

FIRMA ELECTRÓNICA Y SERVICIOS AVANZADOS DE CERTIFICACIÓN



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

LA FIRMA ELECTRÓNICA Y EL CERTIFICADO

El marco normativo de la firma electrónica está regulado principalmente por:

- Ley 59/2003 de 19 de diciembre, de firma electrónica.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio electrónico.
- El Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997 y por el que se deroga el Real Decreto 1290/1999.
- El artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.

El artículo 3 de la Ley 59/2003, define la firma electrónica de la manera siguiente:

- «1. 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.
2. 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.
3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
4. 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.
5. Se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.»

De esta manera, la firma electrónica permite:

- Identificar al remitente de un mensaje de manera fidedigna, asegurando su imputabilidad.
- Verificar que el mensaje no ha sido manipulado.
- Garantizar que el emisor y el receptor del mensaje no puedan negar su existencia, y por lo tanto, su eficacia.
- Otorgar a cada usuario una clave privada propia, de uso exclusivo del titular, y una clave pública accesible por terceros.
- Almacenar la clave privada en el propio ordenador o una tarjeta criptográfica.

Por su parte, el artículo 6 de la misma Ley dice:

- «1. Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.»

El uso de la firma electrónica conlleva importantes beneficios, tanto para la propia Administración, como para las empresas y ciudadanos (ahorro en gastos administrativos, reducción y automatización de tareas, simplificación de procesos, mejora de la calidad del servicio, acercamiento a empresas y ciudadanos, eliminación de desplazamientos y tiempos de espera, reducción de costes y plazos de tramitación, aumento del nivel de servicios: disponibilidad 24 horas al día y los 7 días de la semana, ...).

LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE–REAL CASA DE LA MONEDA (FNMT-RCM) COMO PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Para crear y verificar una firma electrónica y, a su vez, poder autenticar fehacientemente la identidad del firmante, se necesita que una entidad de confianza, ajena al emisor y al receptor del mensaje, nos confirme, mediante la emisión de un certificado electrónico, que las claves con las que se comprueba la firma pertenecen a ese usuario.

En julio de 1996 se inició el Proyecto CERES, que dio como resultado la aprobación del marco legal inicial y el desarrollo de una infraestructura piloto. En 1998 se iniciaron aplicaciones piloto y es en 1999 cuando la Agencia Estatal de Administración Tributaria (AEAT) da a los ciudadanos la posibilidad de presentar la Renta 1998 y el pago del IVA, retenciones a cuenta y declaraciones IRPF para Pymes a través de los certificados emitidos por la FNMT-RCM.

En la actualidad, la FNMT-RCM constituye el primer y más importante prestador de servicios de certificación de España, y uno de los más importantes del mundo, otorgando, entre otros tipos de firma electrónica, la firma electrónica reconocida de acuerdo al contenido previsto en el anteriormente citado artículo 3 de la vigente ley de firma electrónica. La FNMT-RCM igualmente proporciona dispositivos seguros de creación de firma (tarjeta criptográfica). Esta tarjeta criptográfica dispone de chip certificado CC EAL4+ .

La FNMT-RCM se ha sometido a los controles más estrictos de calidad de sus servicios. Como muestra, seguidamente se ofrece un resumen de las encuestas realizadas en los años 2002 y 2003 de satisfacción a los usuarios:

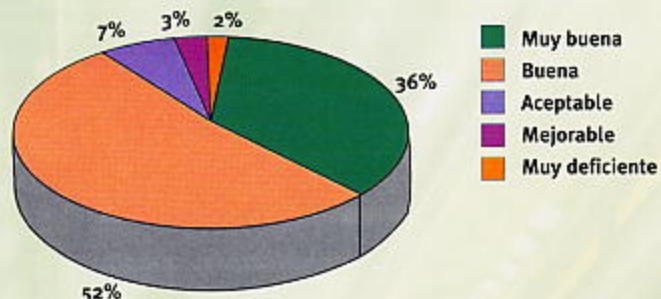
Resultados de encuestas a usuarios: 2002 y 2003 (muestra: 23724)

¿Qué valoración general le merece la utilización de nuestros servicios de certificación?

