FIRMA ELECTRÓNICA EMBEBIDA SOBRE FICHEROS ACROBAT PDF EN LA PLATAFORMA DE NOTIFICAD@S

EXTERNALIZACIÓN DE NOTIFICADOS Y APLICACIONES ONLINE SL
CIF: B85683167 - (+34) 902 570 318 - contacto@notificados.com

VISTA PREVIA

Puede consultar más datos sobre los procesos de **firma electrónica y sellado de tiempo** en el documento incluido en la zona de descargas de la plataforma electrónica de Notificad@s:

Información sobre Procesos de Firma Electrónica y Sellado de Tiempo

informacion_firmaelectronica_notificados.pdf

Como se menciona en dicho documento, así como se puede constatar, los documentos firmados electrónicamente por Notificad@s, son generados con el **certificado electrónico emitido para Notificad@s por la Autoridad Certificadora de la Fábrica Nacional de Moneda y Timbre, FNMT.**

Por defecto, las versiones actuales y anteriores de Acrobat Reader (utilizado como lector mayoritario de ficheros Acrobat PDF) **no incluyen en su lista de Autoridades Certificadoras** a la Fábrica Nacional de Moneda y Timbre, FNMT.

Por ello, para realizar los procesos de validación visual desde el entorno de Acrobat Reader es preciso configurar previamente, una sola vez, el certificado raíz de la Autoridad Certificadora de Notificad@s:

Real Casa de la Moneda - Fábrica Nacional de Moneda y Timbre (www.fnmt.es)

A continuación, se proporciona una guía rápida extraída del Sitio Oficial de Adobe para la validación y verificación de certificados digitales, firmas electrónicas y sellados de tiempo. Visualice detenidamente dicha información para comprender mejor el mecanismo y **revise lo mencionado en el último punto de este documento, para añadir el Certificado Raíz de la Fábrica Nacional de Moneda y Timbre en su aplicación Acrobat Reader.**

GUÍA RÁPIDA PARA LA VALIDACIÓN DE CERTIFICADOS EN FICHEROS PDF

Fuentes obtenidas de Sitio Web Oficial de Adobe (help.adobe.com).

Comprobación de la validez de una firma

De forma predeterminada, las firmas se validan al abrir un PDF. Aparece un icono en el campo de firma de la página del documento para indicar el estado de aquélla. El panel Firmas y el cuadro de diálogo Propiedades de la firma muestran más detalles sobre el estado.

Los controladores de firmas de otros fabricantes pueden proporcionar métodos alternativos para validar las firmas. Compruebe la documentación incluida en el ID digital de otro proveedor.

El icono de firma digital junto con el nombre del campo en el panel Firmas indica la presencia de un campo de firma sin firmar.
El icono de lazo azul  indica que el PDF está certificado; es decir: que contiene una firma de certificación válida. (Las firmas de certificación pueden ser visibles o invisibles.)
El icono de check verde  indica que la firma es válida.
El icono de la **x** roja  indica que la firma no es válida.
El icono del triángulo de precaución  indica que el documento se ha modificado después de la adición de la firma.
El icono de signo de interrogación  indica que la firma no se puede validar porque el certificado de su autor no está en la lista de identidades de confianza.

Si el estado de la firma se desconoce o no está verificado, o si el documento se ha modificado después de firmarlo, valide la firma manualmente para determinar la causa del problema y su posible solución. Si el estado de la firma no es válido (indicado por el icono de la **x** roja), póngase en contacto con su autor para informarle del problema.

Validar una firma manualmente

Puede evaluar la validez de una firma digital comprobando sus propiedades.

1. Establezca sus preferencias de verificación de firmas. Para más información, **consulte Definir preferencias de verificación de firmas.**
2. Abra el PDF que contiene la firma y haga clic en el botón Firmas  situado a la izquierda para abrir el panel Firmas.
3. Seleccione la firma en el panel Firmas y elija Validar firma en el menú Opciones. En Estado de validación de la firma se describe la validez de la firma.
4. Haga clic en Propiedades de la firma y realice una de las acciones siguientes:

- Si se desconoce el estado, haga clic en la ficha Firmante y, a continuación, haga clic en Mostrar certificado para ver los detalles del certificado. Si trabaja con ID digitales con firma personal, confirme que los detalles del certificado son válidos. Si el certificado no es válido, solicite un certificado válido al firmante. Haga clic en Aceptar.
- Haga clic en la ficha Fecha y hora para verificar la marca de hora si es necesario.
- Haga clic en la ficha Legal para obtener más información sobre las restricciones legales de la firma. En la ficha Legal, haga clic en Ver propiedades de integridad del documento para comprobar si el documento es compatible con PDF/SiqQ o si contiene elementos que podrían alterar su aspecto.

Si el documento se ha modificado después de firmarlo, compruebe la versión firmada del documento y compárela con la versión actual.

Definir preferencias de verificación de firmas

Antes de abrir documentos firmados, defina sus preferencias para optimizar la validación de firmas en Acrobat.

1. Elija Edición > Preferencias (Windows) o Acrobat > Preferencias (Mac OS) y seleccione Seguridad en el lado izquierdo.
2. Para validar automáticamente todas las firmas de un PDF al abrir el documento, seleccione Verificar firmas al abrir el documento. Esta opción está activada de manera predeterminada.
3. Haga clic en Preferencias avanzadas y, a continuación, haga clic en la ficha Verificación.
4. Elija las siguientes opciones:

Al verificar

Estas opciones especifican métodos que determinan qué plug-in se debe elegir al verificar una firma. A menudo, el plug-in se selecciona automáticamente. Póngase en contacto con el administrador del sistema para conocer los requisitos de plug-in concretos para validar firmas.

Requerir la comprobación de revocación de certificados al comprobar firmas siempre que sea posible

Seleccione esta opción para requerir la comprobación de los certificados con respecto a una lista de certificados excluidos durante la validación. Si esta opción no está seleccionada, se ignora el estado de revocación de las firmas de aprobación. El estado de revocación siempre se comprueba para las firmas de certificación.

Verificar firmas mediante

Seleccione una opción para determinar si la hora que aparece en la firma digital refleja la hora en que se validó la firma (hora actual), la hora establecida por el servidor de marca de hora predeterminado especificado en la configuración de seguridad, o la hora en que se creó la firma.

Ocultar el icono de validez del campo de firma cuando la firma es válida

Oculta el estado de la firma si ésta es válida, aunque el documento haya cambiado desde que se firmó (lo que se indica con una marca de verificación verde y un icono de triángulo de precaución).

5. Haga clic en la ficha Integración de Windows y especifique si puede importar identidades desde la función Certificados de Windows en la lista de identidades de confianza. Además, especifique si se debe confiar en todos los certificados raíz de la función Certificados de Windows al validar las firmas y los documentos certificados. Tenga en cuenta que al seleccionar estas opciones se puede comprometer la seguridad.

Validar un certificado de marca de hora

Si una firma muestra la fecha y la hora, esa hora es la local en el equipo del autor de la firma. Sin embargo, puede aparecer una segunda fecha y hora en el cuadro de diálogo Propiedades de la firma. Eso indica que el autor de la firma usa un servidor de marca de hora. Para validar una firma que contiene una marca de hora es necesario obtener el certificado del servidor de marca de hora y agregarlo a la lista de identidades de confianza. De lo contrario, la marca de hora aparece en el panel Firmas como no verificada y se debe validar manualmente.

1. Haga clic en el botón Firmas del panel de navegación, seleccione la firma y elija Validar firma en el menú Opciones.

2. Haga clic en el botón Propiedades de la firma en el cuadro de diálogo Estado de validación de la firma.

3. En el cuadro de diálogo Propiedades de la firma, haga clic en la ficha Fecha y hora para ver la autoridad de marcas de hora y, a continuación, haga clic en el botón Mostrar certificado. (Dicho botón aparece en la ficha Fecha y hora sólo si el firmante ha usado un servidor de marca de hora).

