

## INDICE

1	Configuración previa .....	2
1.1	Configuración Internet Explorer para ActiveX .....	2
1.2	Problemas comunes en sistema operativo Windows .....	8
1.2.1	Usuarios con sistema operativo Windows XP con el Service Pack 2 Instalado .....	8
1.2.2	Usuarios con otra versión de windows .....	14
1.3	Configuración para la Versión Applet en un navegador Firefox, Mozilla o Netscape .....	16
1.3.1	Instalación del certificado raíz de la FNMT .....	16
1.3.2	Instalación del Módulo de Seguridad para el uso de Certificados en Tarjeta Criptográfica ...	24

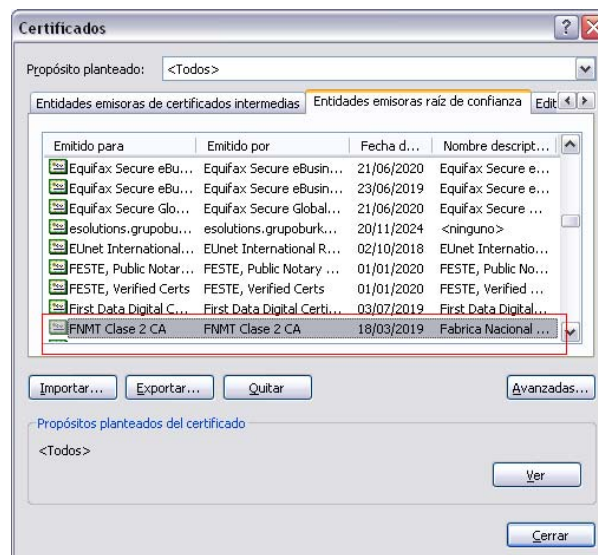
## 1 CONFIGURACIÓN PREVIA

Para que el componente de firma digital se ejecute correctamente en un ordenador cliente es necesario tener en cuenta las siguientes opciones de configuración, las cuales será necesario aplicar en cada uno de los ordenadores clientes.

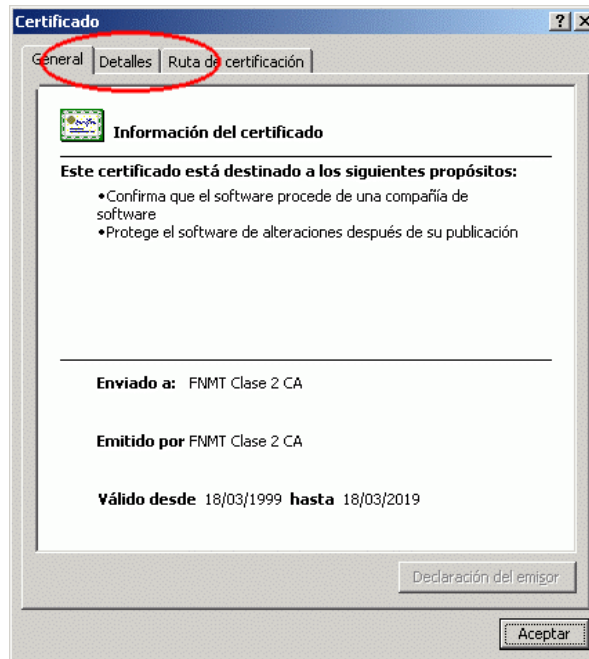
### 1.1 CONFIGURACIÓN INTERNET EXPLORER PARA ACTIVEX

Si el componente de firma que se va a utilizar es la versión ActiveX para un navegador Explorer es necesario tener presente los siguientes detalles:

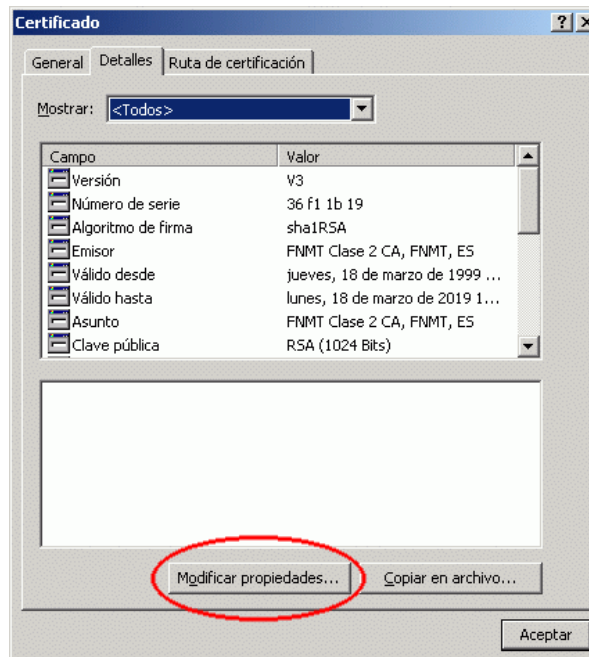
- El certificado Raíz de la FNMT que se encuentra distribuido por defecto en todas las distribuciones existentes hasta la fecha del sistema operativo Windows (es decir, 95, 98, NT, 2000, XP o 2003) no tiene todos los propósitos habilitados. Es decir, para que el componente ActiveX se descargue de forma segura en un ordenador cliente es necesario firmarlo previamente usando un certificado de componentes emitido por una autoridad de certificación. En el caso del Ministerio de Economía y Hacienda dicho certificado de componentes fue emitido por la FNMT, por lo que es necesario que el certificado raíz de la entidad emisora de certificados tenga habilitados los propósitos de Firma de Código.
  - Para identificar si en un ordenador cliente se tiene ese problema basta con acceder a las propiedades del certificado digital, para ello se pueden seguir los siguientes pasos:
    - En Internet Explorer pulsamos en el menú **Herramientas > Opciones de Internet > Pestaña Contenido > Certificados > Entidades Emisoras Raíz de Confianza** y buscamos el certificado con nombre **FNMT Clase 2 CA**. (ver imagen)



- Una vez seleccionado el certificado, hacemos **dobles-click**, se abrirá la ventana con información del certificado de la F.N.M.T. similar a la que se muestra a continuación. Pinchamos en la pestaña **Detalles**.



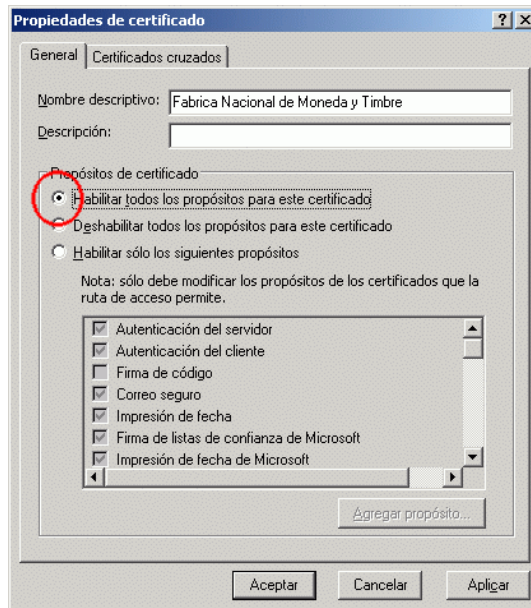
- La pantalla que se muestra después contiene los detalles del certificado de la Fabrica Nacional de Moneda y Timbre (ver imagen). Pulsaremos en el botón **Modificar Propiedades** para visualizar los propósitos del certificado.



