siguientes pasos:

1. Seleccionar del menú ***"Documento"*** > ***"Administrar identidades de confianza ..."*** si tiene instalado Adobe Reader, o ***"Avanzadas"*** > ***"Administrar identidades de confianza ..."*** si tiene instalado Adobe Acrobat.

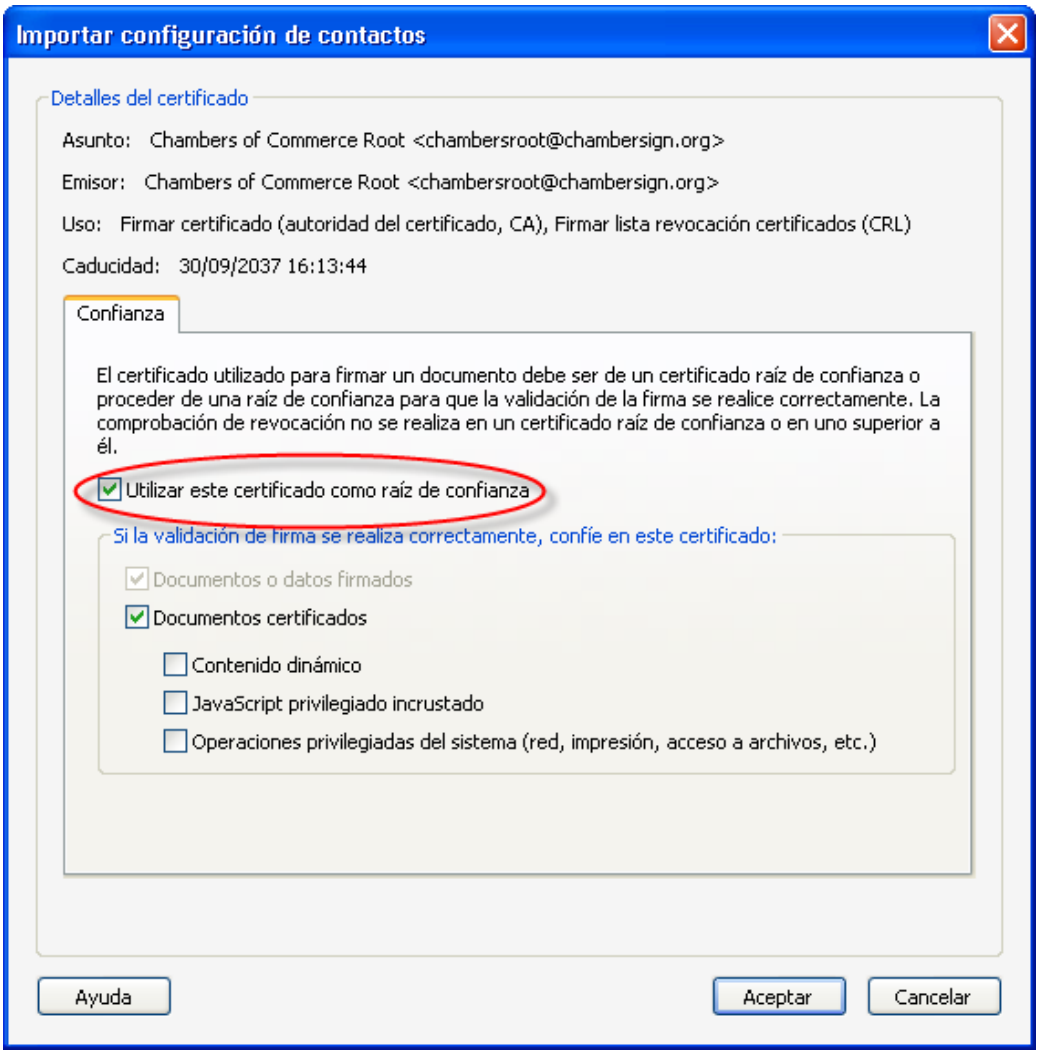
2. En la lista desplegable ***"Mostrar"*** que hay en la parte superior de la ventana, la opción por defecto es *"Contactos"*, cambiar la selección a *"Certificados"*.

3. Seleccionar el **certificado raíz de la lista** (si no está en la lista, utilizar el primer método explicado anteriormente)

4. Con el certificado raíz seleccionado, pulsar el botón ***"Editar confianza"***



5. En la nueva ventana que se muestra, *"**Editar confianza del certificado**"*, marcar en la sección ***"Confianza"*** la casilla *"**Utilizar este certificado como raíz de confianza**"*



6. Pulsar ***"Aceptar"*** para cerrar la ventana ***"Editar confianza del certificado"***.

2.2.2 Confiar en el certificado raíz del certificado de la Autoridad de Sellado de Tiempo

1. Desde la ventana “Administrar identidades de confianza”, seleccionar el certificado raíz del certificado de la Autoridad de Sellado de Tiempo de entre todos los que se muestran en la lista (si no está en la lista, utilizar el primer método explicado anteriormente).

