



---

## **Juegos Escolares**

**Ayuda para la obtención de un  
Certificado de la Fábrica  
Nacional de Moneda y Timbre  
y su Instalación**

---

**Manual de Usuario**

### ORIGEN DEL DOCUMENTO

AUTOR	UNIDAD	DIVISIÓN

### HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	CAMBIOS

### REVISIÓN Y APROBACIÓN

COMPAÑÍA	NOMBRE	FECHA	FIRMA
AST			

## INDICE

<b>1 INTRODUCCIÓN .....</b>	<b>4</b>
<b>2 OBTENER UN CERTIFICADO DIGITAL PARA GESTIONES ONLINE .....</b>	<b>5</b>
2.1.1 Solicitud.....	5
2.1.2 Identificación .....	8
2.1.3 Descarga e instalación.....	8
<b>3 INSTALACIÓN DEL CERTIFICADO .....</b>	<b>10</b>
<b>3.1 PANTALLA DE ACCESO .....</b>	<b>10</b>
3.1.1 Lector criptográfico .....	10
3.1.2 Tarjetas Criptográficas.....	10
3.1.3 Certificados Raíz.....	12
3.1.4 Java Runtime Environment (JRE).....	15
3.1.5 Permisos .....	15
3.1.6 Navegador.....	15
<b>3.2 INSTALACIÓN .....</b>	<b>15</b>
3.2.1 Instalación en MS IExplorer.....	15
3.2.2 Instalación en Firefox.....	18

# 1 INTRODUCCIÓN

El siguiente documento describe como obtener un Certificado de la Fábrica Nacional de Moneda y Timbre y su instalación.

## 2 OBTENER UN CERTIFICADO DIGITAL PARA GESTIONES ONLINE

Obtener un certificado digital es el paso previo para realizar gestiones online con la Administración y otras empresas.

Hay que tener muy claro que la obtención del certificado va ligado con el ordenador y el navegador desde el que se haga la solicitud.

El proceso consta principalmente de tres fases:

- 1.- Solicitud a la entidad encargada de otorgarlo, en la página de dicha entidad.
- 2ª.- Identificación frente al Estado de forma presencial para acreditar los datos y firma de puño y letra.
- 3ª.- Descarga e instalación del certificado en el ordenador y navegador desde dónde se hizo la solicitud. También desde la página de dicha entidad.

### 2.1.1 Solicitud

Para España hay que acceder a la página de la [Fábrica Nacional de Moneda y Timbre](http://www.cert.fnmt.es/) (<http://www.cert.fnmt.es/>):

The screenshot shows the CERES website interface. At the top, there are navigation links: Mapa, Contacto, Enlaces, Legislación, and Noticias. Below this, there are two main buttons: 'Obtenga el CERTIFICADO DE USUARIO CON SU DNIe' and 'Obtenga el CERTIFICADO DE USUARIO'. A menu bar contains links for 'Qué es CERES', 'Ciudadanos', 'Empresas', and 'Adm. Pública'. The main content area features the Real Casa de la Moneda logo and a welcome message: 'BIENVENIDO' followed by a paragraph about the factory's role in digital certification. There are also sections for 'Ahora en Internet', 'DONDE USAR EL CERTIFICADO', and 'Buenas Prácticas en el uso del certificado'. A sidebar on the right contains information about the VII edition of the Jornadas Ceres and details about the FNMT-RCM's services.

Pulsar sobre el botón Ciudadanos y luego sobre el enlace **“Obtener el certificado”**.