## Ayuda para la instalación Componente Firma Digital

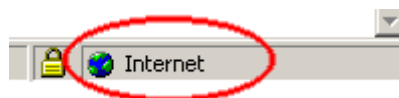


- En esta ventana aparecen los propósitos para los que se ha emitido el certificado, seleccionaremos "Habilitar todos los propósitos para este certificado" y posteriormente pulsaremos en el botón **Aceptar** (ver imagen)



- En los propósitos del certificado tienen que estar todos marcados, especialmente la opción de firma de código. Si no marcamos esta opción el componente de firma no se descargará de forma correcta (ver apartado de errores comunes de Windows para identificar los errores comunes que pueden aparecer).
- Este problema surge debido a un problema en la creación por parte de la FNMT de los propósitos de su certificado de CA y no por un error en cómo se ha desarrollado el componente de firma.
- Habilitar dentro de las opciones de seguridad las opciones adecuadas para permitir la ejecución de controles activeX marcados como seguros. Para ello cada usuario en su navegador deberá tener habilitados las siguientes opciones:
  - Para modificar los permisos de los controles ActiveX hay que acceder a la ventana de Propiedades de Seguridad Internet. Para ello basta con realizar un doble clic en el icono de la barra inferior del explorador según indican las imágenes que se muestran a continuación (El candado indica que es una conexión segura):

**Acceso para  
usuarios de  
Internet:**

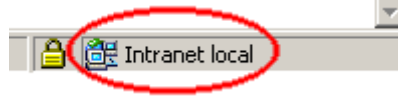


**Ayuda para la instalación  
Componente Firma Digital**



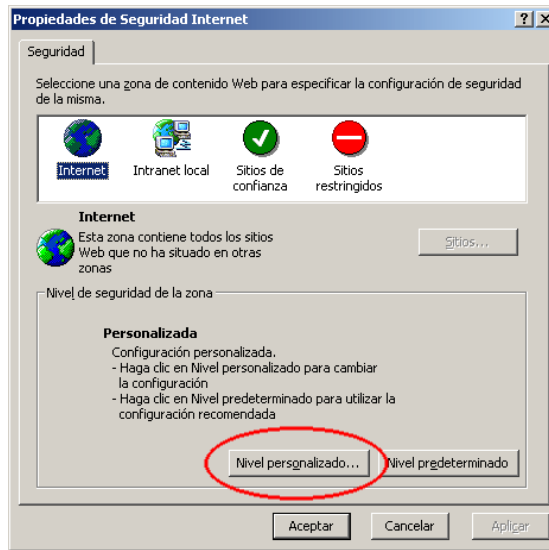
23-03-2006

**Acceso para  
usuarios de  
Intranet:**

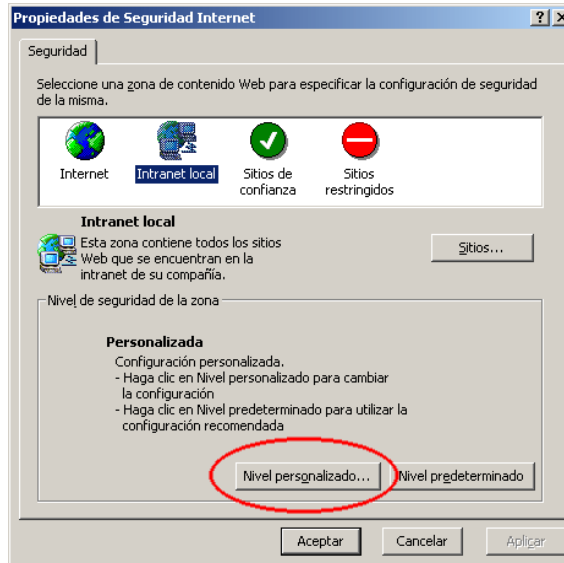


- Una vez pulsado se abrirá una segunda ventana con una única pestaña llamada Seguridad. Dependiendo de si el acceso se ha realizado por internet o intranet una opción estará seleccionada:

**Opción seleccionada  
acceso por Internet:**

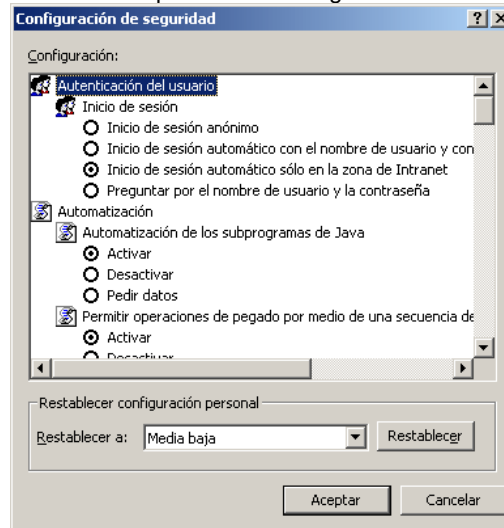


**Opción seleccionada  
acceso por Intranet:**

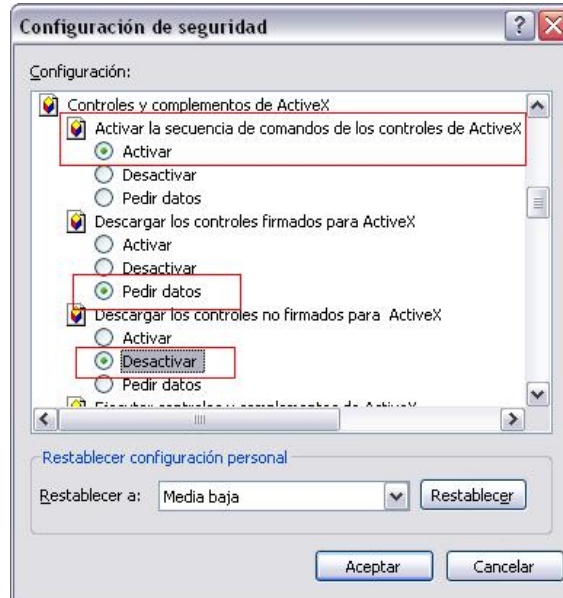


- Para modificar los niveles tanto de internet como de intranet, hay que pulsar el boton Nivel personalizado.

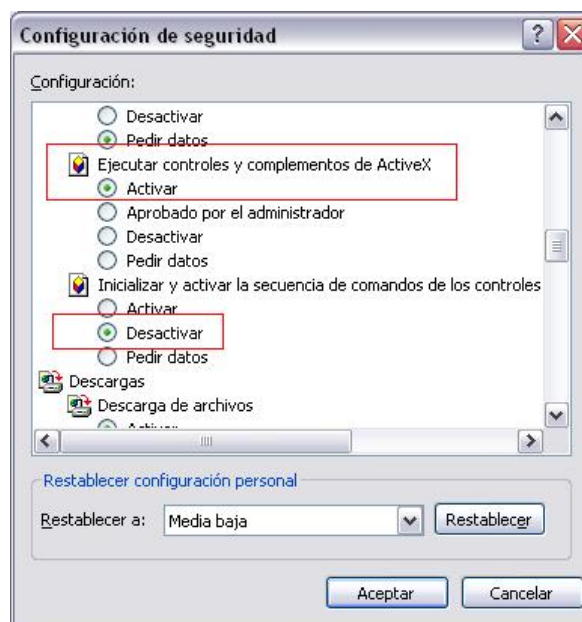
- Seguidamente se abrirá una ventana donde las opciones de configuración son idénticas para los dos entornos (tanto si se accede por Intranet como desde Internet). A continuación se detallan las opciones de configuración recomendadas:



- En la ventana de Configuración de seguridad (imagen anterior) hay que seleccionar los siguientes niveles de seguridad para permitir la descarga segura del componente de firma, para ello nos vamos a la sección que aparece con el título Controles y complementos ActiveX:
  - En la opción *Activar la secuencia de comandos de los controles de ActiveX marcados como seguros* marcaremos la opción Activar o Pedir datos la diferencia de marcar una u otra opción radica en si queremos o no que se nos avise cuando se ejecute el control ActiveX.
  - En la opción *Descargar los controles firmados para Activex* marcaremos la opción Activar o Pedir datos la diferencia de marcar una u otra opción radica en si queremos o no que se nos avise cuando se descargue el control ActiveX.
  - En la opción *Descargar los controles no firmados para Activex* marcaremos la opción Desactivar debido a que supone un riesgo de seguridad tener habilitada esta opción.



