Manual Instrucciones Firma Digital

INDICE

1 INTRODUCCIÓN

El presente documento es una guía para la correcta configuración en los navegadores Internet Explorer (IE en adelante), Firefox y Chrome, para poder utilizar los servicios de uso de la firma digital, para verificación y firma de solicitudes dentro de CDTI.

2 JAVA

El Cliente de Firma es una herramienta de Firma Electrónica que funciona en forma de Applet de Java integrado en una página Web mediante JavaScript

El Cliente de Firma, como su nombre indica, es una aplicación que se ejecuta en cliente (en el ordenador del usuario, no en el servidor Web). Esto es así para evitar que la clave privada asociada a un certificado tenga que "salir" del contenedor del usuario (tarjeta, dispositivo USB o navegador) ubicado en su PC. De hecho, nunca llega a salir del navegador, el Cliente le envía los datos a firmar y éste los devuelve firmados.

2.1 INSTALACION O ACTUALIZACION DE UNA VERSION EXISTENTE DE JAVA

(1) Abra Internet Explorer.
(2) Vaya a Java.com.
(3) Puntee o haga clic en el botón de descarga gratuita de Java y, a continuación, en Aceptar e iniciar la descarga gratuita. Si se le solicita proporcionar una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.
(4) En la barra de notificación, puntee o haga clic en Ejecutar. Si se le solicita proporcionar una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.
(5) Puntee o haga clic en Instalar y después en Cerrar.

2.2 ACTIVACION DE JAVA EN LOS NAVEGADORES

Internet Explorer

1. Haga clic en **Herramientas** y, a continuación en **Opciones de Internet**
2. Seleccione el separador **Seguridad** y pulse el botón **Nivel personalizado**
3. Busque **Automatización de los applets de Java**
4. Seleccione el botón de radio **Habilitar**
5. Haga clic en **Aceptar** para guardar sus preferencias

Firefox

1. Inicie el explorador Mozilla Firefox o reinícielo si ya se estaba ejecutando

2. En la parte superior del explorador, seleccione el botón **Firefox** (o el menú **Herramientas** en Windows XP) y **Complementos**
   Se abrirá el separador del administrador de complementos.
3. En el separador del administrador de complementos, seleccione **Plugins**
4. Haga clic en el plugin **Java (TM) Platform** para seleccionarlo
5. Haga clic en el botón **Activar** (si aparece el botón **Desactivar**, Java ya está activo)

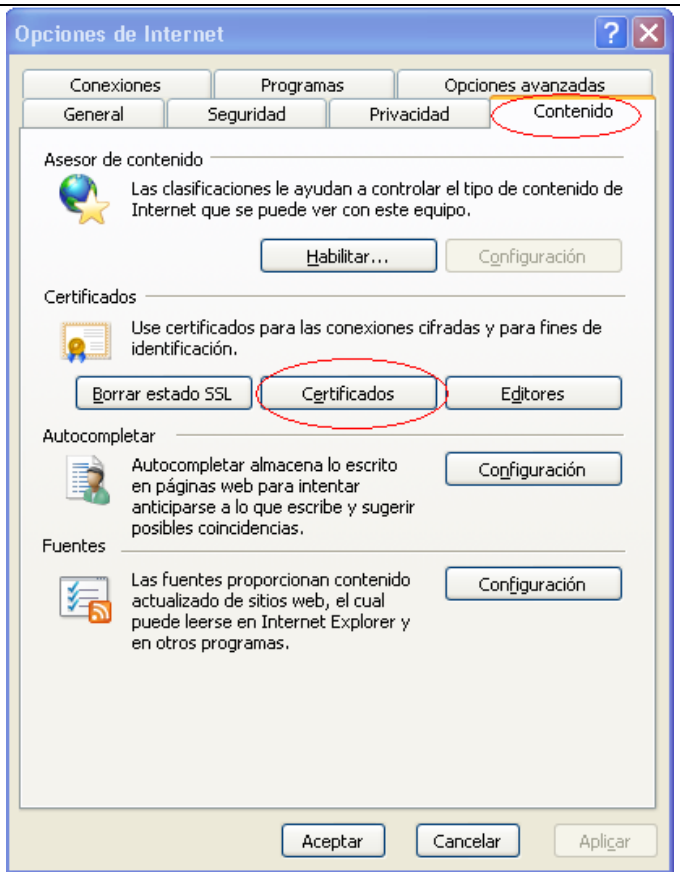
3 INTERNET EXPLORER

3.1 CA

Lo primero que deberemos comprobar es si tenemos instaladas las CAs (ACs en castellano) correctamente, la aplicación actual soporta certificados emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT desde ahora) y el DNI-e.

Abrimos IE y seleccionamos el menú de **herramientas**, realizamos clic sobre la operación **Opciones de Internet**, elegimos el tab **contenido**, hacemos clic sobre el botón **Certificados**.

Internet Explorer 7.0



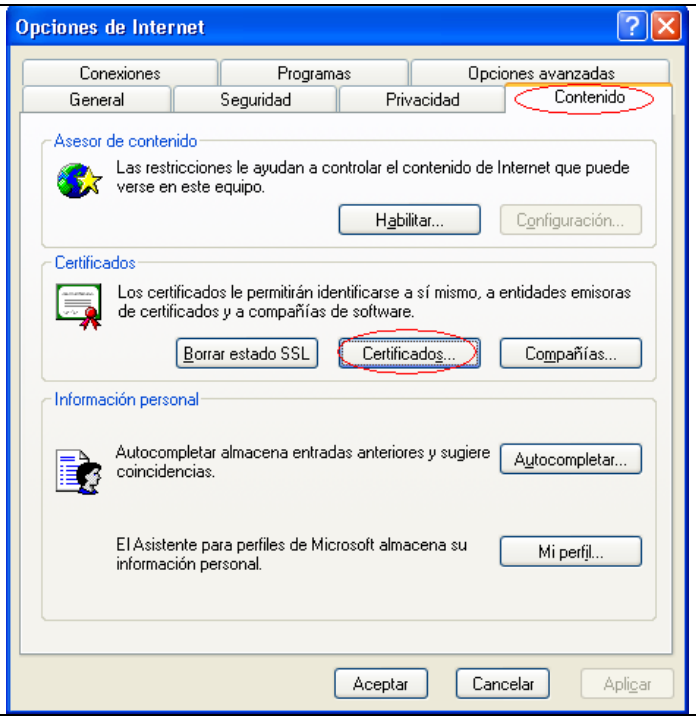
Internet Explorer 6.0	

Fig 2

3.1.1 FNMT

Si el certificado a usar ha sido emitido por la FNMT, a partir del paso 3**.1**, tendremos que ir al tab **Entidades emisoras raíz de confianza**, y buscar en la columna **Emitido para**, el texto **FNMT Clase 2 CA**, en caso de no encontralo, tendremos que descargar la CA del portal de la FNMT CERES, en la siguiente url:

http://www.cert.fnmt.es/index.php?cha=cit&sec=4&page=139&lang=es, una vez en la página buscar el enlace **Descarga del Certificado Raíz FNMT. Certificado de Usuario.**

Instalamos el certificado descargado y verificamos, realizando los pasos anteriores que ahora sí nos aparece el certificado **FNMT Clase 2CA** disponible, realizamos un doble clic sobre dicho certificado, vamos a la pestaña **Detalles,** hacemos clic sobre el botón **Modificar propiedades** (ver Fig. 3), en la pestaña **General**, en la región **Propósitos del certificado**, debemos tener elegida la opción **Habilitar todos los propósitos para este certificado** (ver Fig 4) aceptamos pulsando sobre botón **Aceptar**, aceptando o cerrando según proceda todas las pantallas hasta llegar a la ventana de **Opciones de internet**.

