Firma digital, certificado electrónico y factura electrónica

Firma digital, certificado electrónico y factura electrónica

Ana Mª García Alcázar

Ra-Ma®

Firma digital, certificado electrónico y factura electrónica

Editado por:
RA-MA Editorial
Calle Jarama, 3A, Polígono Industrial Igarsa
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: *editorial@ra-ma.com*
Internet: *www.ra-ma.es* y *www.ra-ma.com*
ISBN: 978-84-9964-990-0
Depósito legal: M-24245-2020
Maquetación: Antonio García Tomé
Diseño de portada: Antonio García Tomé
Filmación e impresión: Safekat
Impreso en España en septiembre de 2020

En memoria de los que ya no están.

ÍNDICE

1

LA FIRMA ELECTRÓNICA

1.1 RÉGIMEN JURÍDICO APLICABLE

La base legal de la firma electrónica está recogida en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y se desarrolla en más profundidad en la sección Base legal de las Firmas que retomaremos en el punto 1.3. *Tipos de firma*. La sección también explora, bajo que circunstancias la ley equipara la firma electrónica a la firma manuscrita, añade notas respecto a la normativa europea y hace distintas referencias legales a firmas con sellos de tiempo y avanzadas.

1.2 CONCEPTO

La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- Identificar al firmante de manera inequívoca.
- Asegurar la integridad del documento firmado (Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación).
- Asegurar el no repudio del documento firmado (Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento).

1.3 TIPOS DE FIRMA

Según la Ley 59/2003, se distinguen entre tres tipos de firma, recogidas en los artículos 3.1) 3.2) y 3.3):

- "*La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante*".
- "*La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control*".
- *"Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma"*.

Según el artículo 3.4) de la ley, la **firma electrónica reconocida** es la única que puede ser considerada equivalente a la firma manuscrita:

- "La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel".

1.4 USOS

La firma electrónica aporta tres características en la comunicación por Internet: **identificación del firmante, integridad de los datos y no repudio.**

Las aplicaciones prácticas de la firma electrónica son muchas y variadas, generalmente, orientadas a realizar operaciones por Internet que en la vida cotidiana requieren de una firma para validarlas.

Algunos ejemplos de operaciones que se pueden realizar actualmente haciendo uso de la firma digital son:

- Realización y presentación de la Declaración de la Renta a través de Internet.
- Presentación de documentación en los registros electrónicos administrativos.
- Petición y descarga on-line de la vida laboral.
- Recepción y firma de notificaciones electrónicas de las Administraciones.
- Firma de correos electrónicos.
- Firma de facturas electrónicas.

1.5 FORMATOS

Se denomina *formato de firma* a **como se genera el documento de firma** y como se guarda o estructura la información de firma en el documento generado.

La existencia de múltiples formatos de firma se debe a razones históricas, a como se ha ido introduciendo la firma en formatos de documentos ya existentes y a como se han ido añadiendo funcionalidades a lo largo del tiempo.

Según las necesidades o escenarios específicos puede interesar realizar la firma electrónica mediante los diferentes formatos existentes de firma existentes.

Existen **formatos básicos,** que aportan todos los elementos necesarios para crear una firma electrónica avanzada o reconocida:

- **XML Signature:** Es una especificación desarrollada bajo el amparo del *w3c* que permite la firma (completa o parcial) de documentos utilizando una notación XML estándar. XML Signature ofrece algunas ventajas frente a la firma tradicional ya que al estar basada en texto plano su estructura es legible por humanos. Funcionalmente, tiene mucho en común con PKCS#7, pero es más extensible y está orientada hacia la firma de documentos XML.

  Las firmas XML se pueden utilizar para firmar datos o recursos de cualquier tipo, normalmente documentos XML, pero cualquier cosa que sea accesible a través de una *URL* puede firmarse. Una firma XML que se utiliza para firmar un recurso fuera del documento XML que la contiene se llama una firma separada (**detached**), *figura 1.1*. Si se utiliza para firmar una parte del documento que la contiene, se llama una firma envuelta (**enveloped**). Si contiene los datos firmados dentro de sí mismo se llama una firma envolvente (**enveloping**).