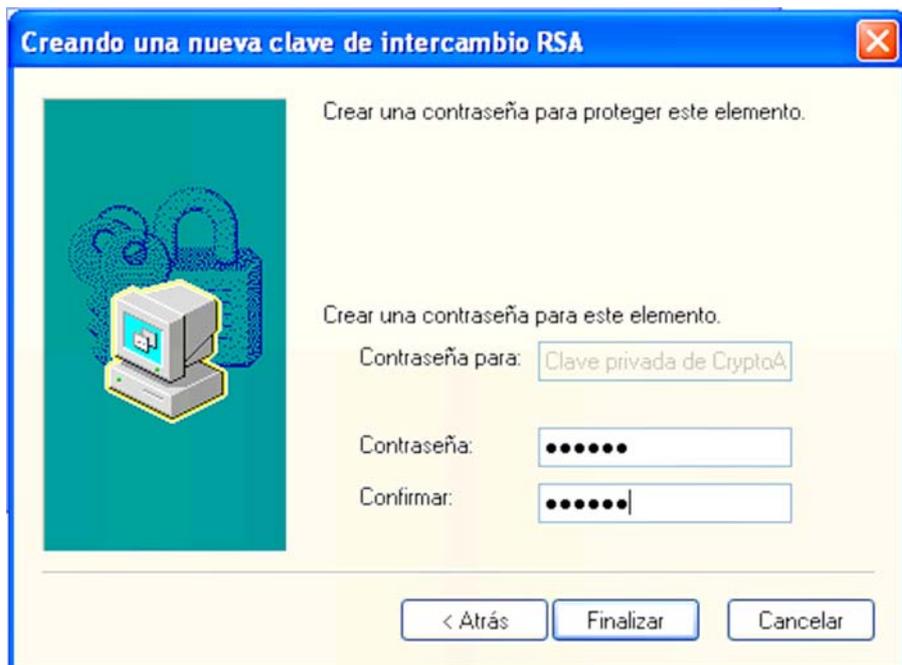
The screenshot shows the CERES web application interface. At the top, there is a navigation menu with links for 'Mapa', 'Contacto', 'Enlaces', 'Legislación', and 'Noticias'. Below this is a banner for 'Obtenga el CERTIFICADO DE USUARIO'. A main menu on the left lists various services, with 'SOLICITUD DEL CERTIFICADO' highlighted. The main content area is titled 'CIUDADANOS' and contains a section for 'OBTENER CERTIFICADO'. Under this section, there is a checkbox for 'SOLICITUD DEL CERTIFICADO' which is checked. Below the checkbox, there is a text input field for 'NIF / NIE o CIF DEL TITULAR DEL CERTIFICADO' and an 'Enviar petición' button. The page also features the logo of the Real Casa de la Moneda.

Pulsar la casilla de **“Solicitud del certificado”** e introducir el número del NIF o CIF. Es importante leer las instrucciones para cada uno de los datos.

Una vez cumplimentada la casilla del NIF, al enviar la petición le aparecerá un aviso informándole de la solicitud del certificado, seleccione la opción **“SI”**. El paso siguiente le mostrará la pantalla de creación de claves y del nivel de seguridad.



Se recomienda que cuando varias personas puedan tener acceso al mismo ordenador, se seleccione la opción **“Alto”** para el nivel de seguridad.



Si ha optado por la opción “alto” el sistema le va a solicitar que establezca una contraseña para el acceso a su certificado y que confirme la misma. Esa contraseña le será solicitada cada vez que pretenda hacer uso del certificado.

Una vez seleccionado el nivel de seguridad y aceptado el mismo, le aparecerá en la pantalla el código de solicitud asociado a su certificado, que deberá imprimir o apuntar para dirigirse a cualquiera de las Oficinas de Registro de los Organismos acreditados



También existe la posibilidad de obtener el certificado en una tarjeta criptográfica. En este caso el solicitante deberá proveerse de la misma así como de un lector de tarjetas en el caso de que su equipo no venga provisto del mismo. El proceso de solicitud del certificado en tarjeta, requiere igualmente la realización de los tres pasos señalados anteriormente, con la diferencia de que la solicitud y la descarga han de hacerse con la tarjeta en el lector. Para el primer paso (solicitud) la opción a elegir será "CERTIFICADO DE USUARIO EN TARJETA CRIPTOGRÁFICA", y habrá de seleccionarse con la tarjeta dentro del lector, de esta forma, las claves se generan en la tarjeta en vez de en el navegador. La descarga ha de seleccionarse igualmente con la tarjeta dentro del lector para que se descargue el certificado en la misma.

### 2.1.2 Identificación

Este punto es de vital importancia puesto que gracias a él proporcionaremos la identidad que figurará en el certificado y, por este motivo, se puede identificar a una persona como "firmante" de los documentos

Con el código de solicitud obtenido en el punto anterior, y el documento identificativos (DNI, NIE. pasaporte), deberá presentarse en la oficina de acreditación que desee.

Para su comodidad, puede usted hacer uso del servicio de localización de las OFICINAS MAS CERCANAS que le aparece en la pantalla de obtención del certificado.

No hay que olvidar que al acudir a la oficina de registro es imprescindible llevar, en el caso de las personas físicas:

- DNI o tarjeta de residencia (NIE) o pasaporte
- Código de solicitud del certificado (paso 1)

Con el fin de garantizar el nivel de seguridad del sistema y para obtener la identidad del titular del certificado de forma fehaciente, el registro de usuario es necesariamente presencial. Sin este registro presencial, no tendría mucha credibilidad la identidad del titular o firmante de un certificado

### 2.1.3 Descarga e instalación

Volviendo a la página de Ceres, se pulsa sobre el botón "**Obtenga el Certificado de Usuario**" y finalmente en Descarga del certificado, del menú de la izquierda. Habrá que introducir el número del NIF o NIE y el código proporcionado en la fase anterior.