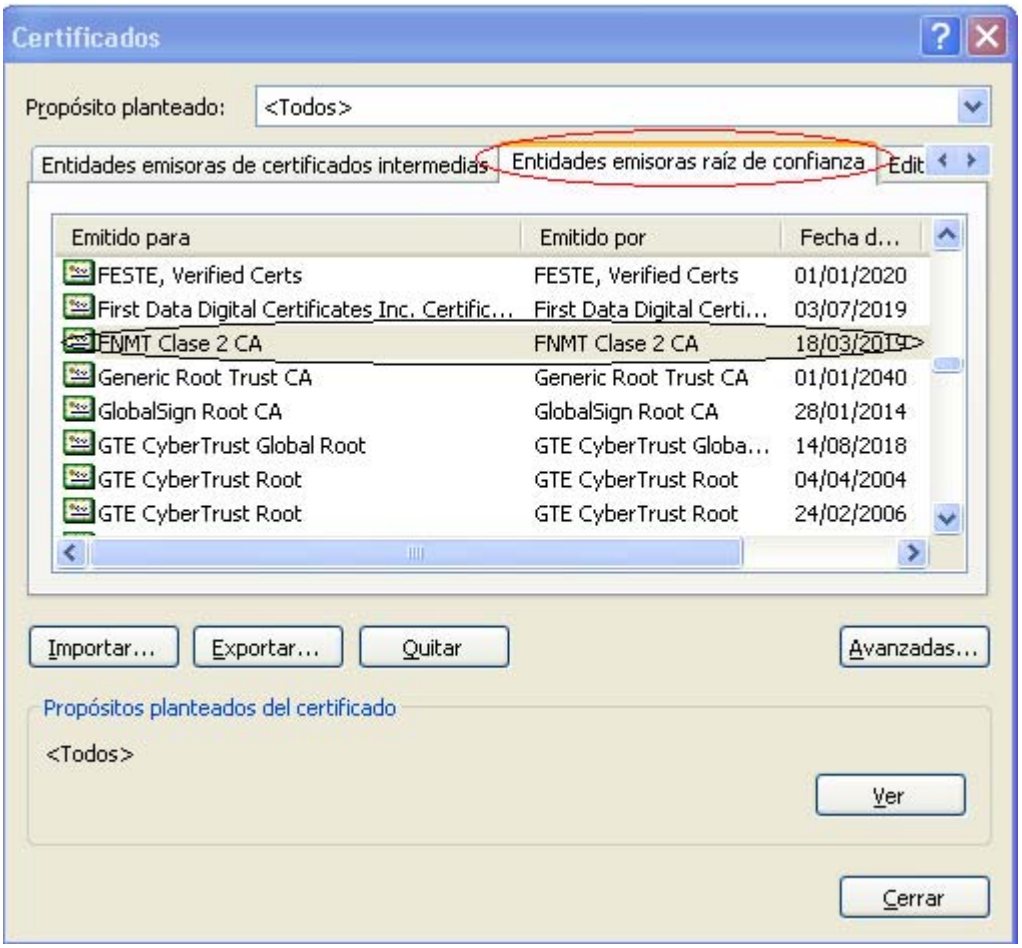

Certificados
Propósito planteado:
<Todos>
Entidades emisoras de certificados intermedias
Entidades emisoras raíz de confianza
Edit
Emitido para
Emitido por
Fecha d...
FESTE, Verified Certs
FESTE, Verified Certs
01/01/2020
First Data Digital Certificates Inc. Certific...
First Data Digital Certi...
03/07/2019
FNMT Clase 2 CA
FNMT Clase 2 CA
18/03/2019
Generic Root Trust CA
Generic Root Trust CA
01/01/2040
GlobalSign Root CA
GlobalSign Root CA
28/01/2014
GTE CyberTrust Global Root
GTE CyberTrust Globa...
14/08/2018
GTE CyberTrust Root
GTE CyberTrust Root
04/04/2004
GTE CyberTrust Root
GTE CyberTrust Root
24/02/2006
Importar...
Exportar...
Quitar
Avanzadas...
Propósitos planteados del certificado
<Todos>
Ver
Cerrar

