



Comisión

Nacional

de Energía

Subdirección de Sistemas

**PROCEDIMIENTO OPERATIVO CON
LOS CERTIFICADOS DIGITALES
CLASE 2 CA DE LA FÁBRICA
NACIONAL DE MONEDA Y TIMBRE
REAL CASA DE LA MONEDA
(FNMT-RCM)**

15 de junio de 2009

1	<u>¿QUÉ ES EL CERTIFICADO DE USUARIO?</u>	2
1.1	PARA QUÉ SIRVE	2
1.2	¿QUÉ NECESITO PARA UTILIZAR UN CERTIFICADO DE USUARIO?	2
1.3	¿CÓMO OBTENER UN CERTIFICADO DE USUARIO?	2
2	<u>OBTENCIÓN DEL CERTIFICADO DE USUARIO EN FORMATO SOFTWARE</u>	3
2.1	PROCESO DE OBTENCIÓN	3
2.1.1	<i>SOLICITUD VÍA INTERNET DE SU CERTIFICADO.</i>	3
2.1.2	<i>ACREDITACIÓN DE LA IDENTIDAD EN UNA OFICINA DE REGISTRO.</i>	3
2.1.3	<i>DESCARGA DE SU CERTIFICADO DE USUARIO.</i>	3
3	<u>COPIA DE SEGURIDAD DEL CERTIFICADO.</u>	4
3.1	INSTRUCCIONES DE EXPORTACIÓN/IMPORTACIÓN DE CERTIFICADOS	4
3.1.1	EXPORTACIÓN DEL CERTIFICADO A FICHERO	4
3.1.2	IMPORTACIÓN DEL CERTIFICADO A OTRO NAVEGADOR DE OTRO ORDENADOR.	5
4	<u>CERTIFICADO DE USUARIO EN TARJETA CRIPTOGRÁFICA.</u>	6
4.1	REQUISITOS PREVIOS A LA SOLICITUD.	6
4.2	OBTENCIÓN DEL CERTIFICADO EN TARJETA CRIPTOGRÁFICA	7
4.2.1	<i>SOLICITUD DEL CERTIFICADO (PARA MICROSOFT INTERNET EXPLORER).</i>	7
4.2.2	<i>ACREDITACIÓN DE LA IDENTIDAD EN UNA OFICINA DE REGISTRO.</i>	7
4.2.3	<i>DESCARGA DE SU CERTIFICADO DE USUARIO.</i>	7
4.3	IMPORTACIÓN DE UN CERTIFICADO QUE SE HA SOLICITADO PREVIAMENTE EN FORMATO SOFTWARE Y EXPORTADO A FICHERO (.PFX) PARA QUE RESIDA EN TARJETA CRIPTOGRÁFICA.	8

Parte de la información descrita en este documento se ha obtenido de la Web de la FNMT-RCM <http://www.cert.fnmt.es>

1 ¿QUÉ ES EL CERTIFICADO DE USUARIO?

El certificado de usuario es un documento digital que contiene, entre otros, sus datos identificativos. Así, el certificado de usuario le permite identificarse en Internet e intercambiar información con otras personas con la garantía de que sólo Ud. y su interlocutor pueden acceder a ella.

[Más sobre criptografía básica](#)

[Más sobre certificados](#)

1.1 PARA QUÉ SIRVE

El Certificado de Usuario le permitirá realizar trámites de forma segura con la Administración Pública a través de Internet. Gracias a su certificado de usuario podrá olvidarse de desplazamientos y esperas innecesarias.

[¿Dónde puedo utilizar mi certificado de usuario?](#)

[Certificado de usuario para correo electrónico seguro](#)

1.2 ¿QUÉ NECESITO PARA UTILIZAR UN CERTIFICADO DE USUARIO?

El certificado de Usuario se utiliza a través de su propio navegador, no siendo necesaria la instalación de ningún programa adicional, excepto si la obtención o uso se realiza utilizando una tarjeta criptográfica que en el punto 4 se indicarán los requisitos necesarios.

[Navegadores válidos](#)

1.3 ¿CÓMO OBTENER UN CERTIFICADO DE USUARIO?

Cuando solicita un certificado de usuario, su navegador genera un par de claves. La clave privada se guarda en su navegador y la clave pública se envía a la FNMT-RCM. La FNMT-RCM asignará un código de solicitud a esa clave que le será remitido vía web. Entonces deberá personarse en una oficina de acreditación con su documento de identidad y dicho código. Finalmente, tras la acreditación, podrá proceder a la descarga del certificado vía web. Este quedará instalado en su navegador.