The screenshot shows the CERES website interface. At the top, there is a navigation menu with links for 'Mapa', 'Contacto', 'Enlaces', 'Legislación', and 'Noticias'. Below this is a banner for 'Obtenga el CERTIFICADO DE USUARIO'. A main navigation table is visible, with columns for 'Qué es CERES', 'Ciudadanos', 'Empresas', and 'Adm. Pública'. The 'Ciudadanos' column is highlighted, showing options like 'Obtener el certificado', 'Renovación de certificado', 'Anulación de certificado', 'Modificar datos', 'Verificar estado', 'Soporte Técnico', 'Preguntas', 'Contacto', and 'Otros servicios'. The 'CIUDADANOS' section is active, displaying the 'Real Casa de la Moneda' logo and the text 'Fábrica Nacional de Moneda y Timbre'. A sidebar on the left lists various services, with 'DESCARGA DEL CERTIFICADO' selected. The main content area includes a heading 'OBTENER CERTIFICADO', a checkbox for 'DESCARGA DEL CERTIFICADO', and instructions for downloading the certificate. It also features a 'FORMULARIO DE DESCARGA' with input fields for 'NIF' and 'Código', and an 'Enviar petición' button. A note at the bottom of the form states: 'En el campo de DNI, rellene con ceros a la izda. si es necesario.'

Si todo ha ido bien, el navegador informará que se ha descargado correctamente.

Si todo el proceso se ha hecho con **Internet Explorer** hay que tener habilitadas en el navegador la ejecución de javascript y SSL. Para comprobarlo hay que ir al Menú Herramientas – Opciones de Internet – Opciones avanzadas. También es aconsejable desactivar cualquier medida de protección como antivirus o cortafuegos que impidan la ejecución de ActiveX.

Comprobación de la correcta instalación del certificado en Internet Explorer y Firefox.

- **Internet Explorer:** Menú Herramientas – Opciones de internet – Opciones avanzadas – Certificados.
- **Firefox:** Menú Herramientas – Opciones – Avanzado – Certificados.

Desde estas misma ubicaciones se puede **exportar e importar** cualquier certificado, una medida muy recomendable para recuperarlo cuando el ordenador donde estaba instalado ha sufrido un percance considerable.

## 3 INSTALACIÓN DEL CERTIFICADO

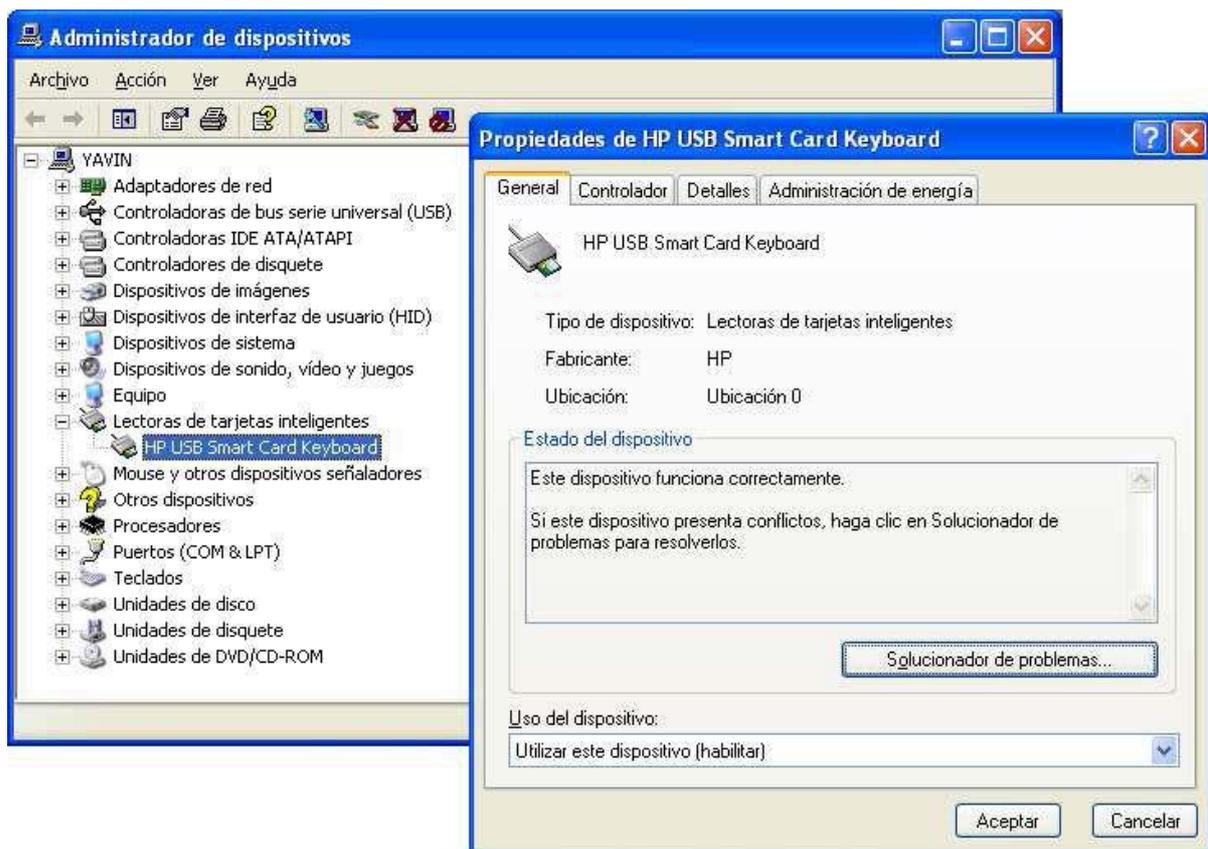
El componente cliente de la plataforma de firma, es el utilizado por las aplicaciones web para poder acceder a los almacenados locales del equipo cliente.