	2002	2003
Muy Buena	31%	36%
Buena	45%	52%
Aceptable	17%	7%
Mejorable	5%	3%
Muy deficiente	2%	2%

Puntuación media:

encuesta 2003: 7,91 - encuesta 2002: 7,41



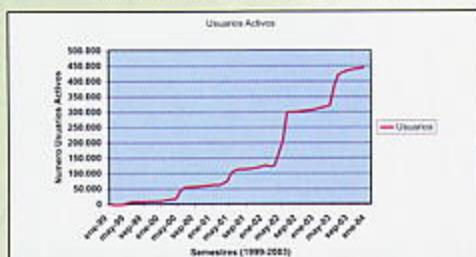
EL CERTIFICADO DE LA FNMT-RCM: UN SISTEMA MUY EXTENDIDO Y CON VOCACIÓN UNIVERSAL.

Como ha sido mencionado, la FNMT-RCM, a través del departamento CERES, es el primer prestador de servicios de certificación de firma electrónica en España y un ejemplo seguido internacionalmente. La principal característica de sus servicios es su carácter universal, esto es, cualquiera de las entidades que reciben los servicios de certificación es beneficiaria de los usuarios que se han adherido al sistema desde otras entidades. De hecho, como muestra de la vocación universal de los servicios que presta la FNMT-RCM, éstos se extienden a un gran número de entidades, organismos y empresas de naturaleza jurídica muy diversa; así nos encontramos con nueve Departamentos Ministeriales (como los de Economía y Hacienda), la Agencia Estatal de Administración Tributaria y la Seguridad Social, Organismos Autónomos (como el Comisionado para el Mercado de Tabacos o el Boletín Oficial del Estado), Entidades Públicas Empresariales (como el ICO), Entes Públicos (como la Comisión Nacional de la Energía, Consejo de Seguridad Nuclear, o la Comisión para el Mercado de las Telecomunicaciones), nueve Comunidades Autónomas (Madrid, Galicia, La Rioja, Murcia, Canarias, Navarra, Castilla-La Mancha, Castilla y León y Andalucía), Ayuntamientos (de gran tamaño como el de Madrid, Valencia, Salamanca, Toledo, Cuenca, Ciudad Real, Guadalajara y Albacete; así como más de 5.500 Ayuntamientos de menos de 50.000 habitantes), 25 Diputaciones Provinciales, (entre las que se encuentran Barcelona, La Coruña, Orense, Lugo, Pontevedra, Cádiz, Córdoba, Huelva, Jaén, Sevilla y Almería), colegios profesionales, (Colegio de Abogados de Madrid), Universidades (como la Carlos III de Madrid o la Universidad de Castilla-La Mancha), así como entidades privadas (Seguros Broker, Sociedad Digital de Autores de España...) Igualmente destaca junto al número de certificados alcanzados (que aparecen especificados en el mapa), la posibilidad que existe para que, en el extranjero, los poseedores de los documentos que el ordenamiento jurídico exige puedan acreditarse para obtener sus certificados a través de los Consulados de las Embajadas de España.

Los usuarios podrán acreditarse en cualquiera de los órganos y organismos del párrafo anterior, así como ante cualquier otro que tenga suscrito un convenio a efectos de acreditación, como es el caso del Colegio de Registradores de la Propiedad y Mercantiles.

Seguidamente se ofrecen datos referentes al número de certificados expedidos por la FNMT-RCM. Dichos datos hablan por sí solos respecto a la situación de la FNMT-RCM respecto a otros certificadores:

Evolución anual del número de certificados de usuario de la FNMT-RCM



Distribución geográfica de usuarios (1/1/2004): 446.239 certificados activos



SERVICIOS MÁS RELEVANTES QUE SE PUEDEN REALIZAR YA A TRAVÉS DE LA FIRMA ELECTRÓNICA

El contenido de estos servicios puede ser consultado con más detalle en: <http://www.cert.fnmt.es/clase2/organismain.htm>.

