

## Firma electrónica

---

### ¿ Para qué sirve la firma electrónica ?

Pues tiene bastantes utilidades:

- ✦ **Asegurar** que la contraparte, en una relación vía Internet, es quien dice ser.
- ✦ **Garantizar** que el mensaje, al ir debidamente cifrado hasta que llega a su destinatario, no puede accederse a su contenido en el caso de que algún tercero no autorizado lo intercepte durante dicho tránsito.
- ✦ **Certificar** que el destinatario recibió el mensaje, registrándose incluso la hora y segundos a los que tal evento ocurrió. A este fenómeno, fruto de una mala traducción del inglés, se le conoce como no repudio.
- ✦ **Posibilitar**, que en caso de interceptación no autorizada del mensaje, e intento igualmente sin consentimiento de modificarlo, ello se detecte automáticamente.
- ✦ **Garantizar**, que en el supuesto de estar ante una página web determinada, estamos ante ella y no ante otra ( recordemos que mediante el fenómeno denominado web spoofing, un cracker o hacker habilidosos podrían hacernos creer que estamos ante una página web concreta, cuando en realidad estamos ante otra, amañada debidamente por éste para sus propios fines ). A este tipo de certificados se le suele llamar de servidor, y es, por poner un ejemplo, el que utilizan los bancos a la hora de acceder a su página web.
- ✦ También, aunque sin excluir otro tipo de prestaciones, pueden sernos útil para certificar el código fuente de programas informáticos, con lo cual, el potencial cliente o usuario autorizado del mismo, puede tener la razonable tranquilidad de que no está ante una obra plagiada, modificada, o contagiada por virus.
- ✦ No está de más aclarar que las utilidades expresadas, aunque inconscientemente nos las representemos mentalmente en el mundo de Internet, pueden también usarse en redes internas o externas, al margen de Internet, como pueden ser intranets o extranets.

### ¿ Hay varios tipos de firma electrónica ?

En efecto. Antes que nada menester es indicar que las primeras que se utilizaron fueron de las llamadas de clave simétrica, lo cual significa o supone que, habiendo dos partes, interesadas en el contenido de una comunicación o transacción electrónica, la clave a usar para decodificar o descifrar el mensaje, será sólo una, que ambas partes poseerán. Pues bien, la firma electrónica de la que hablamos, en el sentido de que la norma española comentada le confiere, a efectos legales, un valor equivalente al de la firma manuscrita, se basa en la llamada infraestructura de clave pública o de sistema asimétrico de claves, lo cual significa que ya no se habla de una única clave, de uso compartido por ambas partes, pues estamos ante un fenómeno bien distinto, que es el consistente en que hay dos claves, distintas - de ahí la expresión "asimétrica" -, una pública, y otra privada, pudiendo darse a conocer a los demás la primera, y debiéndose guardar por el interesado la segunda, sin revelarla a los demás. Esto que a primera vista podría parecer algo complejo, en la práctica no lo es tanto, puesto que los procedimientos técnicos que en este meollo "lidian", están en realidad automatizados por nuestro navegador y/o programa de correo correspondiente.

### ¿Qué es la firma electrónica avanzada?

En realidad, dicha expresión está extraída del Real Decreto-Ley 14/99 que tanto hemos comentado ya estas alturas, y dicha norma la define como aquella firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo

control, de manera: que está vinculada únicamente al mismo y a los datos a los que e refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

No obstante los tecnicismos de esta norma, así como también el lenguaje un tanto oscuro, y poco accesible que la misma usa (lenguaje que para el lego en informática puede tornarse indescifrable en sus primeros contactos en él), hemos de decir, en honor a la simplificación y el pragmatismo, que la FEA - firma electrónica avanzada - es aquella que, cumpliendo determinados requisitos técnicos, la ley la equipara, en cuanto a sus efectos, a la firma manuscrita. Bien, pero ante ello cabe, legítimamente, por supuesto, plantearse la siguiente cuestión : sí, todo esto está muy bien, pero ... ¿ cómo sé yo que estoy ante una firma de este tipo ?. Pues vamos allá: Lo sabremos porque quién emita la clave - nos referimos a la empresa que emite los certificados digitales, y se dedica precisamente a ello, a certificar digitalmente, sin que la confundamos con la otra parte de la comunicación - es una empresa, o más precisamente, un prestador de servicios de certificación que estará, volviendo a acudir a la terminología del decreto, certificado. Bien, pero... ¿por quién?: Pues por el Gobierno. Tal acreditación no es obligada para tales empresas, pero por la cuenta que les trae la llevan a cabo, ya que así inspiran más confianza en el tráfico no sólo jurídico sino mercantil, obteniendo un plus positivo en cuanto a su imagen. Supongamos que, "aún sin saber chino, nos sigue pareciendo un idioma oriental". Bien, que no cunda el "panicum", pues la praxis - muchas veces más inteligente que la "teoritis" - dispone de un método para averiguar cuándo estamos ante una FEA - "con perdón" - : Dependiendo del navegador a usar - nos referimos a los 2 más populares, el Netscape y el Internet Explorer -, nos aparecerá un símbolo en su parte inferior, con forma de candado, pero cerrado, o bien - e incluso simultáneamente a ello -, en donde ponemos la dirección a la que en nuestra navegación queremos ir - ejemplo, en donde ponemos siempre, y tan "compulsivamente", [WWW.opinionvirtual.com](http://www.opinionvirtual.com), si observamos bien, antes de ello está la expresión "http". Pues bien, si en "http" observamos que se añade la letra "S" - abreviatura de "secure", seguridad en inglés -. Estaremos ante una página que usa firma electrónica avanzada. Ejemplo: <https://www.opinionvirtual.com>.