### 3.1 PANTALLA DE ACCESO

Para la correcta utilización del componente cliente y de sus funcionalidades es necesario tener en cuenta cierto número de requisitos previos.

#### 3.1.1 Lector criptográfico

Es necesario tener correctamente instalado el teclado con lector criptográfico y sus drivers.



Administrador de dispositivos de MS Windows XP

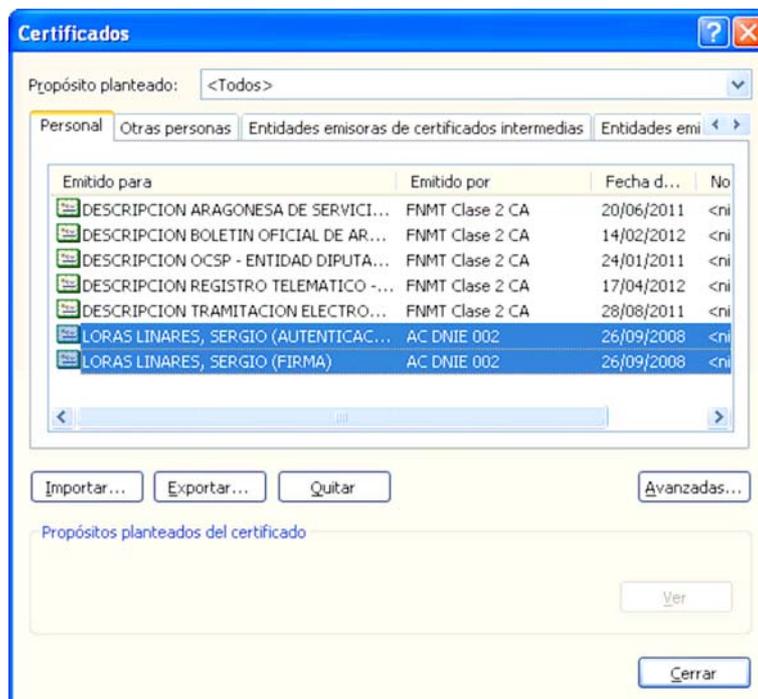
#### 3.1.2 Tarjetas Criptográficas

Disponer de una tarjeta criptográfica y haber instalado sus drivers, que son distintos para cada tipo de tarjeta (**CERES**, **DNI Electrónico**...). Estos drivers deben instalarse tanto para el **MS Certificate Store** como para los diversos clientes que no usen el MS Certificate Store y que puedan hacer uso de las tarjetas (**Firefox**, **Thunderbird**...).