[Obtener un certificado de usuario](#)

[Más sobre obtención de certificados](#)

2 OBTENCIÓN DEL CERTIFICADO DE USUARIO EN FORMATO SOFTWARE

El certificado en formato software se define aquél que una vez obtenido y descargado, queda instalado en el navegador de Internet del ordenador y perfil (usuario) donde se ha realizado todo el proceso.

Previamente, caso de no tenerlo instalado, hay que descargarse el certificado raíz de la FNMT-RCM, puede hacerlo pinchando [aquí](#).

En punto posterior se explicará el proceso de exportación e importación del certificado para instalarlo en otro ordenador/perfil ó en una tarjeta criptográfica.

Si lo desea puede consultar el siguiente documento: ["Manual Firma Electrónica"](#)

2.1 PROCESO de OBTENCIÓN

ES IMPRESCINDIBLE: No formatear el ordenador. Se debe realizar todo el proceso de obtención desde el mismo equipo, con el mismo usuario y el mismo navegador.

El proceso se divide en tres apartados que deben realizarse en el orden señalado.

IMPORTANTE: Para usuarios de Windows Vista y/o Internet Explorer 7 visite este enlace.

2.1.1 Solicitud vía Internet de su certificado.

NIF/NIE DEL TITULAR DEL CERTIFICADO

Introduzca en la siguiente casilla el NIF o NIE del titular del certificado incluyendo las letras, aún en el caso de que Ud. sea el representante del titular.

El NIF o NIE deberá tener una longitud de 9 caracteres. Rellene con ceros a la izquierda si es necesario.

Al final de este proceso obtendrá un código que deberá presentar al acreditar su identidad; es conveniente imprimir dicho código.

2.1.2 Acreditación de la identidad en una Oficina de Registro.

Si usted ha solicitado un certificado de persona física, puede dirigirse a cualquiera de las Oficinas de Registro de los Organismos acreditados.

La CNE dispone de acreditación como oficina delegada de registro de la FNMT-RCM en la planta 0, Registro General.

Para su comodidad, puede usted hacer uso del servicio de localización de las [Oficinas más cercanas](#).

El registro de usuario es presencial y debe acreditar la identidad con la presentación del DNI, pasaporte ó tarjeta de residencia.

2.1.3 Descarga de su Certificado de Usuario.

Unos minutos después de haber acreditado su identidad en una Oficina de Registro, haciendo uso del código de solicitud obtenido en el paso 2.1.1, podrá descargar su certificado desde esta página Web.

NOTA: Si usted ha elegido una Oficina de Registro de la Agencia Tributaria para acreditar su identidad, debe esperar al día siguiente para proceder a la descarga del certificado.

3 COPIA DE SEGURIDAD DEL CERTIFICADO.

Para realizar estas operaciones puede encontrar todas las instrucciones pinchando en el siguiente enlace:

<http://www.cert.fnmt.es/index.php?cha=cit&sec=4&fpage=30&lang=es>

Una vez obtenido el certificado de usuario, ya puede hacer uso del mismo a través del mismo equipo y navegador desde el que realizó el proceso. Sin embargo, es altamente recomendable que el usuario realice una copia de seguridad, en disco u otro tipo de soporte, de su certificado y su correspondiente clave privada. De esta forma no sólo podrá instalarlo en otros navegadores, sino que además no lo perderá en caso de problemas con su equipo actual.

3.1 INSTRUCCIONES DE EXPORTACIÓN/IMPORTACIÓN DE CERTIFICADOS

Estas instrucciones sólo son válidas para el navegador Microsoft Internet Explorer.

3.1.1 Exportación del certificado a fichero.

Para disponer de una contraseña robusta, la recomendación es que ésta sea de una longitud no inferior a 8 caracteres alfanuméricos compuesto por cifras, letras mayúsculas y/o minúsculas y/o símbolos.

Abrimos el navegador y en el menú de Herramientas → Opciones de Internet → Contenido → Certificados, seleccionamos el certificado que queremos exportar y pinchamos en el botón de “Exportar”; nos aparecerá un asistente para la exportación de certificados y pinchamos en “Siguiente”.

La pantalla siguiente nos permite exportar o no la clave privada; hemos de seleccionar “Exportar la clave privada” y pinchamos en “Siguiente”.

Nos aparece otra pantalla donde hemos de seleccionar el formato de fichero a exportar; ha de estar seleccionado la opción “Intercambio de información personal: PKCS #12 (.pfx)” y tener seleccionada las dos opciones siguientes: “Si es posible, incluir...” y “Permitir protección segura ...”; la tercera opción “Eliminar la clave privada si la exportación es satisfactoria” NO se debe marcar porque de lo contrario borraríamos la clave privada del certificado, con lo que quedaría inutilizable en el equipo donde estamos realizando la exportación.