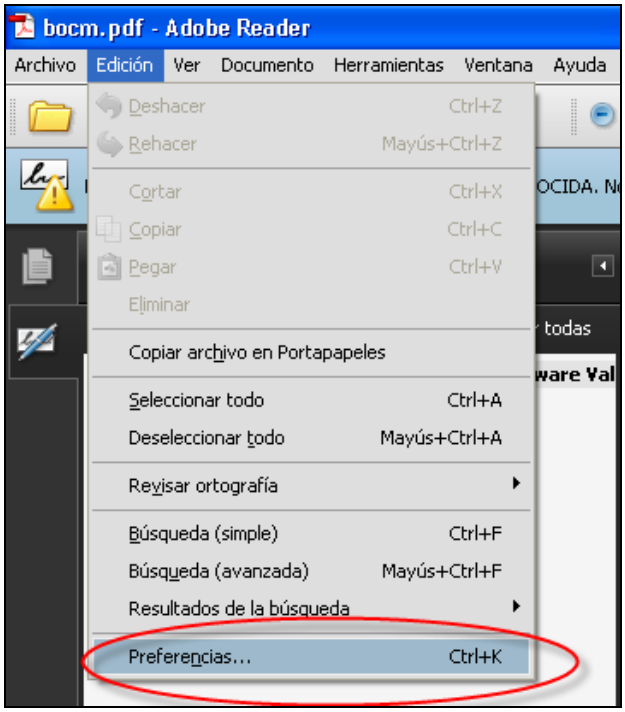
2. Repetir los pasos del 4 al 6 explicados en la sección anterior.

Una vez que se ha establecido la confianza en los certificados raíz del certificado de firma y del certificado de la Autoridad de Sellado de Tiempo, pulsar *“**Cerrar”*** en la ventana ***“Administrar identidades de confianza”***

2.3.1 Tercer método

Si el certificado raíz del certificado de firma, y el certificado raíz del certificado de la Autoridad de Sellado de Tiempo, están registrados en el almacén de certificados de Microsoft Windows, se puede seguir este tercer método que consiste en:

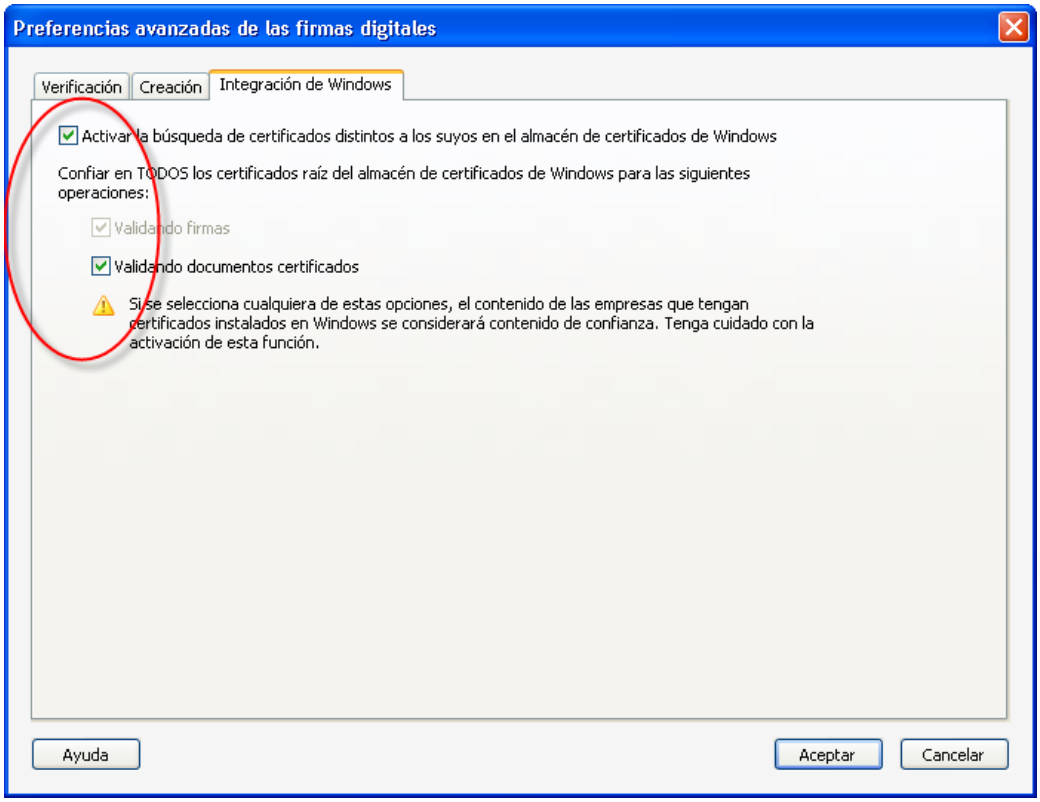
1. Seleccionar en el menú principal ***"Edición" > "Preferencias".***



2. Seleccionar en la ventana que se muestra la opción "**Seguridad"** de entre todas las que hay en el panel de la izquierda.

3. Pulsar el botón "**Preferencias Avanzadas**" para abrir la ventana "**Preferencias avanzadas de las firmas digitales".**

4. En la ventana de *"**Preferencias avanzadas de las firmas digitales**"*, seleccionar la pestaña *"**Integración de Windows"**,* y marcar las opciones *"**Activar la búsqueda de certificados distintos a los suyos en el almacén de certificados de Windows**"*, *"**Validando firmas"** y "**Validando documentos certificados".***



5. Pulsar *"**Aceptar"*** para guardar los cambios y volver a la ventana *"**Preferencias"*** y de nuevo *"**Aceptar"*** para cerrar esta ventana.

