Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

RESPUESTAS A LAS DUDAS INICIALES SOBRE LA FIRMA ELECTRÓNICA

	NOMBRE	FECHA
Elaborado por:	Departamento CERES	10/04/2007
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	10/04/2007	Creación del documento	Departamento CERES
1.1	07/10/2011	Revisión del documento	Departamento CERES
1.2	07/01/2014	Revisión del documento	Departamento CERES
1.3	08/06/2016	Revisión del documento	Soporte Técnico

Documento clasificado como: *Público*

RESPUESTAS A LAS DUDAS INICIALES SOBRE LA FIRMA ELECTRÓNICA

Contenido

1. Introducción 3
2. ¿Qué es un certificado? 4
3. Sí ¿pero dónde está? ¿cómo lo veo? 4
4. ¿Qué tiene un certificado? 4
5. ¿Qué significan todos esos apartados que aparecen al visualizar el Certificado? 5
6. ¿Qué es la firma electrónica? 6
7. ¿Qué es un prestador de servicios de certificación? 6
8. ¿Cómo puedo obtener un certificado? (Persona física) 7
9. Bien, ya tengo certificado. 14
10. ¿Cómo hago una copia de seguridad de mi certificado? 15
11. ¿Qué más puedo hacer con mi certificado? 17
12. Quiero entrenarme con esto de las firmas. 17
13. ¿Y qué hay de los servicios de confidencialidad? 17
14. El certificado y mi correo electrónico 18
15. Más, más, más 18

1. INTRODUCCIÓN

La revolución de las tecnologías de la información, conjuntamente con el desarrollo de las infraestructuras de comunicaciones, está haciendo cambiar significativamente las relaciones entre individuos y organizaciones, tanto en España como en todo el mundo. Estas nuevas formas de comunicación abren un gran abanico de posibilidades tanto para ciudadanos como para empresas y permiten comercializar productos y servicios de una forma ágil y económica.

En España, las distintas Administraciones están apostando decididamente por Internet como vía de comunicación, creando páginas webs con un contenido de interés público que están puestas a disposición de la ciudadanía. Estas iniciativas están teniendo una gran aceptación y una repercusión muy positiva en la opinión pública, que se traduce en una utilización cada vez más generalizada de la red.

Para responder debidamente a esta demanda, se hacía necesario aportar seguridad a las comunicaciones a través de Internet. Esta seguridad se expresa en términos de confidencialidad (sólo se muestran los datos o páginas al usuario autorizado a ello), integridad (nos aseguramos de que los mensajes intercambiados llegan a su destinatario sin modificaciones) no repudio (que el emisor o el receptor no se puede desdecir del propio mensaje).

Por cuanto antecede y como herramienta para alcanzar los objetivos anteriores (confidencialidad, integridad y no repudio), surgen los certificados electrónicos y la firma electrónica. Ambos son instrumentos capaces de garantizar la seguridad en las comunicaciones y la identidad de los usuarios, permitiendo la comprobación de la procedencia y asegurando la integridad de los mensajes intercambiados a través de la red.

Con ayuda de los certificados electrónicos se puede realizar la protección de la información mediante un cifrado o transformación criptográfica (ocultamiento o enmascaramiento de la información de forma que no sea legible sin realizar la operación inversa) de los mensajes, haciendo su contenido ilegible salvo para el destinatario. Con ayuda de los mismos certificados electrónicos y aplicando un algoritmo de firma electrónica, obtenemos de un texto, una secuencia de datos que permiten asegurar que el titular de ese certificado ha "firmado electrónicamente" el texto y que éste no ha sido modificado.

Las claves criptográficas (conjunto de datos o información manejada y gestionada por el usuario para realizar operaciones criptográficas) que posibilitan estas operaciones se generan en el momento de la solicitud del certificado y quedan unidas inequívocamente al titular de las mismas.

Todo lo anterior, se ve reforzado en España con una legislación (Ley 59/2003 de firma electrónica) que permite ofrecer garantía y seguridad jurídica a las transacciones realizadas con los certificados electrónicos.

2. ¿QUÉ ES UN CERTIFICADO?

Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula la identidad de cada usuario con las herramientas de firma electrónica (claves criptográficas), dándole a conocer como firmante en el ámbito telemático.

3. SÍ ¿PERO DÓNDE ESTÁ? ¿CÓMO LO VEO?

El certificado, como documento que es, no es otra cosa que un conjunto de datos cuya representación se puede ver de la siguiente manera:

Por ejemplo, para Internet Explorer, 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.

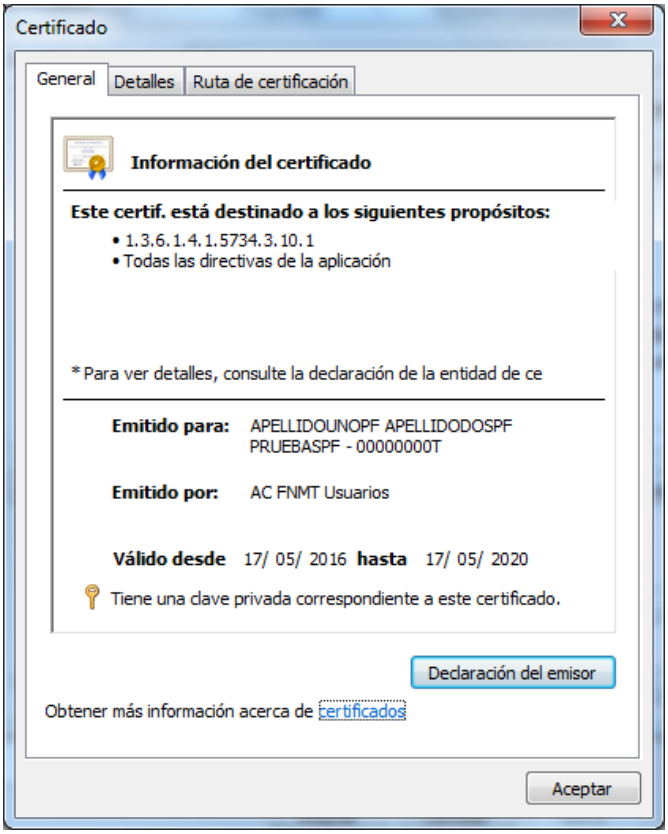
En Mozilla Firefox puede acceder a Herramientas, Opciones, Avanzado, Certificados y el botón Ver Certificados.

4. ¿QUÉ TIENE UN CERTIFICADO?

Un certificado no es otra cosa que un conjunto de datos vinculados entre sí y una identidad, la del titular o firmante, y cuya unión o vínculo viene avalada y garantizada por un prestador de servicios de certificación. Es la herramienta básica para la realización de gestiones desde su propio ordenador sin necesidad de desplazarse.

5. ¿QUÉ SIGNIFICAN TODOS ESOS APARTADOS QUE APARECEN AL VISUALIZAR EL CERTIFICADO?

Si seguimos los pasos del punto anterior, obtendremos una pantalla en la que se nos muestra algunos campos o propiedades del certificado. Ésta tiene un aspecto similar a:



En ella podemos observar que se nos muestra la identidad del titular del certificado y el emisor del mismo.

Por otra parte, se nos indica con una secuencia de números los usos y responsabilidades en relación con el certificado (1.3.6.1.4.1.5734.3.10.1). Esta secuencia de números se corresponde con la Política de Certificación, documento en el que se desarrollan estas materias y que se puede encontrar junto con las Políticas de los demás certificados en https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

Asimismo, también podemos ver el periodo de validez del certificado (Válido desde xx hasta yy).

Si seleccionamos la pestaña “Detalles” se nos muestra más información sobre el certificado. Aquí encontraremos campos como Número de serie, que es un número secuencial que asigna la autoridad de certificación a los certificados que emite y que, por otra parte, es el número que se incluye en la lista de revocados en caso de que se quiera interrumpir la vigencia del certificado. También encontraremos información sobre el tamaño de las claves criptográficas, el uso que se le pueda dar éstas y el algoritmo con el que la autoridad de certificación firma el certificado en cuestión, así como el correo electrónico asociado al certificado.

6. ¿QUÉ ES LA FIRMA ELECTRÓNICA?

La firma electrónica es el conjunto de datos relativos a una persona consignados en forma electrónica, y que junto a otros asociados con ellos, pueden ser utilizados como medio de identificación del firmante, teniendo el mismo valor que la firma manuscrita.

Permite que tanto el receptor como el emisor de un contenido puedan identificarse mutuamente con la certeza de que son ellos los que están interactuando, evita que terceras personas intercepten esos contenidos y que los mismos puedan ser alterados, así como que alguna de las partes pueda "repudiar" la información que recibió de la otra y que inicialmente fue aceptada.

7. ¿QUÉ ES UN PRESTADOR DE SERVICIOS DE CERTIFICACIÓN?

Es aquella persona física o jurídica que, cumpliendo los requisitos que determina la legislación establecida sobre firma electrónica, está capacitado para emitir certificados electrónicos.

En la legislación española a los prestadores de servicios de certificación se les denomina “terceras partes de confianza” o “prestador de servicios de certificación”. Esta denominación se origina por las propias funciones que realizan, y que está dirigida a que los usuarios de esta infraestructura tengan la seguridad de que el sujeto con el que se contacta es quién dice ser sin posibilidad de error.

Es importante seleccionar como tercera parte de confianza una que realmente nos ofrezca la suficiente garantía.

8. ¿CÓMO PUEDO OBTENER UN CERTIFICADO? (PERSONA FÍSICA)

Para obtener un certificado de firma electrónica y si se trata de una persona física (no persona jurídica), es imprescindible contar con un ordenador que tenga acceso a Internet, acceder a la página https://www.sede.fnmt.gob.es/ y seguir los tres pasos que se indican a continuación:

1. Consideraciones previas y configuración del navegador
2. Solicitud del certificado
3. Acreditación de la identidad mediante personación física en una oficina de registro.
4. Descarga del certificado desde Internet.

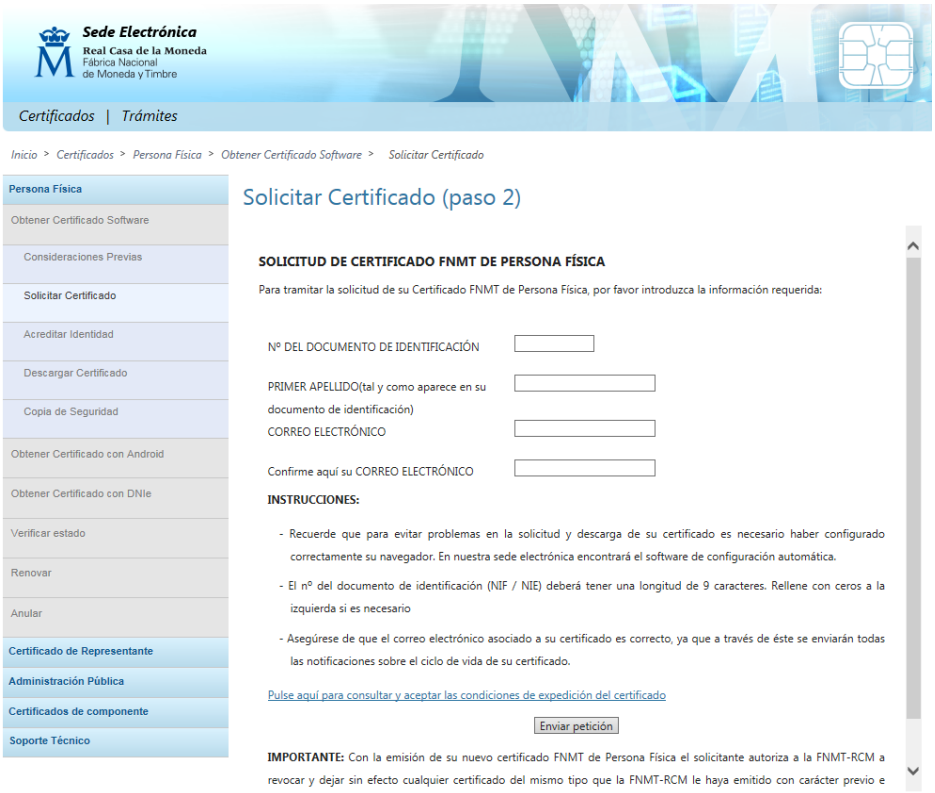
Para realizar estos pasos, primeramente ha de seleccionar el canal "Certificados" y luego el apartado "Persona física" – "Obtener Certificado Software". A partir de aquí, aparecerá en el margen izquierdo un menú con los pasos indicados anteriormente, pasos que hemos de seguir uno a uno y en el orden indicado.

Paso 1: Consideraciones previas y configuración del navegador

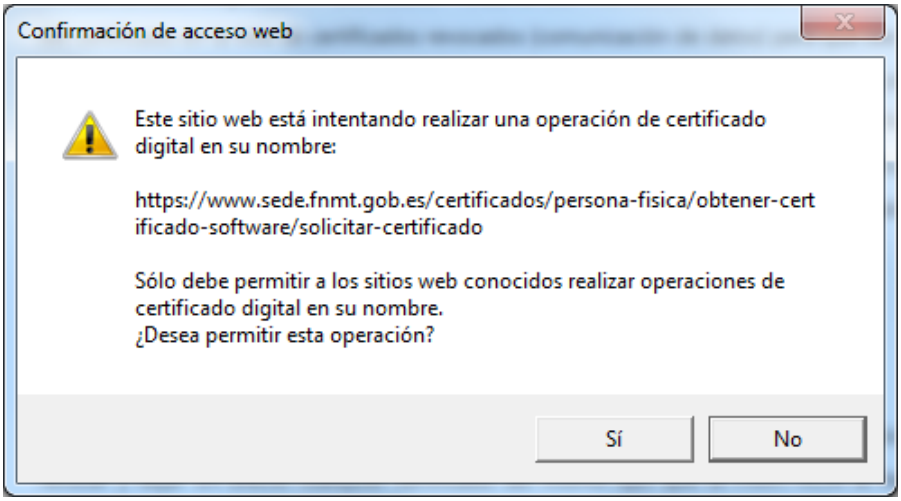
En este paso se informa de los aspectos a tener en cuenta así como los navegadores soportados y las instrucciones para configurar el navegador.

Paso 2: Solicitud del certificado

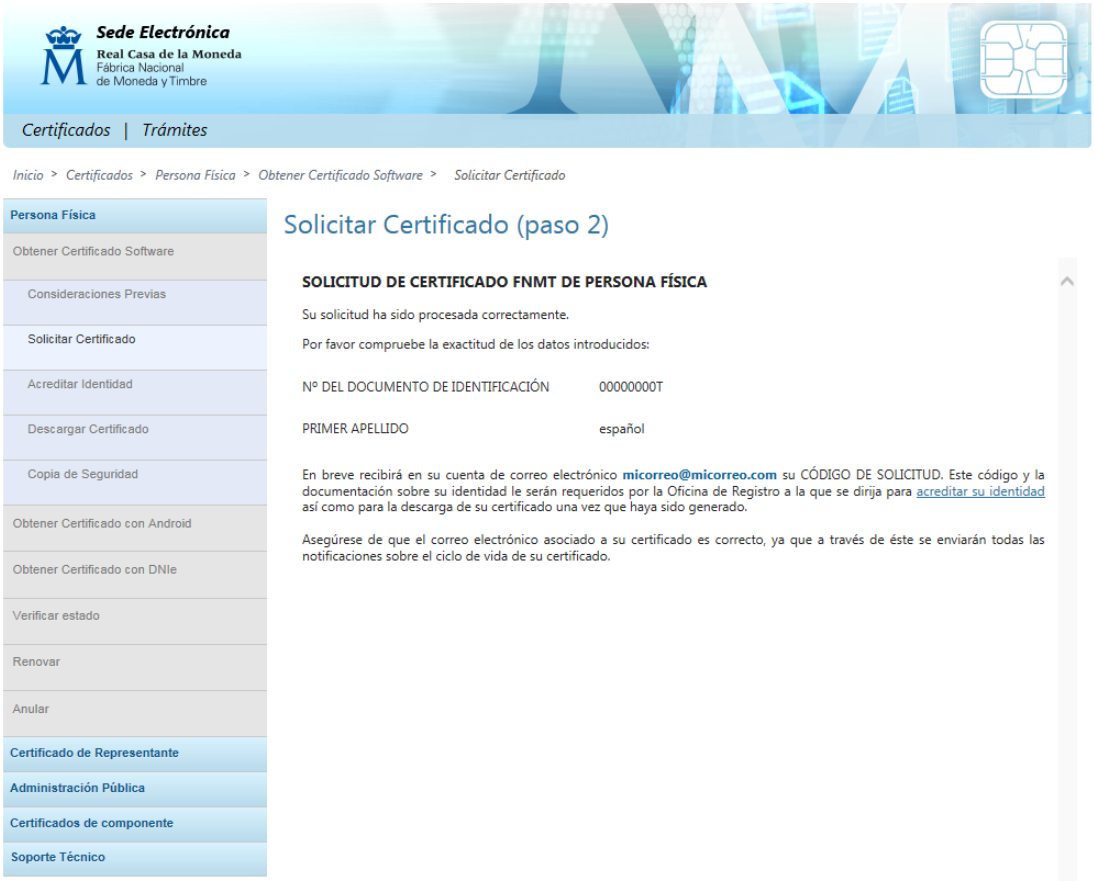
Para realizar este punto, seleccionaremos “Solicitar certificado” (margen izquierdo de la pantalla).



Una vez cumplimentada la casilla del NIF, primer apellido, el correo electrónico con su confirmación y aceptar las condiciones, al enviar la petición le aparecerá un aviso informándole de la solicitud del certificado, seleccione la opción “SI



Una vez aceptado el mismo, le aparecerá en la pantalla la confirmación de su solicitud indicándole que se le enviará al correo electrónico introducido el código de solicitud asociado a su certificado, este correo lo deberá imprimir o llevar en un dispositivo móvil para dirigirse a cualquiera de las Oficinas de Registro de los Organismos acreditados.



Paso 3: Acreditación de la identidad mediante personación física en una oficina de registro.

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 identificativo (DNI, NIE. pasaporte), deberá presentarse en la oficina de acreditación que desee.

La FNMT ha habilitado más de 2.400 Oficinas de Registro distribuidas por todo el territorio nacional. Entre las oficinas de Registro están disponibles las oficinas de la Seguridad Social y las Delegaciones y Administraciones de la AEAT (se requiere cita previa). Para su comodidad, puede usted hacer uso de nuestro servicio de localización de las OFICINAS MÁS CERCANAS.

El solicitante del certificado deberá presentarse en una de nuestras Oficinas de Registro para acreditar sus datos por un documento de identidad válido y vigente:

- Ciudadano de nacionalidad española:
  - El código de solicitud que le ha sido remitido a su cuenta de correo electrónico y
  - El Documento Nacional de Identidad (DNI), pasaporte o carné de conducir.
- Ciudadano extranjero:
  - El código de solicitud que le ha sido remitido a su cuenta de correo electrónico y
  - Documento Nacional de Identificación de Extranjeros o el Certificado de Ciudadano de la Unión donde conste el NIE junto con Pasaporte o documento de identidad de país de origen.

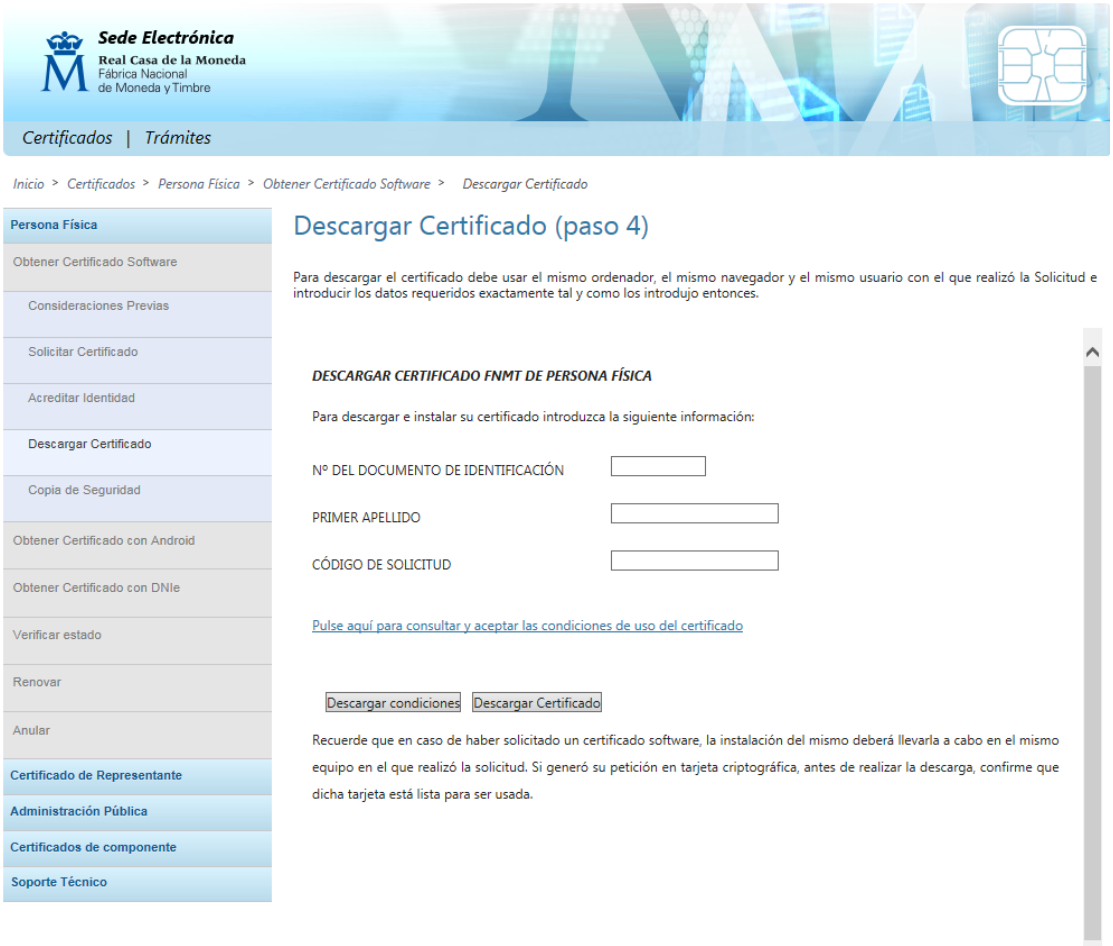
Con el fin de garantizar el nivel de seguridad del sistema y para obtener la identidad del titular del certificado de forma fehaciente, el registro de usuario es necesariamente presencial. Sin este registro presencial, no tendría mucha credibilidad la identidad del titular o firmante de un certificado.

Paso 3: Descarga del certificado

Una vez que haya acudido a la oficina de registro con el código de solicitud obtenido en el paso 2 y haya acreditado su identidad en una Oficina de Registro, podrá descargar su certificado desde la página web, y sin que medie ningún aviso o notificación.

Puede descargar el certificado desde la pantalla que se le mostrará al pulsar la opción "Descarga del certificado"

Para ello necesita su NIF o NIE, el primer apellido y el código de solicitud obtenido en el paso 2 .



El pulsar el botón "Descargar Certificado" el certificado se instalará automáticamente en su navegador.

Para verificar que el certificado se ha instalado correctamente – Ver punto "**3. Sí, ¿pero dónde está? ¿Cómo lo veo?"**

Para que la instalación del certificado funcione correctamente, hay que hacerlo desde el mismo ordenador, mismo navegador y con el mismo usuario que se realizó el paso 2.

También existe la posibilidad de obtener el certificado mediante su DNIe. En este caso el solicitante deberá tener un DNIe válido y vigente así como un lector de tarjetas en el caso de que su equipo no venga provisto del mismo. El proceso de solicitud del certificado de persona física con DNIe, requiere igualmente la realización de una configuración previa y de hacer la solicitud en el apartado correspondiente para la obtención con DNIe. Sin embargo con la solicitud con DNIe no hará falta el paso de la acreditación en una oficina de registro sino que cuando se obtenga el código de solicitud se podrá proceder directamente a la descarga del mismo.

9. BIEN, YA TENGO CERTIFICADO.

Si usted ya tiene un certificado electrónico, ya tiene capacidad para realizar firmas electrónicas y acceder a los servicios que las distintas administraciones y empresas ponen a disposición de sus usuarios y clientes a través de Internet.

No obstante, antes de empezar a utilizarlo debe tener en cuenta varios aspectos:

- Como consecuencia de un borrado de datos en el ordenador o una avería es posible que pierda su certificado, luego le recomendamos que haga una **copia de seguridad** para evitarle molestias y tener que volverse a desplazar a una oficina de registro
- El certificado consta de dos partes: una **parte pública** que es la que tiene la identidad del firmante o usuario y otra privada que tiene unas claves criptográficas para llevar a cabo el algoritmo de firma electrónica. Estas dos partes se pueden manejar por separado y hay que tener en cuenta que la **parte privada** es la que da la capacidad de realizar la firma, luego la ha de mantener siempre bajo custodia y no ceder su control a terceros para que se mantenga la propiedad de no repudio de las firmas (si cede la clave privada otros pueden hacer firmas en su nombre)
- Los certificados, al igual que las tarjetas bancarias tienen un periodo de vigencia y además se pueden cancelar o revocar, siempre que el titular lo desee o dude de poseer en exclusiva la clave privada. Cuando el certificado está próximo a su fecha de caducidad (desde 60 días antes hasta el mismo día), usted lo puede **renovar** sin tener que desplazarse a la oficina de registro. Si usted, por accidente o robo, cree que la parte privada del certificado no está bajo su exclusivo control, puede anular la validez del certificado, es decir, lo puede **anular** mediante la web https://www.sede.fnmt.gob.es/certificados/persona-fisica/anular, una llamada telefónica al Servicio de Revocación telefónica (24 x 365) 902 200 616 o mediante presentación en cualquiera de las oficinas de registro que tenemos publicadas en la web.

10. ¿CÓMO HAGO UNA COPIA DE SEGURIDAD DE MI CERTIFICADO?

En primer lugar hay que señalar que si usted tiene el certificado en tarjeta criptográfica, desde la tarjeta no puede realizar copias de seguridad puesto que la tarjeta es en sí mismo un dispositivo seguro.

Si tiene el certificado en el propio ordenador (navegador), por ejemplo, para Internet Explorer, debe seguir los siguientes pasos:

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

1. 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.

   Esto iniciará el procedimiento de copia del certificado para almacenarlo en otra ubicación distinta del navegador.

2. A partir de este momento nos guiará un asistente de Windows, podemos elegir entre exportar la clave privada o no (con parte privada o no) dependiendo del uso que queramos hacer del certificado. Si es una copia de seguridad debemos copiar todo, parte privada y parte pública, por lo que se selecciona exportar la clave privada

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

4. 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. Esta contraseña nos servirá para proteger el certificado cuando está fuera del navegador, hay que tener en guardar y custodiar esta contraseña ya que usted es el único que la posee y si la pierde nadie le puede ayudar a recuperarla.

5. 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'.

6. 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 el certificado ha sido exportado con éxito.

El proceso es similar para otros navegadores y versiones, puede consultarlo más detalladamente en el apartado de "Preguntas Frecuentes" de la página web.

No obstante, en líneas generales hay que subrayar las siguientes consideraciones

1. Los certificados siempre se pueden exportar de dos maneras, con clave privada o sin ella. Tenga en cuenta que la clave privada es la base de la firma electrónica y la custodia exclusiva por su parte es la garantía de no repudio de sus futuras firmas electrónicas. Por tanto, si exporta el certificado con su clave privada no debe cederlo a terceros.
2. Generalmente, uno exporta el certificado con clave privada cuando quiere realizar copias de seguridad o va a realizar una posterior importación en otro ordenador o navegador. El certificado se suele exportar sin clave privada cuando se va a ceder a terceros para que nos envíen información cifrada, información que está destinada para nosotros.
3. El fichero resultante de la exportación varía en función del navegador y de si lleva clave privada o no. De este modo, si seguimos el proceso normal de exportación que nos ofrecen los navegadores actuales, los ficheros con extensión ".cer" y ".p7b" no contienen clave privada y los ficheros con extensión ".p12" y ".pfx" sí contienen la clave privada.

Advertencias: En caso de que un servicio o aplicación o un tercero cualquiera le soliciten su certificado en formato (con extensión de archivo) .pfx no lo ceda nunca. La garantía de no repudio de su firma electrónica está basada en la custodia exclusiva por su parte de esta clave privada.

11. ¿QUÉ MÁS PUEDO HACER CON MI CERTIFICADO?

Un Usuario que tenga su certificado electrónico FNMT puede realizar todo tipo de trámites de forma que queda garantizada su verdadera identidad.

Algunos permiten firmar electrónicamente formularios y documentos electrónicos con la misma validez jurídica que si firmara con su "puño y letra" el mismo documento en papel.

Esto ha permitido que a día de hoy se puedan realizar multitud de gestiones desde casa, evitando desplazamientos y colas, durante las 24 horas del día.

Tan solo debe disponer de una conexión a Internet y del certificado electrónico FNMT, cuya obtención es gratuita.

Los servicios a los que se pueden acceder con el certificado no dependen de la FNMT y cada entidad desarrollará los que considere más oportunos. No obstante, se proporciona una lista de entidades donde se han desplegado servicios accesibles con el certificado electrónico en la dirección: https://www.cert.fnmt.es/certificados/donde-usar-certificado

12. QUIERO ENTRENARME CON ESTO DE LAS FIRMAS.

Usted puede realizar firmas electrónicas y verificarlas (las suyas propias o las de terceros que hayan sido realizadas con certificados de la FNMT) en la dirección:

https://valide.redsara.es/valide/

13. ¿Y QUÉ HAY DE LOS SERVICIOS DE CONFIDENCIALIDAD?

El certificado electrónico se puede utilizar para dotar de confidencialidad a la información de varias formas. La primera sería cifrando o codificando la información de modo que sólo un grupo de personas puedan realizar el proceso inverso para obtener la información en claro. Hay que señalar que para cifrar la información para terceros es necesario tener el certificado (la parte pública) de aquel al que queremos hacer llegar la información.

Otra manera de ver la confidencialidad de la información es a través de un proceso mediante el cual, previa identificación del usuario o receptor de la información, se muestran los datos pertinentes. Esta situación es la que se da en la mayoría de los servicios disponibles a través de Internet; accedemos a una página, nos identificamos con nuestro certificado y posteriormente el servicio nos muestra nuestros datos y las operaciones que podemos realizar, operaciones en las que puede intervenir una firma electrónica para darles validez jurídica.

A estos sitios web se accede a través del protocolo HTTPS (situación que es notoria porque la dirección web a la que se accede es del tipo https://) y si el proceso requiere identificación del usuario, el navegador nos muestra una pantalla para seleccionar el certificado con el que nos queremos identificar. Lo seleccionamos y la operación se completa mostrando la página a la que queremos acceder.

En este momento el servidor, a través de la identidad que se incluye en el certificado, tiene total certeza sobre quién accede al servicio, luego puede presentar unas páginas personalizadas con datos particulares.

14. EL CERTIFICADO Y MI CORREO ELECTRÓNICO

El certificado también puede ser utilizado por algunos agentes de correo electrónico, como por ejemplo, MS Outlook. Para ello es necesario que la dirección de correo electrónico incluida en el certificado (proporcionada en el momento de la acreditación) coincida con la dirección de correo que queremos utilizar para enviar un correo firmado.

Al igual que en los casos anteriores, el utilizar certificados con las aplicaciones de correo electrónico proporciona confidencialidad a la información e integridad y no repudio.

De esta forma, si queremos cifrar nuestros mensajes con el certificado deberemos:

1. Tener instalados los certificados de aquellos para los que queremos cifrar. Para ello aquellos a los que hayan querido establecer comunicaciones cifradas con nosotros, deberán haber exportado su certificado **sin clave privada** y habérnoslos proporcionado.
2. Una vez construido el mensaje buscaremos en la barra de herramientas una opción que es cifrar, lo pulsaremos, y aparecerá un símbolo (candado), indicando que el mensaje va a ser mandado cifrado. Por supuesto, deberemos seleccionar aquellas personas para las que queremos cifrar y que se corresponderán con los certificados de "Otras personas" que tengamos instalado en nuestro navegador (evidentemente, estos certificados no contienen la clave privada correspondiente)

Si queremos firmar electrónicamente nuestros correos:

1. Componemos el mensaje que queremos firmar.
2. Para firmarlo buscaremos en la barra de herramientas un botón que dice firmar, lo pulsaremos y automáticamente aparecerá un símbolo (distintivo) indicando que dicho mensaje es firmado por el emisor. Evidentemente, el mensaje será firmado con nuestra clave privada asociada a nuestro certificado y que está bajo nuestro exclusivo control, por eso se garantiza nuestra identidad como firmantes.

Como corolario de este apartado, señalar que la dirección de correo electrónico es uno de los datos anejos al certificado y que va avalada con la firma del Prestador de Servicios de Certificación. Por este motivo, el cambio de dirección de correo electrónico, para que se vea reflejado en el propio certificado, ha de ser notificado en una nueva emisión de certificado. La propia firma electrónica que el prestador de servicios de certificación realiza al certificado, garantiza integridad en los datos de éste, por tanto y por definición, los datos no pueden ser variados sin que se "refirme" el certificado, esto es, sin que se emita uno nuevo.

En otras palabras, los datos contenidos en un certificado están firmados electrónicamente por la autoridad de certificación o prestador de servicios de certificación, por tanto, no se pueden variar "alegremente" sino que el certificado en sí mismo ha de ser regenerado.

15. MÁS, MÁS, MÁS

Para conocer más en profundidad los servicios, el manejo del certificado y las posibilidades que existen, se puede encontrar más información en la página http://www.ceres.fnmt.es, en cada uno de los apartados, o bien en las Preguntas Frecuentes.