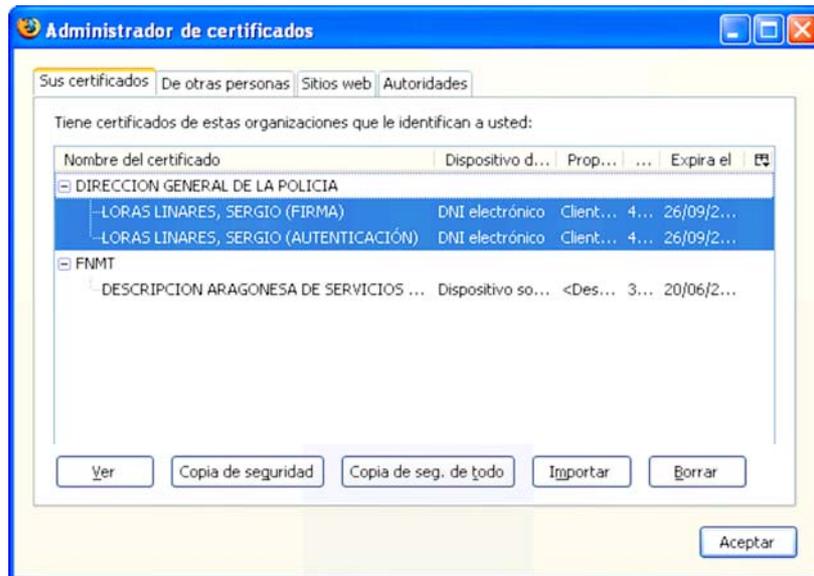
Tarjetas mas comunes	URL de descarga de sus drivers
<b>DNI Electrónico</b>	<a href="http://www.dnielectronico.es">http://www.dnielectronico.es</a>
<b>Tarjeta CERES</b>	<a href="http://www.cert.fnmt.es">http://www.cert.fnmt.es</a>

Los drivers de estas tarjetas son independientes de los certificados y claves privadas que contengan, ya que las tarjetas son solamente un contenedor. En el caso del **DNI Electrónico**, éste solamente contendrá los certificados y claves de firma y autenticación emitidos por la **Dirección General de la Policía**, mientras que en las tarjetas **CERES**, al poder escribirse en ellas, podrán contener todo tipo de certificados y claves, como las emitidas por **FNMT**, **Camerfirma**, **Firmaprofesional**, **Ancert**...

Para comprobar que sus correspondientes drivers han sido instalados correctamente, basta con observar si podemos ver los certificados alojados en las tarjetas desde los distintos navegadores.



Certificados del DNI Electrónico en MS Certificate Store

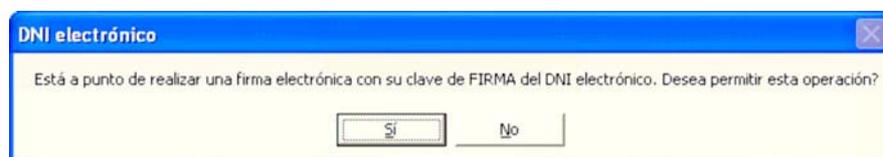


Certificados del DNI Electrónico en Firefox

Estas tarjetas tienen funcionamientos diferentes respecto a su PIN. Mientras que la tarjeta CERES solo pide el PIN cuando se accede a una clave privada y éste se cachea temporalmente, el DNI Electrónico pide el PIN cada vez que tiene que acceder al propio chip criptográfico, ya sea solamente para acceder al certificado público o para usar la clave privada, adicionalmente cuando se vaya a hacer uso de la clave privada de firma, aparecerá un aviso para indicar que esta apunto de realizarse una firma electrónica reconocida (Ley 59/2003).



Petición del PIN del DNI Electrónico



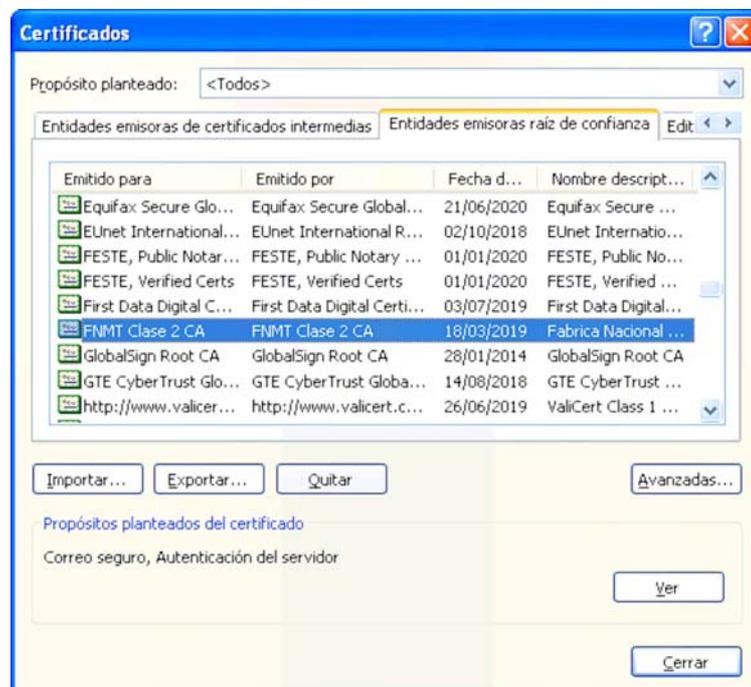
Aviso del DNI Electrónico de creación de firma electrónica reconocida

