

FIRMA ELECTRÓNICA Y CERTIFICACIÓN DIGITAL

LA FIRMA ELECTRÓNICA

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

Permite por tanto que, tanto el receptor como el emisor de un contenido, puedan identificarse mutuamente con la certeza de que son ellos los que están interactuando, evitando 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.

Es una herramienta fundamental para la mejora de la seguridad de la información y la generación de confianza, dado que permite efectuar una comprobación de la identidad del origen y de la integridad de los mensajes intercambiados en Internet.

La facilidad de comprobar la identidad de una firma manuscrita no tiene ninguna similitud en el mundo virtual.

Para comprobar la veracidad de una firma electrónica se requiere el uso de la criptografía y el empleo de propiedades matemáticas en los mensajes codificados.

EL CERTIFICADO DIGITAL

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.

Es un documento digital mediante el cual un tercero (la autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto y su clave pública.

Componentes de un Certificado Digital

- El dueño del certificado: es la persona física o representante de la sociedad que solicita el certificado digital ante una autoridad de certificación y cuya identidad quedará identificada ante entidades que acepten ese certificado.
- La clave pública: es el dato que vincula la identidad del propietario del certificado. Se identifica al emisor de un mensaje mediante esa clave pública que está contenida en el certificado y garantiza la autenticidad del origen y el no repudio. Utiliza complejas técnicas de cifrado durante el envío de información.
- El emisor del certificado: también conocido como Autoridad Certificadora es la entidad en la confían tanto el emisor como el receptor de una comunicación. Se encarga de emitir los certificados una vez acreditada la identidad del solicitante, así como su renovación o revocación.
- Período de Validez: cuando una Autoridad Certificadora (CA) emite un Certificado Digital tiene un período de validez determinado. Dos meses antes de expirar ese período se puede renovar sin necesidad de personarse en ninguna oficina de registro.

¿Cómo obtener un Certificado Digital?

Solicitud del Certificado por Internet.

La Fábrica Nacional de Moneda y Timbre está erigida como Autoridad de Certificación y permite a los ciudadanos obtener Certificados de usuario a través de su página web: <http://www.cert.fnmt.es>

Pasos a seguir:

- Solicitud indicando CIF/DNI solicitante (anotar número de solicitud).
- Personarse en la oficina de registro a acreditar la identidad.
- Con el código recibido en la oficina de registro, descargar el certificado (este último proceso hay que realizarlo desde el mismo ordenador en el que se realizó la solicitud). El Certificado se instalará en el navegador de Internet.
- Exportación del Certificado: Una vez descargado el Certificado, es conveniente hacer una copia y guardarla en lugar seguro.

Utilidad del Certificado Digital

- Factura Electrónica
- Agencia Tributaria
- Seguridad Social
- Comercio Electrónico
- Gestiones bancarias
- Certificados de Ayuntamientos
- Etc.

Fuentes: Ministerio de Industria, Turismo y Comercio