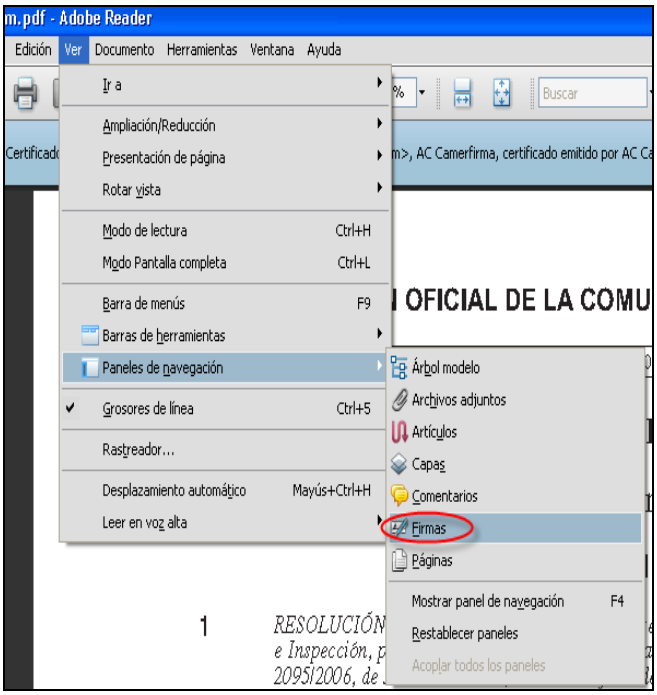
3. VALIDACIÓN DE LA FIRMA DIGITAL

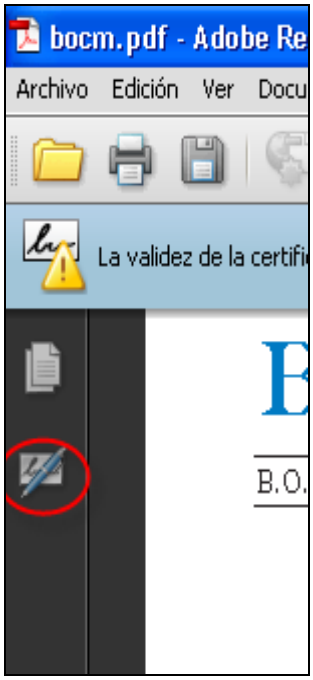
3.1. Validación manual

Para validar la firma digital de forma manual tenemos que seguir los pasos que se indican a continuación:

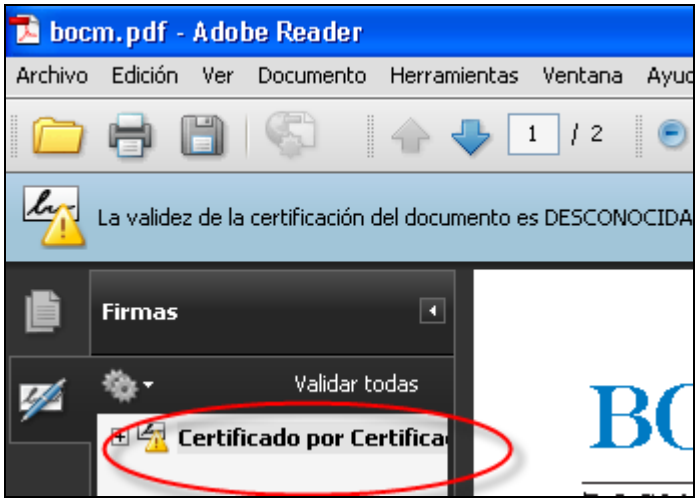
1. Abrir el documento

2. Seleccionar la ficha de firmas, bien eligiendo del menú principal *"**Ver**"* > ***"Paneles de navegación" > "Firmas"*,** o bien seleccionando la ficha **"Firmas"** que se muestra en la parte izquierda del documento.





3) Seleccionar la firma (si no se ha validado aún se mostrará el icono  , o uno similar, junto a la firma)



4) Una vez seleccionada la firma, pulsar el botón derecho del ratón y elegir la opción "**Validar firma".**

5) Una vez **validada la firma**, si todo ha ido bien, debería mostrarse junto a la firma el icono  , o similar.

