

## La “Firma Electrónica” paso a paso

Qué es y para qué sirve  
LA FIRMA ELECTRONICA

Todas las marcas citadas en este documento se reconocen como de sus legítimos propietarios.

Todos los derechos intelectuales de este documento son reservados. No se puede reproducir este documento ni aprovechar partes del mismo sin la previa autorización de su propietario, por escrito o por correo electrónico firmado electrónicamente.

Este documento es Propiedad de "Consulting y Seguridad Digital, SL"

Historial del Documento:

Ideado	Diciembre 2003
Creado	Noviembre 2004
Revisado	Marzo 2006

**AVISO:**

La presente Guía es para orientación de los Usuarios. Se han obviado, al máximo y voluntariamente, los tecnicismos. Se persigue, como objetivo, facilitar el entendimiento cabal de cómo se procede con el uso de una Firma en el correo electrónico. Habrá, razonablemente, diferencias entre usos debidos a instalaciones distintas y/o Firmas de proveedores (Autoridades de Certificación) distintos. Debe, pues, considerarse esta Guía como orientativa. En ningún caso es determinante y sus autores no pueden asumir ninguna responsabilidad derivada de diferencias entre lo expuesto y el resultado en un ordenador u ordenadores. La tenencia de esta Guía presupone la aceptación de estos extremos y la renuncia expresa a cualquier acción legal derivada de diferencias entre lo que se expone y lo que el usuario obtiene, incluida la pérdida de información.

## Introducción

---

En un sistema de correo normal, el mensaje se introduce en un sobre, de manera que éste no pueda ser leído ni por el cartero. Adicionalmente, a los efectos de que llegue al destinatario que deseamos, en un lado del sobre ponemos su dirección completa y, en el otro lado del sobre, ponemos el remitente –nuestros datos- para que en caso de pérdida nos sea devuelto y, además, antes de abrir el sobre, el destinatario pueda saber quién le manda el mensaje.

Si observamos que la solapa de cierre tiene una 'forma' rara o está abierta, indudablemente sospechamos que alguien en el camino entre ambas direcciones la ha abierto y se ha enterado del contenido del mensaje.

Naturalmente, si no cerráramos el sobre, nunca podríamos llegar a sospechar que alguien ha tenido conocimiento del contenido, pero tampoco tendríamos la tranquilidad de saber que el mensaje nos llega sin que nadie se haya enterado del contenido.

Adicionalmente, si por algún motivo queremos asegurarnos más con respecto a que nadie tenga conocimiento del contenido sin que el destinatario observe anomalías visibles en el sobre, puede ponerse un trozo de "celo" pegado.

Este suele, en la mayoría de los casos, el método que empleamos para enviar y recibir cartas, mensajes, etc... asegurándonos de que:

1. YO lo envío a 'A'
2. Solo 'A' recibe lo que YO le mando.
3. YO recibo lo que me envió 'B'
4. 'B' está convencido de que solo YO recibiré lo que él me mandó.

Además observamos otras prácticas habitualmente. Por ejemplo, si la fecha de la carta que está dentro del sobre nos sorprende, miramos el matasellos del sobre, ya que nos muestra la fecha en la que un tercero –habitualmente el Servicio Oficial de Correos- tramitó el envío de la carta.

También podríamos mencionar los sistemas de Correo Certificado, Acuse de Recibo, etc.

Por consiguiente,

*Dado el uso cada vez más extensivo del Correo Electrónico, ¿cómo es que todavía enviamos nuestras "cartas" sin sobre?*

---

## La Firma electrónica

---

Una "Firma" es, brevemente explicado, un pequeño fichero que se 'añade' de forma informática a un correo electrónico de tal modo que, esencialmente:

- a- El emisor le asegura al destinatario que el remitente es quién dice ser,
- b- El receptor se asegura que el mensaje no pudo ser abierto en el camino entre el emisor y él mismo.
- c- Además, ambos pueden asegurarse de que sólo lo recibió el destinatario;

Hay cuatro grandes tipos de certificados electrónicos :

- 1- Firma electrónica de prueba o demostración. Sirve para que un usuario se convenza de la bondad y simplicidad de su uso.
- 2- Firmas Personales. Son aquellas en las que el usuario es quién asume la responsabilidad de manifestar quién dice ser.
- 3- Firmas reconocidas son las que están amparadas por una Autoridad de Certificación. En este caso, existe una Entidad que asume la responsabilidad de confirmar que el que 'firma' es quién dice ser.
- 4- Firmas de empresa. Son las que emite una Entidad (normalmente una empresa privada) al conjunto de sus empleados y/o personas relacionadas con ésta y que sirven para acreditar que un individuo pertenece a dicha entidad.

### Firmas de Prueba ('DEMO-CERT')

Las Sociedades que las emiten les conceden una caducidad standard de 30 días, sin embargo algunas ofrecen hasta 90 días de prueba. Llegadas a la caducidad, o se renuevan o son consideradas "no válidas" (en lenguaje técnico, REVOCADOS).

### Firmas Personales ('PERSONAL-EMAIL')

Son fáciles de obtener. Las Sociedades que las emiten les conceden una caducidad, habitualmente de un año aunque pueden ser más duraderas.

Son Firmas gratuitas y su principal característica reside en el hecho de que inicialmente nadie externo a su titular comprueba ni da fe de que la persona que emite el correo electrónico sea realmente quien dice ser.

Para su obtención, normalmente hay que contestar un conjunto de preguntas que se supone que sólo quién está solicitando el Certificado conocerá sus respuestas en el futuro.

Existe la posibilidad de que, una vez obtenida la firma, dos o más personas que dispongan de un Certificado emitido por la misma Entidad ratifiquen o den fe de que el poseedor del

certificado es quien dice ser. De este modo se puede llegar a establecer una red de Fedatarios interrelacionados entre sí.

### **Firmas reconocidas**

Son las emitidas por "alguien" que acredita la identidad de una persona.

Este "alguien" se denomina Autoridad de Certificación [en España: AC; aunque es también es usual denominarlas con las siglas en Inglés: CA –Certification Authority-].

Estas Autoridades están reguladas por disposiciones legales tanto de la Unión Europea, como de España. En nuestro país, entre otros, hay que tener en cuenta el Real Decreto Ley 12/2003. En este Decreto se define una Firma (Certificado) como un conjunto de datos, en forma electrónica que se utilizan como medio para identificar formal e inequívocamente al autor del documento que la recoge.

Una Firma permite, pues, la identificación de la persona que suscribe un documento gracias a que una Entidad ajena a ésta -pero ampliamente reconocida por de organismos públicos, empresas privadas y particulares- da fe de que el Certificado le pertenece y unívocamente le identifica.

Cuando es posible detectar que una Firma reconocida se ha modificado, es cuando se habla de firma electrónica avanzada (certificado electrónico avanzado).

### **Firmas de Empresa**

En el mercado hay empresas de software que están dedicadas a suministrar aplicaciones (sofisticadas) que posibilitan a una organización determinada emitir certificados en el ámbito de los individuos relacionados con ella. Estos certificados dan fe del vínculo que existe entre el firmante y dicha organización.

También hay algunos sistemas operativos, como es el caso de Windows (en versiones de sistemas operativos para servidores ) que ofrecen las herramientas necesarias para instalar una AC, y que permiten la puesta en marcha y emisión de Certificados desde la propia Empresa o Entidad.

En este supuesto, el coste es asumido por la propia organización que los emite y su vigencia suele ser mientras dure la relación entre el individuo y la organización con una revisión periódica, muy especialmente si cambia el ámbito de responsabilidad de la persona.

TIPO FIRMA	Coste / Vigencia	AMBITO	Sin Internet
Sin firma	✓ Sin coste directo.	Lo más común actualmente.	Un papel cualquiera, sin firma ni sobre: libre acceso de otras personas a su contenido.
De Demostración	<ul style="list-style-type: none"> <li>✓ Gratuita.</li> <li>✓ Un mes / tres meses.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Comprobar por sí mismo la operativa.</li> <li>✓ Firmar correos.</li> </ul>	No aplicable.
Personales	<ul style="list-style-type: none"> <li>✓ Gratuita.</li> <li>✓ Un año renovable automáticamente. Al alcanzar cinco años, hay que volver a pedirlo.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Protección de correo electrónico sin repercusión económica o legal.</li> </ul>	Firmar la carta y cerrar el sobre.
Reconocidos	<ul style="list-style-type: none"> <li>✓ Coste de mas de 15 euros al año.</li> <li>✓ Normalmente, anual renovable con un coste de renovación.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Que supongan repercusiones legales, mercantiles y/o económicas.</li> <li>✓ Relación con la Administración pública.</li> </ul>	<p>Enviar una carta vía Notario.</p> <p>Realizar una transferencia bancaria.</p>
De Empresa	<ul style="list-style-type: none"> <li>✓ Coste asumido por la empresa.</li> <li>✓ La vigencia, la determina la Entidad.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Relaciones internas y externas de la organización</li> </ul>	<p>Antefirma.</p> <p>Tarjeta de visita.</p>

## *Consideraciones de seguridad*

---

La firma electrónica ofrece seguridad a su propietario cuando se comunica con su entorno a través de Internet.

Pero si este fichero electrónico que denominamos Firma lo dejamos almacenado en el propio ordenador, no hemos avanzado demasiado en nuestra seguridad: lo dejamos al alcance de cualquiera que acceda a nuestro ordenador.

Es, pues, altamente recomendable almacenar la firma electrónica en un dispositivo externo al PC y de uso personal.

Además, si para acceder a la firma personal tenemos que usar un dispositivo externo y teclear –por ejemplo- un PIN de seguridad, como cuando usamos una tarjeta de crédito, mucho mejor.

En resumen: se aconseja disponer de un sistema externo y personal para almacenar nuestra firma, del tipo **tarjeta inteligente** o **"llave" USB** que, en esencia es un chip de tarjeta inteligente en un soporte con comunicación USB. Estos dispositivos caben cómoda y fácilmente en el bolsillo o en la cartera.

## *Obteniendo una firma electrónica*

---

El proceso para la obtención de una firma requiere un cierto tiempo pero no resulta en absoluto complicado.

La primera cosa que hay que tener en cuenta es que el léxico empleado por todas las Autoridades de Certificación, así como los diversos proveedores de hardware relacionado con la firma, es un tanto complicado.

A decir verdad parece redactado para disuadir usuarios deseosos de disponer de elementos de seguridad.

Lo cierto es que la explicación de los pasos necesarios para conseguir la firma todavía está en manos de técnicos que prefieren dar importancia al contenido técnico que al propio proceso aproximándolo al usuario.

- ❖ Muy especialmente: no se deje apabullar por la terminología.
- ❖ Tenga un poco de paciencia.
- ❖ Sea condescendiente, si como en algunos casos, las instrucciones han sido traducidas al castellano y pueden ayudar más a la confusión que a poder seguir el proceso para disponer de una Firma.

---

## *Nuestras "guías"*

---

Fruto de la experiencia personal, más que un soporte de soluciones concretas de Firma, ponemos a su disposición unas "guías" para ayudarle.

Forman el conjunto: **La "Firma Electrónica" paso a paso**. Encontrará:

1. La introducción, que es ésta 'guía'.
2. Instalación de una llave de salvaguarda de Firmas ChipKit
3. Instalación de un lector ChipKit para el uso de una tarjeta Inteligente de alta seguridad
4. Solicitud de una firma electrónica y su instalación en una llave ChipKit
5. Solicitud de una Firma e instalación en una Tarjeta Inteligente mediante el lector ChipKit
6. Exportación de una Firma desde el PC para importarla a su llave ChipKit
7. Exportación de una Firma desde el PC para importarla a una Tarjeta mediante el lector ChipKit
8. Varios documentos de apoyo al uso de la Firma Electrónica, recuperación de Firma electrónica y demás, de alto interés para los usuarios.

"Consulting y Seguridad Digital, SL" trabaja permanentemente tanto en hallar dispositivos y soluciones tremendamente sencillas y prácticas para un usuario, como en suministrar documentos de apoyo al uso de éstos.

Comentarios y consultas con respecto al uso de estas prácticas soluciones de seguridad personal (y corporativa) serán bien recibidas:

[Info@cysd.net](mailto:Info@cysd.net)