Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Manual Curso de Registro Certificado de clase 2

Internet Explorer

Índice

1. Introducción

En el presente documento el usuario va a obtener información completa sobre la obtención del Certificado de Clase 2, tanto en soporte software como en tarjeta, la exportación e importación de los mismos de uno a otro soporte y su uso.

Comenzaremos este manual dando unas ligeras nociones sobre los certificados.

Definición del certificado según el Real Decreto-Ley 14/1999, de 17 de Septiembre, sobre firma electrónica: es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

El certificado de clave pública, también denominado certificado de usuario contiene las claves públicas de un usuario, junto con alguna otra información, hechas infalsificables por el cifrado con la clave privada de la autoridad de certificación que lo emitió.

2. Obtención del certificado de clase 2

Existen principalmente dos formas de obtener el certificado de clase 2, una es en software y otra en tarjeta, a continuación se detallan los pasos a seguir y que se debe de hacer cuando ya se tiene un certificado y posteriormente se desea importar a una tarjeta.

Accediendo a la página CERES FNMT-RCM http://www.cert.fnmt.es/ se obtendrá toda la información relativa a la Entidad Certificadora y la forma de obtener el certificados de clase 2.

Los pasos para la obtención de ambos certificados son similares, a excepción de la realización de la copia de seguridad del certificado, ya que si genera la clave privada del certificado directamente en la tarjeta no podrá realizar una copia del certificado al ser imposible extraer esta clave de la tarjeta.

PROCESO DE OBTENCIÓN DEL CERTIFICADO

El primero de los pasos consiste en la descarga del certificado raíz de la CA, esto permite al navegador del usuario reconocer a la FNMT-RCM como Autoridad de Certificación.

Para comenzar el proceso, abra su navegador en la página
http://www.cert.fnmt.es/clase2/tarjeta/main.htm
y acceda al enlace
Descarga del Certificado Raíz de la FNMT·RCM.

Se deberá indicar que desea "**Abrir**" el fichero que contiene el certificado raíz de la FNMT-RCM. Aparecerá una pantalla con información sobre el contenido del certificado. Pulse en el botón "**Instalar certificado**". Se iniciará un asistente para la instalación del certificado raíz de la FNMT-RCM. Continuar el asistente eligiendo el repositorio de certificados indicado por defecto. Al finalizar el asistente, aparecerá una caja de diálogo en la que se indicará que se va a instalar un certificado que contiene la siguiente información:

- **Emisor**: "FNMT Clase 2 CA".
- **Número de serie** expresado en hexadecimal: "36:F1:1B:19".
- **Huella digital** expresada con el algoritmo md5: "25: 9D: CF: 5E: B3: 25: 9D: 95: B9: 3F: 00: 86: 5F: 47: 94: 3D".
- **Fecha de caducidad: 18 de marzo del año 2019**

Indicar que “sí” se desea agregar el certificado raíz al repositorio de certificados.

Para que la instalación del certificado raíz no interfiera en el posterior funcionamiento del certificado cliente será necesario que otorgue una serie de permisos al mismo. Estos permisos se configuran en las **opciones avanzadas** del certificado. A estas podemos acceder a través del navegador en el menú:
Herramientas → Opciones de Internet →Contenido → Certificados → Entidades Emisoras de Certificados Raíz de Confianza

en este apartado seleccionaremos el certificado **FNMT CLASE 2 CA** y pulsaremos en **Avanzadas,** en esta nueva pantalla veremos las acciones para las que esta habilitado el certificado, lo más recomendable es que todas estén marcadas.

Este paso no es necesario realizarlo en este momento y puede realizarse a posteriori, pero si se realiza en primer lugar evita pequeños problemas que aumentan el número de incidencias de forma considerable.

Una vez instalado el certificado raíz de la CA se pasará a **solicitar el certificado de usuario.**

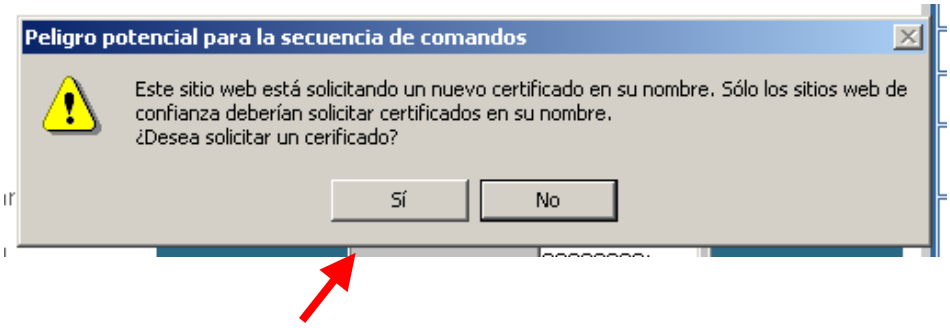
2.1. Certificados software

Una vez en http://www.cert.fnmt.es/ iremos al enlace CERTIFICADO DE USUARIO DE LA FNMT OBTENCIÓN donde se presenta el proceso a seguir.

- **Solicitud vía Internet de su Certificado**

Una vez en esta página de deberá cumplimentar el NIF siguiendo los patrones indicados en la figura y pulsar en **Enviar petición.**

Aparece una advertencia sobre la solicitud del certificado a su nombre, pulse **Si**.



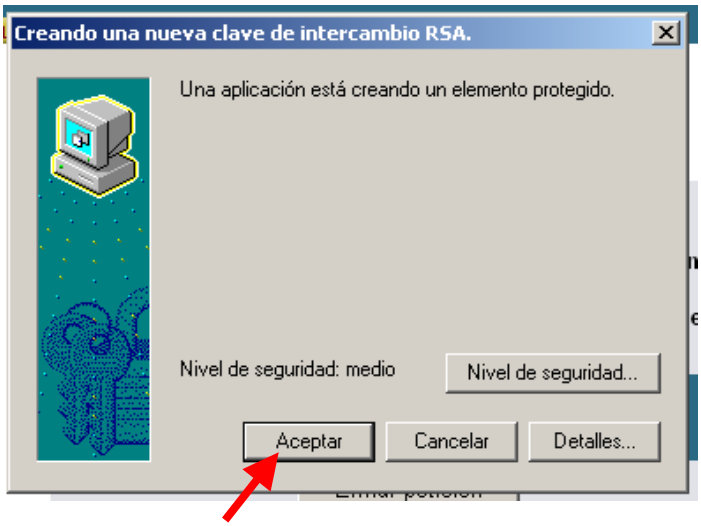
El navegador generará entonces su pareja de claves pública y privada. La longitud de la clave es elegida automáticamente por la página escogiendo la mayor longitud disponible en el navegador.