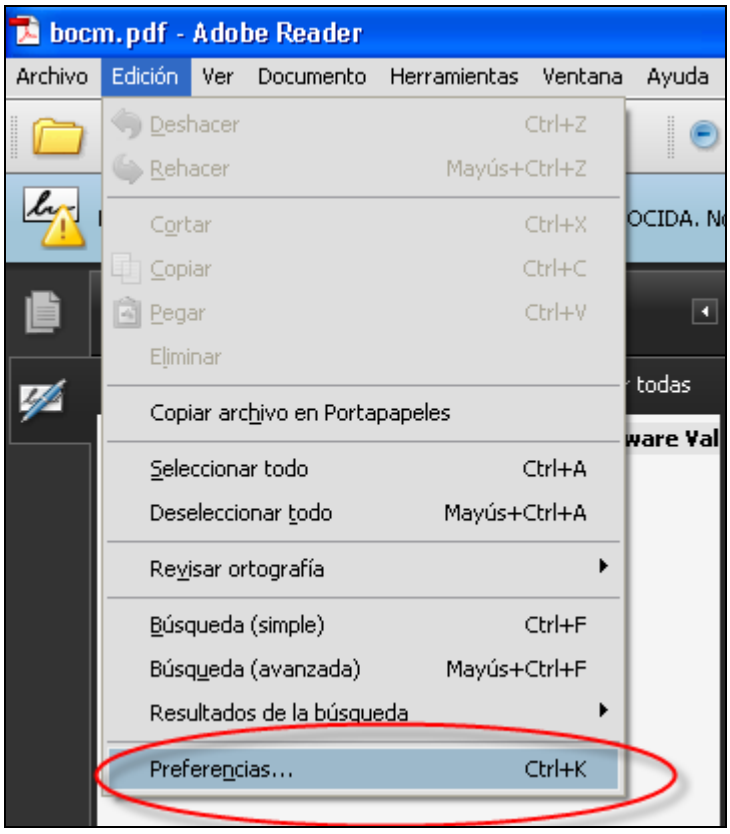
3.2. Validación automática

Se puede configurar la aplicación para que l**a firma de un documento PDF se valide automáticamente** al abrirlo, pero hay que tener en cuenta que esta operación consume un pequeño lapso de tiempo cada vez que se abra el documento.

Para establecer la validación automática hay que configurar las preferencias de las firmas digitales de Adobe Reader de la siguiente manera:

1) Abrir el documento

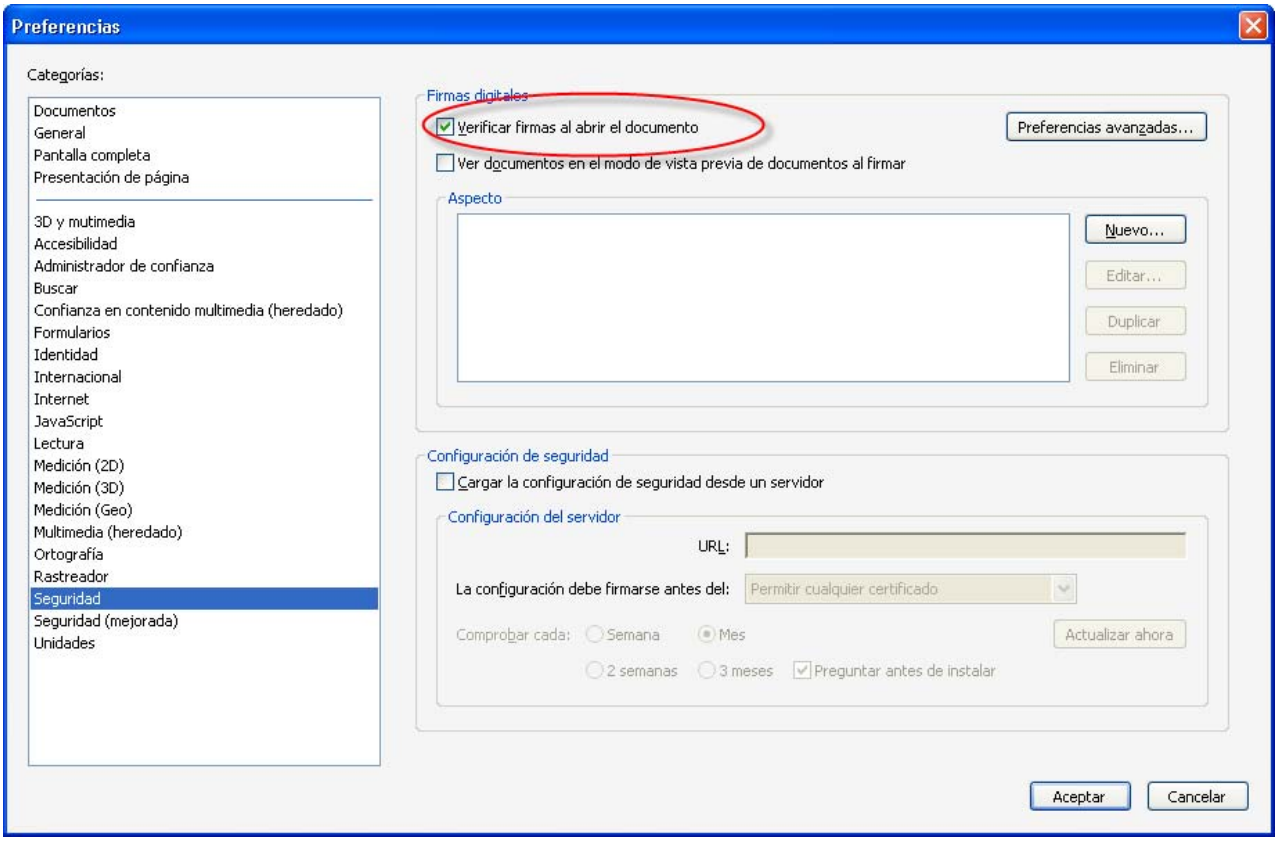
2) Seleccionar del menú principal *"**Edición" > "Preferencias"**.*



3) Seleccionar en la ventana que se muestra la opción **"Seguridad"** de entre todas las que hay en el panel de la izquierda.