- En la opción Ejecutar controles y complementos ActiveX marcaremos la opción Activar.
- En la opción Inicializar y activar la secuencia de comandos de los controles de ActiveX no marcados como seguros marcaremos la opción Desactivar debido a que supone un riesgo de seguridad tener habilitada esta opción.



- El hecho de tener que activar estas opciones de seguridad depende del nivel de seguridad establecido para el usuario. Las opciones configuradas anteriormente coinciden con el nivel de

seguridad óptimo para garantizar que no se permiten la ejecución de controles activeX no marcados como seguros, aunque de por si la ejecución de controles activeX ya suponga un problema de seguridad.

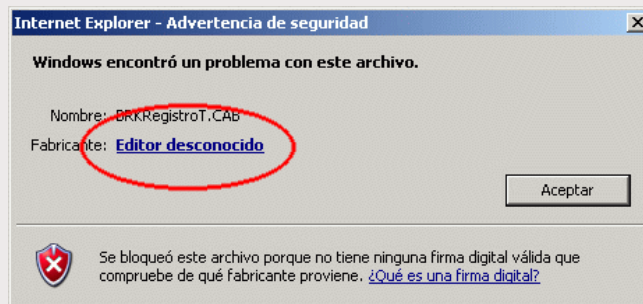
## 1.2 PROBLEMAS COMUNES EN SISTEMA OPERATIVO WINDOWS

A continuación se detallan los principales errores que pueden aparecerle a un usuario cuando se descargue el componente activeX.

### 1.2.1 USUARIOS CON SISTEMA OPERATIVO WINDOWS XP CON EL SERVICE PACK 2 INSTALADO

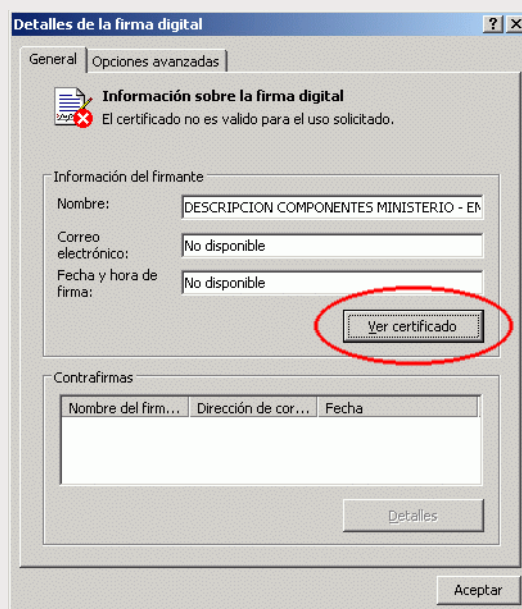
Debido al incremento de los niveles de seguridad establecidos con el Service Pack2 de Windows XP, los usuarios de este sistema operativo deben realizar adicionalmente los siguientes pasos para poder instalar el control ActiveX, Además de los descritos para ejecutar controles ActiveX

- 1 Al entrar en la página del formulario donde se descargue el componente se mostrará la siguiente ventana:



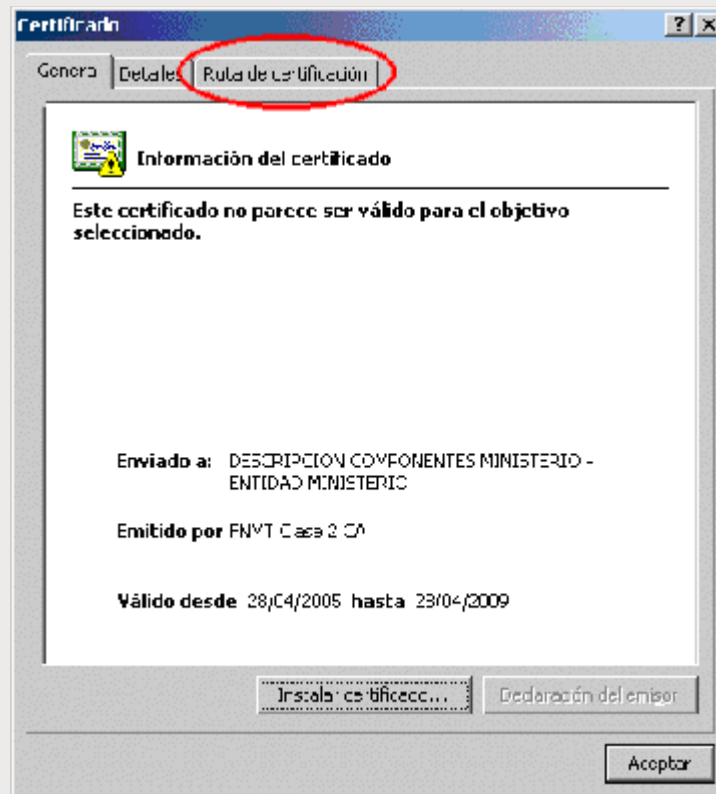
Dicha ventana aparece debido a que no se encuentran habilitados los permisos para la instalación de componentes seguros firmados por la FNMT. Este mensaje avisa de que no va a instalar el componente ActiveX debido a que no tiene seguridad acerca de la entidad emisor del certificado de componentes. A pesar de pulsar en el botón **Aceptar** el componente ActiveX **NO** se instala. Para subsanar este problema pulsaremos en el vínculo **Editor Desconocido** (ver imagen anterior)

- 2 Al pulsar sobre el vínculo se abrirá una ventana (ver imagen) donde se puede acceder a los detalles del certificado usado para firmar el componente de firma:



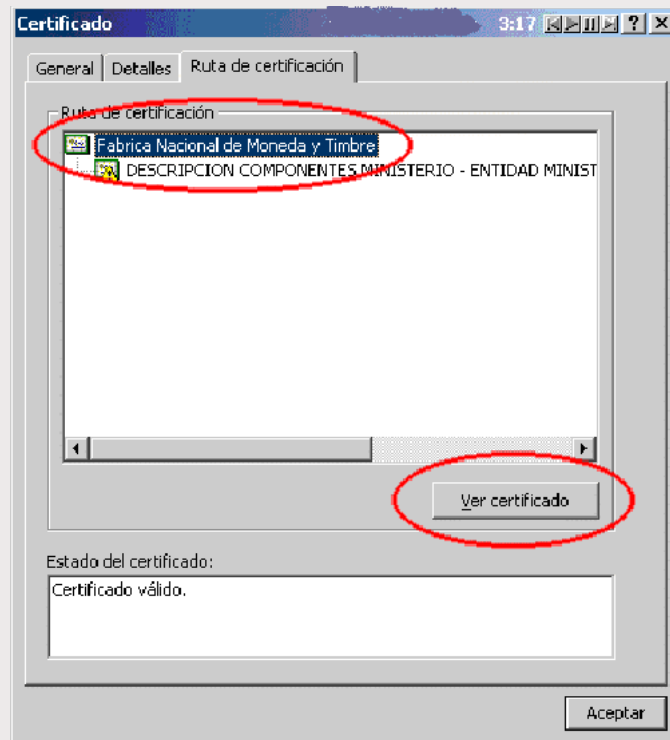
Según indica la ventana el certificado no es válido para el uso seleccionado (*Firma de código*). Para verlo en detalle pulsaremos en el botón **Ver certificado**.