Nos aparece otra pantalla en la que se nos pide introducir una contraseña para proteger el fichero que va a ser generado y para que esté protegido contra accesos de terceros; esta contraseña se pedirá en el proceso de importación y es importante no olvidarla.

Una vez introducida la contraseña, pinchamos en siguiente y aparece otra pantalla donde nos solicita un nombre de fichero”; por defecto, la ubicación del mismo suele ser el escritorio pero le

podemos indicar la ubicación que se quiera; se introduce el nombre que deseemos, pinchamos en siguiente y aparecerá un breve resumen de las operaciones que se van a realizar.

Pinchamos en “Finalizar” y aparece una pantalla de advertencia de acceso a un elemento protegido, pinchamos en “Aceptar” y dependiendo de la configuración que se tenga establecida puede que se nos pida la contraseña de acceso al certificado, pinchamos en “Aceptar” y aparece una ventana indicando que la exportación se ha realizado con éxito; el fichero que contiene el certificado con la clave privada y la pública tendrá una extensión tipo “nombre_fichero.pfx”.

3.1.2 Importación del certificado a otro navegador de otro ordenador.

Abrimos el navegador y en el menú de Herramientas → Opciones de Internet → Contenido → Certificados, pinchamos en el botón de “Importar” y aparece el asistente para la importación de certificados.

En la pantalla que se nos muestra deberemos indicar el nombre del archivo que contiene el certificado a importar que deberá tener la extensión “.pfx” (usualmente tiene la extensión indicada, aunque también puede tener extensión .p12, .p7b ó .sst); al pinchar en “Examinar” deberemos tener la precaución de seleccionar en “Tipo” que sea Intercambio de información personal (.pfx, .p12).

En la pantalla siguiente, nos va a solicitar la contraseña de acceso al fichero que fue exportado (ver 3.1.1, párrafo 4) y dos opciones:

- “Habilitar protección segura de claves privadas”, esta opción se marcará si queremos que cada vez que se vaya a usar el certificado, nos solicite una contraseña (no confundir con la contraseña del punto 3.1.1, párrafo 4, aunque si se hace coincidir nos ahorramos una contraseña de más). Si no se marca, no se pedirá contraseña cuando vaya a ser utilizado el certificado. Opción recomendada: MARCADA
- “Marcar esta clave como exportable”, esta opción se marcará si queremos exportar el certificado en un futuro; si no se marca, la clave privada jamás se podrá recuperar y no se podrá exportar el certificado. Opción recomendada: MARCADA

Aparece otra pantalla donde se indica el almacén de certificados donde se va a guardar el que pretendemos importar; por defecto, se selecciona la primera opción: “Seleccionar automáticamente el almacén ...” y pinchamos en “Siguiente”.

Se nos mostrará una pantalla con un breve resumen de las operaciones que se van a realizar y al pulsar en finalizar, aparece una pantalla de advertencia de acceso a un elemento protegido; pinchamos en “Nivel de Seguridad” y se nos mostrarán 2 opciones: Medio ó Alto:

- Alto: se nos pedirá introducir una contraseña (la que se quiera, aunque recomendable que sea la misma que la del punto 3.1.1, párrafo 4) y cada vez que se vaya a usar el certificado, seremos informados de acceso a un elemento protegido y nos solicitará la contraseña. OPCIÓN RECOMENDADA

- Medio: cada vez que se vaya a usar el certificado, sólo seremos informados del acceso a un elemento protegido, pero no se solicitará contraseña.

Pulsamos en Aceptar y se nos muestra la pantalla de “importación satisfactoria”.

4 CERTIFICADO DE USUARIO EN TARJETA CRIPTOGRÁFICA.

El certificado de usuario se puede obtener e instalar en una tarjeta criptográfica que por su fabricación, requisitos y tecnología hace que se incremente la seguridad del sistema de certificación por varios motivos:

- La tarjeta criptográfica se le suministra con un PIN de acceso y un código de desbloqueo; el PIN, es modificable, pero el código de desbloqueo no; esta información es personal e intransferible y se recomienda guardarla en lugar seguro.
- Las claves privadas que se generan en la tarjeta criptográfica no se pueden copiar ya que la propia tecnología hace que nunca salgan de la tarjeta; no son exportables.
- Cada vez que va a ser usado el certificado, se le va a solicitar el PIN de acceso, el cual se puede modificar con el código de desbloqueo.
- Al tercer intento fallido de acceso con un PIN erróneo, la tarjeta se bloquea y es necesario utilizar el código de desbloqueo.

Si desea información técnica sobre las tarjetas criptográficas de la FNMT-RCM puede ir al siguiente enlace:

<http://www.cert.fnmt.es/index.php?cha=cit&sec=9&page=85&lang=es>

4.1 REQUISITOS PREVIOS A LA SOLICITUD.

- a. Caso de no tenerlo instalado, hay que descargarse el certificado raíz de la FNMT-RCM e instalarlo en el equipo donde vaya a trabajar, puede hacerlo pinchando [aquí](#).
- b. Disponer de lector de tarjetas y tenerlo instalado con los drivers suministrados por el fabricante del mismo (ha de ser administrador del equipo para realizar la instalación).
- c. Caso de ser usuario de WindowsXP ó VISTA (con otros sistemas operativos, consultar la Web de la FNMT-RCM), descargar e instalar el software módulo criptográfico de la FNMT-RCM necesario para el uso de las tarjetas; puede descargarlo pinchando [aquí](#) e instalarlo siguiendo las indicaciones del programa (ha de ser administrador del equipo para realizar la instalación).

4.2 OBTENCIÓN DEL CERTIFICADO EN TARJETA CRIPTOGRÁFICA

Una vez cumplidos los puntos a, b y c, podemos realizar la solicitud del certificado siguiendo el siguiente enlace: <http://www.cert.fnmt.es/index.php?cha=cit&sec=4&fpage=32&lang=es>

4.2.1 Solicitud del certificado (para Microsoft Internet Explorer).

ES IMPRESCINDIBLE: No formatear el ordenador. Todo el proceso de obtención del certificado se debe realizar desde el mismo equipo, con el mismo usuario y el mismo navegador.

El proceso se divide en tres apartados que deben realizarse en el orden señalado.

IMPORTANTE: Para usuarios de Windows Vista y/o Internet Explorer 7 visite este enlace.

Introduzca la tarjeta criptográfica en el lector de tarjetas y pulse en el siguiente enlace: <http://www.cert.fnmt.es/index.php?cha=cit&sec=4&fpage=32&lang=es>

Al pulsar el enlace que encontrará al final de la página anterior, "Solicitud de Certificado" aparecerá un formulario que deberá cumplimentar con el NIF del titular del certificado.

Aparecerá un cuadro de diálogo mediante el cual deberá validarse como usuario de la tarjeta introduciendo el PIN de la misma. En este momento se generarán las claves, tanto la pública como la privada y 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".

4.2.2 Acreditación de la identidad en una Oficina de Registro.

Si usted ha solicitado un certificado de persona física, puede dirigirse a cualquiera de las Oficinas de Registro de los Organismos acreditados.

La CNE dispone de acreditación como oficina delegada de registro de la FNMT-RCM en la planta 0, Registro General.

Para su comodidad, puede usted hacer uso de nuestro servicio de localización de las [Oficinas más cercanas](#).

El registro de usuario es presencial y debe acreditar la identidad con la presentación del DNI, pasaporte ó tarjeta de residencia. Esto aumenta el nivel de seguridad del sistema.

4.2.3 Descarga de su Certificado de Usuario.

Unos minutos después de haber acreditado su identidad en una Oficina de Registro, introduzca la tarjeta en el lector y haciendo uso del código de solicitud obtenido en el paso 4.2.1, podrá descargar su certificado desde esta página Web.

NOTA: Si usted ha elegido una Oficina de Registro de la Agencia Tributaria para acreditar su identidad, debe esperar al día siguiente para proceder a la descarga del certificado.

4.3 IMPORTACIÓN DE UN CERTIFICADO QUE SE HA SOLICITADO PREVIAMENTE EN FORMATO SOFTWARE Y EXPORTADO A FICHERO (.pfx) PARA QUE RESIDA EN TARJETA CRIPTOGRÁFICA.

Si hemos obtenido el certificado de usuario siguiendo los puntos 2 y 3 y disponemos de una tarjeta criptográfica con el PIN de acceso y el código de desbloqueo facilitados con la misma, podemos importar el certificado a dicha tarjeta, siempre y cuando se reúnan todos los requisitos enumerados en el punto 4.1.

Con la tarjeta introducida en el lector, ejecutamos Inicio → Todos los programas → FNMT-RCM → Tarjeta → Importador de Certificados; se abre el asistente para la importación de certificados, pinchamos en “Siguiente” y seleccionamos el fichero *nombre_fichero.pfx* generado en el punto 3.1.1, escribimos la contraseña que protege al fichero y se solicitará el PIN de acceso a la tarjeta; después de esto, el certificado estará exportado en la tarjeta criptográfica

[Más sobre certificados y FAQ's de la FNMT-RCM.](#)