De cualquier forma, lo últimamente expuesto - candado o letra "s" - no es precisamente riguroso, pero normalmente coincide. No está de más, precisamente por ello, que hagamos click - o doble click - sobre el candado mencionado, y si lo hacemos, comprobaremos que aparecen las notas o características a las que precisamente, y en el apartado siguiente, nos adelantaremos.

### ¿ Qué son los certificados digitales ?

Son documentos, digitales, emitidos por las llamadas entidades prestadoras de servicios de certificación. Las más conocidas son [www.feste.com](http://www.feste.com), , [www.ace.es](http://www.ace.es), [www.fnmt.es](http://www.fnmt.es) y [www.ips.es](http://www.ips.es) ( Fundación para el estudio de la seguridad de las telecomunicaciones; Agencia de certificación electrónica; Fábrica Nacional de Matasello y Timbre; e Internet Publishing Services, respectivamente ). Sirven para garantizar la identidad de las partes en la transacción; la privacidad de la misma; la comprobación de la posible alteración no autorizada del mensaje; y el no repudio.

A su vez, y como comentábamos en el apartado anterior, a través de la correspondiente activación del candado mencionado, podemos acceder al contenido del certificado, el cual, según la regulación nacional española, ha de, como mínimo, contener las siguientes informaciones - para ser considerados como incorporadores de firma electrónica avanzada - : La indicación de que se expiden como tales; El código identificativo único del certificado; La identificación del prestador que lo ha expedido o librado, con mención de su nombre o razón social, domicilio, e-mail, nº de identificación fiscal, y en su caso, sus datos de identificación

registral; La firma electrónica avanzada del prestador emisor de tal certificado; La identificación del signatario - el que intenta hacer valer su firma a través del certificado - por su nombre y apellidos, o un pseudónimo, pudiéndose también incorporar cualquier otra circunstancia personal cuando esta sea significativa, siempre y cuando se dé consentimiento en cuanto a ello por parte del firmante; En los casos de actuarse por representación, indicarán el documento en el que la misma se base; Los datos de verificación de firma -clave pública - que correspondan a los de creación de firma - clave privada -

### ¿ Qué es el no repudio ?

Es una característica de los certificados digitales que incorporan la llamada firma electrónica avanzada - regulada en el Real Decreto Ley de firma electrónica, cuyo texto y otros está en [www.fnmt.es](http://www.fnmt.es), en el apartado de legislación -, y consiste en que tanto el emisor, como el receptor, no pueden negar haber efectuado el mensaje; también permite evitar la copia o duplicación de los certificados, así como su uso fuera del tiempo para el que hayan sido emitidos.

### ¿ Qué tipos de certificados hay ?

Los hay desde para transacciones en las que una o ambas partes son administración pública - [www.fnmt.es](http://www.fnmt.es) -, o con finalidad exclusivamente mercantil, entre empresas - obtenibles sobre todo en [www.ace.es](http://www.ace.es) -, o para uso exclusivamente entre particulares - que se pueden conseguir en [www.feste.es](http://www.feste.es) -. Se pueden usar para transacciones por la red, o simplemente, y a título de ejemplo, para garantizarnos que la página web que visualizamos es auténtica, y no es otra falsificada, o para "lacrar" nuestro correo electrónico.

### ¿ Cuánto cuestan los certificados digitales ?

A pesar de que no hay uniformidad de precios al permitir el Gobierno su concurrencia en un régimen de libre competencia, se puede decir, a modo de ejemplo, que para un particular, sin ánimo de lucro, puede oscilar entre diez mil o doce ptas. el primer año, con una renovación anual de sobre las mil o dos mil ptas., o bien, para establecer una web segura, desde las doscientas mil. De cualquier forma, también los hay, de tipo personal, desde unas 2000/ptas. año, hasta 8 ó 10 indicadas. Hemos de comentar, no obstante, que el precio dependerá - entre otras cosas - del grado de certificación que nos reporten con el uso del certificado : Ejemplo : No es lo mismo que no comprueben nuestra identidad a la hora de solicitarlo - con lo cual no se acreditará, con el uso del mismo, nuestra verdadera identidad -, que otro en el que previamente, y de forma presencial, sí se haya comprobado dicha circunstancia.