La siguiente ventana muestra un cuadro de dialogo que le permite establecer el nivel de seguridad para almacenar el certificado en el navegador.

Si desea seleccionar un nivel de seguridad determinado deberá pulsar el botón 'Nivel de Seguridad'

Se pueden establecer tres niveles de seguridad:

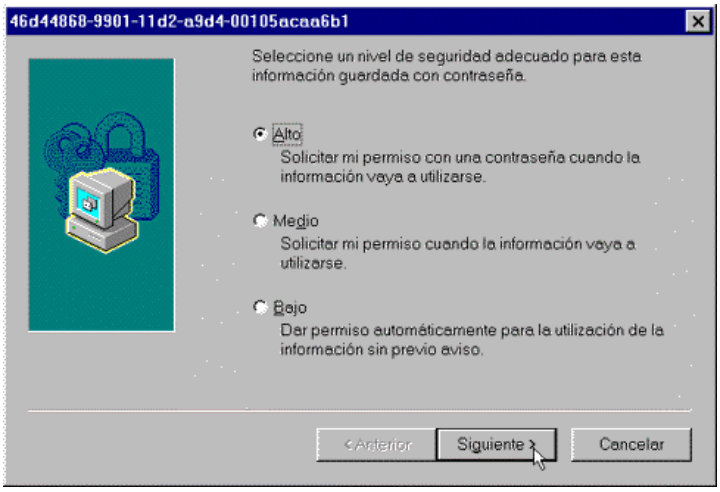
- Alto: Se indicará que el perfil va a ser utilizado y se pedirá un nombre descriptivo para el certificado y una contraseña que será solicitada cada vez que se requiera el mismo.
- Medio: Se indicará que el perfil va a ser utilizado
- Bajo: El uso del certificado se realizará de forma transparente.



Pulse Aceptar

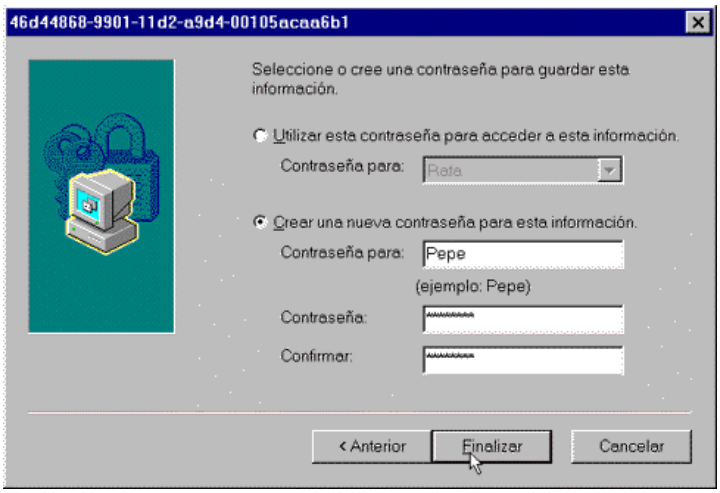
NOTA

Si pulsa el botón 'Nivel de seguridad' se mostrará la siguiente ventana:



En el caso de que usted no sea la única persona que tenga acceso a su PC se recomienda encarecidamente que active la opción 'Alto'.

Pinche el botón "Siguiente". Se mostrará la siguiente pantalla:



Si es la primera vez que crea una contraseña para este tipo de información, deberá:

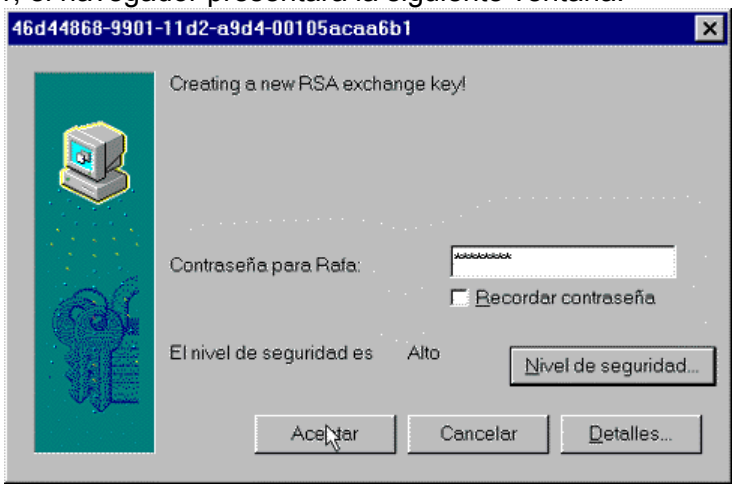
Identificar la contraseña con un nombre en la casilla <**Contraseña para**:> .

- Teclear la contraseña en la casilla <Contraseña>.
- Repetir la contraseña en la casilla <Confirmar>.

En el caso de que ya hubiera creado contraseñas anteriormente, podrá activar la opción <Utilizar esta contraseña para acceder a mi información> y seleccionar la que desee.

Importante :Recuerde sus contraseñas, si las olvida no podrá hacer uso de sus certificados.

En el caso de que el usuario haya seleccionado las opciones Alto o Medio en la ventana anterior, el navegador presentará la siguiente ventana:



El usuario deberá teclear la contraseña en la casilla <**Contraseña para**:>.

Pinche el botón "Aceptar". Si el navegador le muestre algún mensaje de error deberá volver al primer paso.

Si no ha habido ningún error el navegador habrá enviado su clave pública a la FNMT-RCM y le mostrará una pantalla en la que figura su código de solicitud del certificado.

Este código deberá ser presentado obligatoriamente en las oficinas de acreditación y cuando vaya a realizar la descarga del certificado. Por ello le recomendamos que lo imprima.