- 3 La ventana que se abre muestra la información detallada del certificado:



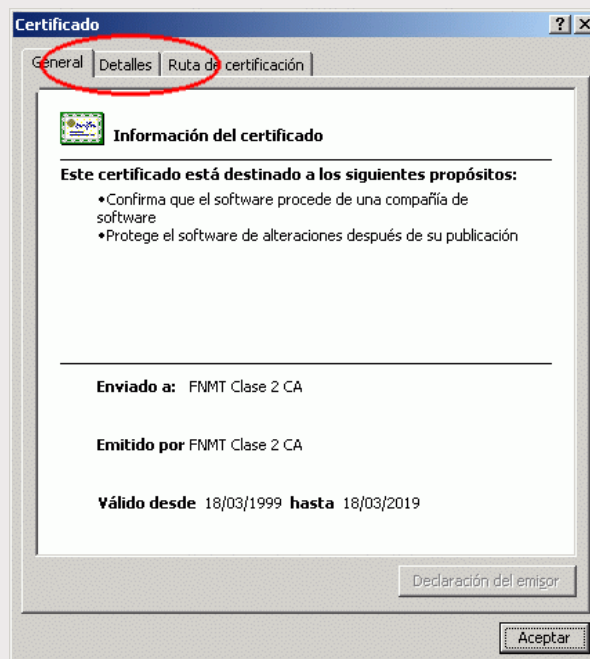
En dicha ventana se indica, otra vez, que el certificado usado no parece ser válido para el propósito especificado. Dicho problema aparece debido al certificado de la Fabrica Nacional de Moneda y Timbre (FNMT) instalado en nuestra máquina. Para ver éste certificado pulsaremos en la pestaña **Ruta de certificación**.

- 4 La ruta de certificación se usa para validar el origen del componente de firma.



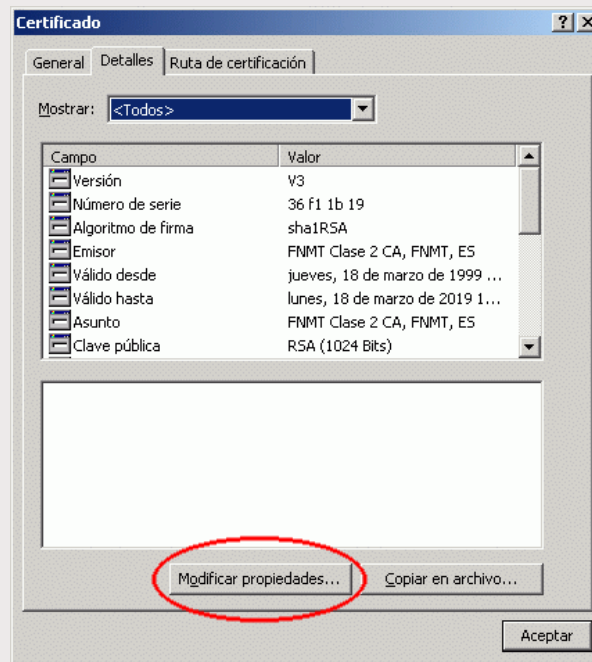
Seleccionar el certificado de la "Fabrica Nacional de Moneda y Timbre", y después hacer clic en el botón "Ver Certificado" para mostrar los detalles del certificado raíz

- 5 Se abrirá la ventana con información del certificado de la F.N.M.T.



Seleccionar la pestaña de "Detalles" para ver los propósitos de éste certificado.

- 6 La pantalla que se muestra después contiene los detalles del certificado de la Fabrica Nacional de Moneda y Timbre:



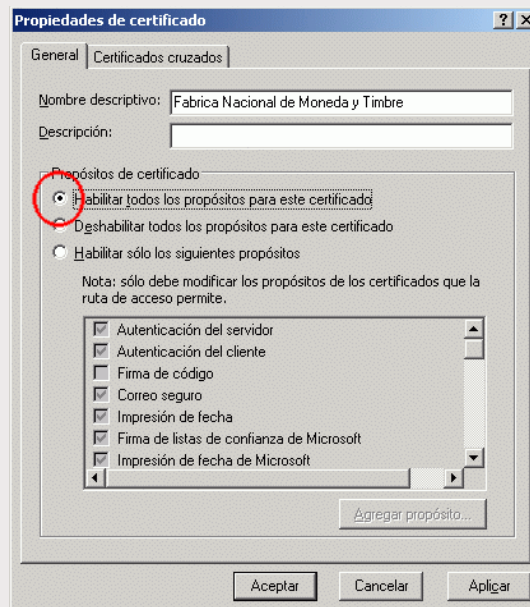
Hacer clic en el botón "Modificar propiedades" para mostrar la ventana de "Propiedades de certificado".

- 7 Los Propósitos de certificado definen la funcionalidad del certificado:

**Ayuda para la instalación  
Componente Firma Digital**



23-03-2006




Seleccionar "Habilitar todos los propósitos para este certificado" y posteriormente pulsar el botón "Aceptar".

- 8 A continuación, cerrar el navegador y acceder de nuevo al formulario. Se mostrará a continuación una ventana parecida a la siguiente donde ya se reconoce que el componente se encuentra firmado por un certificado reconocido y válido garantizando la autenticidad y procedencia del componente de firma:



Seleccionar el botón "Instalar" para instalar el componente de firma (ActiveX).

	<p><b>Ayuda para la instalación Componente Firma Digital</b></p>	 <b>MINISTERIO DE ECONOMÍA Y HACIENDA</b> <hr/> <b>23-03-2006</b>
--	--	--

## 1.2.2 USUARIOS CON OTRA VERSIÓN DE WINDOWS

En caso de no tener la versión de Windows XP con el Service Pack 2 instalada al descargar el componente de firma en caso de no tener habilitado el propósito del certificado de la FNMT de firma de código, aparece un mensaje similar al que se muestra a continuación:



Donde se indica que “no se ha habilitado el certificado de raíz para el uso requerido”, precisamente porque el certificado de la FNMT no tiene habilitado el propósito de **Firma de código**. A pesar de éste mensaje si pulsamos sobre el botón **Sí** el componente se descarga y se instala correctamente, a diferencia de lo que pasaba en XP con SP2. (Siempre y cuando también tengamos habilitado la ejecución de controles ActiveX marcados como seguros).

	<p><b>Ayuda para la instalación Componente Firma Digital</b></p>	 <p>MINISTERIO DE ECONOMÍA Y HACIENDA</p> <p><b>23-03-2006</b></p>
--	--	---

Si queremos que no aparezca éste mensaje de alerta que podría llegar a confundir a un usuario deberíamos habilitar el propósito del certificado de la FNMT. Si lo hacemos el mensaje que recibiría el usuario sería similar al que se muestra a continuación:



En este mensaje ya se le indica al usuario que es un componente seguro y que puede confiar en él, incluso si marcara la opción *Confíar siempre...* no le volvería a aparecer el mensaje.

Como una posible solución para evitar que el usuario tuviera que realizar todo este proceso se forma manual se podría desarrollar un instalador de Windows que realizase todos los pasos de instalación de forma automática. Aunque esto supone modificar propiedades del registro de Windows por lo que es posible que el programa instalador no tuviera permisos suficientes para ejecutarse.

### 1.3 CONFIGURACIÓN PARA LA VERSIÓN APPLET EN UN NAVEGADOR FIREFOX, MOZILLA O NETSCAPE

Para este caso el problema que se presenta es algo similar al que ocurre para Internet Explorer. A diferencia de Internet Explorer donde el certificado digital de la FNMT no dispone de los atributos suficientes, en Firefox, Mozilla o Netscape dicho certificado no viene incluido por defecto en las distribuciones de dichos navegadores por lo que no existe y hay que instalarlo previamente. Adicionalmente a este problema está el hecho de utilizar certificados digitales incluidos en tarjetas criptográficas y no en el navegador, dado que es necesario la configuración manual del proveedor de certificados para el acceso a la tarjeta criptográfica (como por ejemplo los de la FNMT). En este sentido de momento CERES no ha suministrado un instalador automático para navegadores Firefox o Mozilla, únicamente existe para navegadores Internet Explorer y Netscape.

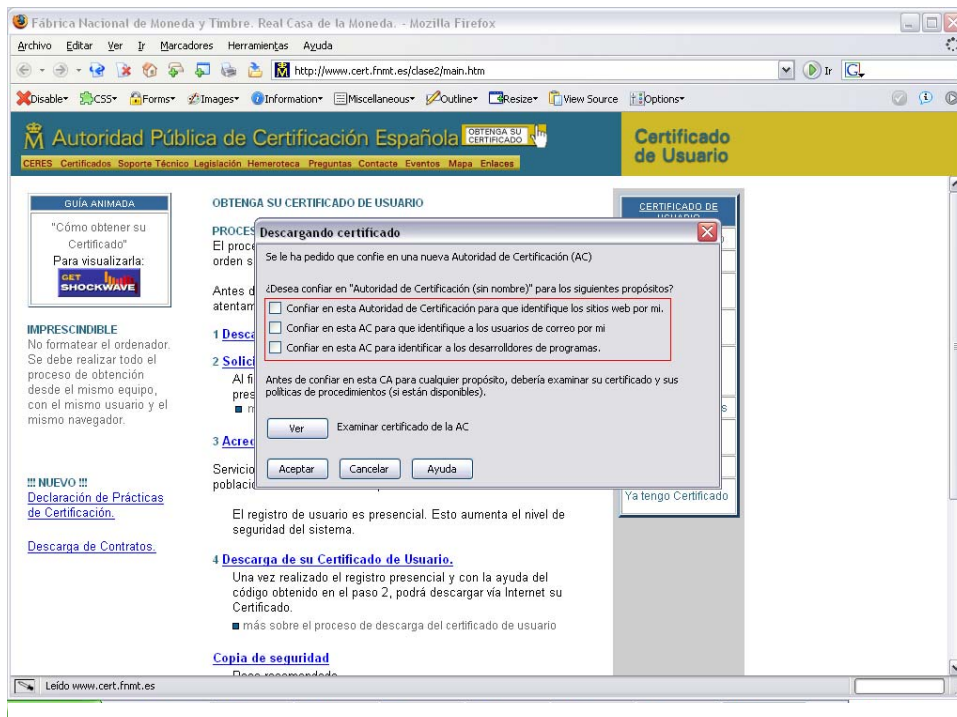
Para el correcto funcionamiento del componente de firma digital es necesario tener en cuenta el tipo de certificados digitales que va a permitirse utilizar. En caso de tener que soportar el DNI electrónico la única versión del entorno de ejecución Java soportado es la versión JRE de Sun 1.5\_X, en caso de no utilizarse el DNI electrónico la versión de Java utilizada puede ser JRE de Sun 1.4.2\_X o superior.

#### 1.3.1 INSTALACIÓN DEL CERTIFICADO RAÍZ DE LA FNMT

Para descargar el certificado raíz de la FNMT accederemos desde el navegador Firefox, Mozilla o Netscape a la siguiente dirección:

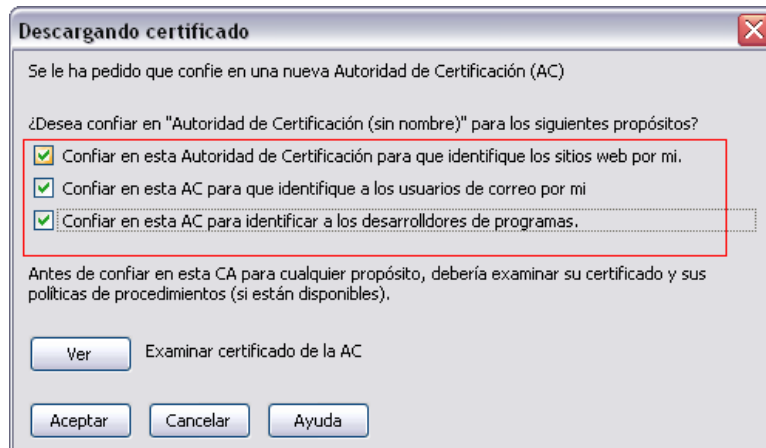
<http://www.cert.fnmt.es/clase2/main.htm>

En esa dirección se encuentra un enlace con el texto "Descarga del certificado raíz de la FNMT", pinchamos en el enlace y se nos mostrará una ventana similar a la que se muestra en la siguiente imagen:



NOTA: Este proceso sería equivalente para cualquier otra autoridad de Certificación Reconocida.

En ella aparecen desmarcadas tres opciones las cuales deberemos marcar, una vez realizado pulsaremos en el botón **Aceptar**.



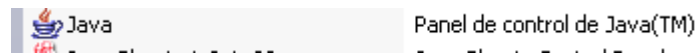
Una vez realizado esto, se instalará el certificado raíz de la FNMT lo que habilita la descarga del componente de firma.

Una vez instalado el certificado de la CA cuando se accede a la página donde se descarga el componente si se utiliza el navegador Firefox, Mozilla o Netscape es posible que aparezca una ventana de aviso similar a la que se muestra a continuación:



Esta ventana aparece debido a que en el panel de control de Java no se encuentra configurado el certificado raíz de la FNMT que se utilizó para firmar digitalmente el certificado. Si esto ocurre los pasos para realizar la correcta configuración son los siguientes:

Abrimos el **Panel de Control (Inicio > Configuración > Panel de Control)** del ordenador y buscamos el icono del **Panel de Control Java** que aparece identificado con el icono



Hacemos doble clic y se nos abrirá el panel de control de Java donde se nos visualizará la siguiente información:

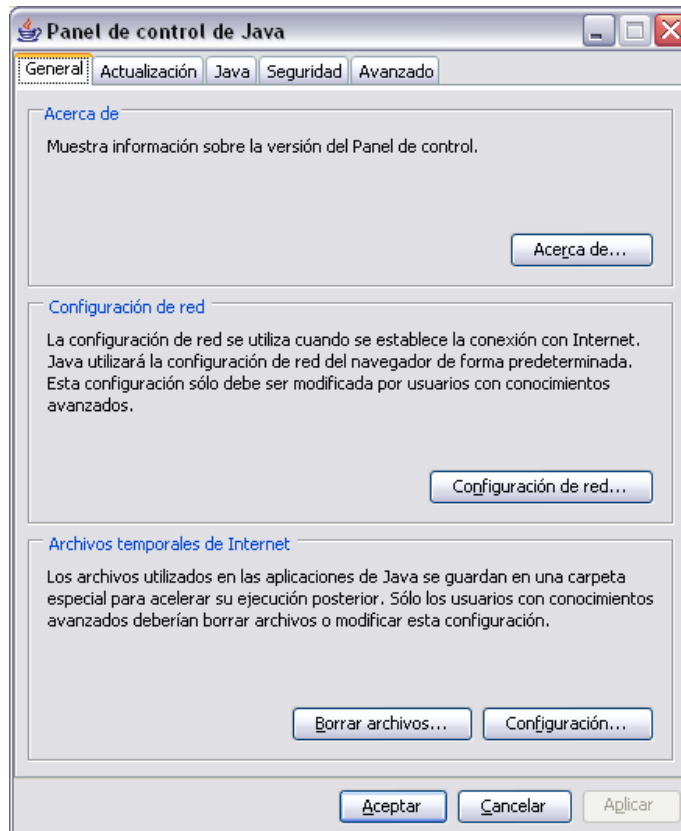
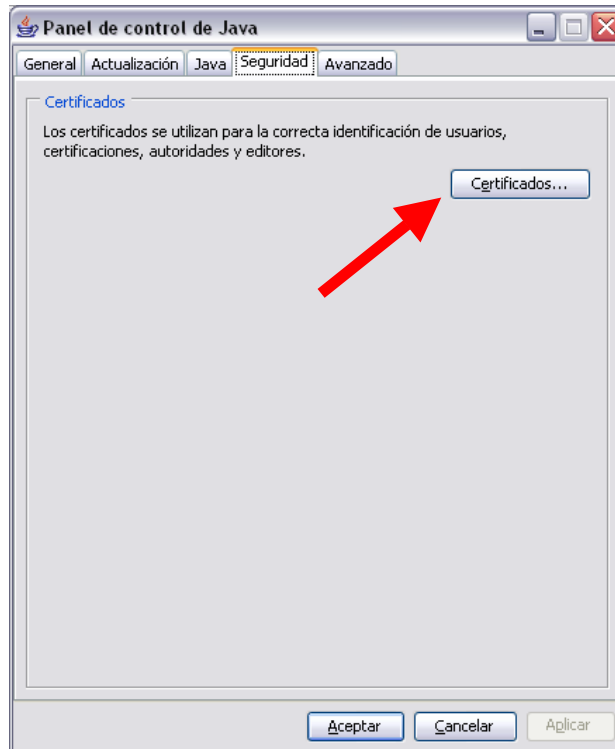


Figura: Panel de Control de la Versión JRE de Sun 1.5\_X

Accedemos a la pestaña **Seguridad** y pulsamos en el botón **Certificados**:



En la siguiente ventana que nos aparece seleccionamos del menú desplegable la opción **CA de firmante** según se muestra en la figura:

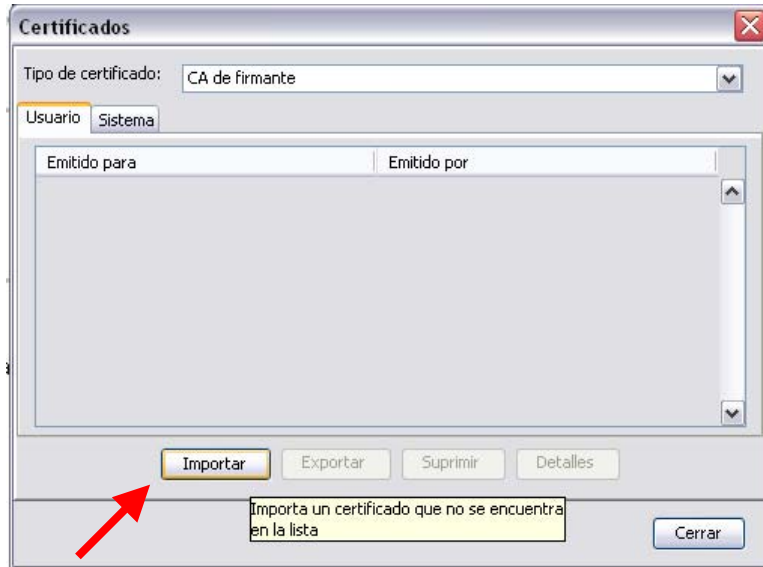


## Ayuda para la instalación Componente Firma Digital



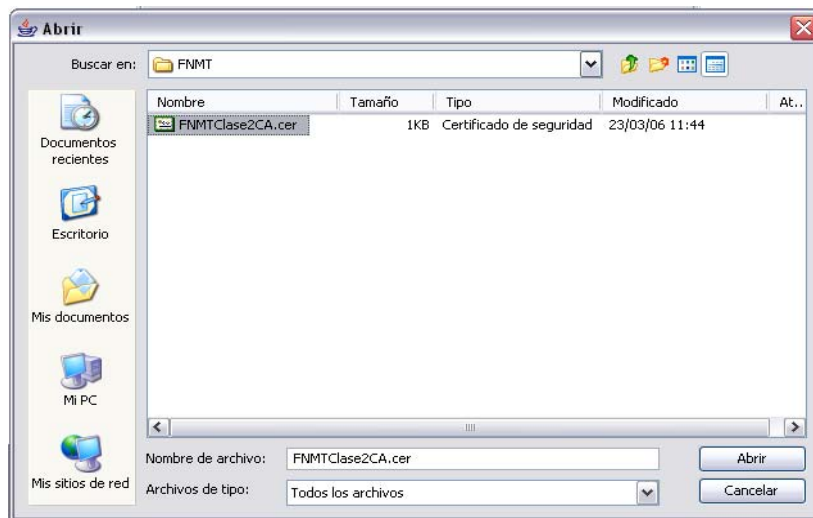
23-03-2006

Y en la pestaña de **Usuario** pulsamos en el botón **Importar**:



El certificado que debemos importar dentro del panel de control Java es el de la FNMT el cual corresponde a la autoridad de certificación que garantizó que el componente que se descarga en el ordenador es seguro. Para ello, accederemos a la dirección <http://www.cert.fnmt.es/clase2/main.htm> desde donde podremos descargar el certificado raíz de la FNMT a nuestro ordenador.

Un vez descargado lo importaremos pulsando en el botón **importar** el cual nos abrirá una ventana de explorador de nuestro disco para que seleccionemos el certificado a importar. Buscaremos el certificado raíz de la FNMT descargado de forma similar a la que se muestra en la figura:

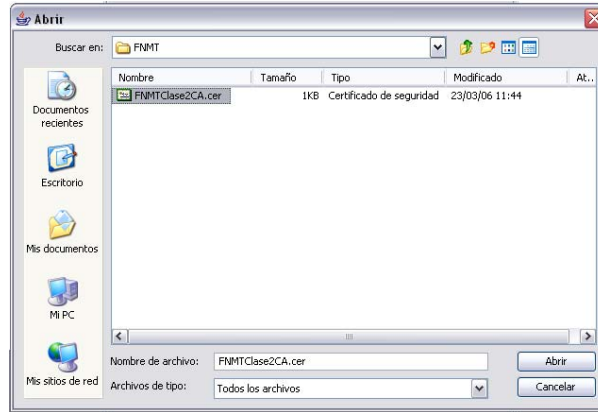


## Ayuda para la instalación Componente Firma Digital

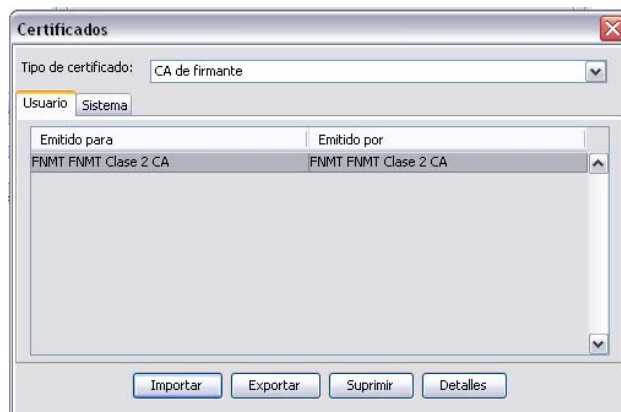


23-03-2006

Una vez seleccionado pulsamos en el botón **Abrir** lo que cargará el certificado dentro del almacén de confianza de la máquina virtual Java:



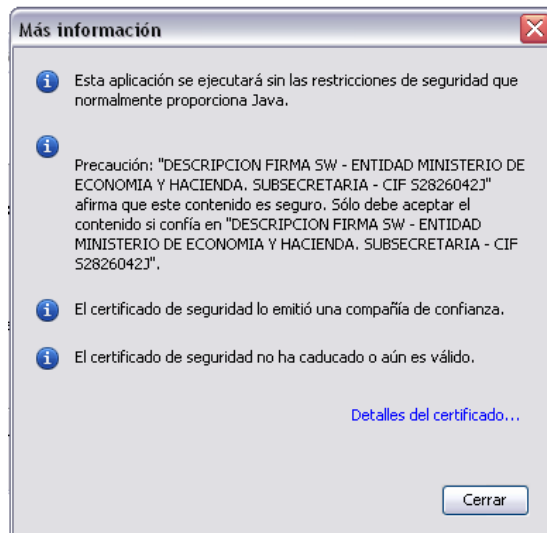
Tras seleccionarlo visualizaremos la siguiente pantalla:



Tras importar el certificado al descargarse el componente de firma en el navegador se visualizará una ventana similar a la que se muestra a continuación:



En el mensaje que se visualiza podemos acceder a la información del certificado digital que se utilizó para firmar digitalmente el componente que se descarga y garantizar así la procedencia. Para ello pulsaremos sobre el texto **Más información...** lo que nos visualizará una ventana como la que se muestra a continuación:



En la ventana se indica que el componente ha sido firmado por el certificado de software del Ministerio de Economía y Hacienda, que el certificado es válido y que además es de confianza.

Este mensaje se visualizará siempre que se ejecute el componente de firma salvo que deseemos confiar siempre en el contenido, para lo que se marcará la opción **Confiar siempre en el contenido de este editor** según se indica en la imagen siguiente:



Una vez marcado pulsaremos en el botón **Ejecutar** para permitir que el componente se instale correctamente.

	<p><b>Ayuda para la instalación Componente Firma Digital</b></p>	 <p>MINISTERIO DE ECONOMÍA Y HACIENDA</p> <p><b>23-03-2006</b></p>
--	--	---

En caso de utilizar una máquina virtual Java versión 1.4\_X, cuando se descarga el componente de firma al usuario le aparecerá siempre la ventana de confirmación de instalación de componente de firma excepto si en dicha ventana pulsa en el botón **Siempre**, lo que le indicará a la máquina virtual Java que es un componente de confianza. Sin embargo si pulsa en el botón **Sí** el componente se descargará e instalará correctamente pero si cierra el navegador y posteriormente vuelve a acceder a una página donde resida el componente le volverá a preguntar si desea instalarlo.

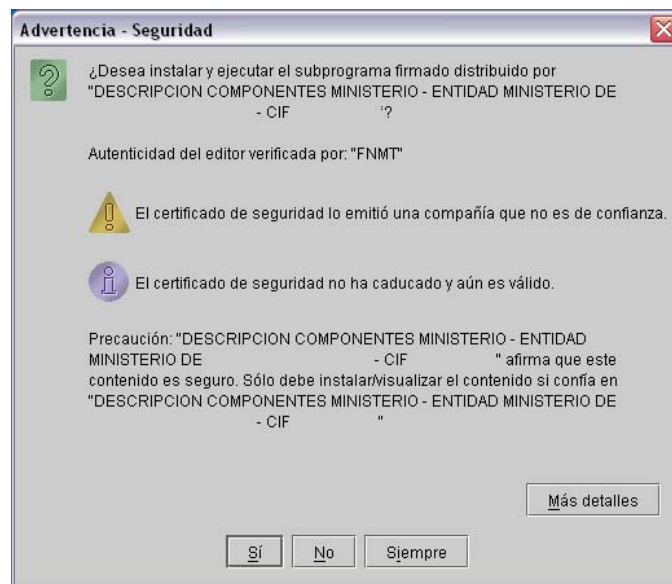


Figura: Ventana de Aviso utilizando JRE 1.4\_X

### 1.3.2 INSTALACIÓN DEL MÓDULO DE SEGURIDAD PARA EL USO DE CERTIFICADOS EN TARJETA CRIPTOGRÁFICA

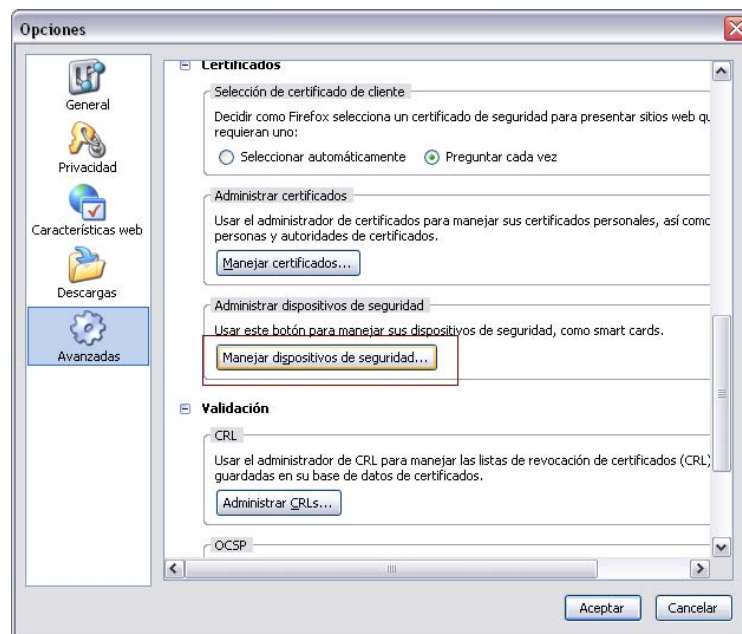
Para los certificados digitales del DNI electrónico existe un programa que permite la configuración automática de los Proveedores Criptográficos necesarios para su utilización tanto en navegadores Internet Explorer, como en Firefox o Netscape. Para obtener dicho software basta con instalar en el programa que se encuentra en la dirección:

[http://www.dnielectronico.es/descargas/CSP\\_para\\_Sistemas\\_Windows/index.html](http://www.dnielectronico.es/descargas/CSP_para_Sistemas_Windows/index.html)

El cual configura correctamente los módulos necesarios para la utilización del DNI Electrónico.