4) Marcar, si no lo está, la opción "**Verificar firmas al abrir el documento".**

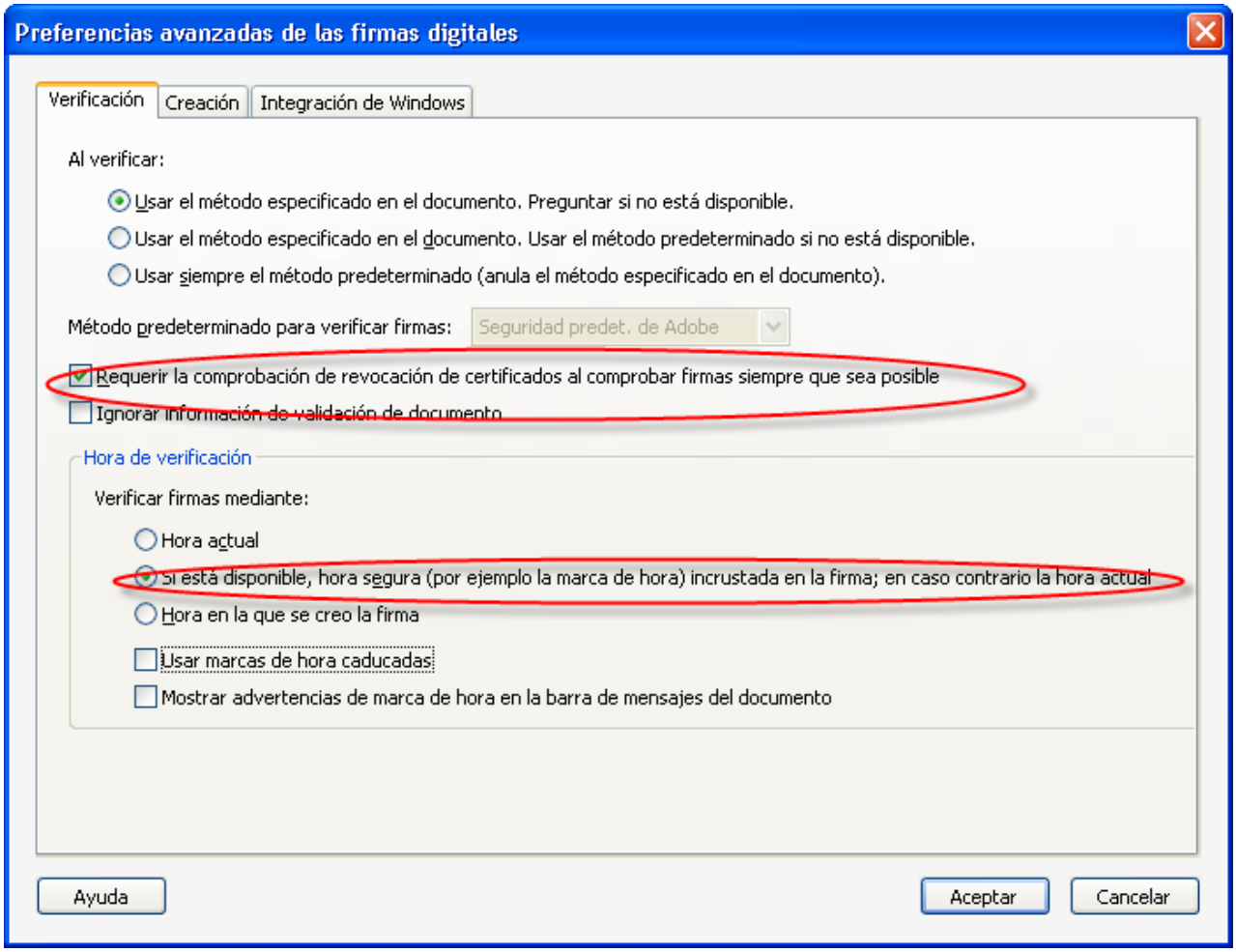
5) Pulsar el botón ***"Preferencias Avanzadas"*** para abrir el cuadro de diálogo ***"Preferencias avanzadas de las firmas digitales".***



6) Seleccionar la pestaña **"Verificación**", y en la opción "**Al verificar**:" **marcar "Usar el método especificado en el documento"**. Preguntar si no está disponible".

7) Marcar la opción "**Requerir la comprobación de revocación de certificados al comprobar firmas siempre que sea posible".**

8) En el recuadro **"Hora de verificación**" seleccionar la opción "**Si está disponible, hora segura (por ejemplo la marca de hora) incrustada en la firma; en caso contrario la hora actual".**



9) Pulsar **"Aceptar**" para cerrar la ventana de **"Preferencias avanzadas de las firmas digitales",** y de nuevo en **"Aceptar**" para cerrar la ventana **"Preferencias".**

La próxima vez que se abra el documento, se validará la firma automáticamente.

4. COMPROBAR LA VALIDEZ DE LA FIRMA ELECTRÓNICA

Una vez validada la firma digital por cualquiera de los métodos anteriores se puede **comprobar la validez de la firma** a través de la ficha ***"Firmas"***, para verla seleccionar del menú principal ***"Ver"*** > ***"Paneles de navegación"*** > ***"Firmas"***, o seleccionar la ficha ***"Firmas"*** que se muestra en la parte izquierda del documento.

En esta ficha se muestra un listado de todas las firmas electrónicas que tiene el documento e información sobre su validez.