Finalmente, deberá pulsar "**Volver a la página principal**"

AVISO Importante

- La solicitud y la obtención del certificado de usuario deben ser realizadas desde el mismo equipo, navegador y usuario.
- No actualice su versión de navegador, formatee su disco duro, o cambie de ordenador o versión de Windows entre la solicitud del certificado y la obtención del certificado.
- Si ocurre alguna de las circunstancias anteriores, no acuda a acreditarse con el código de solicitud del certificado que haya obtenido, deséchelo, realice una nueva solicitud y acuda a acreditarse con el nuevo código de solicitud.
- Los usuarios de Microsoft Internet Explorer cuyo Nombre o Apellidos contengan la letra "ñ", deberán solicitar su certificado con la Versión 5.0 de IE o superior.

➢ Acreditación de la Identidad

Con el código de solicitud del paso anterior, deberá personarse en una oficina de registro para acreditar su identidad aportando la documentación necesaria:

- DNI, pasaporte español o tarjeta de residencia (NIE)
- Código de solicitud del certificado

Una vez identificado, el interesado deberá proceder a firmar el modelo de solicitud del certificado y sus condiciones de utilización.

➢ Descarga del Certificado

Pasadas 48 horas desde la acreditación en la oficina de registro podrá procederse a la **descarga del certificado de usuario**.

Para descargar el certificado debe usar el mismo ordenador que en el paso de Solicitud.

Para comenzar el proceso, abra su navegador en la página

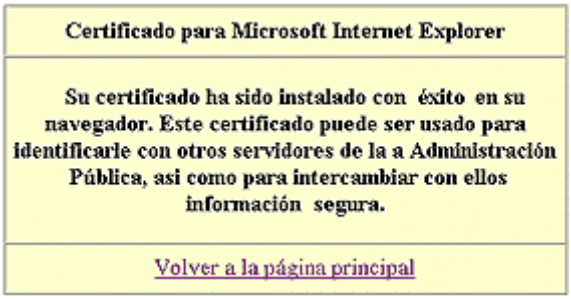
http://www.cert.fnmt.es/clase2/descargacert/maindesca.htm

Una vez en el apartado de descarga aparecerá una pantalla solicitando su NIF y el código de usuario adquirido en el paso de **solicitud del certificado de usuario:**

Cumplimentar el formulario teniendo en cuenta que si es necesario hay que rellenar con ceros a la izquierda el campo de DNI y pulsar el botón "**Descargar el Certificado**" para completar la obtención del Certificado de Usuario de la FNMT.

Si no se rellenasen de forma correcta los datos o existiese algún error como estar intentando descargar el certificado en un equipo diferente o con un usuario diferente al que se generó la clave privada se mostrará en pantalla, en caso contrario se indicará que la operación se ha realizado con éxito.

Una vez que el navegador haya obtenido el certificado le mostrará la siguiente pantalla:



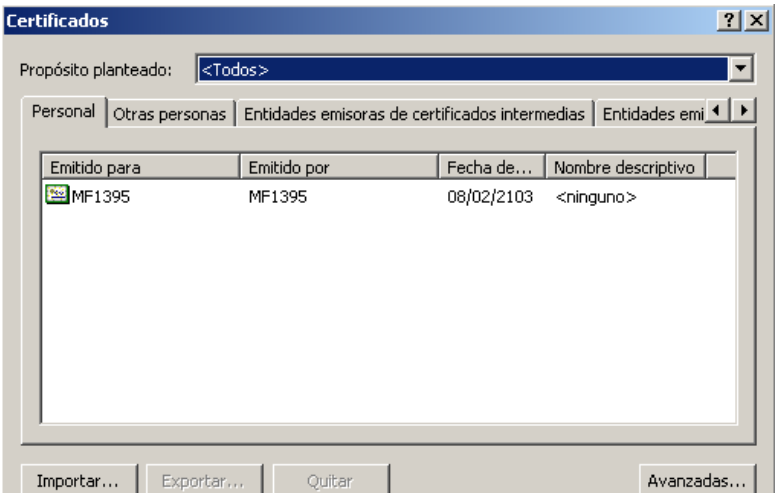
El Certificado de Usuario habrá quedado instalado en su navegador Internet Explorer.

Comprobación

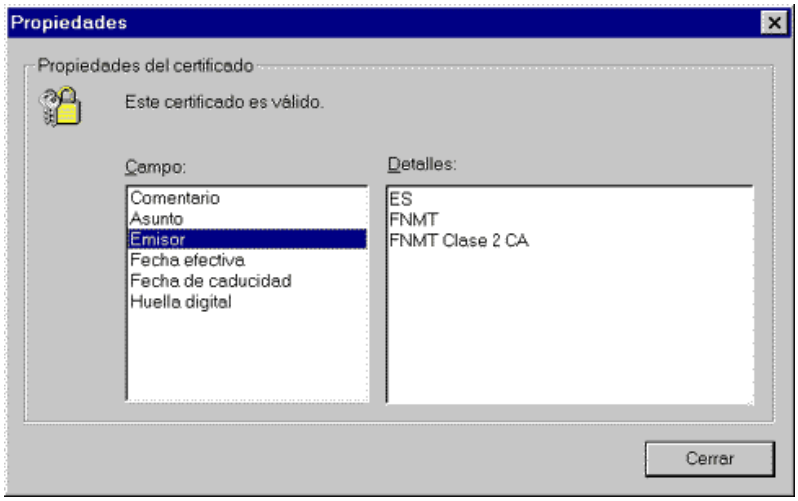
Para comprobar si la descarga del certificado ha sido correcta:

- Diríjase al menú 'Herramientas'
- Seleccione 'Opciones de Internet'
- Seleccione la solapa 'Contenido'

Aparecerá una entrada con su nombre.



Al pulsar **"Ver certificado"** deberá ver, entre otros datos, que el emisor del certificado es FNMT Certificado de Usuario.



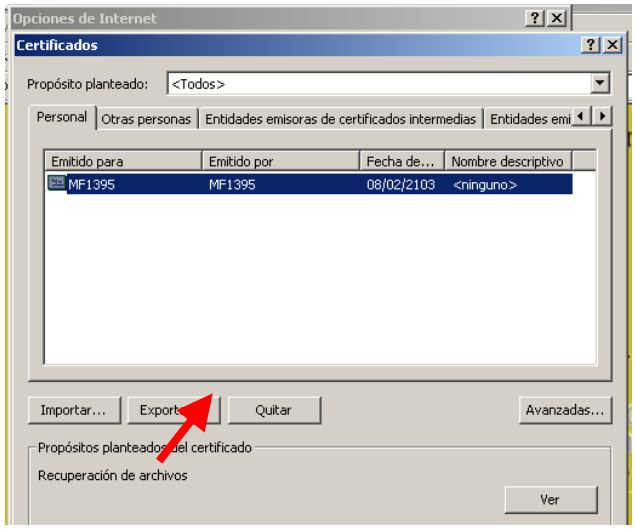
Para habilitar los propósitos para los que puede utilizar el certificado deberé ir a **Herramientas** → **Opciones de Internet** → **Contenido** una vez en este apartado ir a la opción **Certificados** seleccionar la opción **Personal,** seleccionaremos el certificado y pulsaremos en **Avanzadas** donde ya seleccionaremos las utilidades que queramos darle al certificado, es recomendable seleccionar todas las opciones.

Copia de Seguridad (Exportación del Certificado)

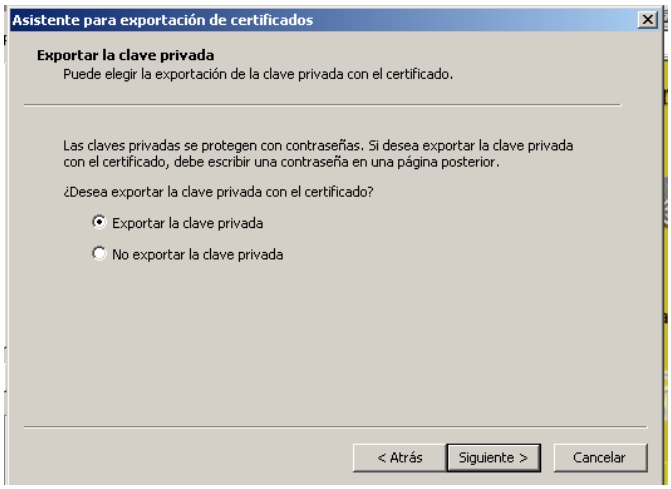
Si el certificado se genera en formato software es conveniente realizar una **copia de seguridad** del certificado, esto se consigue haciendo una exportación del certificado.

Para exportar certificados personales en Internet Explorer deberemos seguir los siguientes pasos:

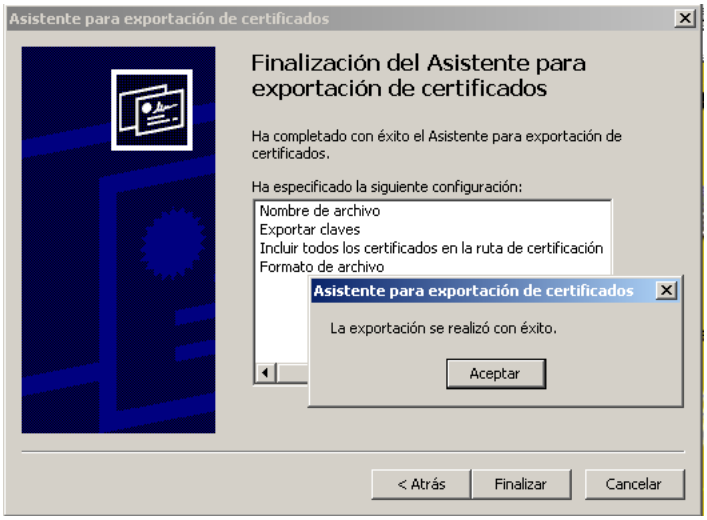
Acceder al menú:
Herramientas → **Opciones de Internet** → **Contenido**. En el apartado de certificados pulsaremos el botón de **Certificados** y una vez en la ventana pulsaremos la pestaña **Personal**. Aquí se nos muestra una pantalla con la relación de certificados personales instalados en nuestro navegador, seleccionamos el que queremos exportar y pulsamos el botón de **Exportar**.



A partir de este momento nos guiará un asistente de Windows, podemos elegir entre exportar la clave privada o no, dependiendo del uso que queramos hacer del certificado.



En el caso de que decidamos exportar la clave privada (necesario para volver a exportar el certificado con su clave privada), seguiremos los siguientes pasos:
Dejaremos las opciones tal y como se nos muestran por defecto y pulsamos **Siguiente**. Llegaremos a una pantalla donde se nos pide una contraseña y su validación para proteger el archivo que contiene el certificado exportado, la introducimos y pulsamos el botón **Siguiente**. En el siguiente cuadro de diálogo indicaremos la ruta y el nombre del archivo que queremos que contenga el certificado exportado, pulsamos el botón **Siguiente**. A continuación se nos muestra una ventana con las características del certificado exportado, pulsamos el botón **Finalizar** y nos aparece un mensaje de aviso diciendo que la clave privada va a ser exportada, pulsamos **Aceptar** y si la operación ha sido correcta se nos mostrará un cuadro informándonos de que la exportación se realizó con éxito.



En el caso de que no se desee exportar la clave privada deberemos seguir los siguientes pasos:

Seleccionamos la opción de **No exportar la clave privada** y pulsamos **Siguiente**. Marcaremos la opción de Estándar de sintaxis de mensajes cifrados y pulsamos **Siguiente**. Introducimos la ruta y el nombre del archivo que contendrá el certificado exportado. A continuación se nos muestra una pantalla con las propiedades del certificado exportado, pulsamos **Finalizar** y si la operación la hemos realizado correctamente nos aparecerá un mensaje confirmándonos la exportación correcta del certificado.

Exportar el certificado con su clave privada solo para su uso personal o como copia de seguridad. La clave privada servirá para realizar firma digital.

El certificado sin la clave privada podrá exportarlo para entregarlo a todo aquella persona con la desee comunicarse de forma segura.

2.2. Certificados Tarjeta

La identidad del usuario, al igual que su capacidad de firma, se encuentra, en el caso de máxima seguridad, almacenada en una tarjeta inteligente, que no puede ser accesible salvo por su propietario cuando introduzca el número de identificación personal, similar a la clave de una tarjeta de crédito.

Para comenzar el proceso, abra su navegador en la página

http://www.cert.fnmt.es/

y acceda al apartado de "INFORMACIÓN Y SERVICIOS" soporte "**en tarjeta criptográfica".**
Acceda al enlace "Solicitud del Certificado de Usuario":

Aun tratándose del mismo interfaz deberá hacerse la selección del proceso adecuado, es decir, utilizar el procedimiento de obtención del certificado en tarjeta.