Las principales actividades y proyectos del Departamento CERES son:

- Explotación, mantenimiento y administración de la infraestructura.
- Desarrollo de nuevos servicios.
- Mejora de la gestión, y certificación asociada, en aseguramiento de la Calidad (ISO 9001: 2000), de la Seguridad (ISO 17799 y UNE 71502), de los servicios como Prestador de Servicios de Certificación (ETSI TS 101456), de los productos (dispositivos seguros de creación de firma CWA 14169) y de los servicios en la red (IQUA).

- Apoyo a clientes y usuarios.
- Oficinas de registro.

Los servicios disponibles son:

- **Servicios de certificación:**

Como se ha mencionado, existen 450.000 usuarios activos de los servicios de certificación de la FNMT-RCM, distribuidos a lo largo de todo el territorio nacional, que hasta la fecha han realizado decenas de millones de transacciones seguras de todo tipo sin que se haya producido reclamación alguna sobre las mismas. Además, el número de usuarios no solo se duplica cada año, sino que se verá incrementado notablemente, con la aparición de nuevos aplicativos, que tanto empresas como organismos de la Administración están comprometidos y decididos a ofrecer para mejorar su gestión y su servicio.

- **Validación *on-line* vía CRLs u OCSP:**

Dentro de los servicios de certificación se dispone de la validación de los mismos vía OCSP, lo que permitirá la validación de las transacciones al instante, garantizando, gracias al marco normativo vigente y a los servicios de la FNMT-RCM la realización de transacciones seguras en Internet y la imputabilidad de estos actos a los firmantes, incluso para transacciones económicas.

- **Certificados de personas jurídicas, certificados de representación, certificados de servidor y certificados de firma de código.**

Con esta oferta de certificados se desea presentar un modelo global de seguridad y flexibilidad en Internet, con plenas garantías técnicas y jurídicas para empresas y particulares, al amparo de la nueva legislación de Firma Electrónica y las nuevas políticas de certificación de la FNMT-RCM.

- **Tarjeta criptográfica CERES v.2.0.:**

La FNMT-RCM en cumplimiento de la Ley 59/2003 y de la Decisión de la Comisión Europea de 14 de julio de 2003 (L 175/45, 15/7/2003) fabrica y distribuye dispositivos seguros de creación y verificación de firma electrónica que soportan generación y custodia de claves en la propia tarjeta, así como la personalización que corresponda. Esta tarjeta es la única que a la fecha está siendo evaluada por la autoridad nacional competente (Centro Nacional de Inteligencia – Centro Criptológico Nacional). La tarjeta CERES v.2.0. es capaz de soportar más de 15 certificados X.509 distintos, con independencia de la CA y presentar unas capacidades y velocidades que la sitúan en una posición de liderazgo en el ámbito internacional.

Además el software necesario para el funcionamiento de la tarjeta CERES v.2.0 estará disponible en breve en la web de Microsoft para Windows XP y Windows 2000, así como para las futuras versiones que se implemente de los mismos. Permitiendo el reconocimiento automático de las mismas y la integración con las soluciones de autenticación de Microsoft.

- **Logín único en Windows®.**

Windows 2000 y Windows XP permiten el uso de tarjetas inteligentes con certificado para realizar el inicio de sesión, pero, a la fecha, se requiere que dichos certificados tengan implementada una extensión o atributo específico de Microsoft conteniendo el nombre del usuario que desea realizar logon. Dado que los certificados tienen carácter personal, y no parece conveniente vincular estos datos personales con datos de la vida laboral, como puede ser el «logon name» de la empresa u organismo al que pertenece el usuario; en breve se podrá emplear, por primera vez en el mundo, un certificado no Windows, estándar X.509 (certificados de la FNMT-RCM actuales), con tarjetas inteligentes criptográficas e implementar un entorno seguro de inicio de sesión en Windows XP, Windows 2000 y sucesivas versiones.