- **CMS (Cryptographic Message Syntax) / PKCS#7**: Formato binario usado para la firma, autenticación, resumen y encriptación de documentos. Fue diseñado, principalmente, para el intercambio de información a partir de correos electrónicos. Usa el estándar PKCS#7. Este formato además incorpora información de sellado de tiempo obtenidos por una TSA (Time Stamp Authority).

También existen **formatos avanzados:**

- **XAdES (Firma electrónica avanzada XML)**: Es una familia de firmas avanzadas, basadas en formatos XML. A diferencia que un formato embebido (como pudiera ser el PDF-Signature), es un lenguaje pensado para "conversar entre máquinas", es decir, el intercambio de información entre sistemas automatizados es el propósito de usar un formato basado en XML. Dentro de este formato de firmas, se han ido evolucionando distintas extensiones que dan respuesta a distintas necesidades y escenarios, las extensiones descritas a continuación no tienen que considerarse de menos a más en el grado de robustez, fiabilidad o seguridad, sino que deben considerarse como evoluciones del formato que dan respuesta a escenarios distintos, y no por ello compiten entre sí.
  - **XAdES-BES**: Firma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada.
  - **XAdES-EPES**. XAdES-BES al que se le incorpora información sobre la política de firma, como pudiera ser aquella información sobre el certificado empleado y la CA que lo emitió.
  - **XAdES-T (timestamp)**. Es un XAdES-EPES al que se le añade una segunda firma, pero en esta ocasión, una firma realizada por una TSA (Time Stamp Authority). Esta segunda firma aporta información específica sobre la fecha y hora exacta de la firma.
  - **XAdES-C (complete)**. Es un XAdES-T al que se le añaden referencias sobre los certificados y listas de revocación utilizadas para la validación del propio certificado utilizado para la firma. Por ejemplo: fue firmado por Certificado CCC emitidos por CA AAA y cuya CRL RRRR fue consultada en el momento de la validación.
  - **XAdES-X (extended)**. Es un XAdES-C al que se le añade información sobre la fecha y hora de los datos introducido para la extensión C.

- **XAdES-XL (extended long-term).**Es un XAdES-X al que se le incorporan los certificados (sólo clave pública) y las fuentes de validación que se usaron. A diferencia del C, donde sólo se incluía una referencia (un puntero), en este formato se embebe toda esa información. Por ejemplo, en el caso de una CRL, se incorpora la lista firmada de certificados revocados que fue consultada en ese momento. Esto se utiliza para garantizar la validación muchos años después de la firma incluso en el caso que la CA que emitió el certificado, o la fuente de validación (CRL) que se consultó, ya no esté disponibles (publicadas por ejemplo). Es decir, garantiza la validación off-line a largo plazo.
- **XAdES-A (archivado)**. Este formato incluye toda la información anterior pero incluye metainformación asociada a políticas de refirmado. Una política de refirmado establece un período de caducidad de la firma digital, y superado este tiempo, se procede a un refirmado. El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: hipotecas, títulos universitarios, escrituras, etc. 15, 20, 50 años, etc.

En el caso de firma de facturas electrónicas, en formato Facturae, el formato de firma es el XAdES.

- **PAdES (Firma electrónica avanzada en formato PDF):** Es un conjunto de restricciones y extensiones a PDF y al estándar ISO 32000-1 haciéndolo adecuado para la firma electrónica avanzada.

  Mientras que con PDF y el ISO 32000-1 se da un marco para firmar electrónicamente los documentos, la firma PAdES específica perfiles precisos para el uso de firmas electrónicas avanzadas bajo la Directiva de la Unión Europea 1999/93/EC**.**

  Un beneficio importante de PAdEs es que los documentos firmados electrónicamente permanecen válidos durante largos periodos de tiempo, incluso si los algoritmos criptográficos subyacentes están rotos.

  Los documentos firmados electrónicamente con formato PAdES pueden ser usados o archivados durante muchos años, incluso décadas, de manera que, en cualquier momento en el futuro, a pesar de los posibles avances tecnológicos, debe ser posible validar el documento para confirmar que la firma era válida en el momento en el que fue firmada, un concepto conocido como “Long-Term Validation” (LTV).

Para documentos en formato PDF, los datos de la firma se incorporan directamente en el documento PDF firmado, permitiendo que el contenido del archivo PDF sea copiado, almacenado y distribuido como un archivo electrónico simple. La firma también puede tener una representación visual como un campo de formulario, tal como podría tenerla en un documento impreso.

Una ventaja significativa del formato PAdES es que se despliega por medio de un software ampliamente reconocido como son los lectores PDF, es decir, no se requiere el desarrollo o la personalización de software especializado.

En la siguiente lista se definen brevemente los perfiles definidos por PAdES (ETSI TS 102 778):

- **PAdES Basic**. Perfil básico que cumple con los requisitos especificados en la norma ISO 32000-1.
- **PAdES-BES Profile (Enhaced).** Este perfil especifica una firma PDF avanzada basada en CAdES-bes e incorpora opción de incluir en la firma un sello de tiempo (CADES-T).
- **PAdES-EPES Profile (Enhaced)**. Este perfil especifica una firma PDF avanzada basada en CAdES-EPES. Es el PAdES-BES Profile añadiendole un identificador de política de firma y, opcionalmente, una referencia al tipo de compromiso adquirido.
- **PAdES-LTV Profile (Long Term).**Es el formato de firma longeva. Este perfil permite prorrogar por tiempo indefinido la validez de las firmas en formato PDF. Puede ser usado en conjunción con el PAdES-CMS, PAdES-BES o perfiles PADES-EPES. Este perfil es utilizado para garantizar la validación tras muchos años después de la realización de la firma. Es decir, garantiza la validación a largo plazo.

Es muy recomendable firmar documentos en formato PDF (formato de firma PAdES) pues el destinatario de la firma puede comprobar fácilmente, desde el mismo visualizador del PDF "Adobe Reader", la firma y el documento original firmado. Con otros formatos de firma esto no es posible si no se utilizan herramientas externas.

- **CAdES (Firma electrónica avanzada CMS Advanced Electronic Signatures)**: Es un conjunto de extensiones de datos firmados con sintaxis de mensajes criptográficos (CMS)por lo que es adecuada para la firma electrónica avanzada.

Mientras el formato CMS es un CAdES-T (timestamp) marco general para firmar documentos digitalmente, tales como E-Mail (S / MIME) o PDF, CAdES especifica perfiles precisos de datos firmados con CMS para su uso con firma electrónica avanzada en el marco de la Directiva Europea 1999/93/CE.

Un beneficio importante del formato CAdES es que los documentos firmados electrónicamente pueden seguir siendo válidos durante largos períodos, incluso si los algoritmos criptográficos subyacentes se rompen.

El principal documento que describe este formato es el ETSI TS 101 733 Firma Electrónica e Infraestructura (ESI) – CMS Advanced Electronic Signature (CAdES).

El formato CAdES tiene definidos 6 perfiles diferentes, según el nivel de protección ofrecido. Cada perfil incluye y mejora al anterior:

- **CAdES.** Forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada.
- **CAdES-T (timestamp).** Se le incorpora información el campo con sello de tiempos para proteger los datos de un posible repudio.
- **CAdES-C (complete).** Es un CAdES-T al que se le añade referencias sobre los certificados y listas de revocación utilizadas para permitir la validación off-line y su verificación en el futuro (sin almacenar los datos actuales de verificación).
- **CAdES-X (extended).** Es un CAdES-C al que se le añade información sobre la fecha y hora de los datos introducidos para la extensión C.
- **CAdES-X-L (extended long-term).**Es un CAdES-X al que se le incorporan los certificados (sólo clave pública) y las fuentes de validación que se usaron. Garantiza la validación off-line a largo plazo incluso si la fuente original no estuviera disponible.
- **CAdES-A (archivado).** Este formato incluye toda la información anterior pero incluye metainformación asociada a políticas de refirmado. Una política de refirmado establece un período de caducidad de la firma digital, y superado este tiempo, se procede a un refirmado. El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: hipotecas, títulos universitarios, escrituras, etc. 15, 20, 50 años, etc.

¿Como sabemos si una firma es válida?

Podemos comprobar la validez de la firma de un documento, ver quién es el firmante y el documento firmado en VALIDe.

1.10 SERVICIOS DE CERTIFICACIÓN

Con carácter previo a la aprobación del eIDAS, cada estado miembro emitía sus propios certificados digitales, que son los documentos electrónicos que sirven para identificar a las personas y a las empresas.

El problema era que la validez de estos certificados fuera de las fronteras del país de emisión no estaba garantizada, y dependía de la existencia de convenios

entre la entidad emisora del certificado y su contraparte (en este caso, cualquier otro estado de la UE).

Para lograr el objetivo del mercado único digital, este problema debía ser resuelto. Y de esta necesidad nace el Reglamento eIDAS, cuyas siglas corresponden a Electronic Identification and Authentication Services, para fijar un estándar de identificación electrónica para armonizar y volver seguras las transacciones online en toda Europa. Y para ello, el Reglamento se apoya en lo que se denominan los servicios electrónicos de confianza.

Por tanto, con el objetivo muy claro de eliminar las fronteras a las transacciones electrónicas en la UE y construir un clima de confianza, el eIDAS establece y regula a nivel europeo dos conceptos:

1. El de los servicios electrónicos de confianza.
2. El del prestador de esos servicios electrónicos de confianza (lo desarrollaremos en el siguiente punto).

Básicamente, los servicios electrónicos de confianza permiten comprobar la identidad de origen en Internet, y también la integridad de los mensajes que se intercambian a través de la Red. Son por tanto un elemento fundamental en la eliminación de las barreras al mercado digital, puesto que refuerzan la seguridad de la información y contribuyen a la generación de confianza (de ahí su nombre).

El artículo 3 del Reglamento eIDAS recoge la definición de los servicios electrónicos de confianza. En el subapartado 16 se establece que "servicio de confianza" es el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

1. "La creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o
2. La creación, verificación y validación de certificados para la autenticación de sitios web, o
3. La preservación de firmas, sellos o certificados electrónicos relativos a estos servicios."

1.11 CONCEPTO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN SUJETO A LA LEY

Un prestador de servicios de certificación es una persona, física o jurídica, que expide certificados electrónicos o que presta otros servicios en relación con la firma electrónica.

Para ser un prestador cualificado de servicios electrónicos de confianza se deben prestar servicios electrónicos de confianza cualificados y se debe tener el reconocimiento como tal por parte de un organismo de supervisión

En España, como en el resto de los países de la Unión Europea, los prestadores de servicios de certificación (PSC) se regulan mediante el Reglamento eIDAS (910/2014) por el que se deroga la Directiva 1999/93/CE.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, establece en su artículo 30 que los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología (actual Ministerio de Asuntos Económicos y Transformación Digital), el inicio de su actividad, así como información relativa a los servicios que prestan y sus correspondientes certificaciones de calidad. Esta información deberá ser convenientemente actualizada por los prestadores de servicios de certificación y será objeto de publicación en la dirección de Internet del citado Ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

En España, en la página del Ministerio de Asuntos Económicos y Transformación Digital se puede consultar el listado de prestadores de servicios cualificados o no cualificados, tal y como establece el Reglamento:

una Persona Jurídica en calidad de representante legal con su cargo de administrador único o solidario inscrito en el Registro Mercantil.

- Representante de persona jurídica: Certificación electrónica que vincula un Firmante a unos Datos de verificación de firma y confirma su identidad. Este certificado sustituye al tradicionalmente utilizado por las Administraciones Públicas para el ámbito tributario y que, posteriormente se utilizó para otros casos. Por tanto, este certificado se expide a las Personas Jurídicas para su uso en sus relaciones con aquellas Administraciones Públicas, Entidades y Organismos Públicos, vinculados o dependientes de las mismas.

- Certificados de entidad sin personalidad jurídica. Vinculan a su suscriptor unos datos de verificación de firma y confirma su identidad para ser utilizados únicamente en las comunicaciones y transmisiones de datos por medios electrónicos, informáticos y telemáticos en el ámbito tributario.

Clasificación según el ámbito de aplicación

Según este criterio encontramos múltiples Certificados, que son algunos de los que ofrecen los distintos proveedores de servicios de certificación:

- Certificado de servidor.
- Certificado de pertenencia a empresa.
- Certificado de representante.
- Certificado de apoderado.
- Certificado de sello de empresa.
- Certificado de factura electrónica.
- Certificado de colegiado.
- Etc.

Certificados software y certificados hardware

Según este criterio, podemos clasificar los certificados electrónicos en dos categorías:

- **Certificados software:** Un Certificado electrónico es un documento digital que se puede guardar en una memoria USB, en un ordenador (en el almacén de certificados) o en el disco duro. A ese Certificado se le conoce como certificado software.

- **Certificados hardware:** Un certificado también puede estar almacenado en una tarjeta criptográfica, que es una tarjeta que incorpora un chip electrónico. Un ejemplo claro de una tarjeta criptográfica es el DNI electrónico. En estas tarjetas es posible almacenar uno o varios certificados electrónicos, lo que se conoce como certificado hardware.

Certificados de la Ley 11/2007

La Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos en su capítulo II establece las formas de identificación y autenticación que pueden ser usadas para la identificación de la Administración y de la actuación administrativa.

De esos apartados de la Ley y de su reglamento de desarrollo, se derivan los siguientes certificados electrónicos.

- **Certificado de Sede Electrónica:** El certificado de Sede es un certificado de Servidor que identifica y autentifica al servidor como Sede Electrónica de una Administración Pública.

  Las sedes electrónicas, cuando sea necesario, dispondrán de sistemas que permiten el establecimiento de comunicaciones seguras. Además, utilizarán sistemas de firma basados en certificados de dispositivo seguro o medio equivalente para identificarse y mantener una comunicación segura.

- **Certificado de Sello Electrónico:** Según la Ley, es el certificado usado para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada.

  Esto quiere decir que el Sello Electrónico es el que debe usarse para todos los trámites administrativos que se realizan por medios telemáticos, tanto para la identificación de los servidores y la firma de los documentos electrónicos, como para el establecimiento de comunicaciones seguras entre máquinas

- **Certificado de Empleado Público:** Son los certificados que cada Administración Pública puede proveer a su personal para la identificación y autenticación del ejercicio de la competencia de la Administración Pública.

  Identifican de forma conjunta al titular del puesto de trabajo o cargo, y a la Administración u órgano en la que presta sus servicios.

Existen tres términos que debemos desarrollar en este ámbito:

- **La Identidad Digital**

  La Identidad Digital abarca todos los procesos, mecanismos, tecnologías que sirven a un individuo u organización para identificarse y para reconocer o descubrir la identidad de otros en medios y por medios digitales.

- **Identificación de los Ciudadanos**

  Según la Ley 11/2007, los ciudadanos pueden utilizar los siguientes sistemas para identificarse ante la Administración:

  - El DNI Electrónico.
  - Sistemas de firma electrónica avanzada, incluyendo los que se basan en certificado electrónico reconocido. Cada Administración Pública puede decidir que certificados electrónicos admite para la identificación de los ciudadanos en los procedimientos y actuaciones que le competen.
  - Otros sistemas como claves concertadas en un registro previo o la aportación de información conocida por ambas partes u otros sistemas no criptográficos. En este caso, la Administración tiene que justificar las razones por las que usar estos mecanismos.

- **Identificación de las Administraciones Públicas**

  La Ley 11/2007 establece los mecanismos que pueden utilizar las Administraciones Públicas para identificarse electrónicamente y autenticar los documentos electrónicos que produce.