### ¿ Como se obtienen los certificados ?

En principio es vía on line, aunque según los casos hace falta presentar determinada documentación física, y acreditar nuestra personalidad en persona, ya sea a través de corredores de comercio, notarios, o ante la misma administración, según los casos. De todas formas, el primer paso es contactar vía internet con las entidades de certificación - como por ejemplo Ace : [www.ace.es](http://www.ace.es); Feste : [www.feste.es](http://www.feste.es); o FNMT : [www.fnmt.es](http://www.fnmt.es) -, para así poder ver sus precios, servicios, y modalidad de pago y tramitación.  
¿ Existen certificados para todo tipo de transacciones ?

Se recomienda usar, al menos, los basados en las especificaciones técnicas denominadas X.509 y SET.

¿ Qué ordenador hace falta ?

Actualmente basta para ello con un ordenador tipo Pentium, con un mínimo de 8 megas de memoria RAM; también se requiere usar Windows como sistema operativo, en sus versiones 95 en adelante, o NT, a la vez que el navegador ha de ser Netscape o Internet explorer 4.0 o posterior.

Actualización: 08/septiembre/2004

[Principal](#) ▶ [Información Fiscal](#) ▶ [Trámites](#) ▶ [Guía de Requisitos y Trámites Fiscales](#) ▶ [Firma Electrónica Avanzada](#)

**Nota:** Es importante señalar, que el contribuyente que desee obtener un certificado de Firma Electrónica Avanzada, deberá concertar vía telefónica una cita para acudir a la Administración Local de Asistencia al Contribuyente.

D.F. y área metropolitana: 5447- 4070

Monterrey: 8150- 0277

Del resto del país, llame sin costo: (01 800) 849-9370

De lunes a sábado, de 8:30 a.m. a 9:30 p.m.

El asesor telefónico que le atienda, antes de registrar su cita validará su situación fiscal. Para validarla se verificarán los siguientes datos:

RFC.

Nombre (personas físicas), razón social (personas morales).

Domicilio fiscal.

## Firma Electrónica Avanzada

**Fundamento Legal:** CFF 17-D; RMF 2.3.7 y 2.22.1

-Descargar el software denominado SOLCEDI y generar el requerimiento de Certificado de Firma Electrónica Avanzada.

Acudir a la ALAC con lo siguiente:

Tratándose de personas físicas:

-Copia certificada, copia fotostática certificada por un funcionario público y fotocopia simple del acta de nacimiento. (copia certificada para cotejo)

- Tratándose de mexicanos por naturalización, original o copia certificada y fotocopia simple de la carta de naturalización expedida por autoridad competente debidamente certificada o legalizada, según corresponda. (original o copia certificada para cotejo)

- Tratándose de extranjeros, original y fotocopia simple del documento migratorio

vigente que corresponda, emitido por autoridad competente con la debida autorización para realizar los actos o actividades que manifiesten en su aviso. (original para cotejo). Asimismo, deberán proporcionar fotocopia debidamente certificada, legalizada o apostillada por autoridad competente con que acrediten su número de identificación fiscal del país en que residan, cuando tengan obligación de contar con este en dicho país.

- Original y fotocopia de Identificación oficial del contribuyente. (original para cotejo)

- Original y fotocopia de Comprobante de domicilio fiscal. (original para cotejo)

Tratándose de Personas Morales:

- Copia certificada y fotocopia simple del documento constitutivo debidamente protocolizado. (copia certificada para cotejo)

- Tratándose de personas distintas a sociedades mercantiles, original o copia certificada y fotocopia simple del documento constitutivo de la agrupación o, en su caso, fotocopia simple de la publicación en el órgano oficial, periódico o gaceta. (original o copia certificada para cotejo)

- En caso de Asociaciones en Participación, fotocopia simple del contrato de la asociación en participación, con firma autógrafa del asociante y asociados o sus representantes legales. (original para cotejo)

- En caso de Fideicomiso, original y fotocopia simple del contrato de fideicomiso, con firma autógrafa del fideicomitente, fideicomisario o sus representantes legales, así como del representante legal de la institución fiduciaria. (original para cotejo)

- En caso de Sindicatos, original y fotocopia simple del estatuto de la agrupación y de la resolución de registro emitida por la autoridad laboral competente. (original para cotejo)

Tratándose de residentes en el extranjero con o sin establecimiento permanente en México, deberá acompañar original y fotocopia simple del documento notarial con el que haya sido designado el representante legal para efectos fiscales. (original para cotejo)

Las personas morales residentes en el extranjero deberán proporcionar, además de su número de identificación fiscal del país en que residan, cuando tengan obligación de contar con éste en dicho país, su documento constitutivo debidamente apostillado o certificado, según proceda. Cuando el documento constitutivo conste en idioma distinto al español deberá presentarse una traducción autorizada.

