

LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Por Javier Ignacio Camargo Nassar.-
Notario Público No. 3 del Distrito Judicial Bravos, Chihuahua, México.

El proceso interno que conlleva el deseo de celebrar un acto jurídico debe ser exteriorizado para que la persona con quien pretendemos celebrarlo conozca de nuestra intención de hacerlo, es decir, debemos exteriorizar, a través de una declaración expresa o tácita, a la persona determinada o indeterminada, los elementos estructurales del acto que deseamos realizar, a fin de que esa persona, una vez conocida nuestra intención, realice -a su vez- el proceso interno que conlleva su deseo de realizar el acto jurídico que proponemos celebrar, el cual -a su vez- debe exteriorizar, para que quien propuso la celebración de ese acto -nosotros- conozca de su aceptación. Este proceso de comunicación permite la formación del consentimiento, que es un elemento de existencia de los actos jurídicos bilaterales.

A través de los medios convencionales que conocemos para llevar a cabo ese proceso de comunicación que lleva a la formación de los actos jurídicos, podemos suponer, primero, de la forma más conocida, que la comunicación se realiza de manera directa entre dos personas que se encuentran presentes, o no, al momento de convenir la celebración del acto jurídico y que, después de hacerlo, asientan en un documento los términos en que han convenido contratar, para después proceder a firmarlo en presencia del otro interesado o en presencia de una persona investida de fe pública, para reconocer su contenido y dejar constancia de su aceptación.

El segundo supuesto que hasta ahora pudiéramos concebir, fuera del procedimiento convencional a que nos referimos en el apartado que antecede, es el de que este acto jurídico sea convenido por medio del teléfono o del telégrafo, que son dos medios conocidos por todos nosotros, con los cuales nos encontramos fuertemente familiarizados, y que son reconocidos y regulados por el Derecho.

Pero ahora, como antes vimos, con el advenimiento de las TIC, encontramos una posibilidad distinta, resultado de los avances de la ciencia y de la tecnología, que significa que el mismo acto jurídico sea celebrado mediante la utilización de *medios electrónicos, ópticos o de cualquier otra tecnología*, entre personas que comúnmente no se encuentran presentes y que es posible incluso que no se conozcan en forma personal.

A partir de este hecho, debemos determinar la forma a través de la cual podremos otorgar a este “proceso de comunicación electrónico” la misma certeza que se atribuye tradicionalmente a los métodos convencionales que conocemos.

En el caso de la celebración de un acto jurídico bilateral por *medios electrónicos*, específicamente el *Internet*, suponemos que una persona, después de haber realizado el proceso interno de donde concluye su intención de celebrar un acto jurídico, exterioriza esa voluntad haciéndolo saber a la persona con quien desea contratar, utilizando un medio de comunicación electrónico como es el Internet, y envía a través del “correo electrónico” un *mensaje de datos*. La persona a la que va dirigida esta oferta -a su vez-, tomada la decisión de celebrar el acto, por el mismo medio lo hace del conocimiento del oferente, con objeto de formalizar así la celebración del acto jurídico. La celebración de actos jurídicos por *medios electrónicos, ópticos o de cualquier otra tecnología*, supone desde luego la comunicación entre dos o más personas que interactúan a través de algunos de los medios de comunicación a que nos hemos referido. Esta comunicación, por su naturaleza, ante la ausencia física de las partes contratantes, representa el inconveniente de que los sujetos que intervienen en la celebración del acto jurídico, requieren tener certeza de la identidad de la persona con la que contratan y de la integridad del contenido del *mensaje de datos* recibido.

Estos dos objetivos, la autenticidad e integridad del *mensaje de datos*, se logra, en forma segura, a través del uso de la *firma* que contiene un *certificado digital -firma digital-*, que permite al receptor de un *mensaje* verificar la autenticidad del origen de la información y que dicha información no ha sido modificada desde que se generó en forma original. De este modo, ofrece el soporte para establecer la autenticidad e integridad de los *mensajes de datos*, consecuentemente, el no repudio. De este modo, el creador de un *mensaje* firmado digitalmente no puede negar su autenticidad e integridad, por los atributos que hemos apuntado en este Trabajo.

Para este proceso, se requiere de la intervención de un tercero confiable, denominado *prestador de los servicios de certificación*, pues el *certificado digital* es un *documento electrónico* expedido y firmado en forma electrónica por un *prestador de servicios de certificación*. Es un *documento electrónico* generado y firmado digitalmente por una entidad de certificación, el cual vincula a un par de *claves (pública y privada)* con

una persona física o moral, confirmando su identidad. Mediante el *certificado digital*, podemos confirmar que el firmante o signatario identificado en un *certificado digital* posee, de manera exclusiva, la *clave privada* correspondiente a la ya mencionada *clave pública* de dicho certificado.

4.1. FUNCIÓN DE LOS PRESTADORES DEL SERVICIO DE CERTIFICACIÓN

Para utilizar una *firma digital* es necesario contar con un *certificado digital*. No puede existir una *firma digital* sin el *certificado digital*.

La *firma digital* es una especie de la *firma electrónica*, que permite asegurar la identidad del firmante y la integridad del *mensaje de datos*. Utiliza una técnica basada en el uso de una *clave privada* y de una *clave pública*, ambas relacionadas matemáticamente, de tal manera que una no pueda operar sin la otra. La función de esta *firma* es asegurar que el *mensaje de datos* fue enviado y firmado con la *clave privada* del titular de la *firma digital*, la integridad del *mensaje de datos* y que el titular de la *firma digital* no pueda repudiar o desconocer un *mensaje de datos* que ha sido firmado digitalmente usando su *clave privada*.

Así pues, es la *firma digital* acompañada de su *certificado digital* expedido por un *prestador de servicios de certificación* la que brinda confianza a las partes de la integridad y autenticidad del o los *mensajes de datos* que contienen los términos del contrato que pretenden celebrar.

Recordemos que, al momento de expedir un *certificado digital*, la autoridad certificadora verifica la identidad del titular del *certificado* que expide, de manera que podemos confiar en que esta autoridad confirmó la identidad de quien utiliza tal *certificado*. Si la *clave privada* que permite su utilización se encuentra bajo el control del titular, podemos confiar entonces que el *certificado* es utilizado por él, o por una persona a quien él permitió su acceso, lo cual lo hace responsable de su uso. La identificación del titular de un *certificado digital* puede realizarse inclusive en cierta clase de certificados, mediante la comparecencia ante notario público, quien hace constar la identidad del titular del *certificado*.

Sin embargo, si bien un *certificado digital* nos garantiza la identidad y la autenticidad de un *mensaje de datos*, ¿cómo podemos confiar en que un *certificado* es válido, que no ha sido falsificado, alterado o revocado? La razón por la que las partes que intervienen en la celebración de un acto jurídico por este medio pueden confiar en el *certificado digital* que cada una de ellas utiliza, a pesar de que nunca han tenido alguna relación personal, es por la confianza que les brinda una tercera parte que interviene en este proceso, que es el *prestador de los servicios de certificación* que expidió los mismos *certificados*.

Así, dos usuarios pueden confiar recíprocamente entre sí. Ambos tienen relación con una tercera parte, en la que confían y es quien garantiza la fiabilidad de los *certificados* utilizados en el proceso de comunicación. Este tercero es el *prestador de los servicios de certificación*, el cual, mediante su *firma digital*, ampara -a su vez- el *certificado* utilizado por las partes.

La entidad encargada de la *firma digital* de los *certificados* de los usuarios de un entorno de *clave pública* se conoce con el nombre de autoridad de certificación o *prestadora de los servicios de certificación*, que según lo define el Código de Comercio es la persona o institución pública que preste servicios relacionados con *firmas electrónicas* y que expide los *certificados*, en su caso. La importancia de esta clase de instituciones radica precisamente en la emisión de estos *certificados*, que son base fundamental para el proceso de comunicación segura.

Los elementos personales que intervienen en este proceso de comunicación para la celebración de un acto jurídico, tratándose de la celebración de actos jurídicos por *medios electrónicos*, se denominan *emisor* y *destinatario*, según el momento y el papel con que cada uno de ellos interviene en el proceso que mencionamos. Estos elementos personales en la formación del consentimiento tienen el nombre de oferente y aceptante. Cuando alguna de ellas actúa sobre la base de la garantía que establece un *certificado digital* o una *firma electrónica*, el Código de Comercio la denomina "*parte que confía*", y a favor de ella establece una serie de presunciones legales, precisamente por actuar con base en la confianza que brindan tales *certificados*.

El *emisor*, según lo define el Código de Comercio, es toda persona que al tenor de un *mensaje de datos*, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese *mensaje* antes de ser archivado, siempre que no haya actuado con el carácter de intermediario.

El *destinatario* es la persona designada por el *emisor* para recibir el *mensaje de datos*, siempre que no esté actuando con el carácter de intermediario respecto de ese *mensaje*.

Dentro de este proceso de comunicación segura, el *emisor* debe enviar el *mensaje de datos* con la *llave pública* del *destinatario*, firmado con su *llave privada*. El *destinatario*, al recibirlo, debe verificar que el *mensaje de datos* provenga precisamente del *emisor* y que éste no haya sido alterado. Para hacerlo, aplica al *mensaje de datos* la *llave pública* del *emisor* -por ser pública, es conocida por todos- y verificar la autenticidad y vigencia del *certificado digital*, dirigiéndose a la página de *Internet* de la autoridad que expidió tal *certificado*.

La vigencia del *certificado digital* -en su caso, su revocación- puede ser consultada en la página electrónica de la entidad que expidió dicho *certificado*.

En los términos del artículo 109 del Código de Comercio, un *certificado* dejará de surtir efectos para el futuro, en los siguientes casos:

I. Expiración del periodo de vigencia del *certificado*, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido.

II. Revocación del certificado por el *prestador de servicios de certificación*, a solicitud del firmante o su representante.

III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho *certificado*;

IV. Por haberse comprobado que al momento de su expedición, el *certificado* no cumplió con los requisitos establecidos en la ley y por resolución judicial o de autoridad competente que lo ordene.

4.2. CLASES DE CERTIFICADOS DIGITALES

Los *prestadores de los servicios de certificación* expiden distintas clases de *certificados digitales*, los cuales pueden variar de acuerdo a los fines y la seguridad que cada uno de ellos brinda al usuario. Los *certificados* son ofrecidos al público con distintas denominaciones de acuerdo a la entidad emisora. Por ejemplo, la empresa Advantage Security, en el contrato de prestación de servicios de certificación incluye los siguientes:¹

i) Certificados clase 1. Ofrecen el nivel más bajo de seguridad. Los *certificados* se emiten únicamente a los suscriptores y los procedimientos de autenticación se basan en la garantía de que el nombre del suscriptor es único y no es ambiguo dentro del dominio de un prestador particular y que cierta dirección de correo electrónico está asociada con una *clave pública*. Los certificados de la clase 1 son apropiados para *firmas digitales*, códigos, y control de acceso para transacciones que no sean comerciales o que tengan poco valor, donde la prueba de identidad no es necesaria.

ii) Certificados clase 2. Ofrecen un nivel medio de seguridad. Se emiten a suscriptores individuales únicamente. Incluyen procedimientos que se basan en una comparación de información proporcionada por un solicitante, contra la información en los registros comerciales o en bases de datos de los servicios de verificación de identidad aprobados de Advantage Security. Se pueden utilizar para *firmas digitales*, códigos y accesos de control, incluyendo la verificación de identidad en transacciones de valor medio.

iii) Certificados clase 3. Brindan el mayor nivel de seguridad. Son emitidos a personas físicas o morales para usarse tanto con el software del cliente como del servidor. Estos *certificados* pueden usarse para *firmas digitales*, códigos y control de acceso, incluyendo la verificación de la identidad en transacciones con un valor alto. Garantizan la identidad del suscriptor con base en la presencia personal (física) del suscriptor ante una persona que confirme su identidad, utilizando -al menos- una forma de identificación reconocida emitida por el gobierno y otra credencial de identificación.

El costo de un *certificado* puede variar entre \$ 1,000.00 y \$ 6,000.00 según la clase del *certificado* y la entidad que lo expide.

¹ www.advantage-security.com/es/repositorio/verificador. Consultada el 4 de agosto del 2007.

4.3. PROCESO PARA LA UTILIZACIÓN DEL CERTIFICADO DIGITAL

El proceso de *firma digital* de un *mensaje electrónico* comprende en realidad dos procesos sucesivos: la *firma* del *mensaje* por el *emisor* del mismo y la verificación de la *firma* por el receptor del *mensaje*. Esos dos procesos tienen lugar de la manera que se expresa a continuación:

Primero. *Firma digital* de un mensaje electrónico.

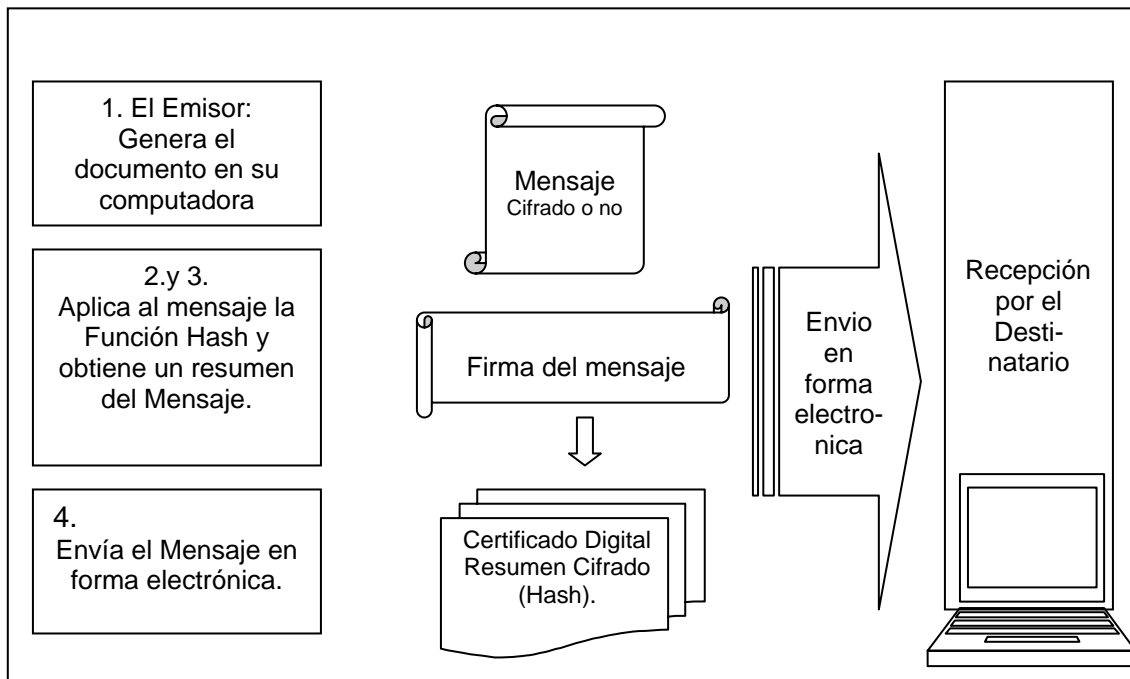
1. El *emisor* crea o redacta un *mensaje electrónico* determinado.
2. El *emisor* aplica a ese *mensaje electrónico* una *función hash* (algoritmo), mediante la cual obtiene un resumen de ese mensaje.
3. El *emisor* cifra ese *mensaje-resumen* utilizando su *clave privada*.
4. El *emisor* envía al receptor un correo electrónico que contiene los siguientes

elementos:

- El texto del *mensaje*, que es el mensaje en claro; es decir, sin cifrar. Si se desea mantener la confidencialidad del *mensaje*, éste se cifra también, pero utilizando la *clave pública* del receptor.
- La *firma* del *mensaje*, que a su vez se compone de dos elementos:
 - El *hash* o *mensaje-resumen* cifrado con la *clave privada* de *emisor*.
 - El *certificado digital* del *emisor*, que contiene sus datos personales y su *clave pública*, y que está cifrado con la clave privada del *prestador de servicios de certificación*.

Existen diferentes medios de almacenar el certificado, como el “*chip card*” que se almacena en una tarjeta inteligente y el usuario puede utilizar en cualquier computadora; el “*Browser*”, que se almacena en la computadora del usuario, modificando el Browser del usuario y únicamente puede utilizarse en la computadora en donde se almacena y “*el servidor*”, que se almacena en un servidor al que el usuario puede acceder mediante una clave desde cualquier computadora.

Para mejor comprensión de lo expuesto, a continuación exponemos gráficamente el procedimiento para firmar, enviar, recibir y verificar la autenticidad de un *mensaje de datos* utilizando la *firma* y el *certificado digital*.



Segundo. Verificación por el *receptor* de la *firma digital* del *mensaje*.

1. El *destinatario* recibe el correo electrónico que contiene todos los elementos mencionados anteriormente. En primer lugar, descifra el *certificado digital* del *emisor*, incluido en el correo electrónico, utilizando para ello la *clave pública* del *prestador de servicios de certificación* que ha expedido dicho *certificado*. Esa *clave pública* la tomará, por ejemplo, de la página *web* del *prestador de servicios de certificación*, donde existirá depositada dicha *clave pública* a disposición de todos los interesados.

2. Una vez descifrado el *certificado*, el *destinatario* podrá acceder a la *clave pública* del *emisor*, que era uno de los elementos contenidos en dicho *certificado*. Además, podrá saber a quién corresponde dicha *clave pública*, dado que los datos personales del titular de la *clave* constan también en el *certificado*.

3. El *destinatario* utilizará la *clave pública* del *emisor* obtenida del *certificado digital* para descifrar el *hash* o *mensaje-resumen* creado por el *emisor*.

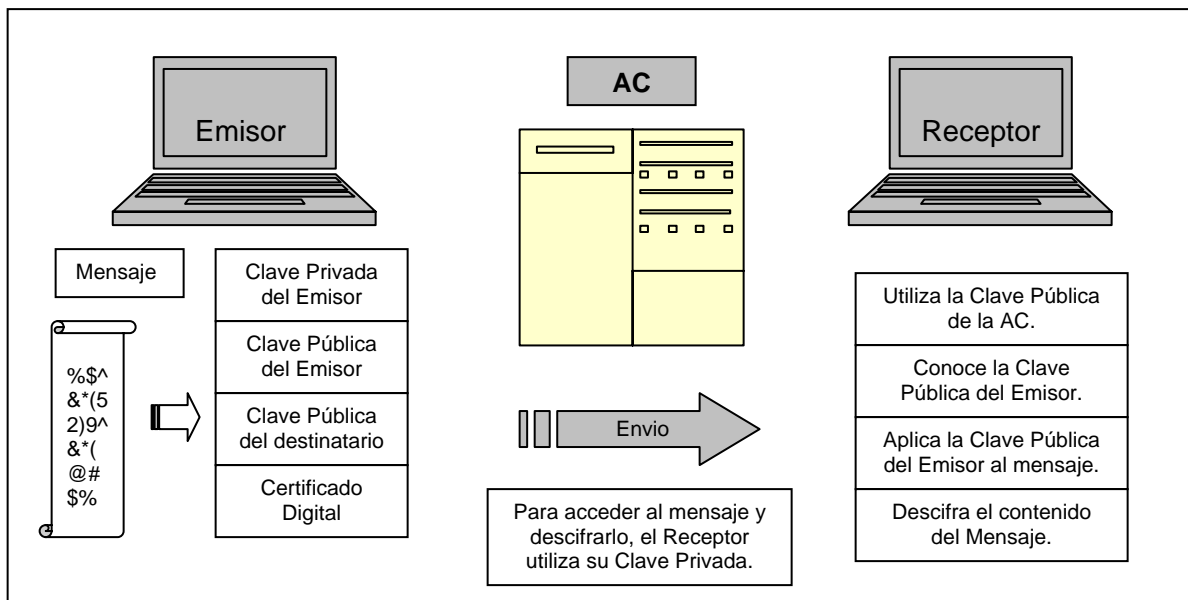
4. El *destinatario* aplicará al cuerpo del *mensaje*, que aparece en claro o no cifrado, que también figura en el correo electrónico recibido, la misma función *hash* que utilizó el *emisor* con anterioridad, obteniendo igualmente un *mensaje-resumen*. Si el

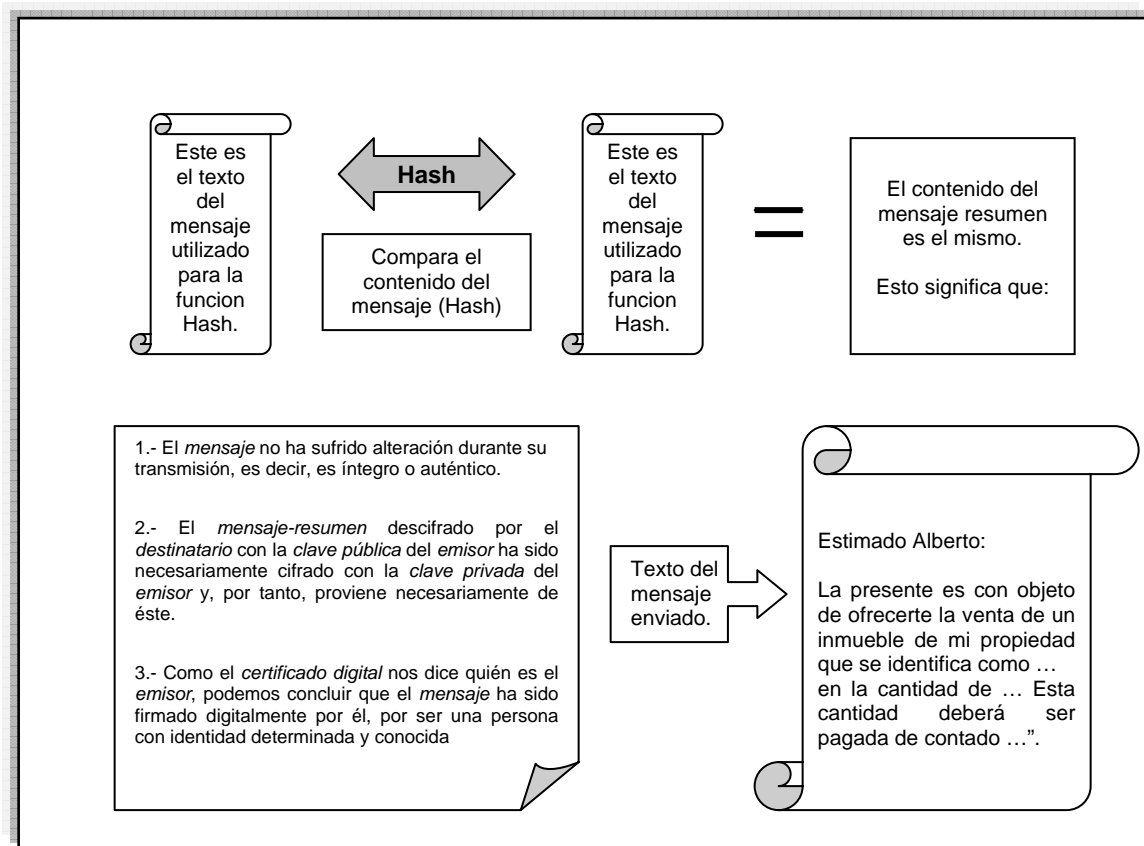
cuerpo del *mensaje* también ha sido cifrado para garantizar la confidencialidad del mismo, previamente, el receptor deberá descifrarlo utilizando para ello su propia *clave privada*. Recordemos que el cuerpo del *mensaje* había sido cifrado con la *clave pública* del *destinatario*.

6. El *destinatario* comparará el *mensaje-resumen* o *hash* recibido con el *mensaje-resumen* o *hash* obtenido. Si ambos *mensajes-resumen* o *hash* coinciden totalmente significa lo siguiente:

- El *mensaje* no ha sufrido alteración durante su transmisión, es decir, es íntegro o auténtico.
- El *mensaje-resumen* descifrado por el *destinatario* con la *clave pública* del *emisor* ha sido necesariamente cifrado con la *clave privada* del *emisor* y, por tanto, proviene necesariamente de éste.
- Como el *certificado digital* nos dice quién es el *emisor*, podemos concluir que el *mensaje* ha sido firmado digitalmente por él, por ser una persona con identidad determinada y conocida.

Por el contrario, si los *mensajes-resumen* no coinciden, ello quiere decir que el *mensaje* ha sido alterado por un tercero durante el proceso de transmisión. Si el *mensaje-resumen* descifrado es ininteligible quiere decir que no ha sido cifrado con la *clave privada* del *emisor*. En consecuencia, el *mensaje* no es auténtico o el *mensaje* no ha sido firmado por el *emisor*, sino por otra persona.

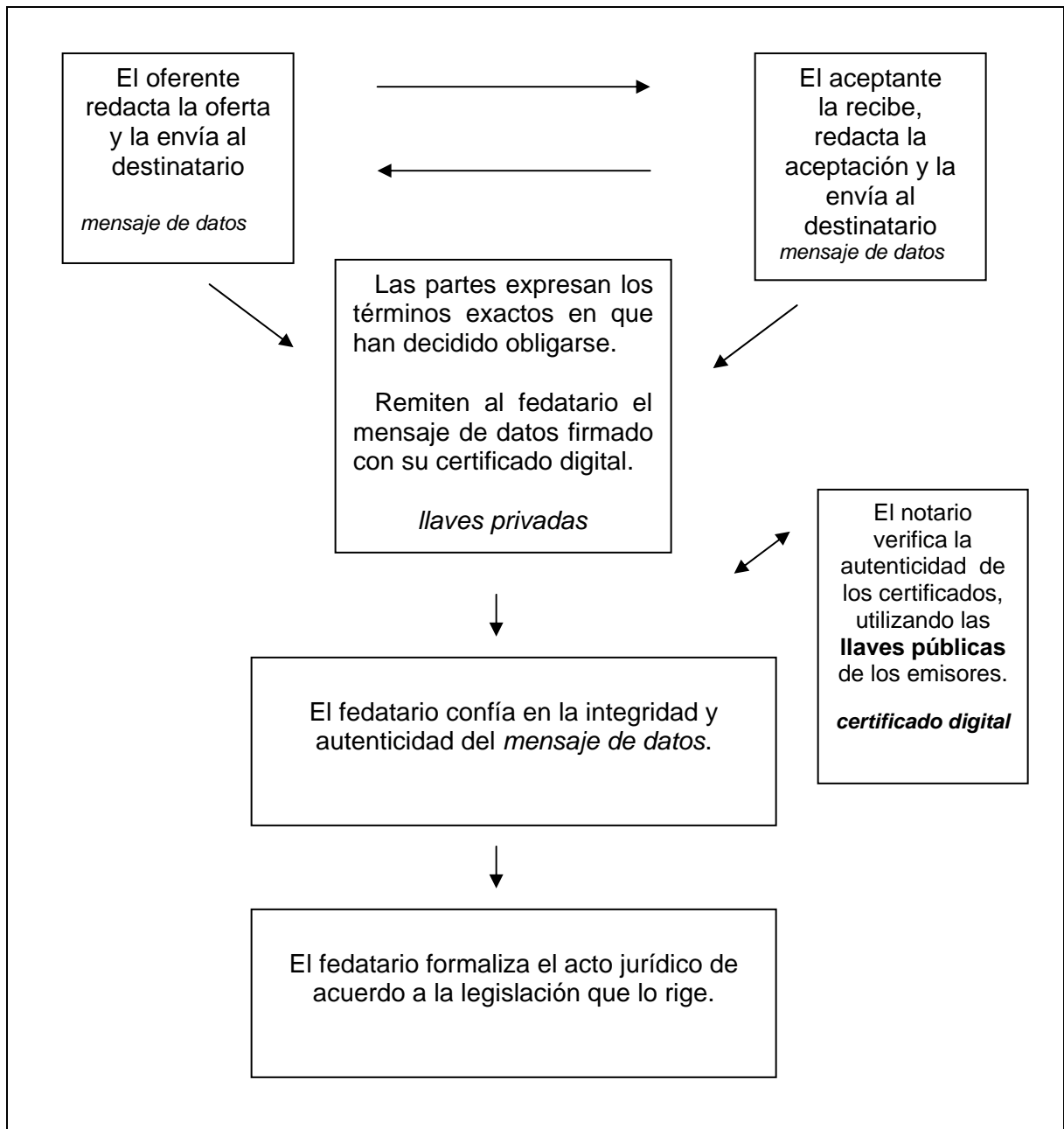




Finalmente, hay que tener en cuenta que las distintas fases del proceso de firma y verificación de una *firma digital* que han sido descritas no se producen de manera manual, sino automática e instantánea, por el simple hecho de introducir la correspondiente tarjeta magnética en el lector de tarjetas a la computadora y activar el procedimiento.

Este acto jurídico, según lo establece el Código de Comercio y la legislación Civil, puede ser celebrado a través de un fedatario público, cuando el acto de que se trate requiera para su validez de esta formalidad.

Aplicando los pasos del procedimiento antes ilustrado, en el caso específico de que el acto sea celebrado con la intervención de un fedatario público, este proceso se realiza como a continuación se indica en forma gráfica:



Al momento de enviar cada una de las partes que intervienen en este proceso el *mensaje de datos*, lo firma con su *llave privada* y asienta la *llave pública* del *destinatario*. A su vez, quien lo recibe aplica su *llave privada* para el acceso al documento, y la *llave pública* del remitente, para confirmar la autenticidad e integridad del *mensaje*.

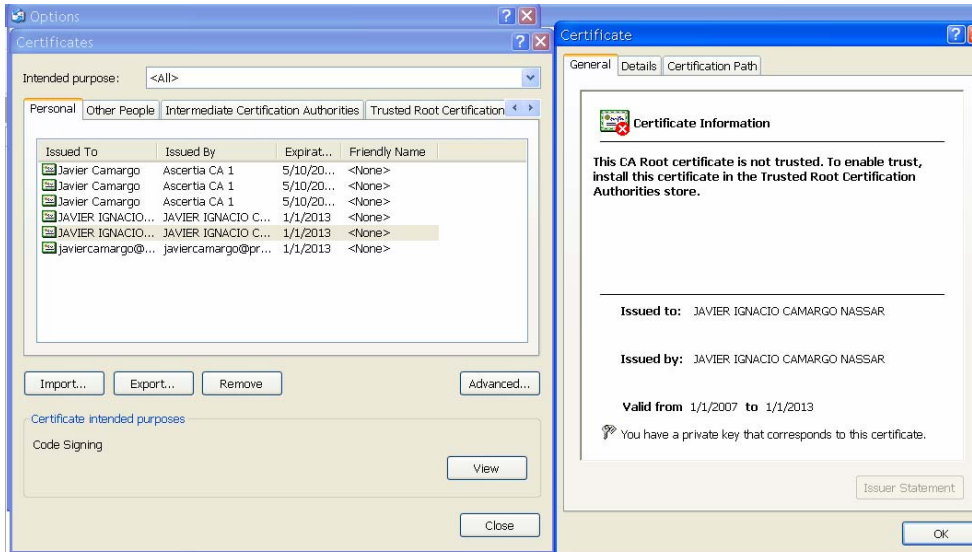


Figura 1. Imagen de un certificado real

Ejemplo de la llave pública que corresponde a este certificado:

```

30 81 89 02 81 81 00 d0 a1 43 3c 8c 25 1a 4c 77 f2 73 22 f8 19 58 03 d0 7b
c0 46 f7 0f a8 18 ea ad e5 df e4 f1 d2 ff df 97 d0 c4 10 c0 eb 8d 0b ad 16
fb 75 6e 84 97 ce 3b 37 ea 66 f0 df ad 43 96 03 e7 09 1e e3 9a 60 50 75 7b
e3 5c 06 67 b9 09 62 50 b2 47 24 aa 10 c2 47 1c 5f 19 f1 00 77 f0 a0 a3 5e
7b cf 89 78 8f 9c a5 98 ec 8c a7 96 97 30 f3 fc 36 9a 2f 2c 1e bb e0 e9 30
b2 ef 37 f4 ba 2e e4 8f e6 29 02 03 01 00 01

```

Ejemplo de una llave privada del tipo RSA -----BEGIN RSA PRIVATE KEY-----

```

MIICWQIBAAKBgQC63MxNw1knrELe6leK2ETGNKbam2z0bS1Ean7LgL+DA5lkZx2g
1M/sc3ix42+mSVz6qvhFsNiXQWXU981M8R9CNb671xHD5mdcQoaiOoIC6NTzCtvV
vrUaUm+p5bvdSh28VF2wD/WVboufUhLoSDh7G/BPqv5s2ZVwSs2MtKRG5QIBIwKB
gCAImA1CsDKv0PMDmfqLeYEQVx4XccN/ve54qAWhCuNCfhe2P5fp98IibHZEPwaQ
eTWh1+6re/hWQcU4uadofeWYW8Oz7lTeyMvrP+BvnZI jakEA5ba8//4LJtWR+44s
dvExzvHK5hhG7d0NTxzXq9V7V+CqTEuE65hatJgmrhd/m4fX3m/8b3ANPUj0C+lt
tT/+GwJBANA+xK19paFuv4IJAhCHGGeEMuJNkcdgJgCBvFP/gpOkroKmkDwKEhge
ei5rGCB85+9pCEyGzNj/KKaLHRNHv8CQFVSGLbas69Wo++4dupZ1ihLlhrzEwfk
ZAdxHOGNdvTBKU+Jw6f2wprZbXPc16ArJEtOKo/KiJMBGNE5ceQ8VxECQE1zJHr0
J507a7P0t5+9JlImIYdBYgg5zlf1hDx02Lp+/v1Tzyw+QTwok8gZJjFz4R5o1zJn
Wo9uR+Sf qhyRrG0CQCKgBvVgBkXr+aeg3X1nhjwzQ100gmWm53cUNTm/HWmq3v6F
Yyz+8fnkEuB+jDozOFev6cTlXpvkLSDxGwjH2R8=- END RSA PRIVATE KEY -

```

4.4. REGULACIÓN JURÍDICA

Las autoridades certificadoras son responsables de emitir, revocar, renovar y entregar *certificados digitales*. Ellas deben seguir rigurosos procedimientos para autenticar la identidad de las personas y organizaciones para las cuales emiten *certificados*. Todos los *certificados digitales* se "firman" con la *llave privada* de la autoridad certificadora. Su *llave pública* se encuentra a disposición del público en general.

Para conocer la importancia de la intervención de los *prestadores de servicios de certificación* dentro del proceso de comunicación electrónica, debemos hacer mención de la regulación jurídica de estas entidades en el Código de Comercio y en el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, de donde podemos destacar lo siguiente:

Pueden actuar como *prestadores de servicios de certificación* los notarios y corredores públicos, las personas morales de carácter privado creadas con ese fin y entidades del poder público.

Las personas morales creadas con el fin apuntado tienen por objeto:

1. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica.
2. Comprobar la integridad y suficiencia de los *mensajes de datos* del solicitante y verificar la *firma electrónica* de quien realiza la verificación y,
3. Llevar un registro de los elementos de identificación de los firmantes y de aquella información con la que hayan verificado el cumplimiento de fiabilidad de las *firmas electrónicas avanzadas* y emitir el *certificado*.

Para prestar el servicio de certificación, es necesario obtener la acreditación como tal por parte de la Secretaría de Economía. La acreditación queda sujeta a que se vean satisfechos los siguientes requerimientos:

i) Recursos humanos necesarios para la prestación del servicio: un profesional del derecho, un profesional de la informática y cinco auxiliares de apoyo informático.

ii) Recursos materiales: espacio físico y políticas de seguridad del área; económicos, que incluyan un seguro de responsabilidad civil; y tecnológicos: equipo electrónico.

iii) Procedimientos definidos y específicos para la tramitación y expedición del *certificado*.

iv) Medidas necesarias para garantizar la seriedad de los *certificados* emitidos, la conservación y consulta de los registros. Los *prestadores de servicios de certificación* deben exhibir una fianza y registrar su *certificado* ante la Secretaría de Economía.

La acreditación deberá ser publicada en el Diario Oficial de la Federación.

El Código de Comercio y el reglamento en esta materia, establecen las obligaciones de estas entidades. El cumplimiento de tales deberes justifica su existencia y su trascendencia en el proceso de comunicación electrónica y contribuye a fortalecer el principio de la *comunicación segura*, que se logra a través de la intervención de los *prestadores del servicio de certificación*. Dentro de todas ellas, podemos destacar las siguientes obligaciones que debe cumplir cada una de estas entidades para dar certeza y seguridad a la utilización de la *firma electrónica avanzada* y del *certificado digital*:

I. Debe comprobar la identidad de los solicitantes de los *certificados* y poner a disposición del firmante los dispositivos de generación de los datos de creación y de verificación de la *firma electrónica*;

II. Antes de la emisión de un *certificado*, debe hacer saber a la persona que lo solicite las condiciones precisas para la utilización del *certificado*, sus limitaciones de uso y la forma en que garantiza su posible responsabilidad;

III. Debe mantener un registro de los *certificados* expedidos, incluyendo las circunstancias que afecten la suspensión, pérdida o terminación de su vigencia.

A este registro podemos acceder por *medios electrónicos*, su contenido es público y está a disposición de las personas que lo soliciten, en tanto que el contenido privado estará a disposición del *destinatario* y de las personas que lo soliciten, cuando así lo autorice el firmante, debiendo guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación.

IV. Debe asegurar las medidas para evitar la alteración de los *certificados* y mantener la confidencialidad de los datos en el proceso de generación de los datos de creación de la *firma electrónica*;

V. Debe proporcionar medios de acceso que permitan a la *parte que confía* en el *certificado* determinar:

- a) La identidad del *prestador de servicios de certificación*;
- b) Que el firmante nombrado en el *certificado* tenía bajo su control el dispositivo y los datos de creación de la *firma* en el momento en que se expidió el *certificado*;
- c) Que los datos de creación de la *firma* eran válidos en la fecha en que se expidió el *certificado*;
- d) El método utilizado para identificar al firmante;
- e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la *firma* o el *certificado*;
- f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el *prestador de servicios de certificación*;
- g) Si existe un medio para que el firmante dé aviso al *prestador de servicios de certificación* de que los datos de creación de la *firma* han sido de alguna manera controvertidos, y
- h) Si se ofrece un servicio de terminación de vigencia del *certificado*.

La Secretaría de Economía actúa -a su vez- como autoridad certificadora respecto de los *prestadores de servicios de certificación*.

El *prestador de servicios de certificación* que incumpla con las obligaciones apuntadas podrá ser sancionado por la Secretaría de Economía con suspensión temporal o definitiva de sus funciones, sin perjuicio de la responsabilidad civil o penal y de las

penas que correspondan a los delitos en que, dado el caso, incurran los infractores. Si así ocurre, el registro y los *certificados* que haya expedido pasarán, para su administración, a otro *prestador de servicios de certificación* que para tal efecto señale la Secretaría de Economía.

Con fecha diez de agosto del dos mil cuatro, la Secretaría de Economía publicó en el Diario Oficial de la Federación las reglas generales a las que deberán sujetarse los *prestadores de servicios de certificación*, las cuales fueron modificadas mediante el acuerdo publicado en el Diario Oficial de la Federación el cinco de marzo del dos mil siete.

Las citadas reglas tienen por objeto establecer a cargo de los *prestadores de los servicios de certificación* la obligación de contar con personal confiable y procedimientos rigurosamente observados con el propósito de garantizar la confiabilidad y la seguridad de la información con que cuentan estas entidades para la prestación de sus servicios, entre los que se encuentran los servicios de *firma electrónica*, la conservación de *mensajes de datos*, el sellado digital de tiempo y la validación de *certificados*, conforme lo prevé el artículo 89 del Código de Comercio.

De acuerdo a estas reglas, las áreas y los servicios en los cuales se maneja información confidencial requerirán procedimientos de controles de acceso, y deberán estar supervisados continuamente, a efecto de reducir al mínimo los riesgos. La implantación de los controles deberá evitar riesgo, daño o pérdida, de los activos, alteración o sustracción de información. Los accesos físicos a las áreas de generación de *certificados*, gestión de revocación de *certificados* y área de residencia de servidores, deberán estar protegidas con puertas y muros sólidos y firmes, chapas seguras, controles de acceso, sistemas de extinción de incendios y alarmas de seguridad, y se encontrarán limitados sólo al personal autorizado mediante controles de autenticación de por lo menos dos factores para asegurar que no habrá accesos no autorizados. Los servicios compartidos por otra entidad distinta al *prestador de servicios de certificación* o por personal de éste no dedicado al servicio de certificación, deberán estar fuera del perímetro de seguridad.

Fin de texto.