- **Time stamping. Servicios de fechado digital. Constancia de fecha y hora de las transacciones.**

¿Cuándo se emitió una factura? ¿Presentó a tiempo su reclamación? Cuando se realizan operaciones en Internet el conocimiento del tiempo es importante y solicitar a un tercero que de constancia de ello es fundamental a la hora de aportar pruebas.

La FNMT-RCM desarrolló este servicio en 1998 para la DG XXII de la Unión Europea. En octubre de 2002 se aprobó por unanimidad como norma internacional ISO/IEC 18014, siendo esta casa, a través de sus colaboradores, sus redactores.

- **Voto electrónico en Juntas Generales de Sociedades.**

El voto electrónico para sociedades es un mecanismo alternativo al voto tradicional efectuado en este tipo de sociedades. El voto electrónico mantiene todas las características de seguridad del tradicional, a la vez que permite mejorar otras como rapidez, participación, ... La base de este sistema es la firma digital, y gracias a ella se incluyen y se garantizan la solicitud pública de representación, delegación de voto o el propio voto del accionista.

- **Voto electrónico seguro con soporte en tarjeta criptográfica.**

La FNMT-RCM ha desarrollado una serie de aplicaciones, con el correspondiente soporte hardware, que junto con el correspondiente equipo humano permiten la realización de estos procesos democráticos en cualquier punto de nuestra geografía en un tiempo record. Sin embargo, como soporte de la firma electrónica se emplea la tarjeta criptográfica de la FNMT-RCM resultando las operaciones que se realizan sobre la tarjeta totalmente transparentes para el usuario.

- **Servicios de tercero de confianza:**

Según la legislación sobre comercio electrónico, las partes pueden pactar que un tercero archive las declaraciones de voluntad que integran el contrato, con constancia de la fecha y la hora en que tuvieron lugar. Cuando las

declaraciones se hayan realizado por vía telemática, el tercero debe archivarlas en soporte informático por el tiempo estipulado, que nunca será inferior a cinco años.

Por tanto, la custodia de las transacciones y documentos electrónicos es un factor importante en el desarrollo de las relaciones electrónicas entre partes ya que permiten dotar a las mismas de seguridad jurídica preventiva preconstituyendo tanto una prueba testimonial como documental de la realización de la transacción entre las partes. Este sistema de custodia facilita la captura de cualquier transacción electrónica que se haya realizado en Internet proporcionando a la misma seguridad jurídica, esto es, garantizando que ninguna de las partes puede alterar en el futuro el contenido de lo acordado.

- **Servicios de Notificación segura a ciudadanos con no repudio en destino.**

El servicio de notificaciones electrónicas es un servicio de web mail con acuse de recibo, cuyo acceso se realizará mediante identificación por procedimientos de firma electrónica. El servicio provee a los notificadotes de un sistema de no repudio en destino. Las notificaciones practicadas serán selladas y custodiadas electrónicamente. El servicio de notificación electrónica se podrá complementar adicionalmente con un servicio de notificación tradicional para completar una solución de correo mixto.

- **Facturas electrónicas.**

La nueva legislación sobre facturación telemática obliga al uso de la firma electrónica y la consiguiente validación de los certificados de firma empleados.

Adicionalmente, la base técnica de la facturación telemática permite la implementación de servicios diferentes susceptibles de combinarse con los ya conocidos de custodia, notificación, OCSP y sellado de tiempo.

Por lo que se refiere más en concreto al sector público, en la actualidad existen importantes servicios que se prestan a los ciudadanos a través de Internet de forma segura gracias al certificado de la FNMT-RCM. Podemos destacar, entre otros, los siguientes:

Administración General del Estado

El Ministerio de Economía, a través de su oficina virtual, permite iniciar más de 100 procedimientos administrativos sin utilizar el soporte papel:

- Presentación telemática de recursos y reclamaciones.
- Pago telemático de tasas.
- Trámites diversos con la Dirección General de Seguros y Fondos de Pensiones.
- Cumplimentación de los datos del Censo de Población y Vivienda que elabora el Instituto Nacional de Estadística.
- Compra – Venta de Deuda del Estado.
- Realización diversos trámites por los titulares de la Red de Expendedurías de Tabaco y Timbre, tales como: solicitudes de cierre temporal, de comercialización de artículos y servicios, de extensión transitoria, de transmisión mortis causa y comunicaciones de cierre y de información requerida.
- Presentación de solicitudes de licencias de importación-exportación de productos agroalimentarios y productos industriales.
- Gestión interna del propio Departamento, a través del conocido como sistema Pro@, accesible a través de la página Intranet. Este sistema permite la tramitación, sin utilizar papel, de más de 40 procedimientos que constituyen una parte esencial de la gestión diaria de una gran organización como el Ministerio de Economía. Dichos procedimientos se refieren a recursos humanos (solicitud de vacaciones, licencias, permisos, ayudas de acción social...), régimen interior (reserva de salas de reuniones, petición de material de oficina, incidencias...) y servicios informáticos (solicitud de medios tecnológicos, incidencias, etc...)

La Agencia Estatal de Administración Tributaria ofrece por su parte la realización de las siguientes tramitaciones telemáticas, entre otras:

- Presentación de declaraciones-autoliquidaciones (en la campaña de 2003 se han presentado a través de Internet casi 2.000.000 de declaraciones).
- Constitución de depósitos y participación de subastas On-line.
- Solicitud de cambio de domicilio fiscal.
- Recursos.
- Aplazamiento de deudas.
- Obtención y comprobación de certificaciones tributarias.
- Información On-line: consulta detallada del estado de tramitación de procedimientos, censo de operadores intracomunitarios de IVA, datos fiscales, devoluciones, verificación del NIF de empresarios y profesionales.

Administración Autonómica

- Consulta y petición de subvenciones de los Ayuntamientos a las Comunidades a través de sus páginas web certificadas.
- Firma digital de documentos oficiales y expedición de copias compulsadas.
- Envío de las disposiciones a publicar en los Boletines Oficiales de las distintas Comunidades.
- Diversos servicios y procedimientos On-line.

Administración Local

- El Ayuntamiento de Madrid permite la consulta de inscripción en el Padrón Municipal de habitantes, la domiciliación bancaria de Impuestos y Tasas periódicas y la obtención de información sobre Multas de Circulación.
- En los Ayuntamientos de Paterna y Alboraya (Valencia) los ciudadanos pueden acceder On-line a sus expedientes administrativos, solicitar certificados del Padrón Municipal y tramitar quejas y sugerencias.
- El Ayuntamiento de Valencia permite la consulta de instancias y expedientes así como el Padrón Municipal.
- La Diputación de Barcelona posibilita la gestión de impuestos a través de Internet, así como la publicación y la gestión del cobro de tasas del Boletín Oficial de la Provincia.

CÓMO SE OBTIENE EL CERTIFICADO

Si está interesado en obtener un certificado de la FNMT-RCM, seguidamente se explica el proceso que consta de tres apartados que deben realizarse en el orden señalado.

1 Solicitud vía Internet de su Certificado de Usuario

El usuario se conecta a la página web de la FNMT en la dirección www.cert.fnmt.es/clase2. Al final de este proceso obtendrá un código que deberá presentar al acreditar su identidad.

2 Acreditación de la identidad en una Oficina de Registro

El registro de usuario es presencial verificando la identidad y registrando los datos de su solicitud. Esto aumenta el nivel de seguridad del sistema.

3 Descarga de su Certificado de Usuario

Una vez realizado el registro presencial y con la ayuda del código obtenido en el paso 1, podrá descargar vía Internet su Certificado.

En cualquier caso, para cualquier información ulterior puede dirigirse a:

FÁBRICA NACIONAL DE MONEDA Y TIMBRE

Departamento CERES
C/ Jorge Juan 106 – 28009 Madrid
Tel.: 91 566 69 04. Fax: 91 566 69 05
E-mail: ceres@fnmt.es
<http://www.ceres.fnmt.es>

Servicio de atención telefónica (24x7): 902 181 696
Servicio de revocación telefónica (24x7): 902 200 616



CERES

www.cert.fnmt.es



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre