

# GUÍAS FÁCILES DE LAS TIC

del

**COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN**

**Trabajo Premiado 2006**

**Firma Electrónica**

**Autor:**

**D. Víctor Requena Trujillo**

17 de Mayo 2006  
**DIA DE INTERNET**



colegio oficial  
**ingenieros de telecomunicación**

## ¿Qué es la firma electrónica?

En nuestra vida cotidiana, cuando cerramos un acuerdo, o cuando firmamos un contrato estampamos nuestra firma de puño y letra en los documentos en papel. Esta firma supone una aceptación de los puntos o condiciones que se estipulan en el documento.

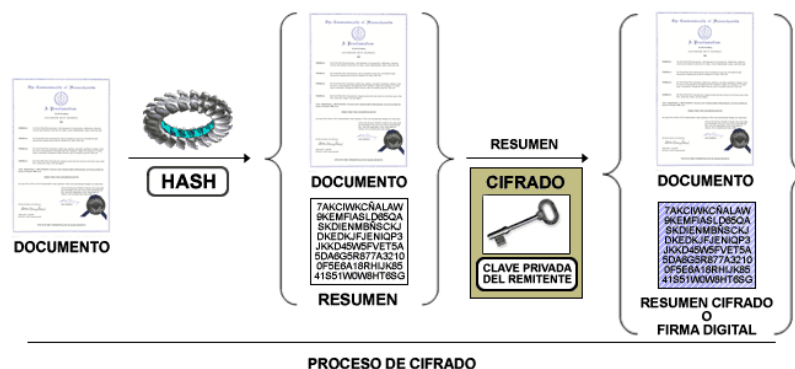
La firma electrónica, como su nombre indica, es el equivalente electrónico de nuestra firma manuscrita. Para resumirlo de forma sencilla, es una firma que nos permite acreditar y cerrar acuerdos por medios electrónicos, principalmente por Internet. Desde el año 2003 la firma electrónica tiene el mismo valor a efectos legales que la firma manuscrita. La firma electrónica se conoce también con el nombre de firma digital.

Las funciones fundamentales que proporciona la firma electrónica son tres:

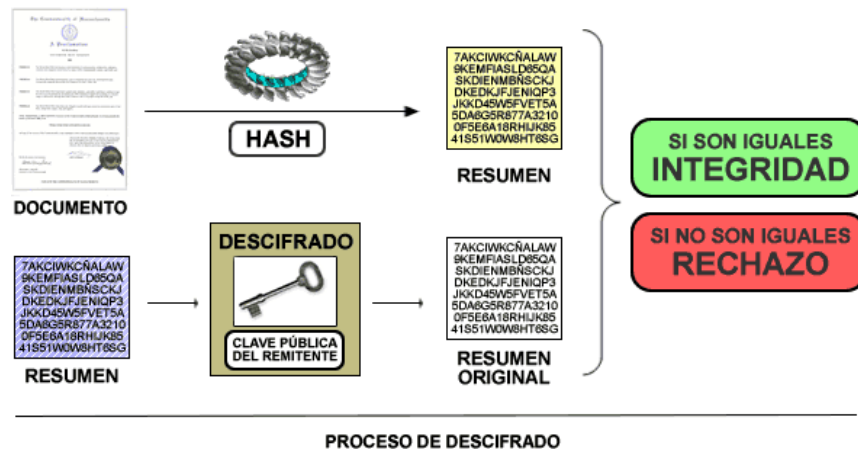
- **Identificación del firmante:** la firma identifica al firmante de forma única igual que su firma manuscrita.
- **Integridad del contenido firmado:** es posible verificar que los documentos firmados no han sido alterados por terceras partes.
- **No repudio del firmante:** un documento firmado electrónicamente no puede repudiarse por parte de su firmante.

En el intercambio de información firmada electrónicamente son necesarias dos claves: una clave pública y una clave privada. La clave privada se almacena en el ordenador del emisor y sólo la conoce él. La clave pública se distribuye entre todos los posibles destinatarios de nuestros mensajes o documentos firmados. La clave pública y la privada están relacionadas de forma que lo que cifra una lo puede descifrar la otra. La clave privada debe ser secreta y la pública no es necesario que lo sea.

Cuando se firma electrónicamente un documento en el ordenador del emisor se obtiene un resumen del documento a través de una función de hash. Un resumen es un conjunto de caracteres que se obtienen a partir del documento inicial. La propiedad más importante del resumen es que dos documentos diferentes producen siempre resúmenes diferentes. Incluso dos documentos con una diferencia mínima producen un resumen distinto. La probabilidad de obtener resúmenes iguales de un documento manipulado y de un documento original es tan pequeña que se considera imposible la alteración de un documento firmado electrónicamente. El resumen obtenido se cifra con la clave privada del firmante y se obtiene la firma electrónica del documento.

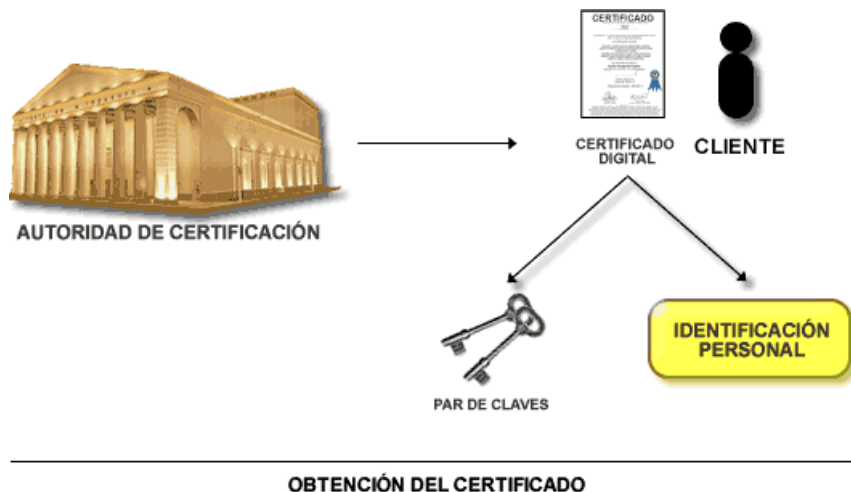


El receptor del mensaje firmado utiliza la clave pública para descifrar la firma y obtiene el resumen. Obtiene el resumen del documento recibido y comprueba que es igual que el resumen que le ha llegado cifrado en la firma electrónica. De esta forma se garantiza que el contenido del mensaje no ha sido manipulado.



La firma electrónica no aporta confidencialidad al mensaje por sí misma pero ocurre habitualmente que los mensajes firmados electrónicamente se suelen enviar cifrados con la misma clave privada utilizada en la firma para mayor seguridad. La identidad del firmante está asociada a su firma, como se explica en los párrafos siguientes. La integridad del mensaje la proporciona el resumen que, como hemos visto, nos asegura que el documento es original y no ha sido alterado por terceras partes.

Para poder firmar digitalmente documentos es necesario disponer de un certificado electrónico. Este certificado es un documento electrónico que es expedido a través de Internet por una Autoridad Certificadora. La misión del certificado es, como su nombre indica, validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta.



Este certificado contiene toda la información necesaria para poder realizar la firma electrónica y para identificar al usuario. Entre otros datos que se incluyen en el certificado de usuario encontramos: nombre completo, DNI, algoritmo y claves de firma, fecha de expiración y organismo que lo expide. La misión de la Autoridad Certificadora es dar fe de que la firma electrónica se corresponde con un usuario

concreto. Con el fin de cumplir esto las Autoridades Certificadoras deben mantener y proteger todos los datos de los certificados que expiden.

Los certificados tienen un período de validez. Habitualmente suele ser de tres años aunque puede variar en función del certificado. Tras ese período deben renovarse. El certificado también puede revocarse de forma que deja de ser válido desde su revocación. Los motivos más comunes de revocación son el cambio de datos del firmante y la posibilidad de que sus claves secretas de firma no sean seguras.

**Información del certificado**

Este certificado está destinado a los siguientes propósitos:

- Protege los mensajes de correo electrónico
- Asegura la identidad de un equipo remoto
- 1.3.6.1.4.1.4231.3.3

\* Más info. en declaración de entidades emisoras de certificados.

**Enviado a:** NOMBRE GARCIA PEREZ PEPE - NIF 12345678H

**Emitido por:** FNMT Clase 2 CA

**Válido desde:** 10/1/2006 **hasta:** 10/1/2009

Tiene una clave privada correspondiente a este certificado.

**Contenido del certificado**

Campo	Valor
Número de serie	3c 88 76 32
Algoritmo de firma	sha1RSA
Emisor	FNMT Clase 2 CA, FNMT, ES
Válido desde	martes, 10 de enero de 2006 21:45:53
Válido hasta	sábado, 10 de enero de 2009 21:45:53
Asunto	NOMBRE GARCIA PEREZ PEPE
Clave pública	RSA (1024 Bits)

CN = NOMBRE GARCIA PEREZ PEPE - NIF 12345678H  
OU = 746593746  
OU = FNMT Clase 2 CA  
O = FNMT  
C = ES

Propiedades del Certificado

Existen certificados personales de usuario y también certificados de empresa. Estos certificados contienen información adicional diferente pero su funcionamiento es muy similar. La firma digital de una empresa equivale a la firma manuscrita de los apoderados de la misma.

### ¿Cómo se utiliza la firma electrónica?

Utilizar la firma electrónica es sencillo ya que no requiere ningún conocimiento especial. Únicamente tenemos que instalar los certificados en las aplicaciones que los utilicen. El proceso de instalación de certificados es bastante sencillo y se basa en la exportación e importación a fichero de los datos del certificado.

Las aplicaciones más comunes que utilizan la firma electrónica son el navegador y el cliente de correo electrónico. Una vez instalado el certificado electrónico las operaciones de firma electrónica se realizarán de forma automática con unas pocas pulsaciones de botón.

En ocasiones se nos invitará a aceptar certificados que aún no son de nuestra confianza. Aceptarlos o no es también cuestión de unos pocos clic de ratón. Cuando aceptemos confiar en un certificado debemos ver si el emisor es de nuestra confianza.

El receptor de la información deberá tener los datos del certificado de usuario del emisor y reconocerlo como de su confianza. La diferencia es que el receptor no conoce la clave privada del emisor porque dispone de su certificado exportado sin esta clave. El único dato secreto del certificado electrónico es su clave privada, el resto de datos no comprometen la seguridad. Esta es la razón por la que se pueden intercambiar certificados exportados sin la clave privada.

## **¿Qué utilidad tiene la firma electrónica?**

Ya hemos visto que la firma electrónica aporta tres características en la comunicación por Internet: identificación, integridad de datos, y no repudio. Pero, ¿cuáles con las aplicaciones prácticas de la misma? Son muchas y variadas, tareas que hasta ahora suponían un gasto incómodo de tiempo se simplifican al poder realizarlas por Internet con nuestra firma electrónica. En general la firma electrónica permite operaciones por Internet que en la vida cotidiana requieren de una firma para validarlas.

En este listado se ponen como ejemplo algunas de las aplicaciones más importantes de la firma electrónica que se pueden realizar actualmente:

- Realización de la Declaración de la Renta a través de Internet.
- Recepción y envío de documentos con las Administraciones Central, Local y Autonómica.
- Firma de correos electrónicos.
- Firma de facturas con su consiguiente validez.

Una aplicación que ha surgido como consecuencia de la firma electrónica y que pronto se generalizará entre los ciudadanos es el recién creado DNI Electrónico. Este documento identificativo, además de su uso tradicional incorporará un certificado de usuario que proveerá de firma electrónica a todos los ciudadanos. Esta firma electrónica nos permitirá realizar transacciones electrónicas más seguras y permitirá que se generalicen todavía más los posibles servicios que utilicen la firma electrónica.

## **¿Cómo puedo conseguir mi certificado para firmar digitalmente?**

La Agencia Tributaria pone a disposición de todos los ciudadanos la posibilidad de solicitar un certificado de usuario. La solicitud de estos certificados se divide en tres pasos de los cuales dos de ellos se realizan de forma sencilla a través de Internet y sólo uno de ellos requiere presencia física en una oficina. Los pasos de solicitud de forma ordenada son los siguientes:

1. Solicitud del Certificado: en este primer paso se introduce en NIF y se obtiene un número de petición que debemos anotar y conservar hasta tener el Certificado.
2. Acreditación de la identidad en una Oficina de Registro: con nuestro número de petición y una fotocopia del DNI debemos dirigirnos a una oficina en la que se compulsarán nuestros datos a partir de nuestro DNI.
3. Descarga de su certificado: tras uno o dos días a partir del segundo paso se descarga su Certificado y se añade a su navegador.

Todos estos pasos están convenientemente detallados en un enlace de la Fábrica Nacional de Moneda y Timbre donde se pueden realizar los pasos comentados anteriormente. Un enlace en el que se puede obtener el certificado es el siguiente:

<http://www.cert.fnmt.es/clase2/main.htm>