4. En el Visor de certificados, haga clic en la ficha Confiar para ver si el certificado de marca de hora es de confianza. Si no es de confianza, haga clic en Agregar identidades de confianza. Si un certificado del servidor de marca de hora no aparece en la lista, pídaselo al autor de la firma.

Determinar el nivel de confianza de un certificado

Puede cambiar la configuración de confianza de los certificados. Por ejemplo, si ha verificado la huella digital incluida en un certificado enviado por otra persona, puede cambiar la configuración para confiar explícitamente en todas las firmas digitales y documentos certificados creados con ese certificado. Puede elegir incluso confiar en el archivo JavaScript incrustado y en el contenido dinámico del documento certificado.

Se deberá confiar explícitamente en un certificado antes de poder utilizarlo para codificar archivos PDF para la persona asociada a dicho certificado. Si dispone de múltiples certificados para una persona, defina niveles de confianza para al menos uno de sus certificados.

También puede confiar en un certificado si el certificado raíz se considera de confianza. El certificado raíz es la autoridad de origen en la cadena de autoridades de certificados que emitieron el certificado. Si confía en el certificado raíz, confía en todos los certificados emitidos por esa autoridad de certificados. Tenga cuidado al confiar en certificados raíces.

1. Elija Avanzadas > Administrar identidades de confianza.
2. Seleccione un contacto y haga clic en Detalles.
3. Seleccione el nombre del certificado y haga clic en Editar Confianza.
4. En la ficha Confianza, seleccione cualquiera de los elementos siguientes para confiar en este certificado:

   Firmas y como una raíz de confianza

   Confía en las firmas de este certificado y confía en el certificado como raíz de confianza para que otros certificados que lo tengan como raíz en una cadena de certificados se consideren también de confianza.

   Documentos certificados

   Confía en documentos que el autor ha certificado con una firma de autor.

   Contenido dinámico

   Confía en películas, archivos de sonido y otros elementos dinámicos.

   JavaScript privilegiado incrustado

   Confía en secuencias de comandos incrustadas.

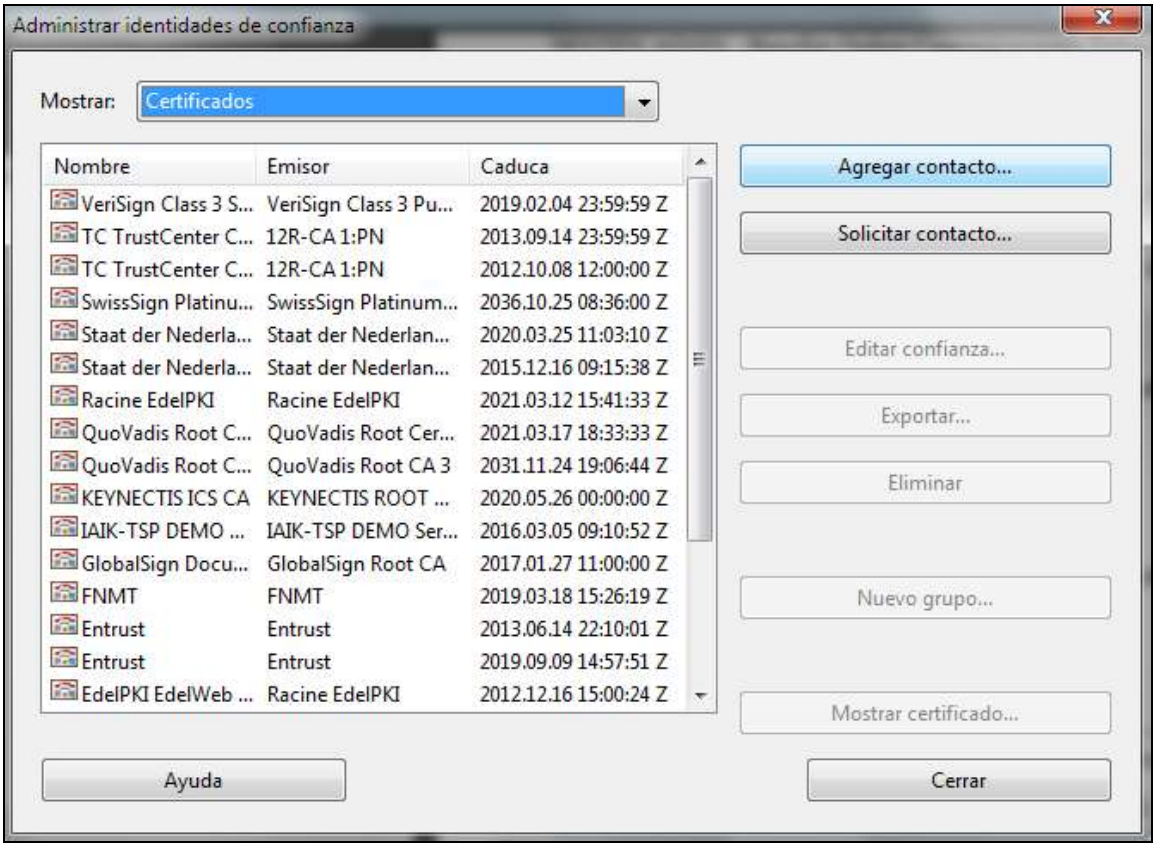
5. Haga clic en Aceptar, haga clic de nuevo en Aceptar y, a continuación, haga clic en Cerrar.

Añadir el certificado raíz de la Fábrica Nacional de Moneda y Timbre en su aplicación Acrobat Reader

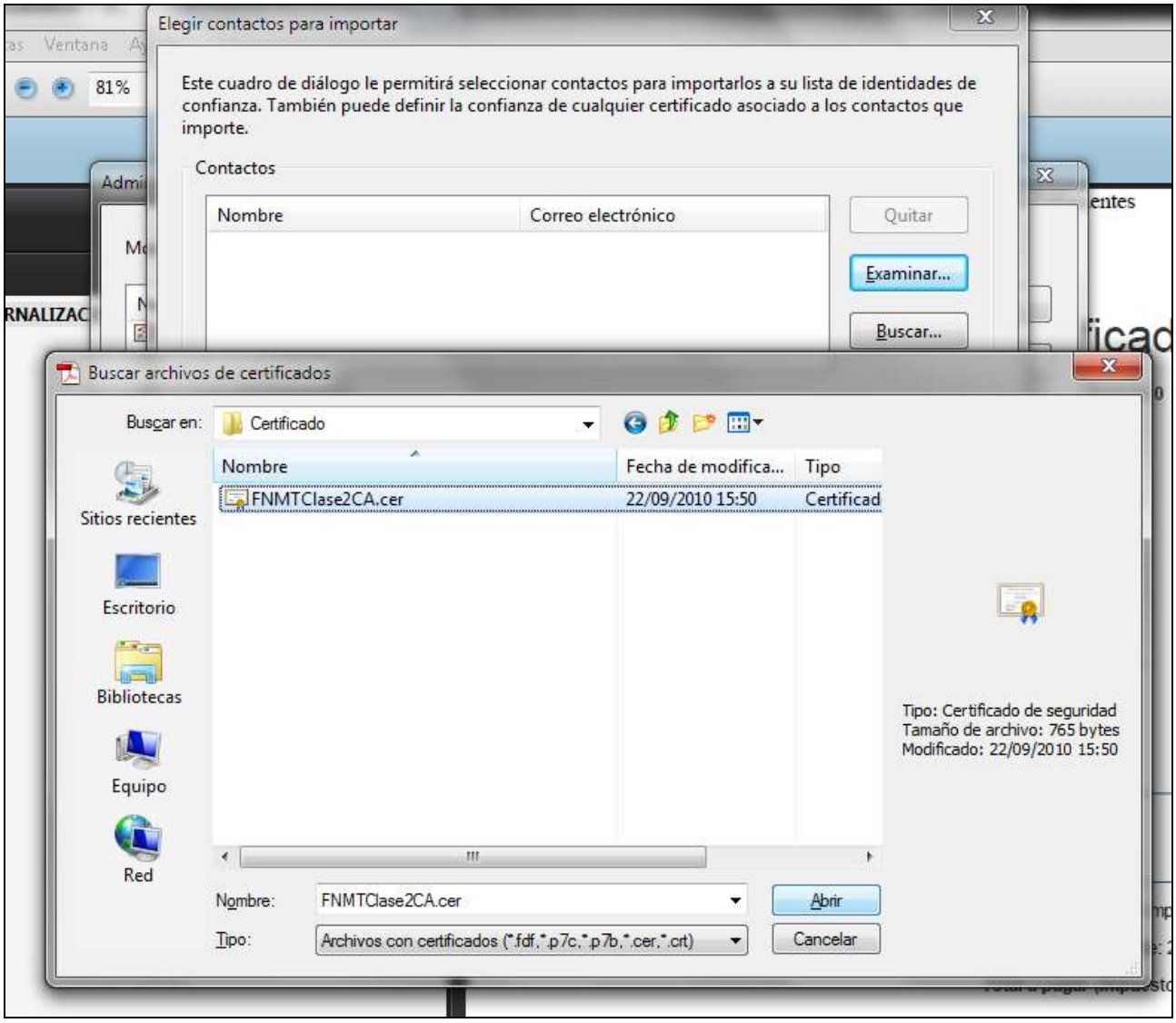
Como hemos visto en el punto anterior, se pueden añadir nuevos certificados raíz y cambiar el nivel de confianza asociado a los mismos. Para validar la firma electrónica embebida en los ficheros PDF firmados electrónicamente por Notificad@s debe realizar el proceso descrito en el punto anterior: "Determinar el nivel de confianza de un certificado".

Para ello, realice los siguientes pasos:

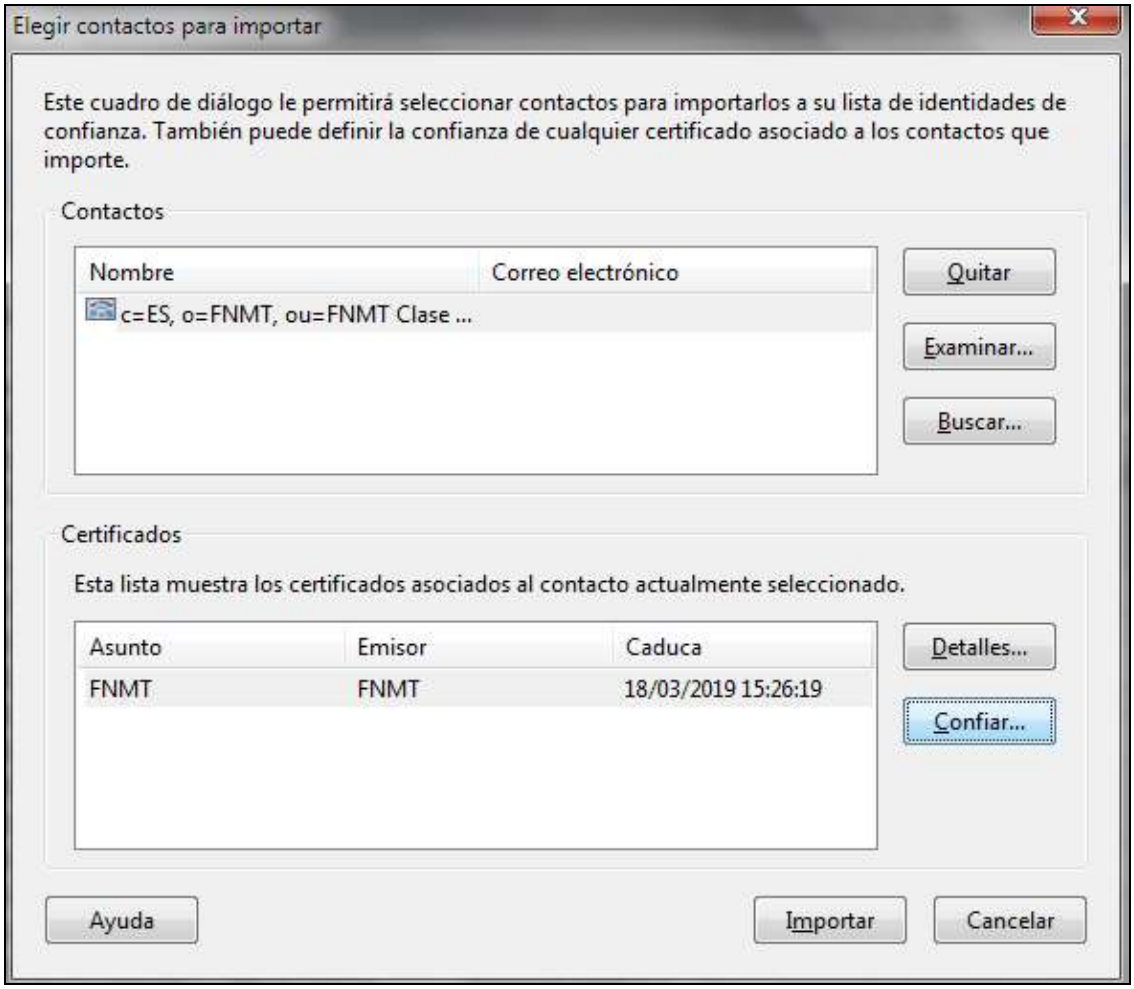
1. Descargue el certificado raíz de la Fábrica Nacional de Moneda y Timbre desde www.fnmt.es o desde el enlace directo: http://www.cert.fnmt.es/content/pages_std/certificados/FNMTClase2CA.cer
2. Instale el certificado que ha descargado.
3. Elija Avanzadas > Administrar identidades de confianza.
4. En la ventana que puede verse en la siguiente figura, seleccione en la lista desplegable "Mostrar": la opción "Certificados" y pulse el botón "Agregar contacto…":



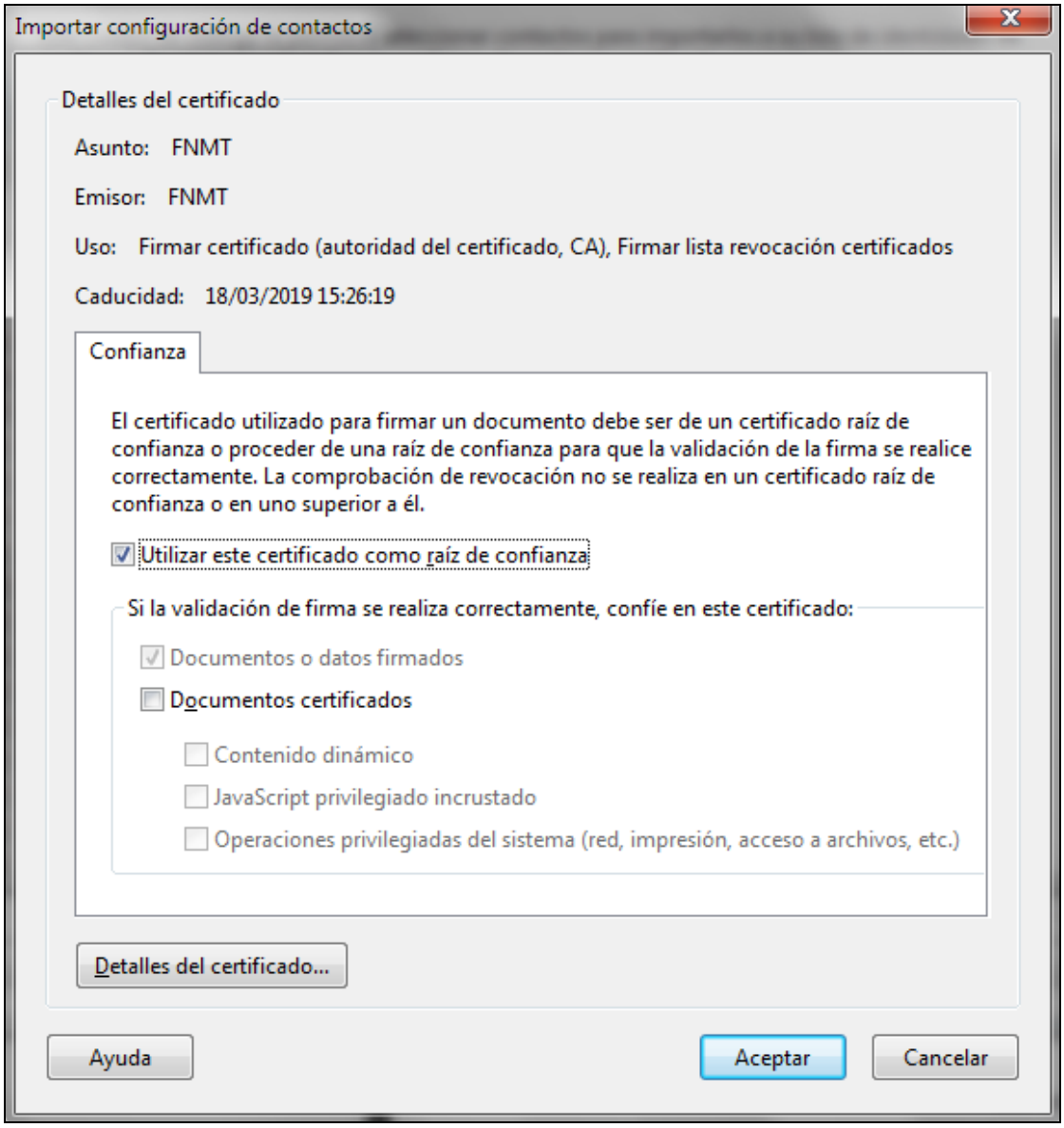
5. En la siguiente ventana, pulse el botón "Examinar…", seleccione el archivo que ha descargado en el punto 1. y pulse el botón "Aceptar":



6. Seleccione el certificado que acaba de abrir, y pulse en el botón "Confiar…":



7. Marque la casilla de verificación: "Utilizar este certificado como raíz de confianza" y pulse el botón "Aceptar", cuando se cierre la ventana, pulse el botón "Importar" (de la ventana del proceso 6) para terminar de importar el certificado raíz de la Fábrica Nacional de Moneda y Timbre:



Una vez completados estos sencillos pasos, podrá visualizar correctamente los documentos firmados electrónicamente por Notificados mediante el certificado electrónico emitido por la Fábrica Nacional de Moneda y Timbre.

Si usted decide co-firmar los documentos de envío de burofax desde la plataforma de Notificad@s, puede repetir esta operación para la Autoridad Certificadora que haya emitido su certificado electrónico con el cuál realiza el proceso de firma electrónica.

En dicho caso, si su certificado electrónico proviene de la Fábrica Nacional de Moneda y Timbre, no es necesario realizar este paso de nuevo; en caso contrario, contacte con su Autoridad Certificadora para que le de instrucciones de descarga de su certificado raíz y realice el proceso tal y como se ha indicado, reemplazando el certificado raíz de la Fábrica Nacional de Moneda y Timbre por el certificado raíz de su Autoridad Certificadora.