Sin embargo, en caso de querer utilizar otros certificados digitales que se encuentren en tarjetas criptográficas, por ejemplo emitidos por la FNMT, es necesario realizar la instalación manual del dispositivo de seguridad dentro del navegador Firefox. Para ello es necesario realizar las siguientes tareas:

- Descargar el software de seguridad de la FNMT disponible en la dirección <http://www.cert.fnmt.es/pilotos/soporte.htm> . Este software funciona correctamente para navegadores Netscape e Internet Explorer, pero hasta la fecha, no instala de forma automática las librerías de acceso a la tarjeta criptográfica para Firefox. Una vez instalado el software será necesario realizar tareas adicionales para que Firefox permita el uso de certificados en tarjeta criptográfica.
- Abriremos el Firefox e iremos al menú **Herramientas > Opciones > Avanzadas > Manejar dispositivos de seguridad.** (ver imagen)

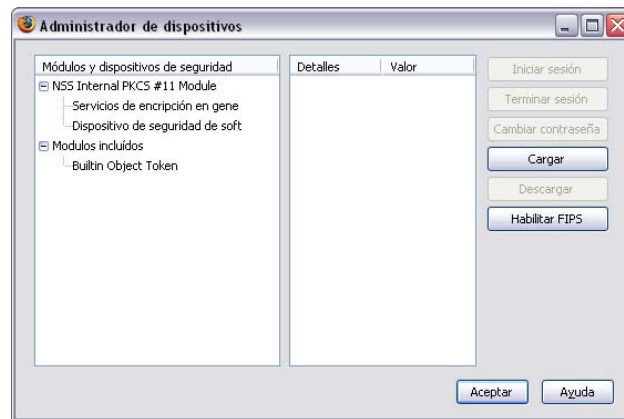


## Ayuda para la instalación Componente Firma Digital

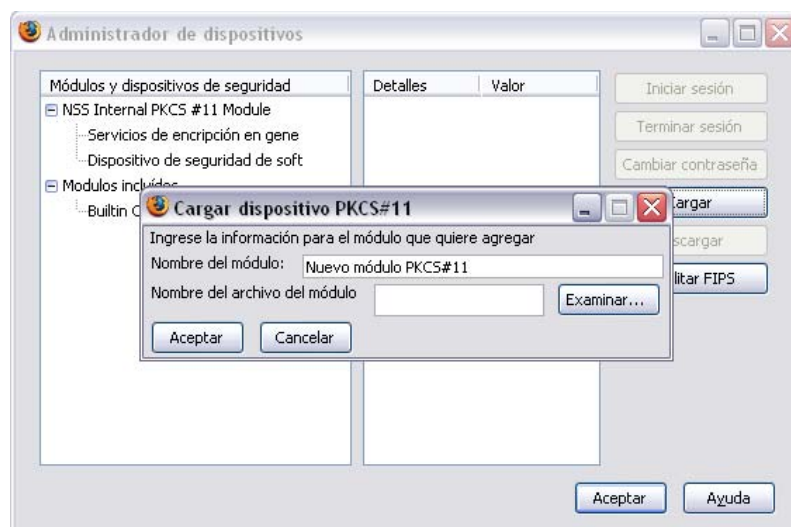


23-03-2006

- Una vez pulsado el botón nos aparecerá una ventana donde se nos muestran los módulos de seguridad instalados, la ventana mostrará un contenido similar al de la siguiente imagen



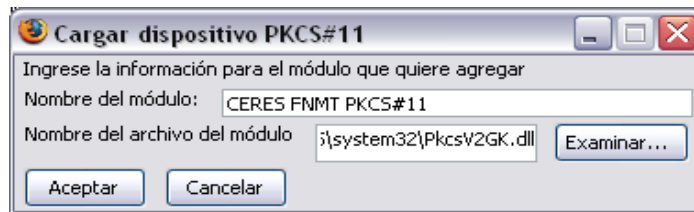
- Seguidamente procederemos a instalar el módulo de seguridad para el acceso a la tarjeta CERES de la FNMT (este proceso sería similar para cualquier otro proveedor de certificados). Para ello, pulsaremos el botón **Cargar** y nos aparecerá una ventana como la siguiente



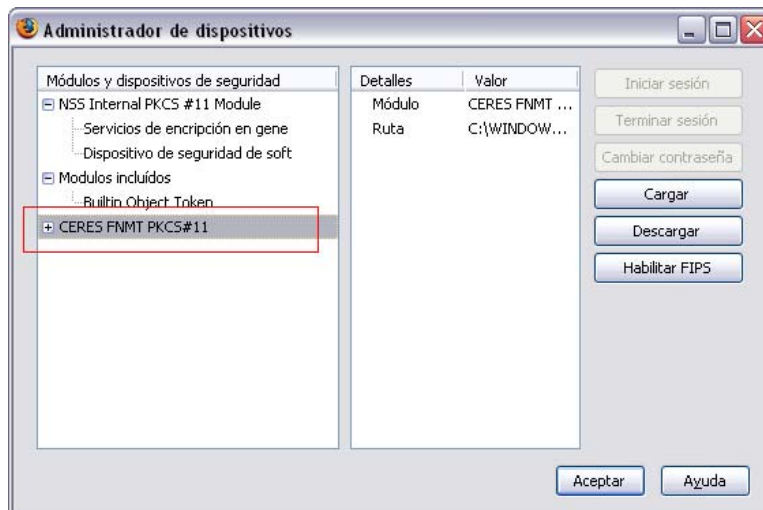
## Ayuda para la instalación Componente Firma Digital



- Borraremos el texto “Nuevo módulo PKCS#11” y teclearemos el nombre que le vamos a dar al módulo de seguridad, por ejemplo *CERES FNMT PKCS#11*. A continuación de tenemos que indicar qué librería del sistema contiene las funciones de comunicación, pulsaremos en el botón Examinar... y buscaremos en la ventana de explorador del sistema un fichero con el nombre **PkcsV2GK.dll** (dependiendo del sistema operativo Windows que posea el usuario puede encontrarse dentro del directorio WINDOWS/system32 o WINDOWS/system). El resultado de este proceso será algo similar a lo que muestra la siguiente imagen:



- Una vez rellenado pulsaremos en el botón **Aceptar**, se nos volverá a pedir confirmación de la instalación, volveremos a pulsar en **Aceptar**. Una vez instalado correctamente volveremos a la ventana anterior resultando en algo similar a la que se muestra en la siguiente imagen:



- A continuación pulsamos en **Aceptar** para finalizar el proceso. Aceptaremos otra vez para cerrar la ventana de opciones y seguidamente cerraremos y volveremos a abrir el Firefox para que los cambios realizados tengan efecto. A partir de ese momento el navegador ya será capaz de manejar los certificados de la FNMT que se encuentren en tarjetas criptográficas.

Todo este proceso no es posible realizarlo de forma automática debido a que el software criptográfico ofrecido por la FNMT no lo permite.