1. Descarga del Certificado Raíz de la FNMT·RCM
2. En caso de no tener instalado el lector de tarjetas
    1. Instalación de los Componentes Base de Microsoft en el caso de Windows 95 y 98.
    2. Instalación de los drivers del lector.
3. Instalación del Software incluido en el CD-ROM que habrá recibido junto a la tarjeta criptográfica. Siga las instrucciones contenidas en dicho CD-ROM. Si no ha recibido el software, descárguelo.
4. Solicitud de Certificado de Usuario
5. Acreditación de la Identidad
6. Descarga del Certificado

Los pasos 4 al 6 son semejantes a los del certificado en software

AVISOS IMPORTANTES

- La solicitud y la obtención del certificado de usuario deben ser realizadas desde el **mismo equipo, navegador y usuario.**
- **Asegúrese de cual es su usuario de Windows.** Si Ud. no está seguro del usuario de Windows que está utilizando, reinicie su equipo antes de realizar la solicitud del certificado.
- **No actualice su versión de navegador, formatee su disco duro, o cambie de ordenador o versión de Windows** entre la solicitud del certificado y la obtención del certificado.

- Si ocurre alguna de las circunstancias anteriores, no acuda a acreditarse con el código de solicitud del certificado que haya obtenido, deséchelo, realice una nueva solicitud y acuda a acreditarse con el nuevo código de solicitud.
- Recuerde: los usuarios de Microsoft Internet Explorer cuyo **Nombre o Apellidos contengan la letra "Ñ"**, deberán solicitar su certificado con la Versión 5.0 de IE o superior.
- Guarde el sobre que contiene las claves de su tarjeta.
- En caso de error a la hora de solicitar el certificado, podrá repetir el proceso hasta **tres veces**.

PASOS A SEGUIR 4 a 6

Paso 4.

Introduzca la tarjeta criptográfica en el lector de tarjetas.

Al pulsar el enlace "Solicitud de Certificado" aparecerá un formulario que deberá cumplimentar con el NIF del titular del certificado.

Pulse **"Enviar petición"**.

Aparecerá un cuadro de diálogo mediante el cual deberá validarse como usuario de la tarjeta introduciendo el PIN que se le ha facilitado con la tarjeta.

Si no ha habido ningún error el navegador habrá enviado su clave pública a la FNMT-RCM y le mostrará una pantalla en la que figura su código de solicitud del certificado.

Este código deberá ser presentado **obligatoriamente** en las oficinas de Registro y cuando vaya a descargar el certificado.

Imprima la pantalla en la que figura su código para no olvidarlo.

Finalmente, pinche el botón **"Volver a la página principal"**

Paso 5

El titular deberá personarse en una Oficina de Registro aportando la documentación necesaria. Una vez identificado, el interesado deberá proceder a firmar el modelo de solicitud del certificado y sus condiciones de utilización.

La documentación necesaria para el registro es:

Documento que acredite su identidad (DNI, pasaporte o tarjeta de residencia).
El código de solicitud del certificado.

Paso 6

Pasadas 48 horas desde la acreditación en la oficina de registro podrá procederse a la **descarga del certificado de usuario**.
Para comenzar el proceso, abra su navegador en la página http://www.cert.fnmt.es/clase2 y acceda al apartado de "soporte en tarjeta criptográfica". Acceda al enlace "Descarga del Certificado".

Importante: habrá de utilizar el mismo navegador que haya utilizado para solicitar el certificado y el mismo usuario.

Si va a obtener su certificado en tarjeta debe estar introducida en el lector antes de descargar el certificado.

Deberá cumplimentar los datos que se le presenten y pinchar el botón **Descargar**.

En caso de que la cumplimentación se haya realizado de forma incorrecta el navegador mostrará una página informándole del error y deberá cumplimentar de nuevo los datos

Importación del certificado software a tarjeta

Si usted tiene un certificado con una longitud de clave de 1024 bits emitido ya sea con Netscape o con Internet Explorer podrá importarlo en una tarjeta criptográfica desde el navegador.

Para comprobar la longitud de clave de su certificado en Internet Explorer deberá ir a ver las propiedades avanzadas del mismo y comprobar la entrada Clave pública.

Primero.- Exportación del certificado en software a disquete:

Acceder al menú Herramientas, Opciones de Internet, y una vez allí seleccionaremos la pestaña Contenido. En el apartado de certificados pulsaremos el botón de Certificados y una vez en la ventana pulsaremos la pestaña Personal. Aquí se nos muestra una pantalla con la relación de certificados personales instalados en nuestro navegador, seleccionamos el que queremos exportar y pulsamos el botón de Exportar.

A partir de este momento nos guiará un asistente de Windows, podemos elegir entre exportar la clave privada o no, para su posterior paso a tarjeta es necesario exportar la clave privada seguiremos los siguientes pasos:

1. Dejaremos las opciones tal y como se nos muestran por defecto y pulsamos Siguiente.

2. Llegaremos a una pantalla donde se nos pide una contraseña y su validación para proteger el archivo que contiene el certificado exportado, las introducimos y pulsamos el botón Siguiente.

3. En el siguiente cuadro de diálogo indicaremos la ruta y el nombre del archivo que queremos que contenga el certificado exportado, pulsamos el botón 'Siguiente'.

4. A continuación se nos muestra una ventana con las características del certificado exportado, pulsamos el botón Finalizar y nos aparece un mensaje de aviso diciendo que la clave privada va a ser exportada, pulsamos Aceptar y si la operación ha sido correcta se nos mostrará un mensaje confirmándonos la exportación correcta del certificado.

Segundo.- Importación a Tarjeta

Una vez que el certificado se ha exportado al disquete procedemos a importarlo a la tarjeta siguiendo los siguientes pasos:

Inicio → Programas → FNMT-RCM → Tarjeta → Importador de certificados

1. Aparecerá el asistente para la importación de certificados
2. Seleccionar el archivo del certificado (en disquete)
3. Introducir la contraseña del disquete

Continuar las indicaciones del asistente hasta finalizar el proceso.

3. Uso de los certificados

En este apartado se explica el uso de los certificados para los elementos que instala Internet Explorer en nuestro equipo en este caso el propio navegador y el Outlook Express.