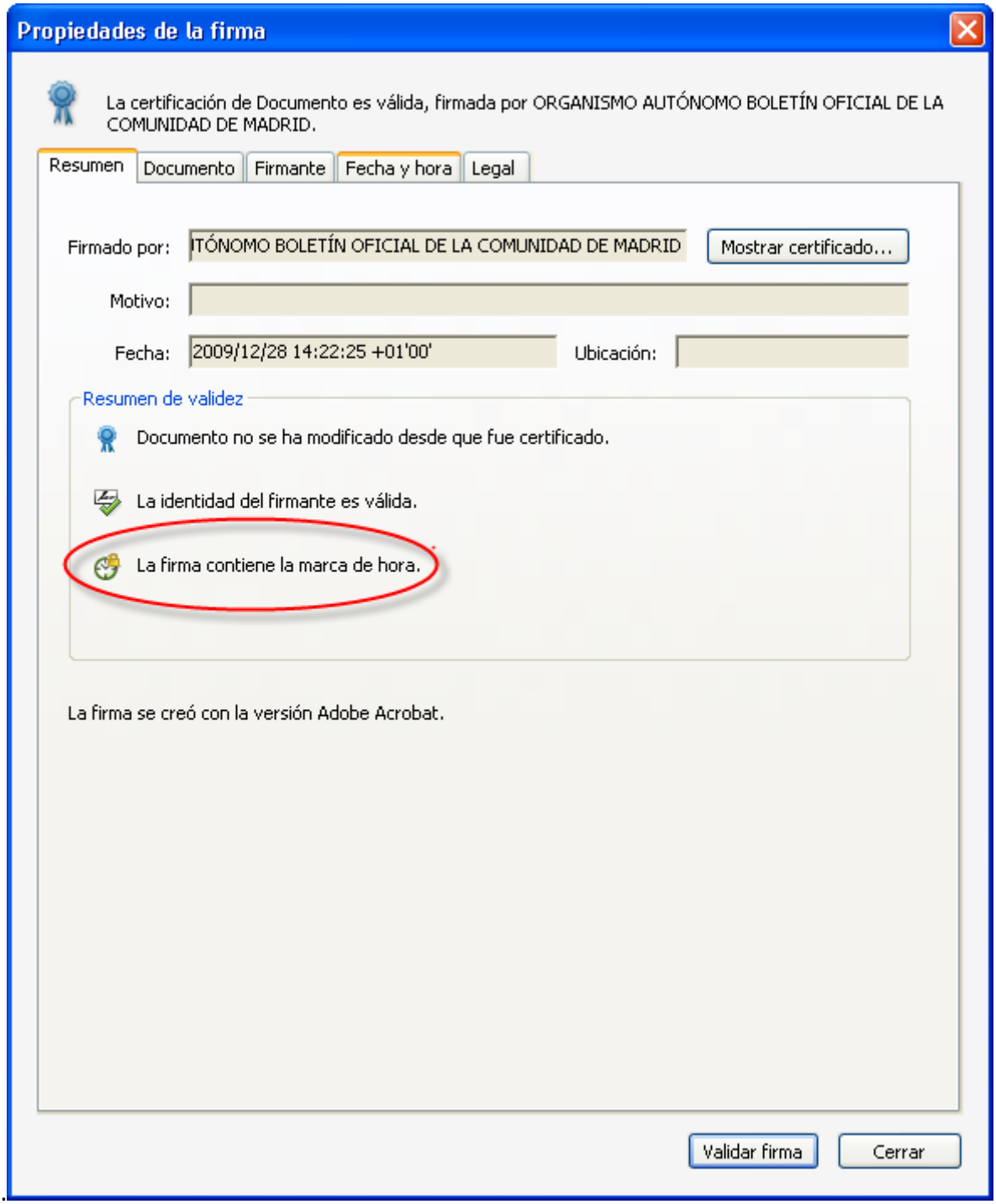
Para consultar los detalles sobre la firma y la validez del certificado con el que se hizo, pulsar con el botón derecho del ratón sobre la firma, y elegir la opción ***"Mostrar propiedades de firma..."*** del menú que se despliega.

Se abrirá una ventana, en la que se muestran varias pestañas, seleccionar la primera ("**Resumen")** y pulsar el botón *"**Mostrar certificado ..."*.**

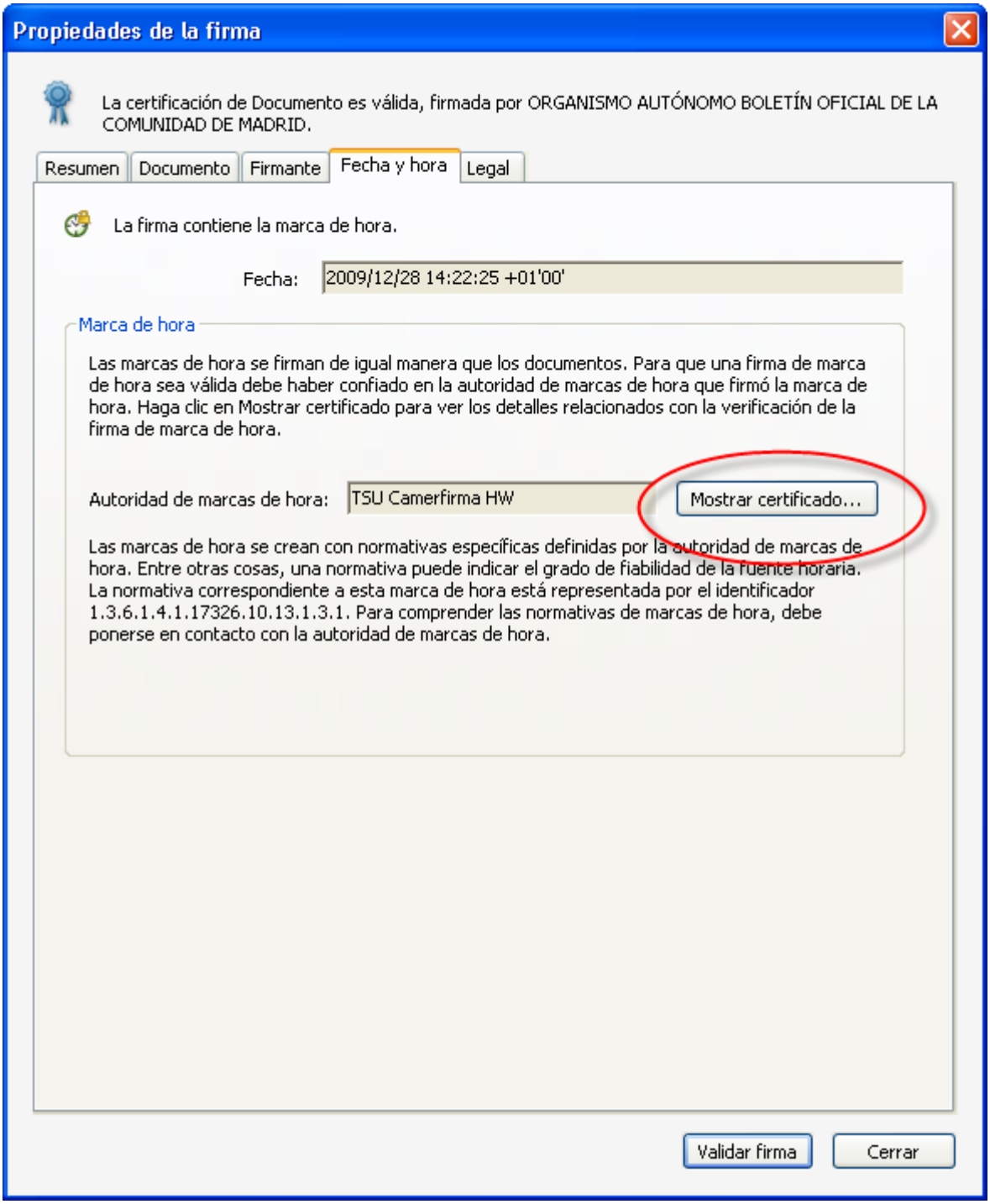
Se abrirá una nueva ventana ***"Visor de certificados"*** en la que se seleccionará la pestaña *"Revocación"*. En la sección *"**Detalles"*** se muestra información sobre el estado de revocación del certificado.

5. COMPROBAR LA VALIDEZ DEL SELLO DE TIEMPO

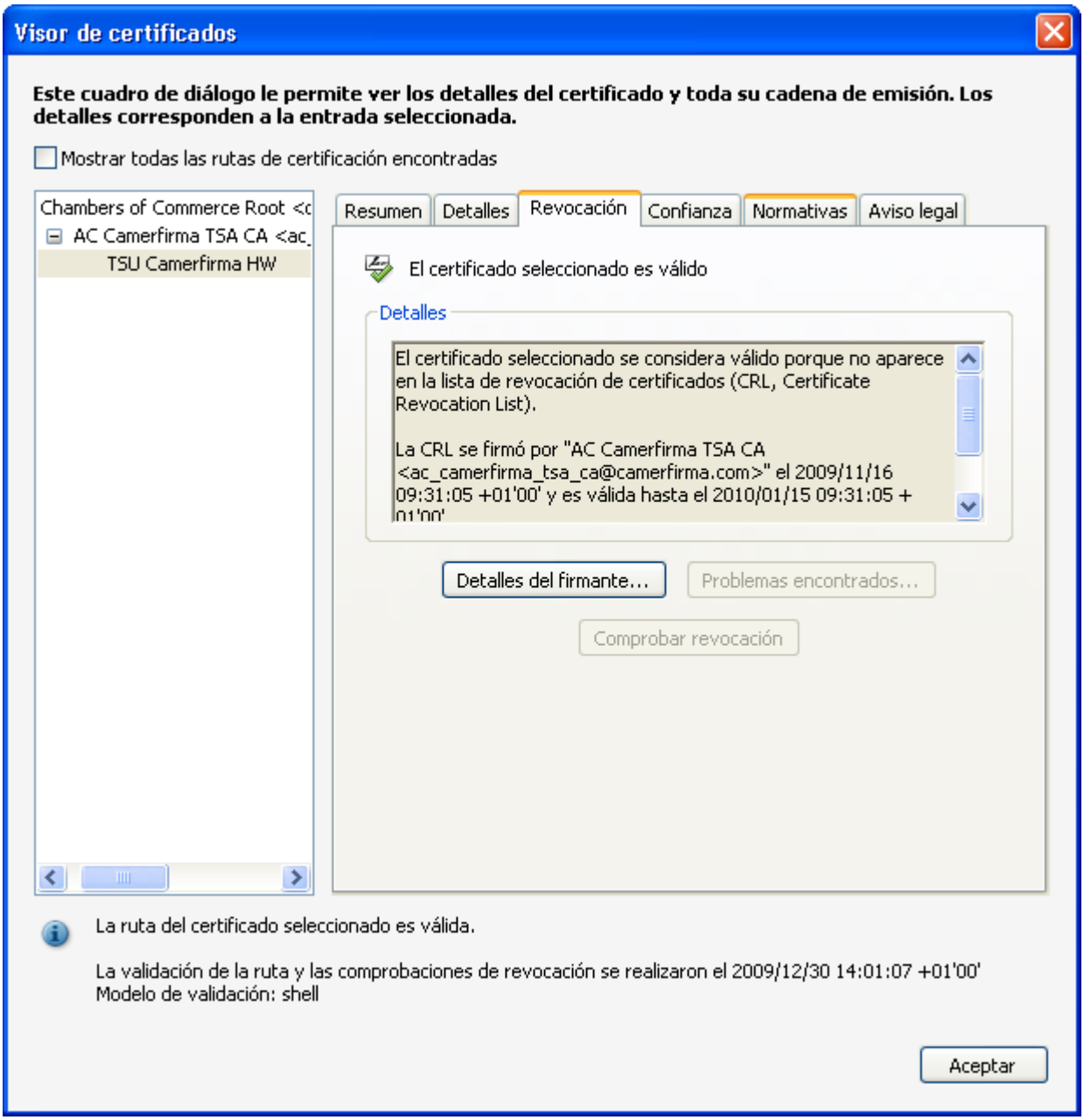
1) Si en la ventana ***"Propiedades de la firma"***, en la pestaña ***"Resumen"*** se muestra en la sección ***"Resumen de validez"*** el mensaje ***"La firma contiene la marca de hora"***, significa que cuando se firmó el documento, se solicitó a una Autoridad de Sellado de Tiempo un sello temporal que garantiza, por esta tercera parte de confianza, que la firma se realizó en la hora indicada.



2) Se puede comprobar la validez del sello temporal seleccionando la pestaña **"Fecha y hora" de la ventana "Propiedades de la firma**", y en ella pulsando el botón ***"Mostrar certificado..."*.**


Propiedades de la firma
La certificación de Documento es válida, firmada por ORGANISMO AUTÓNOMO BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID.
Resumen
Documento
Firmante
Fecha y hora
Legal
La firma contiene la marca de hora.
Fecha:
2009/12/28 14:22:25 +01'00'
Marca de hora
Las marcas de hora se firman de igual manera que los documentos. Para que una firma de marca de hora sea válida debe haber confiado en la autoridad de marcas de hora que firmó la marca de hora. Haga clic en Mostrar certificado para ver los detalles relacionados con la verificación de la firma de marca de hora.
Autoridad de marcas de hora:
TSU Camerfirma HW
Mostrar certificado...
Las marcas de hora se crean con normativas específicas definidas por la autoridad de marcas de hora. Entre otras cosas, una normativa puede indicar el grado de fiabilidad de la fuente horaria. La normativa correspondiente a esta marca de hora está representada por el identificador 1.3.6.1.4.1.17326.10.13.1.3.1. Para comprender las normativas de marcas de hora, debe ponerse en contacto con la autoridad de marcas de hora.
Validar firma
Cerrar

3) Se abrirá una nueva ventana *"**Visor de certificados**"* en la que se seleccionará la pestaña ***"Revocación"***. En la sección *"**Detalles**"* se muestra información sobre el estado de revocación del certificado de la Autoridad de Sellado de Tiempo.



6. POSIBLES PROBLEMAS Y SOLUCIONES

1. La firma tiene el icono  junto a ella.

Este problema surge normalmente si el documento se abre desde un navegador.
Para algunos de ellos, si la aplicación Adobe Reader se ha configurado para validar la firma automáticamente, es necesario recargar el documento para que lo haga.
En caso de que no esté configurada así, validar la firma manualmente (ver apartado correspondiente de este documento)

2. La firma no tiene el icono  junto a ella, sino el icono 

Este problema se debe a que Adobe Reader no ha podido verificar la firma, las causas y posibles soluciones pueden ser:

Si al mostrar las propiedades, bien del certificado de la firma, bien del certificado de la Autoridad de Sellado de Tiempo, en la pestaña ***"Revocación"***, se muestra un mensaje diciendo que no se ha podido verificar porque la raíz del certificado no es una entidad de confianza, entonces tenemos que repasar la sección **"Configurar Adobe Reader para que confíe en el certificado raíz del certificado de firma y del certificado de la Autoridad de Sellado de Tiempo**" de este documento.

Si al mostrar las propiedades, bien del certificado de la firma, bien del certificado de la Autoridad de Sellado de Tiempo, en la pestaña *"**Revocación**"***,** se muestra un mensaje diciendo que no se ha podido verificar la validez del certificado, y pulsando en el botón *"**Problemas encontrados ...**"* indica que no se ha podido descargar la lista de distribución o acceder al servidor OCSP embebido en el certificado, verificar que Adobe Reader puede acceder a internet.

En algunos entornos donde se utiliza un proxy es posible que se tenga que adaptar la configuración de Adobe Reader para que pueda conectarse a internet (en el menú principal seleccionar *"**Edición**"* **>** *"**Preferencias...**"* **>** *"**Internet**"***,** y en la sección *"**Opciones de Internet**"* pulsar el botón *"**Propiedades de Internet...**"***).**
En ese caso, consultar al administrador de la red.

7. GLOSARIO

- **Certificado raíz:** es un certificado auto-firmado o sin firmar un certificado de clave pública que forma una parte importante de la Infraestructura de Clave Publica.

- **Sellado de tiempo:** es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

- **Prestador de servicios de certificación:** Persona física o entidad jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

  Al prestador de servicios de certificación se le conoce también como Autoridad de Certificación (CA) ya que no sólo emite certificados sino que certifica la titularidad de los mismos lo que permite que se establezca la confianza necesaria para intercambiar mensajes entre el emisor y el receptor