### 3.1.3 Certificados Raíz

Los certificados raíz de las Autoridades de Certificación emisoras de los certificados con los que vamos a trabajar, deben estar instalados tanto en el MS Certificate Store como en los almacenes de los diversos clientes que no usen el MS Certificate Store (Firefox, Thunderbird...).

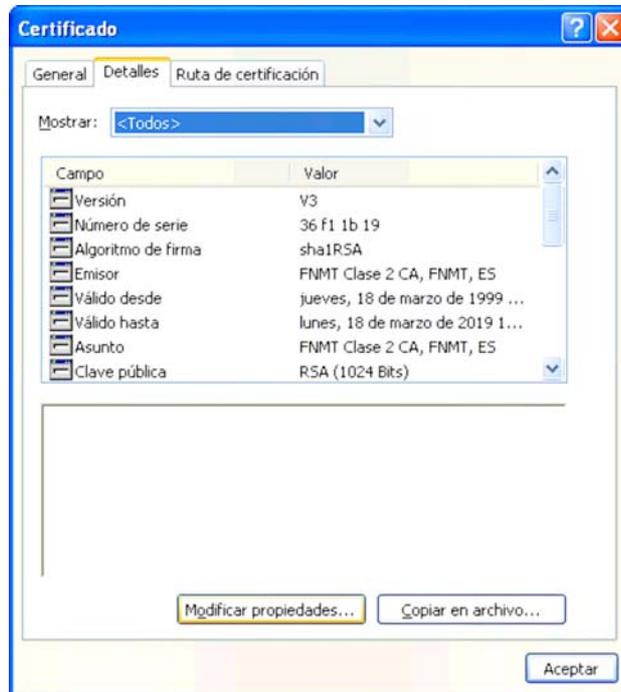


Almacén de certificados de Firefox

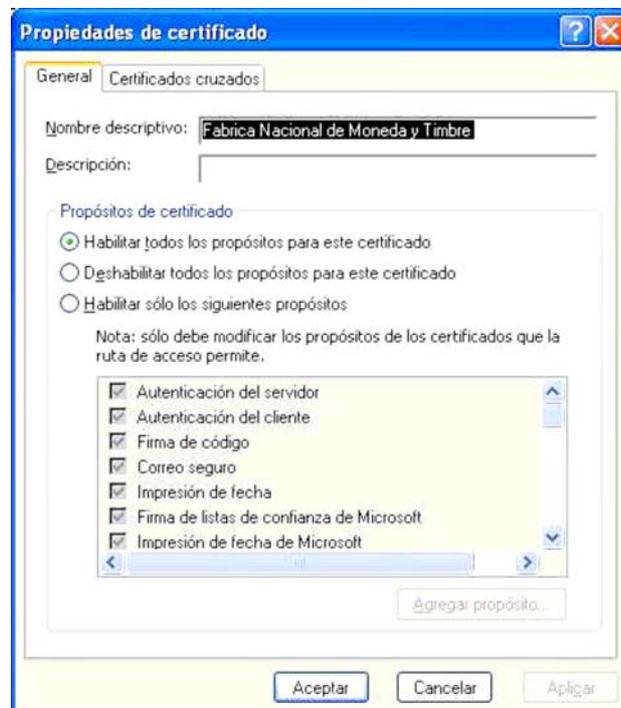


Almacén de certificados MS Certificate Store

En el MS Certificate Store el certificado raíz de la FNMT debe estar habilitado para soportar todos los propósitos:



En el botón de *Modificar propiedades...* de la pestaña *Detalles* de las propiedades de un certificado.



Deben estar habilitados todos los propósitos para este certificado.

### 3.1.4 Java Runtime Environment (JRE)

Para la utilización del componente cliente, será necesario tener instalada una **JRE 1.4.2** o superior, en el caso de querer utilizar DNI Electrónico, como mínimo será necesaria una **JRE 5**.