Información sobre versiones: se recomienda la utilización de una versión actualizada de Microsoft Internet Explorer.

Si tiene su certificado en tarjeta introdúzcala en el lector de tarjetas.
Cuando el navegador se disponga a entrar en una página en la que se solicite un certificado de usuario de Clase 2, mostrará una caja de diálogo en la que estará incluido su certificado.

Una vez seleccionado éste dependiendo de si el certificado está en software y el nivel de seguridad asociado al mismo, o de si el certificado está en tarjeta se le solicitará la clave de acceso al certificado. Si tiene el certificado en software con un nivel de seguridad alto el navegador le requerirá la clave con la que esta protegido el certificado. Si tiene tarjeta le solicitará el PIN de Usuario de la misma.

A partir de ese momento, Vd. se estará identificando ante el servidor Web con su certificado FNMT Clase 2 CA.

4. Correo electrónico seguro

Haciendo uso del certificado FNMT Clase 2 CA podrá enviar y recibir correo electrónico cifrado y/o firmado digitalmente.

Configuración de la aplicación de correo para el uso del certificado

Introduzca su tarjeta criptográfica en el lector de tarjetas, si tiene el certificado en la misma. Acceda al menú **Herramientas Opciones** y, dentro de él, a la pestaña **Seguridad**. Pulsar el botón **Opciones avanzadas...**.En la sección **Mensajes firmados digitalmente**, activar la casilla **Incluir mi identificador digital al enviar mensajes firmados**.

Por otra parte, si Vd. activa la casilla **Agregar certificados de remitentes a mi libreta de direcciones automáticamente**, cuando algún usuario que esté incluido en su libreta de direcciones le envíe un mensaje firmado, su certificado digital será almacenado de forma automática en la entrada correspondiente dentro de la libreta de direcciones.

Enviando CORREOS ELECTRÓNICOS CIFRADOS Y/O FIRMADOS

Vd. podrá configurar su aplicación de correo Microsoft Outlook para que todos los mensajes de correo que Vd. envíe sean automáticamente firmados y/o cifrados electrónicamente.

Para ello, bastará con que acceda al menú **Herramientas Opciones** y, dentro de él, a la pestaña **Seguridad** y active la casilla **Cifrar contenido y datos adjuntos para mensajes salientes** si desea cifrar todos los mensajes salientes, y/o **Firmar digitalmente todos los mensajes salientes**, si desea firmar todos los mensajes salientes.

Si Vd. desea **firmar** digitalmente un determinado mensaje saliente (no todos los mensajes salientes, como se menciona al principio de este apartado), componga su mensaje de correo de la forma habitual y, antes de enviarlo, acceda al menú **Herramientas Firmar digitalmente** de la ventana de composición de mensaje.

Cuando Vd. pulse sobre el botón de envío del mensaje, la aplicación le pedirá que elija el certificado digital para firmar el mensaje. Vd. deberá elegir el certificado contenido en su tarjeta y, a continuación, la aplicación le pedirá que introduzca el PIN de la tarjeta si el certificado esta contenido en la misma o el del certificado en software si el nivel de seguridad del mismo es alto. Seguidamente, procederá al cifrado del mensaje y a su posterior envío a los destinatarios.

Importante: para poder firmar mensajes de correo electrónico, será necesario que su certificado digital contenga la dirección de correo de la cuenta desde la que desea enviar el mensaje. Si no es así, deberá acudir a la oficina de registro para revocar su certificado digital y solicitar uno nuevo con la dirección de correo correspondiente.

Si Vd. desea **cifrar** digitalmente un determinado mensaje saliente (no todos los mensajes salientes, como se menciona al principio de este apartado), componga su mensaje de correo de la forma habitual y, antes de enviarlo, acceda al menú **Herramientas Cifrar** de la ventana de composición de mensaje. Cuando Vd. Pulse sobre el botón de envío del mensaje, la aplicación cifrará el mensaje utilizando el certificado digital de cada uno de los destinatarios y, a continuación, procederá al envío del mensaje.

Importante: para poder cifrar un mensaje para un determinado destinatario será necesario que éste, previamente, le haya enviado un mensaje firmado digitalmente.

De otro modo, no será posible cifrar el mensaje para ese destinatario ya que no se tendrá copia de la clave pública necesaria para ello. Consulte el apartado "RECIBIENDO CORREOS ELECTRÓNICOS CIFRADOS Y/O FIRMADOS" para conocer la forma de copiar el certificado del usuario en su libreta de contactos cuando éste le envíe mensajes firmados.

Si Vd. desea **firmar** y **cifrar** digitalmente un determinado mensaje saliente (no todos los mensajes salientes, como se menciona al principio de este apartado), componga su mensaje de correo de la forma habitual y, antes de enviarlo, acceda a los menús **Herramientas Firmar digitalmente** y **Herramientas Cifrar** de la ventana de composición de mensaje.

Cuando Vd. pulse sobre el botón de envío del mensaje, la aplicación le pedirá que elija su certificado de Clase 2 y, a continuación, le pedirá que introduzca el PIN de la tarjeta si el certificado esta contenido en la misma o el del certificado en software si el nivel de seguridad del mismo es alto. Seguidamente, procederá a la firma digital y cifrada del mensaje, para a continuación enviarlo a sus destinatarios.

Recibiendo CORREOS ELECTRÓNICOS CIFRADOS Y/O FIRMADOS

Cuando Vd. reciba un correo electrónico **firmado** digitalmente por otro usuario, dicho mensaje tendrá asociado un icono que contendrá un sello lacrado, el cual indicará que el mensaje está firmado.

Al hacer doble click sobre el mensaje, la aplicación automáticamente procederá a la verificación de la firma digital y mostrará una ventana que contendrá el mensaje y un botón con un sello lacrado que, al pulsarlo, mostrará información sobre el certificado del firmante y sobre el resultado de la verificación de la firma del mensaje.

Según se ha indicado anteriormente, Vd. puede configurar la aplicación para que, de forma automática, cada vez que un usuario le envíe un mensaje de correo electrónico firmado, se almacene su certificado digital en la libreta de direcciones.

Si Vd. no ha configurado dicha funcionalidad, podrá aprovechar cada mensaje firmado digitalmente para extraer el certificado digital del remitente (según se ha comentado anteriormente, necesitará dicho certificado para, posteriormente, poder cifrar mensajes de correo para ese usuario). Para ello, en la ventana del mensaje firmado que le ha enviado el usuario, pulse con el botón derecho del ratón sobre la dirección de correo del remitente del mensaje y, en el menú emergente, elija la opción **Agregar a libreta de direcciones**. De ésta forma, en

caso de que Vd. Ya tuviera una entrada en la libreta de direcciones para dicho usuario, dicha entrada se actualizará con el certificado del usuario y, en caso de que no existiese una entrada, se creará una nueva que incluirá su certificado.

Cuando reciba un correo electrónico **cifrado** digitalmente por otro usuario, dicho mensaje tendrá asociado un icono que contendrá un candado, el cual indicará que el mensaje está cifrado para Vd.

Para poder abrir el mensaje, deberá introducir su tarjeta criptográfica en el lector.

Al hacer doble click sobre el mensaje, la aplicación le pedirá que introduzca el PIN de su tarjeta si el certificado esta contenido en esta o el del perfil software si el nivel de seguridad del mismo esta establecido a alto, a continuación, procederá al descifrado del mensaje para, posteriormente, mostrar su contenido e indicar el resultado del descifrado del mensaje.

Office XP

En este apartado se hará mención a la herramienta de correo instalada por Office XP y a la utilidad de firma de documentos de Word que es aplicable al resto de aplicaciones contenidas en Office XP, no estando esta última opción en versiones anteriores de Office.

CORREO ELECTRÓNICO SEGURO (Tarjeta)

Haciendo uso del certificado FNMT Clase 2 CA introducido en su tarjeta criptográfica, podrá enviar y recibir correo electrónico cifrado y/o firmado digitalmente.

Configuración de la aplicación de correo para el uso del certificado

Si tiene su certificado en tarjeta el primer paso será introducir la misma en el lector. Acceda al menú **Herramientas Opciones** y, dentro de él, a la pestaña **Seguridad.** En la sección **Correo electrónico seguro**, pulsar el botón **Configuración**. Ahora hay que asignar un nombre a la configuración de seguridad que se está creando, por ejemplo "Mi configuración de seguridad" y elegir **S/MIME** como formato de mensaje seguro. Pulsar el botón **Elegir...** tanto en la sección de **Certificado de firma** como en la de **Certificado de cifrado**, eligiendo o bien el certificado FNMT Clase 2 CA contenido en su tarjeta criptográfica o si no posee esta el que tiene configurado en su navegador. Por otra parte, seleccionar las casillas .
Configuración predeterminada para este formato de mensaje seguro,
Configuración predeterminada para todos los mensajes seguros y **Enviar estos certificados con mensajes firmados**. Pulsar el botón **Aceptar**.

Si su aplicación cliente de correo Microsoft Outlook está configurada dentro de una Red de Área Local en la que existe un servidor de correo Microsoft Exchange y en dicho servidor está definida una Libreta Global de Direcciones (Global Address List, GAL), podrá publicar su certificado de usuario en dicha GAL para que los demás usuarios puedan cifrar mensajes de correo para Vd. sin necesidad de que, previamente, Vd. les envíe copia de su certificado. Para ello, bastará con que acceda al menú **Herramientas Opciones** y, dentro de él,

a la pestaña **Seguridad** y pulse sobre el botón **Publicar a la GAL**, con lo que, automáticamente, su certificado será publicado en la GAL. Nota: si no existe dicho botón, es debido a que o bien no existe un servidor de correo Microsoft Exchange, o bien que no hay definida una Libreta Global de Direcciones en dicho servidor.

Enviando CORREOS ELECTRÓNICOS CIFRADOS Y/O FIRMADOS

Vd. podrá configurar su aplicación de correo Microsoft Outlook para que todos los mensajes de correo que Vd. envíe sean automáticamente firmados y/o cifrados electrónicamente.

Para ello, bastará con que acceda al menú **Herramientas Opciones** y, dentro de él, a la pestaña **Seguridad** y active la casilla **Cifrar contenido y datos adjuntos para mensajes salientes** si desea cifrar todos los mensajes salientes, y/o **Agregar firma digital a mensajes salientes**, si desea firmar todos los mensajes salientes.

Si Vd. desea **firmar** digitalmente un determinado mensaje saliente (no todos los mensajes salientes, como en el caso del principio de este apartado), componga su mensaje de correo de la forma habitual y, antes de enviarlo, acceda al menú **Ver ->Opciones** de la ventana de composición de mensaje y pulsar sobre el botón **Configuración de seguridad...**.Active la casilla **Agregar firma digital a este mensaje** y elija la configuración de seguridad que Vd. creó cuando configuró la aplicación de correo (por ejemplo, "Mi configuración de seguridad").

Cuando Vd. pulse sobre el botón de envío del mensaje, la aplicación le pedirá que introduzca el PIN de la tarjeta si el certificado esta contenido en la misma o la contraseña con la que esta almacenado en el navegador si el nivel de seguridad con el que configuro era alto, el mensaje será firmado digitalmente y, a continuación, será enviado a sus destinatarios.

Importante: para poder firmar mensajes de correo electrónico, será necesario que su certificado digital contenga la dirección de correo de la cuenta desde la que desea enviar el mensaje. Si no es así, deberá acudir a la oficina de registro para revocar su certificado digital y solicitar uno nuevo con la dirección de correo correspondiente.

Si Vd. desea **cifrar** digitalmente un determinado mensaje saliente (no todos los mensajes salientes, como se explica en al principio de este apartado), componga su mensaje de correo de la forma habitual y, antes de enviarlo, acceda al menú **Ver -> Opciones** de la ventana de composición de mensaje y pulsar sobre el botón **Configuración de seguridad...**.Active la casilla **Cifrar el contenido del mensaje y los datos adjuntos** y elija la configuración de seguridad que Vd. creó cuando configuró la aplicación de correo (por ejemplo, "Mi configuración de seguridad").

Cuando Vd. pulse sobre el botón de envío del mensaje, la aplicación cifrará el mensaje utilizando el certificado digital de cada uno de los destinatarios y, a continuación, procederá al envío del mensaje.

Importante: para poder cifrar un mensaje para un determinado destinatario será necesario que éste, previamente, le haya enviado un mensaje firmado digitalmente, o

bien que haya publicado su certificado en la Libreta Global de Direcciones (GAL), en caso de que ésta exista. De otro modo, no será posible cifrar el mensaje para ese destinatario ya que no se tendrá copia de la clave pública necesaria para ello.

Consulte el apartado "RECIBIENDO CORREOS ELECTRÓNICOS CIFRADOS Y/O FIRMADOS" para conocer la forma de copiar el certificado del usuario en su libreta de contactos cuando éste le envíe mensajes firmados.

Recibiendo CORREOS ELECTRÓNICOS CIFRADOS Y/O FIRMADOS

Cuando Vd. reciba un correo electrónico **firmado** digitalmente por otro usuario, dicho mensaje tendrá asociado un icono que contendrá un sello lacrado, el cual indicará que el mensaje está firmado.

Al hacer doble click sobre el mensaje, la aplicación automáticamente procederá a la verificación de la firma digital y mostrará una ventana que contendrá el mensaje y un botón con un sello lacrado que, al pulsarlo, mostrará información sobre el certificado del firmante y sobre el resultado de la verificación de la firma del mensaje.

Vd. podrá aprovechar los mensajes firmados digitalmente para extraer el certificado digital del remitente (según se ha comentado anteriormente, necesitará dicho certificado para, posteriormente, poder cifrar mensajes de correo para ese usuario).

Para ello, en la ventana del mensaje firmado que le ha enviado el usuario, pulse con el botón derecho del ratón sobre la dirección de correo del remitente del mensaje y, en el menú emergente, elija la opción "Agregar a contactos". De ésta forma, en caso de que Vd. ya tuviera una entrada en la libreta de contactos para dicho usuario, dicha entrada se actualizará con el certificado del usuario y, en caso de que no existiese una entrada, se creará una nueva que incluirá su certificado.

Cuando Vd. reciba un correo electrónico **cifrado** digitalmente por otro usuario, dicho mensaje tendrá asociado un icono que contendrá un candado, el cual indicará que el mensaje está cifrado para Vd.

Para poder abrir el mensaje, Vd. deberá introducir su tarjeta criptográfica en el lector.

Al hacer doble click sobre el mensaje, la aplicación le pedirá que introduzca el PIN de su tarjeta y, a continuación, procederá al descifrado del mensaje para, posteriormente, mostrar su contenido e indicar el resultado del descifrado del mensaje.

FIRMANDO DOCUMENTOS DE WORD

Esta es una nueva utilidad que añade Microsoft Office XP para las aplicaciones Word, Excel y PowerPoint, y que por el momento sólo sirve para usuarios que disponen de esta versión de Office, desapareciendo la firma si el documento es manipulado. El formato que se utiliza para el almacenamiento de las firmas es propietario de

Microsoft, es decir, la firma generada es un PKCS#7 pero se almacena dentro del .doc. Al estar basada esta utilidad en CryptoAPI es compatible con la tarjeta CERES.

Una vez terminado el documento y grabado puede firmarse digitalmente por uno o varios usuarios.

Para ello deberemos ir a **Herramientas Opciones**, seleccionaremos la pestaña **Seguridad** se pulsa el botón de **Firmas Digitales** aparecerá una ventana con los certificados seleccionados para firmar el documento, pulse en **Agregar** y seleccione los usuarios cuyas firmas desea incorporar en el documento y pulse Aceptar, en la barra de estado del Office aparecerá un nuevo elemento que indica que el documento esta firmado digitalmente.

Siguiendo estos mismos pasos se podrán firmar hojas de Excel y PowerPoint.

5. Estado de revocación de certificados y fecha de caducidad

Los certificados de clase 2 ya estén emitidos en tarjeta o en software tiene una duración de dos años, pudiéndose renovar desde la página web de la FNMT-RCM dos meses antes de que llegue la fecha de caducidad.

Para ver la fecha de caducidad de su certificado deberá si tiene el certificado en la tarjeta introducirla en el lector.

Para comprobar la caducidad de los certificados personales en Internet Explorer deberemos seguir los siguientes pasos:

Acceder al menú **Herramientas**, **Opciones de Internet**, una vez allí seleccionaremos la pestaña **Contenido**. En el apartado de certificados pulsaremos el botón de **Certificados** y una vez en la ventana pulsaremos la pestaña **Personal**. Aquí se nos muestra una pantalla con la relación de certificados personales instalados en nuestro navegador, seleccionamos el certificado del que queremos comprobar la caducidad, pulse en **Ver**, seleccione la pestaña de detalles y seleccione la opción **Válido hasta**.

6. Problemas más frecuentes de la obtención y el uso.

A continuación se explican los problemas más frecuentes que se producen a la hora de utilizar los certificados de clase 2 tanto en la navegación como en la utilización del correo electrónico.

Si se genera el certificado en la tarjeta directamente no se podrá crear una copia del mismo, ya que la clave privada del certificado no puede extraerse de la tarjeta.

Existe la posibilidad de generar el certificado en el navegador con una longitud de clave de 1024 bits y luego importarlo en la tarjeta con Netscape.

Diríjase al menú **Herramientas Opciones de Internet** pestaña **Contenido** botón **Certificados** pestaña **Entidades Emisoras**, busque el certificado raíz de la FNMT-RCM en caso de no estar instálelo, y si esta instalado habilite todos los usos del certificado en las opciones avanzadas.

Es recomendable que se lea las secciones de instalación certificado de la CA.

Si desea disponer en su certificado de otra cuenta de correo deberá revocar su certificado y solicitar uno nuevo con los datos adecuados.

PIN de usuario incorrecto, si no se introduce el PIN de usuario de forma correcta, se le dará la oportunidad de que vuelva a intentar conectar con el servicio de securización, recuerde que si introduce el PIN de forma incorrecta tres veces, está se bloqueará, y deberá procederse a su desbloqueo para que vuelva a ser operativa.

Este aviso aparece cuando seleccionamos un certificado que esta en la tarjeta y la misma no esta introducida en el mismo. Si pulsamos en **Cancelar** se finalizará la navegación, si se introduce la tarjeta este aviso desaparecerá pasando a solicitarse el PIN de la tarjeta.

Office XP: Cuando comprobamos un mensaje encriptado aparece la siguiente advertencia:
Esta advertencia se debe a que la FNMT-RCM emite listas de certificados revocados CRL's de forma fraccionada y este formato no esta soportado por Microsoft