- Original y fotocopia de Identificación oficial del representante legal (original para cotejo)

- Original y fotocopia de Comprobante de domicilio fiscal. (original para cotejo)

- Copia certificada del poder general para actos de dominio o de administración del representante legal.

Tanto personas físicas como personas morales deberán de presentar además lo siguiente:

-Disco magnético de 3.5" con el archivo con terminación .req, que generó el SOLCEDI

- Formato "Solicitud de Firma Electrónica Avanzada (Persona Moral/Persona física)" (duplicado)

## Generación del Certificado Digital

### Descarga de la aplicación SOLCEDI

---

La aplicación de Solicitud del Certificado Digital (**SOLCEDI**), se utilizará para que el contribuyente (persona moral o persona física) pueda generar tanto el archivo de requerimiento (que se deberá presentar el día de su cita), como su clave privada (la cual deberá resguardarse en un lugar seguro).

Esta aplicación, que se encuentra disponible en esta sección, deberá descargarse y ejecutarse en su equipo de cómputo. El programa genera los siguientes productos:

1. El archivo de Requerimiento de Certificado Digital, que contiene los datos mínimos para la generación del Certificado Digital. Este archivo tiene extensión (**\*.req**).
2. El archivo de la Llave Privada del solicitante, cuya extensión será (**\*.key**).
3. Sólo si se solicita el trámite de Renovación se creará un tercer archivo con extensión (**\*.ren**), el cual será enviado a través de un mecanismo implementado en la página de Internet del SAT. El beneficio que el contribuyente recibe de este procedimiento es que no será necesario que se presente en las instalaciones de la ALAC que le corresponda, y podrá realizar este trámite desde la comodidad de su casa u oficina. Consulte la sección de renovación del Certificado Digital.

#### Tutoriales del SOLCEDI:

- Tutorial para personas físicas **FTP HTTP**
- Tutorial para representantes legales **FTP HTTP**
- Tutorial para personas morales **FTP HTTP**

Aplicación y Manual SOLCEDI [Disponible para Windows Xp] (1.64Mb.) **FTP HTTP**



#### **No olvide conservar:**

---

- La llave privada, es decir, el archivo (\*.key)

- La clave de acceso para encriptar su clave privada.
- La clave de revocación.

## **Estándares y especificaciones técnicas para la utilización de aplicaciones informáticas para la generación de claves distintas al SOLCEDI**

---

Los contribuyentes que opten por utilizar aplicaciones informáticas distintas al SOLCEDI, para la generación de claves, deberán cumplir con las especificaciones y estándares siguientes:

**1.-** Los requerimientos digitales deberán estar contruidos de acuerdo con el estándar PKCS10

**2.-** Los campos requeridos para el procesamiento adecuado del requerimiento son los que a continuación se enlistan:

**a.** La clave del RFC a 12 posiciones para las personas morales y a 13 posiciones para personas físicas. Si el requerimiento pertenece a una persona moral, se debe agregar la clave del RFC del representante legal, separada de la del contribuyente con un carácter (/).

Ejemplo: RFC del contribuyente / RFC del Representante Legal.

Este valor deberá registrarse en el campo de los "Nombres Distinguidos" denominado "UniqueIdentifier", con respeto a las reglas de composición y longitud de este campo según la descripción del PKCS10.

**b.** Correo Electrónico, registrado en el campo de "Nombres Distinguidos" denominado "mailAddress", con respeto a las reglas de composición y longitud de este campo según la descripción del PKCS10.

**c.** Clave de Revocación, registrada en el atributo extendido denominado "ChallengePassword", con respeto a las reglas de composición y longitud de este campo según la descripción del PKCS10. Cabe mencionar que según este estándar, el valor corresponde al resultado de aplicar el algoritmo SHA1 sobre el texto de la Clave de Revocación, expresado en Base 64.

**d.** El tamaño de las claves pública y privada deberá ser RSA 1024 bit respectivamente.

**3.-** Adicionalmente y de manera optativa se podrá incluir la clave CURP en el campo de "Nombres Distinguidos" denominado "SerialNumber". La selección de este campo se debe a su correspondencia según el estándar con la intención de almacenar un identificador de objeto en un campo de tipo alfanumérico.

**4.-** De acuerdo al software por el que se opte, campos adicionales podrán ser incluidos en el requerimiento.