### 3.1.5 Permisos

El grupo “usuarios” de un dominio NT (o Active Directory) por defecto no tiene permisos para instalar ActiveX. Debe instalarse el componente cliente por un usuario que tenga, como mínimo, permisos de Administrador de la maquina o prepararse el componente como seguro dentro del ActiveDirectory, consulte la documentación de Microsoft referente a tal efecto.

En Firefox hay que instalar unas librerías, entonces es necesario que el usuario que ejecuta el navegador tenga permisos de escritura en la carpeta de instalación del navegador.

No es valido realizar la instalación desde un usuario Administrador, ya que los componentes se instalarían en el perfil de este usuario Administrador, y no del perfil del usuario que vaya a usar el equipo posteriormente.

Se puede instalar manualmente las DLL incluidas en el XPI, incluyéndolas en la misma carpeta del navegador o en cualquier directorio del PATH, finalmente dar permisos al sitio Web para instalar Complementos y así poder consultar su estado. Una vez realizada la instalación y si ésta ha sido correcta, el usuario no necesita de más privilegios de instalación para ejecutarlo.

### 3.1.6 Navegador

Con la actual versión del componente cliente se soportan los siguientes navegadores:

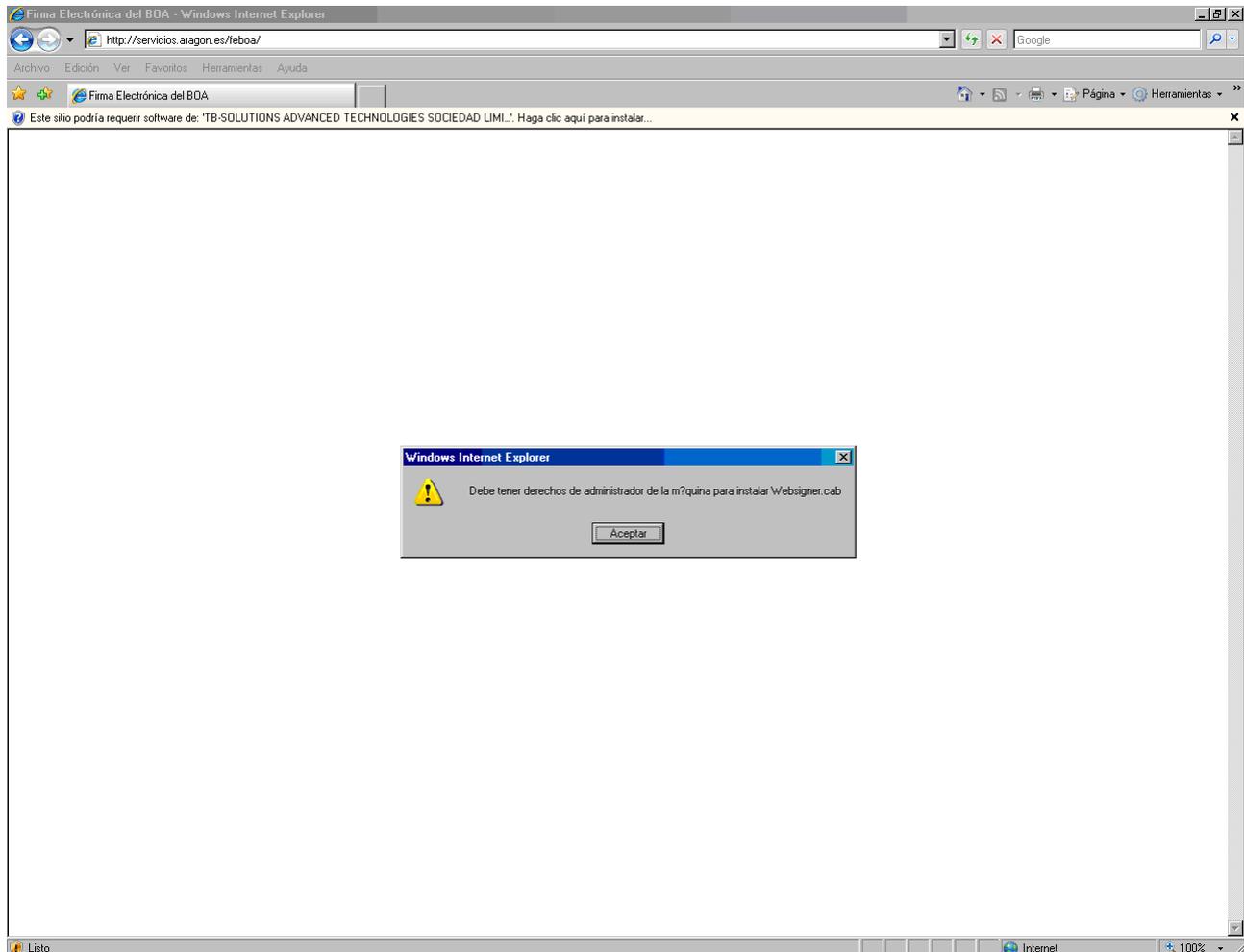
- **MS Internet Explorer** 6.x y 7.x bajo **MS Windows XP**
- **Mozilla Firefox** 1.5.x y 2.0.x bajo **MS Windows XP** y **GNU/Linux**

## 3.2 INSTALACIÓN

Cuando se acceda a una aplicación web que haga uso del componente cliente, si éste no estaba instalado con anterioridad en el equipo cliente o es una versión posterior al instalado, se lanzara el proceso de instalación.

### 3.2.1 Instalación en MS IExplorer

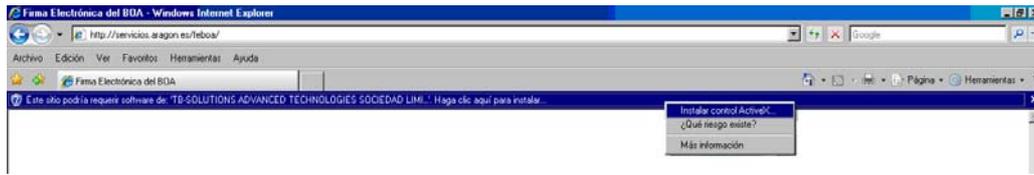
Al acceder desde el MS IExplorer a una web que haga uso del componente cliente, de lo primero que nos advertirá es de que debemos tener privilegios de administrador para poder realizar la instalación del ActiveX:



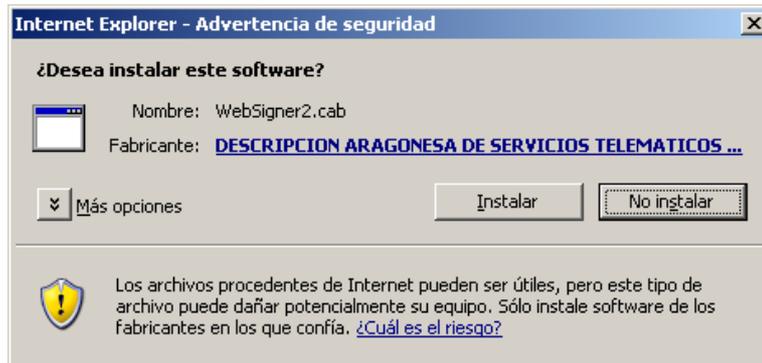
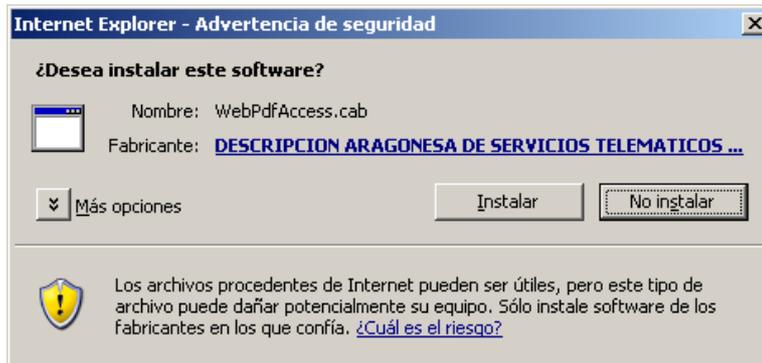
Si no disponemos de ellos se nos mostrara el siguiente error, ya que se estará intentando ejecutar el componente cliente sin que se haya podido realizar la instalación:



Si disponemos de ellos, tendremos que pulsar en la barra superior amarilla para empezar la instalación del ActiveX:



Una vez aceptada la instalación nos aparecerán los componentes a instalar:



Una vez instalados estos componentes, la aplicación web podrá iniciar el componente cliente perfectamente.

### 3.2.2 Instalación en Firefox

Al acceder desde el Firefox a una web que haga uso del componente cliente, se iniciara la ejecución del applet java:



Una vez instalado, el componente cliente podrá iniciarse correctamente.