  - **Identificación de las sedes electrónicas**: La sede electrónica es la dirección electrónica cuyo titular es una Administración Pública y a la que el ciudadano puede acceder a través de redes de telecomunicaciones. Las sedes electrónicas deben utilizar tanto para identificarse como para garantizar las comunicaciones seguras, sistemas de firma basados en certificados de dispositivo seguro. De este requisito de la ley se han derivado los Certificados de Sede.
  - **Identificación mediante sello electrónico**: La identificación y autenticación de la actuación automatizada de la Administración se puede realizar mediante el sello electrónico que también debe estar basado en certificado electrónico.

- Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que transpone la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior (PSD2).
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Es responsabilidad de la entidad certificadora garantizar la autenticidad de la información que aparece en cada uno de los certificados.

A continuación, detallamos los principales proveedores de Servicios de Certificación en España, cuyo certificado es posible validar al lanzar una consulta contra la plataforma @firma del MINHAP.

Es necesario tener en cuenta que los certificados incorporados a la Plataforma han cumplido el procedimiento descrito en el documento "Tratamiento de certificados en @firma", disponible actualmente en el PAE (*http://administracionelectronica.gob.es*) y se hayan clasificados en alguno de los trece tipos de certificados actualmente establecidos, a saber:

- Clasificación 0 Persona física.
- Clasificación 1 Persona Jurídica según Ley 59/2003.
- Clasificación 2 Componente /SSL/no reconocido/sello empresa.
- Clasificación 3 Sede según Ley 40/2015.
- Clasificación 4 Sello según Ley 40/2015.
- Clasificación 5 Empleado Público según Ley 40/2015.
- Clasificación 6 Entidad sin personalidad jurídica según Ley. 59/2003.
- Clasificación 7 Empleado público con seudónimo según R.D. 1671/2009.
- Clasificación 8 Cualificado de sello, según Reglamento (UE). Nº 910/2014.
- Clasificación 9 Cualificado de autenticación, según reglamento. (UE) Nº 910/2014.

Los principales proveedores de Servicios de Certificación en España son:

- ACA. Autoridad de Certificación de la Abogacía:
  https://www.abogacia.es/site/aca/autoridad-de-certificacion-de-la-abogacia/

- ACCV. Autoridad de Certificación de la Comunidad Valenciana:
  https://www.accv.es

- ANCERT. Agencia Notarial de Certificación:
  https://www.ancert.com

- ANF. Asociación nacional de fabricantes - autoridad de certificación:
  https://www.anf.es

- Banco de España:
  https://www.bde.es/bde/es/

- Banco Santander:
  https://www.santander.com.ar/banco/online/empresas/canales-de-atencion/online-banking-empresas/certificado-digital

- CAMERFIRMA. Autoridad de certificación de las cámaras de comercio:
  https://www.camerfirma.com

- CATCERT. Agencia Catalana de Certificación:
  https://www.catcert.cat

- CGCOM. Consejo General de Colegios Oficiales de Médicos de España:
  https://www.cgcom.es/

- CNP. Dirección General de la Policía:
  https://www.policia.es/

- Coloriuris (CIPSC):
  https://www.coloriuris.net/

- DNIe:
  https://dnielectronico.es

- EDICOM:
  https://www.edicomonline.com/es/

- ESCB. European System of Central Banks:
  https://www.ecb.europa.eu/

- ESFIRMA:
  https://www.esfirma.com/

- FIRMAPROFESIONAL:
  https://www.firmaprofesional.com/

- CERES. Fábrica Nacional de Moneda y Timbre:
  http://www.fnmt.es/

- GISS. Gerencia de Informática de la Seguridad Social:
  http://www.seg-social.es

- IVSING / IVNOSYS:
  https://www.ivnosys.com/

- IZENPE. Empresa vasca de certificados y firma electrónica:
  https://www.izenpe.eus

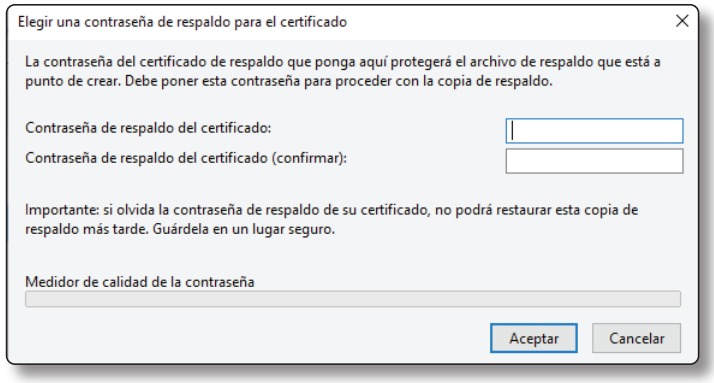
- LOGALTY:
  https://www.logalty.com/

- MINISTERIO DE DEFENSA:
  https://www.defensa.gob.es/

- MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL:
  http://ca.mtin.es/es/CA_MTIN/certificados.htm

- COLEGIO DE REGISTRADORES DE ESPAÑA:
  https://www.registradores.org/

- SERVICIO DE SALUD DE CASTILLA LA MANCHA (SESCAM):
  https://sanidad.castillalamancha.es/



Pulsaremos "Aceptar". Si todo el proceso es correcto, tendremos un nuevo fichero en la ruta seleccionada con extensión *.p12.

Podremos **renovar un certificado** durante los 60 días previos a la fecha de caducidad de su certificado y siempre y cuando no haya sido previamente revocado.

La renovación consiste en tres pasos que deben realizarse en el orden señalado:

1. **Configuración previa**. Para renovar el certificado es necesario tener el software adecuado para ello.

2. **Solicitar la renovación.** El certificado FNMT de Persona Física debe estar instalado en el equipo desde el que va a solicitar la renovación. Al final de este proceso se recibirá Código de Solicitud que se necesita para poder descargar el certificado renovado (ver "Solicitud de certificado" explicado anteriormente).

3. **Descargar el certificado**. Aproximadamente 1 hora después de solicitar la renovación y haciendo uso del código de solicitud recibido en la cuenta de correo electrónico informada a tal efecto, podremos descargar e instalar el certificado renovado y realizar una copia de seguridad.

Si el certificado que se quiere ahora renovar se obtuvo identificándose con otro certificado digital, DNIe o ya fue renovado anteriormente, la FNMT no podrá emitir un nuevo certificado siguiendo los pasos anteriores, sino que se deberá acreditar la identidad presencialmente en una Oficina de Registro de la misma manera que se obtuvo la primera vez.

Verificar estado

Ponemos a su disposición un servicio de verificación con el que podrá confirmar si su Certificado digital FNMT es Válido o ha sido Revocado.

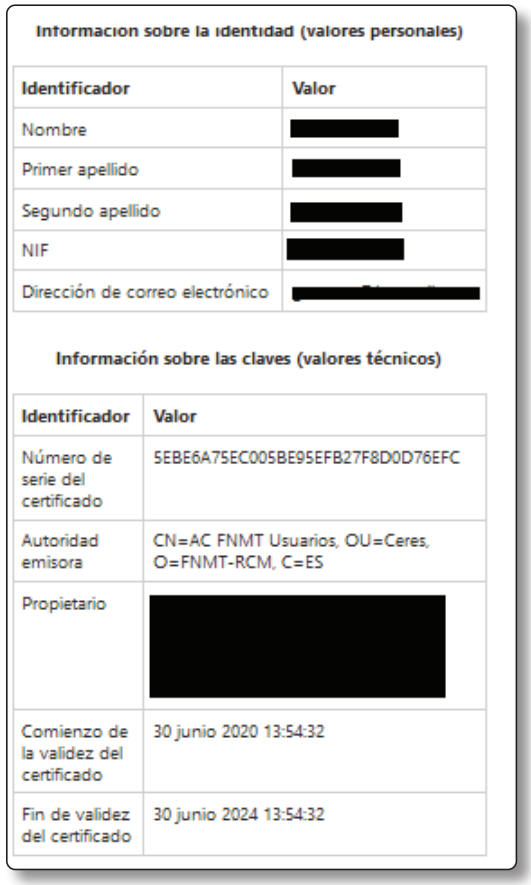
Este servicio está disponible para los siguientes tipos de certificados:

- Certificado FNMT de Persona Física (AC FNMT Usuarios)
- Certificado FNMT de Representante (AC Representación)
- Certificado FNMT de Empleado Público y Sello electrónico (Administración Pública)
- Certificado FNMT de Sello de entidad (AC Componentes Informáticos)
- DNI electrónico

Para comprobar el estado de su certificado, asegúrese de que éste se encuentra correctamente instalado en el navegador de su equipo, o bien listo para ser usado a través de su dispositivo criptográfico.

SOLICITAR VERIFICACIÓN

Pincharemos la opción de "Solicitar verificación" mostrándose a continuación la información vigente del certificado:



Información sobre la identidad (valores personales)

Identificador	Valor
Nombre	[redacted]
Primer apellido	[redacted]
Segundo apellido	[redacted]
NIF	[redacted]
Dirección de correo electrónico	[redacted]

Información sobre las claves (valores técnicos)

Identificador	Valor
Número de serie del certificado	5EBE6A75EC005BE95EFB27F8D0D76EFC
Autoridad emisora	CN=AC FNMT Usuarios, OU=Ceres, O=FNMT-RCM, C=ES
Propietario	[redacted]
Comienzo de la validez del certificado	30 junio 2020 13:54:32
Fin de validez del certificado	30 junio 2024 13:54:32

2.4 LA CONFIDENCIALIDAD DEL CERTIFICADO ELECTRÓNICO

Hablamos de confidencialidad cuando nos referimos a que sólo el destinatario del documento electrónico podrá conocer su contenido.

En relación a los prestadores de servicios de certificación, dos artículos de la Ley 59/2003 se recoge el término de "confidencialidad":

- En el artículo 20, "Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos", como una de las obligaciones del prestador de servicios:

  "Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante. Si el prestador de servicios gestiona los datos de creación de firma en nombre del firmante, deberá custodiarlos y protegerlos frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad para el firmante".

- En el artículo 23, "Limitaciones de responsabilidad de los prestadores de servicios de certificación", en el que se recoge que *"el prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:*

  (…)

  c) Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de éstos o, en su caso, de los medios que den acceso a ellos.

  d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma o, en su caso, de los medios que den acceso a ellos".

2.5 EXTINCIÓN DE LA VIGENCIA DE CERTIFICADO ELECTRÓNICO

En el artículo 8 de la Ley 59/2003, se recogen las "*causas de extinción de la vigencia de un certificado electrónico:*

- *Expiración del período de validez que figura en el certificado.*
- *Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.*
- *Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.*
- *Resolución judicial o administrativa que lo ordene.*
- *Fallecimiento o extinción de la personalidad jurídica del firmante, fallecimiento, o extinción de la personalidad jurídica del representado, incapacidad sobrevenida, total o parcial, del firmante o de su representado, terminación de la representación, disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.*
- *Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquel, sean transferidos a otro prestador de servicios de certificación.*
- *Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.*
- *Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.*

El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cinco años.

La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación".

En su artículo 9 se desarrolla la suspensión de la vigencia de los certificados electrónicos:

1. *"Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:*
   a) *Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.*
   b) *Resolución judicial o administrativa que lo ordene.*
   c) *La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8.1.*
   d) *Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.*
2. *La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación".*

2.6 CERTIFICADOS RECONOCIDOS

El artículo 11 de la Ley 59/2003 recoge el concepto y contenido de los certificados reconocidos.

Entendemos por certificado reconocido, "*los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten".*

Sobre el contenido, en el mismo artículo lo desarrolla:

"(…) Incluirán, al menos, los siguientes datos:

1. *La indicación de que se expiden como tales.*
2. *El código identificativo único del certificado.*