Fig. 3

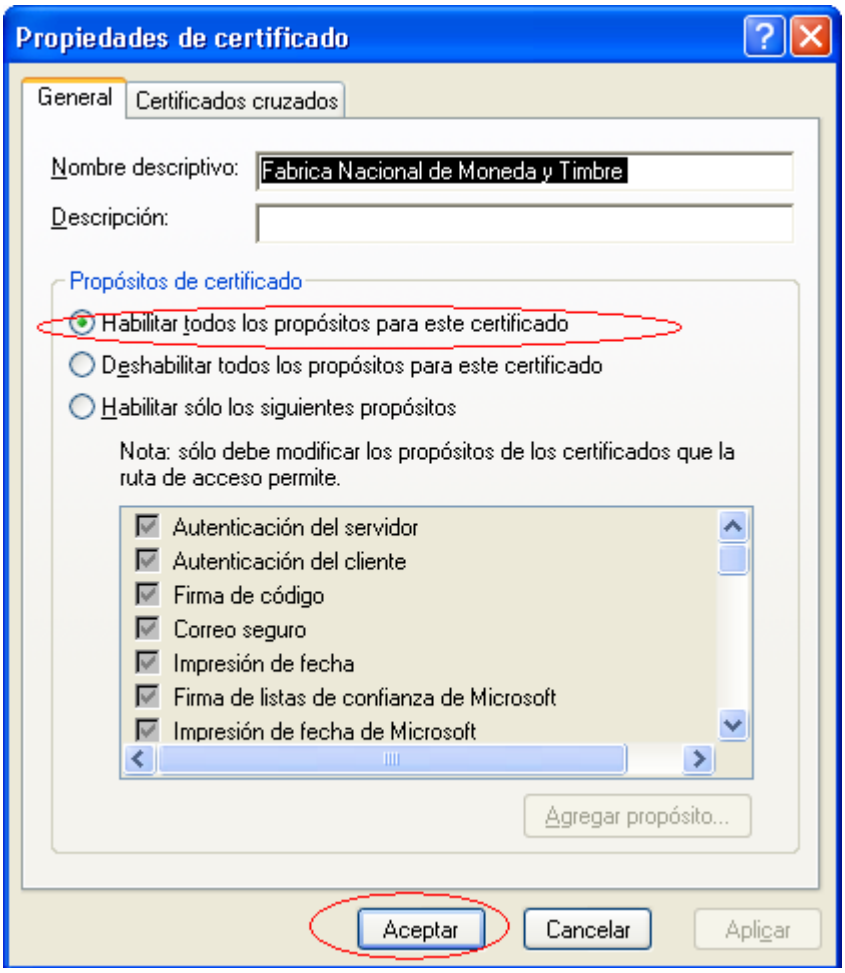


Fig 4

3.1.2 DNI-e

Si el certificado a usar ha sido emitido por la DNIe, a partir del paso 3**.1**, tendremos que ir al tab **Entidades emisoras raíz de confianza**, buscar en la columna **Emitido para**, el texto **AZ RAIZ DNIE**, en caso de no encontrarlo, tendremos que descargar la CA del portal del DNI electrónico, en la siguiente url:

http://www.dnielectronico.es/seccion_integradores/autoridades_cert.html, una vez en la página descargar el Certificado **pkcs1-sha1WithRSAEncryption**.

Cambiamos de tab al de las **Entidades emisoras de certificados intermedias**, buscar en la columna **Emitido para**, el texto **AC DNIE 001**, en caso de no encontrarlo, tendremos que descargar la CA subordinada del portal del DNI electrónico, en la siguiente url:

http://www.dnielectronico.es/seccion_integradores/auto_cert_sub.html, una vez en la página buscar la sección **Autoridad de Certificación Subordinada 001**, descargar el certificado **pkcs1-sha1WithRSAEncryption**.

En ambos casos instalaremos el certificado descargado y realizaremos por cada certificado instalado un doble clic sobre dicho certificado, vamos a la pestaña

Detalles, hacemos clic sobre el botón **Modificar propiedades**, en la pestaña **General**, en la región **Propósitos del certificado**, debemos tener elegida la opción **Habilitar todos los propósitos para este certificado,** aceptamos pulsando sobre botón **Aceptar**, aceptando o cerrando según proceda todas las pantallas hasta llegar a la ventana de **Opciones de internet**.

4 FIREFOX

4.1 CA

En caso de que pueda acceder a la página de firma del aplicativo y le aparezcan sus datos personales en dicha página no debería tener mayor problema para realizar el proceso de firma.

En caso de que no le aparezca su certificado personal instalado como disponible cuando acceda a la parte del aplicativo que requiere del certificado digital o directamente la pantalla indica un error informando que se requiere de un certificado válido, compruebe primero que tiene correctamente instaladas las CAs correspondientes y que tiene habilitados todos los propósitos siguiendo las siguientes instrucciones.

Cuando se esté usando Firefox lo primero que deberemos comprobar es si tenemos instaladas las CAs (ACs en castellano) correctamente, la aplicación actual soporta certificados emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT desde ahora) y el DNI-e.

Abrimos Firefox y seleccionamos el menú de **herramientas**, realizamos clic sobre la operación **Opciones...**, elegimos el icono **Avanzado**, hacemos clic sobre el tab **Cifrado**, en la sección **Certificados**, pulsamos sobre el botón **Ver certificados** (ver Fig 5).

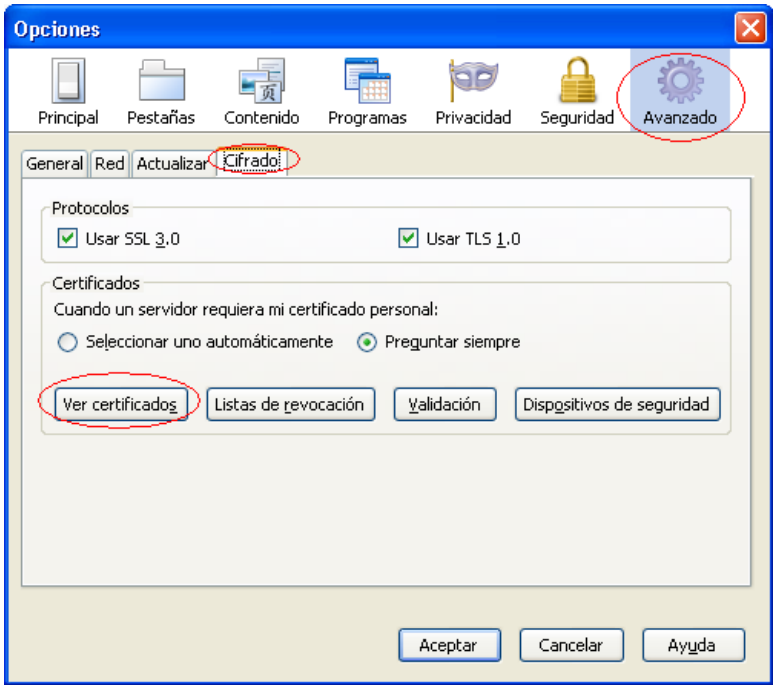


Fig. 5

4.1.1 FNMT

Si el certificado a usar ha sido emitido por la FNMT, a partir del paso **3.1**, tendremos que ir al tab **Autoridades**, y buscar en la columna **Nombre del certificados**, el texto **FNMT** y dentro de este **Fábrica Nacional de Moneda y Timbre** (ver Fig.6), en caso de no encontrarlo, tendremos que descargar la CA del portal de la FNMT CERES, en la siguiente url:

http://www.cert.fnmt.es/index.php?cha=cit&sec=4&page=139&lang=es, una vez en la página buscar el enlace **Descarga del Certificado Raíz FNMT. Certificado de Usuario.**

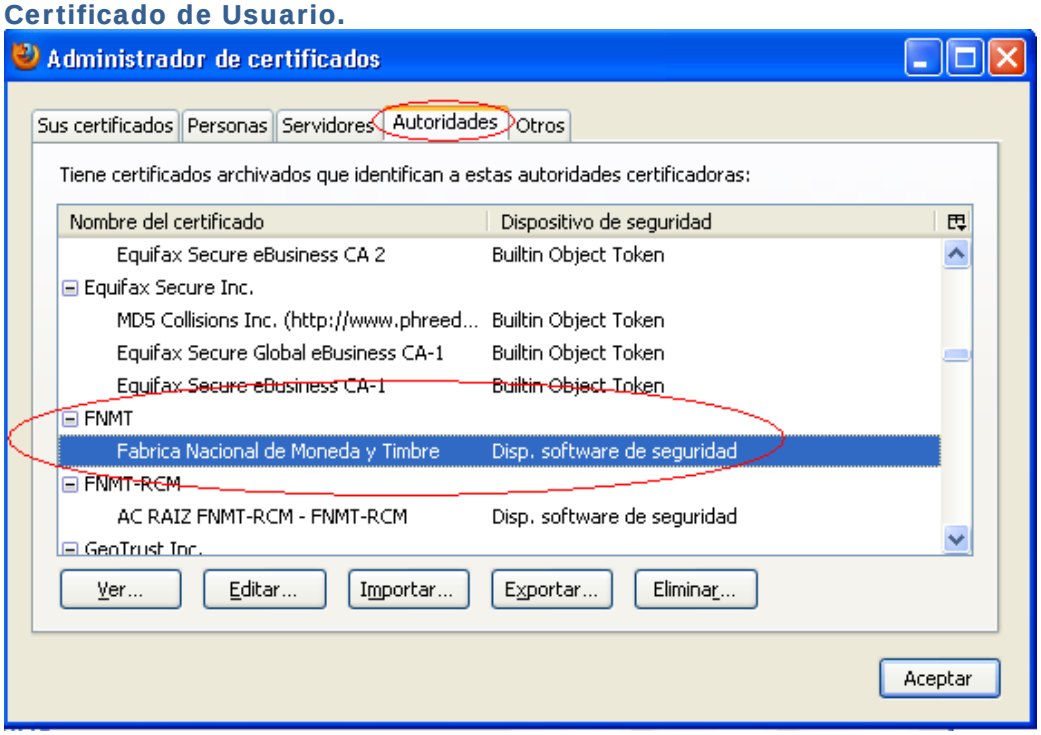


Fig 6

Instalamos el certificado descargado marcando que se quiere confiar en la CA todos los propósitos (ver Fig. 7) y verificamos, realizando los pasos anteriores que ahora sí nos aparece el certificado **FNMT** disponible.

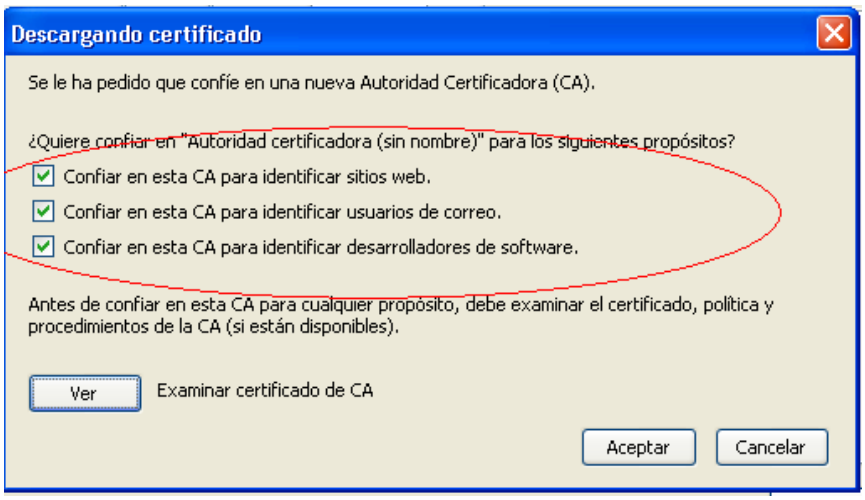


Fig. 7

4.1.2 DNI-e

Si el certificado a usar ha sido emitido por la DNIe, tenemos que tener instalada la CA raíz y la CA subordinada. A partir del paso **3.1** tendremos que ir al tab **Autoridades**, y buscar en la columna **Nombre del certificados**, el texto **DIRECCION GENERAL DE LA POLICIA**, y dentro de este **AZ RAIZ DNIE** (ver Fig.8), en caso de no encontrarlo, tendremos que descargar la CA del portal del DNI electrónico, en la siguiente url:

http://www.dnielectronico.es/seccion_integradores/autoridades_cert.html, una vez en la página descargar el Certificado **pkcs1-sha1WithRSAEncryption**.

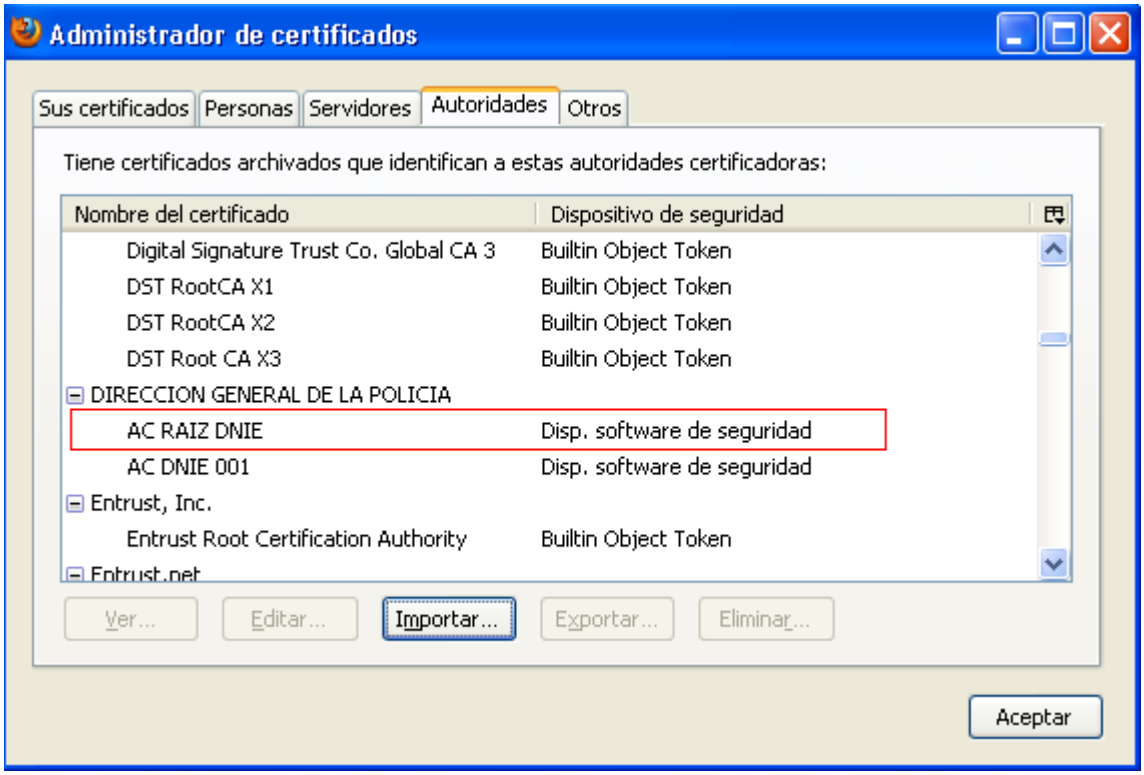


Fig. 8

Otra vez dentro de la pestaña **Autoridades**, y buscamos en la columna **Nombre del certificado**, el texto **DIRECCION GENERAL DE LA POLICIA**, y dentro de este **AZ DNIE 001 (**Ver Fig.9), en caso de no encontrarlo, tendremos que descargar la CA subordinada del portal del DNI electrónico, en la siguiente url:

http://www.dnielectronico.es/seccion_integradores/auto_cert_sub.html, una vez en la página buscar la sección **Autoridad de Certificación Subordinada 001**, descargar el certificado **pkcs1-sha1WithRSAEncryption**.

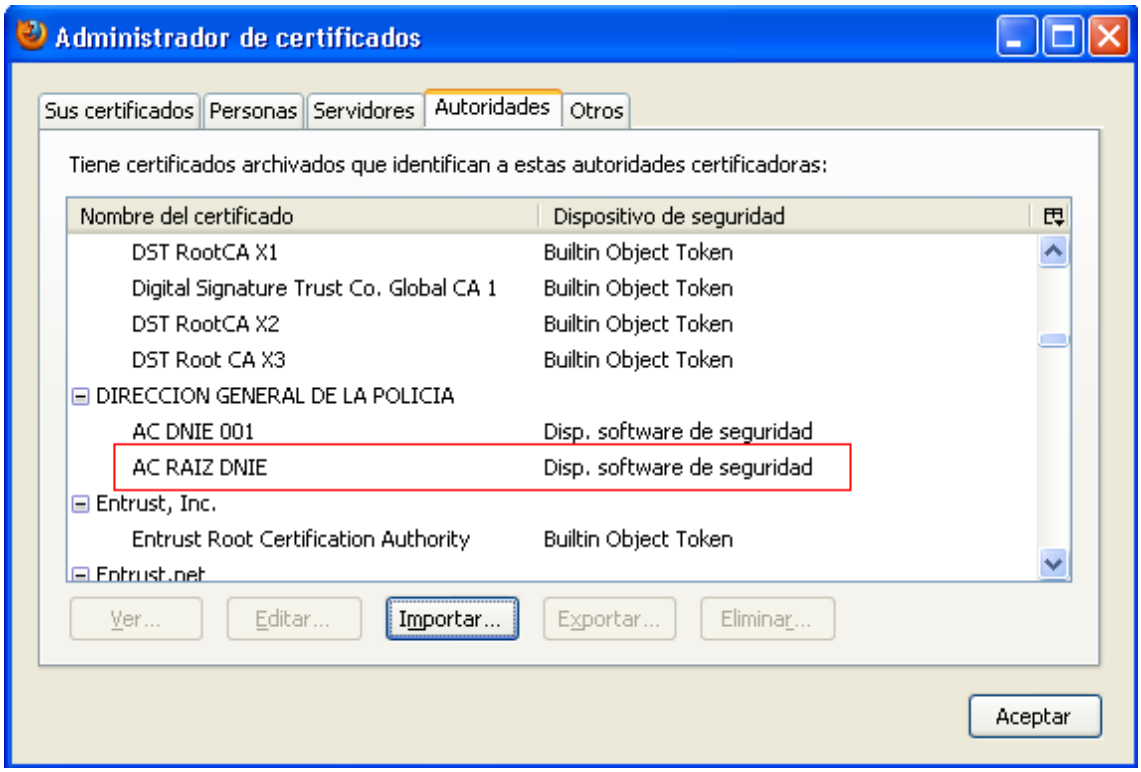


Fig.9

En ambos casos instalaremos el certificado descargado y marcaremos por cada certificado descargado todos los propósitos (ver Fig.10).

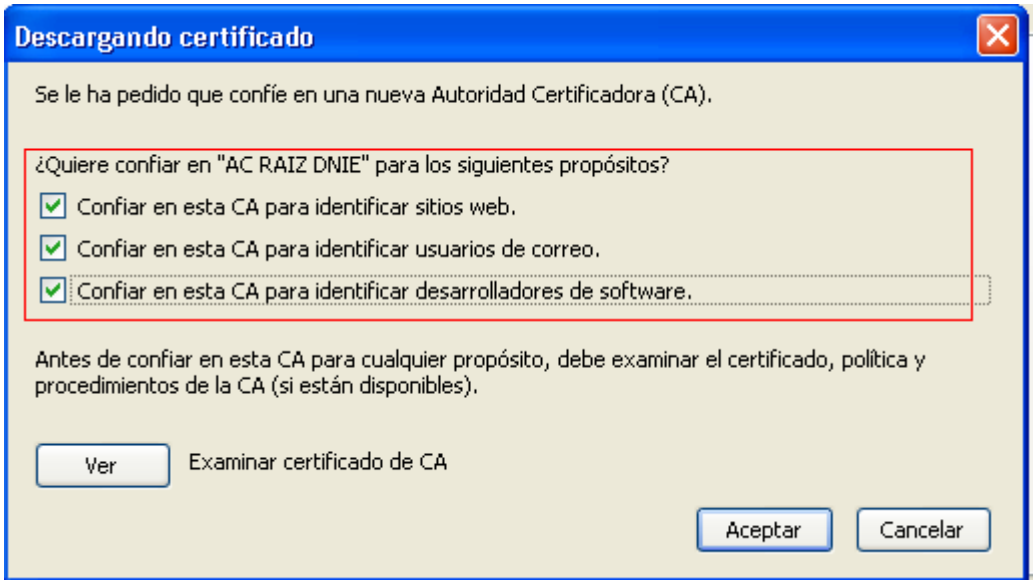


Fig.10

Cerraremos el navegador y volveremos a la página de firma de aplicativo, comprobando que ya no tenemos problemas en la firma.

5 CHROME

El navegador CHROME utiliza la configuración de certificados de Microsoft Windows, por lo que la configuración de estos es externa al navegador. Para poder acceder a dicha configuración debemos escribir **"certmgr.msc"** en la consola de Windows.

Si Internet Explorer ya tiene configurado los certificados, el navegador Chrome hará uso de ellos sin tener que realizar configuración alguna.

6 VERIFICACION DE FIRMA EN LA WEB DE CDTI

Después de realizar la validación del usuario en el área privada de la web de Gestión de Ayudas – Área privada, podemos verificar si la configuración del navegador es idónea para la utilización de la firma digital, para ello debemos hacer click en la opción "Prueba Firma" del menú que se encuentra en la parte superior derecha de la web (Figura 13).

Fig.13

Al seleccionar esta opción se debe abrir una ventana emergente, como la que se muestra en la figura 14, donde debemos presionar en la el boton continuar, accion que abrirá una nueva ventana.

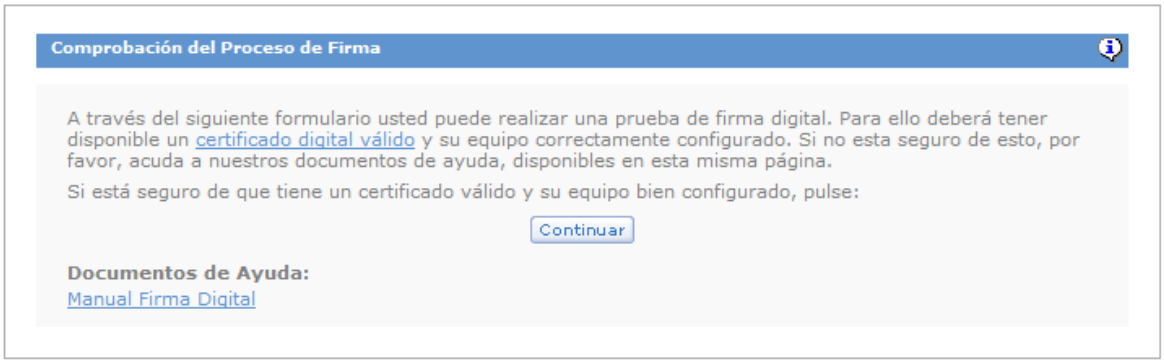


Fig.14

Antes de abrirse la ventana, como la que se muestra en en la figura 16, el navegador puede que muestre un mensaje (figura 15) donde se nos comunica que la web va a acceder a nuestra firma digital, para poder continuar debemos chequear la opción "aceptar …" y luego el botón "Ejecutar".

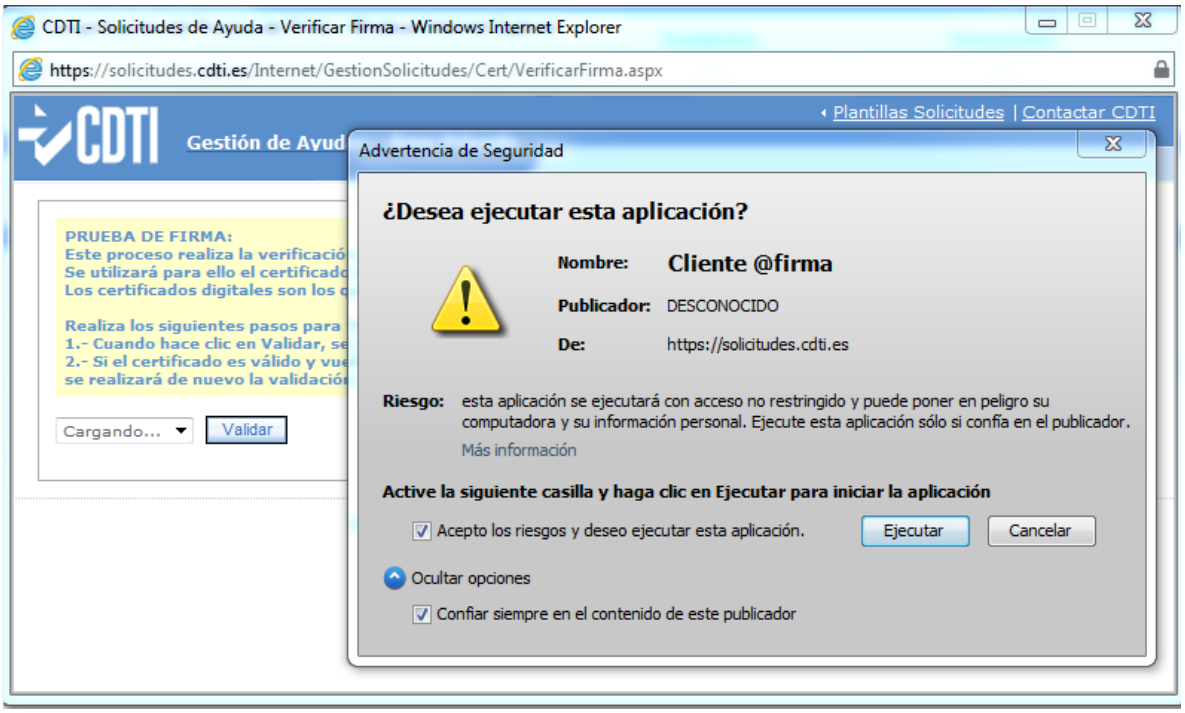


Fig.15

En la siguiente pantalla, primero deberemos elegir el certificado digital en la lista desplegable y luego presionar en el boton "**Validar**" para realizar la comprobacion de la firma, una vez validada la firma, permitirá firmar, para lo cual presionar el botón "**Firmar**".

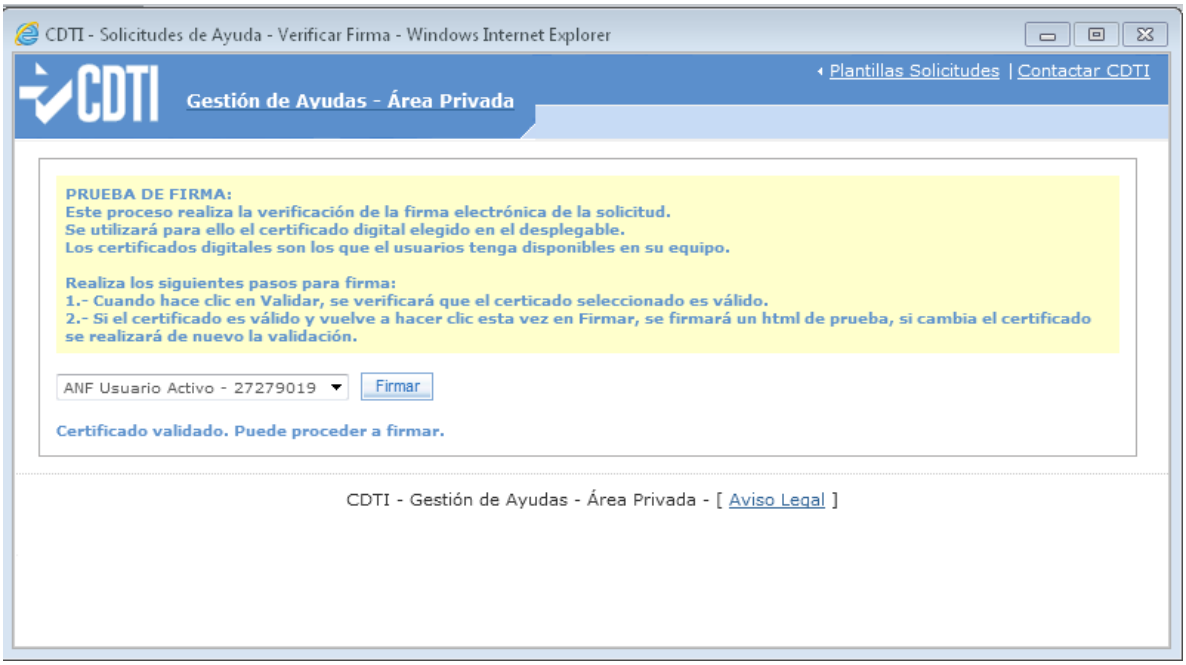


Fig.16

Antes de llevarse a cabo la prueba del certificado digital, el sistema nos informa que la prueba será realizada sobre un archivo temporal, después en la ventana (figura 17) debemos presionar el boton ***Firmar.*** El sistema nos muestra otro mensaje donde se nos comunica que firmará un archivo temporal para la prueba, donde aceptaremos el mensaje y la prueba comenzará.

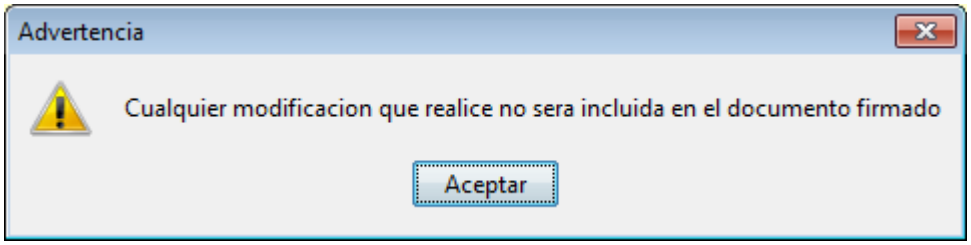


Fig.17

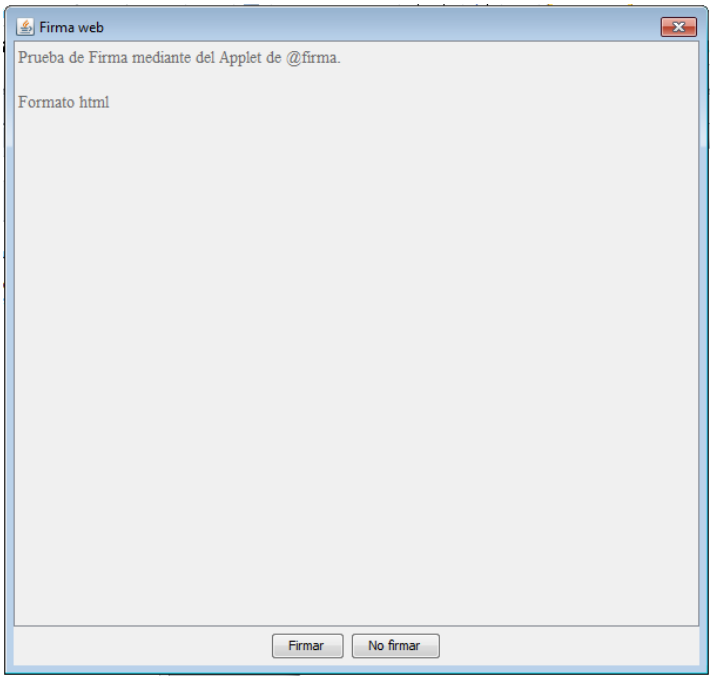


Fig.18

Una vez realizada la prueba el sistema volverá a abrir la ventana de firma y nos comunicará el resultado de la misma (Figura 19)

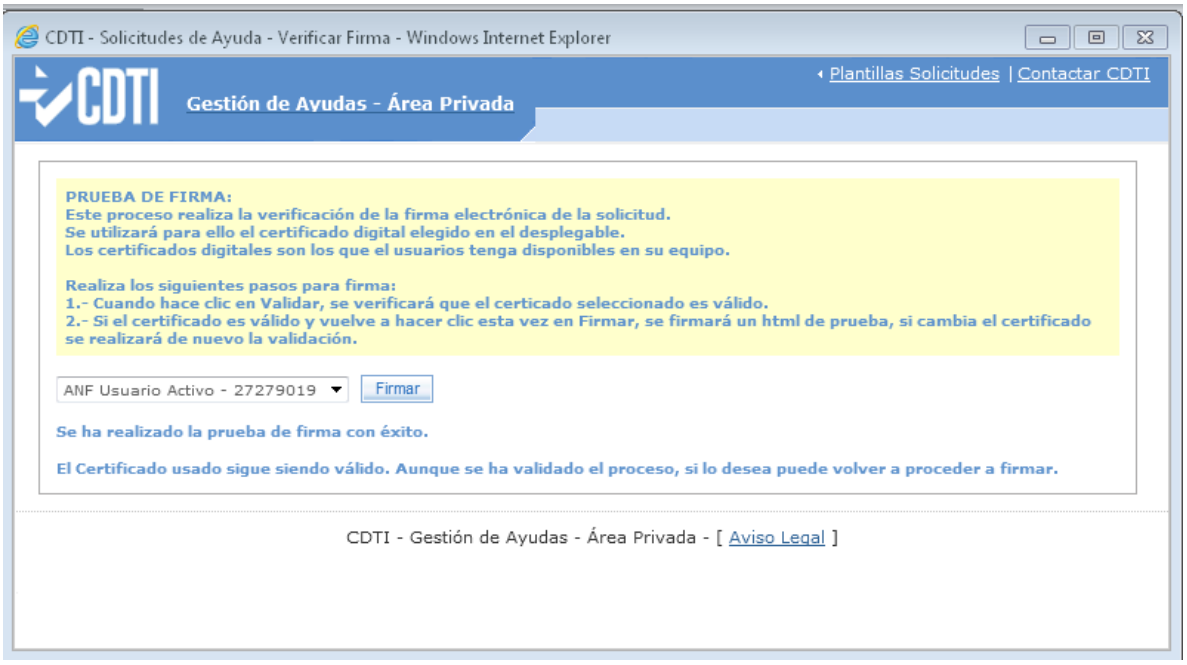


Fig.19

6.1 SOLUCION DE PROBLEMAS

6.1.1 El contenido de la ventana que se ha abierto no es el correcto.

En el caso de que el contenido de la ventana que se ha abierto no sea el correcto y en su lugar haga referencia a Java, como se puede ver en la figura 20, se debe a

que Java no se encuentre instalado en el ordenador o este desactualizado. Para ello debemos seguir los pasos que se explican en el paso 4 de esta guía.

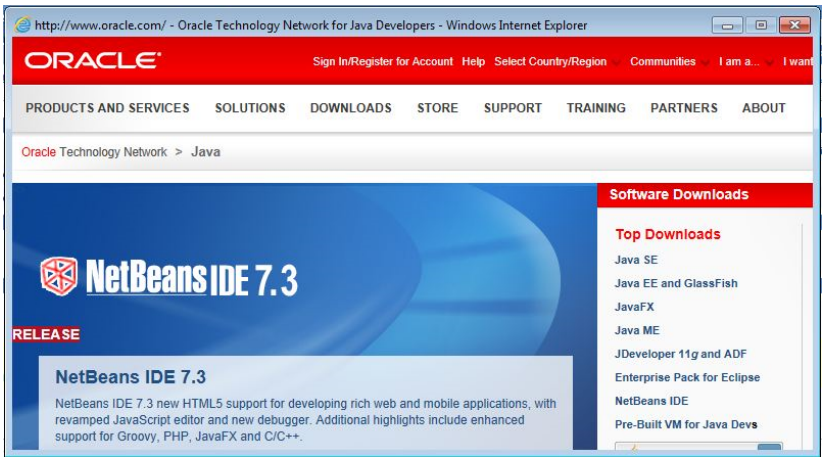


Fig.20

6.1.2 Aceptar los avisos de carga de aplicaciones

En ciertas versiones del navegador, por ejemplo Internet Explorer 8, el comportamiento de la carga de la página puede llegar a ser inestable al cargar applets (aplicativos que se ejecutan en el navegador), puede que se produzcan errores del siguiente tipo (Fig.21) al pulsar sobre el botón firmar:

Fig.21

En dichas situaciones, se debe confiar en el publicador (Fig.22), activando la casilla “Confiar siempre en el contenido de este publicador” y pulsando sobre el botón <Sí>

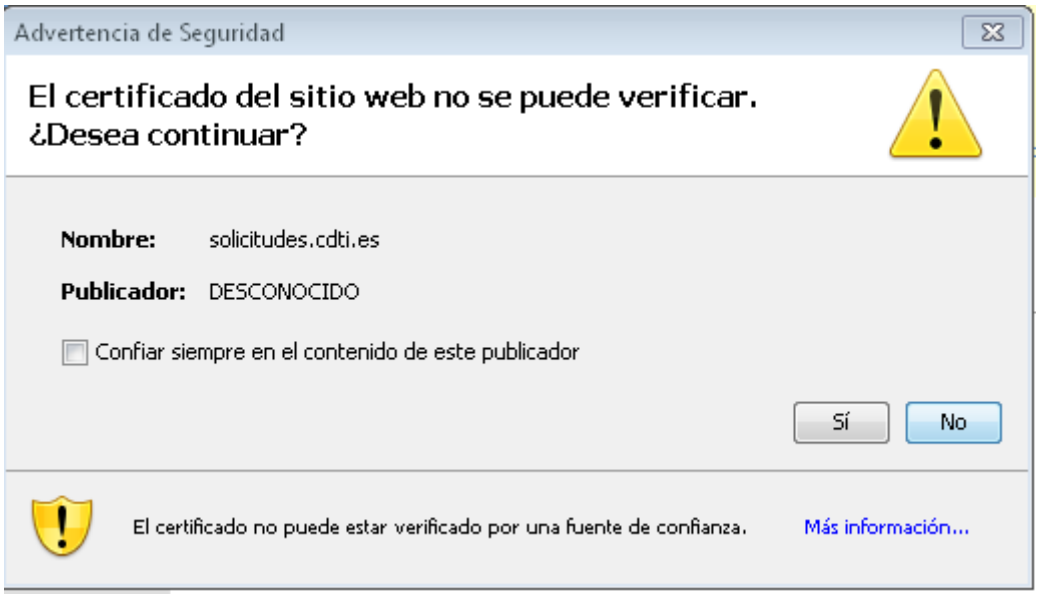


Fig.22

Cuando le aparezca la advertencia de seguridad sobre el uso del applet con nombre "Cliente @firma" (Fig.23), deberá activar los 2 casillas (una de ellas sólo aparecerá cuando expanda las opciones al final del aviso) y hacer clic sobre el botón <Ejecutar> para confirmar.

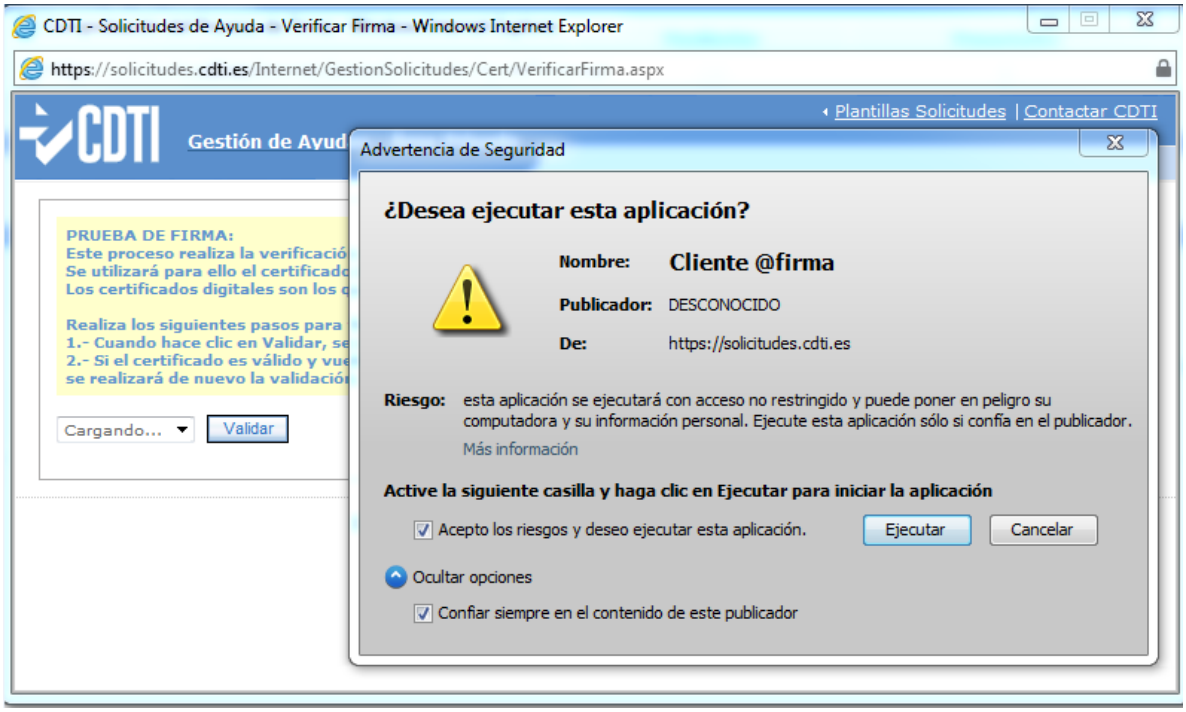


Fig.23