



LA FIRMA DIGITAL EN LOS PROCESOS DE LOS TRÁMITES DE COMERCIO EXTERIOR

I. ANTECEDENTES

El hombre ha buscado la manera de poder comprobar la autenticidad de un documento y de obligar a cumplir lo que en él se establece. Este mecanismo ha variado históricamente, desde el Imperio Romano, cuando simplemente pasaban la mano sobre el documento frente a unos testigos, pasando por el sello de la edad media; y en el siglo XVIII, en Francia, se impone lo que hoy se conoce como firma autógrafa o manuscrita, hasta llegar a la actual firma electrónica o digital.

En los últimos años, la progresiva evolución en la tecnología informática ha transformado el comercio, los servicios financieros y la industria, entre otros; pero uno de los fenómenos mundiales de mayor evolución ha sido el comercio electrónico; cada vez es mayor la demanda de transacciones por medio de redes electrónicas debido a la necesidad de interactuar y hacer negocios de manera simplificada, eficiente, transparente y segura; por lo que cada día se hace necesario el uso de la firma digital.

Algunos antecedentes de la Firma Digital

1976

El concepto de firma digital fue introducido por Diffie y Hellman, establecieron que básicamente una firma digital es un conjunto de datos asociados a un mensaje que permite la identidad del firmante y la integridad del mensaje.

1978

R. Rivest, A. Shamir y L. Adleman proponen el método de firma digital, denominado RSA (sistema criptográfico de clave pública). Hasta hoy, este método es el más usado para cifrar y firmar digitalmente y obedece a los mismo principio de la firma autógrafa.

1985

Se publica la tesis (A public key cryptosystem and a signature scheme based on discrete logarithms) con la que posteriormente se construyó la base del algoritmo de la firma autógrafa.

1991

El Instituto Nacional de Normas y Tecnología de Estados Unidos propone el algoritmo para su uso en su Estandar de Firma Digital. Este Algoritmo sirve para firmar y cifrar información.

1995

En mayo, en el estado de UTAH, Estados Unidos, se publica la primera ley en Materia de Firma Digital denominada: "Utah Digital Signature Act"; cuyo objetivo facilitar mediante mensajes electrónicos y firma digital las transacciones.

Fuente: Tomado del sitio web: http://www.firma-digital.cr/que_es/antecedentes.aspx

El Salvador no cuenta con una legislación aplicable a la firma digital o electrónica, sin embargo, en uso de sus facultades constitucionales y a iniciativa del Presidente de la República, el 18 de octubre de 2012 el Ministerio de Economía presentó a la Asamblea Legislativa de El Salvador, el Proyecto de Decreto de Legislativo que contiene la Ley de Firma Electrónica, para su análisis y posterior aprobación.

El proyecto de ley tiene como objetivos principales equiparar la firma electrónica simple (datos en forma electrónica con los que se puede identificar al signatario) y la firma electrónica certificada con la firma autógrafa, es decir, aquellos datos almacenados digitalmente que al igual que en la firma simple, sirven para identificar al firmante; asimismo, la ley permitirá que los datos almacenados de forma digital que contengan firmas electrónicas certificadas, tengan el mismo equivalente a documentos físicos que posean una firma autógrafa original. Los documentos públicos, por otro lado, también podrán almacenarse de forma electrónica sin perder su validez.

II. CONCEPTO Y FUNCIONAMIENTO DE LA FIRMA DIGITAL

Antes de ahondar en la conceptualización y funcionamiento de la firma digital, se debe distinguir dos términos que a menudo suelen utilizarse indistintamente: firma digital y firma electrónica, cuyo uso depende de la legislación de cada país.

- **Firma digital:** es un conjunto de métodos criptográficos y técnicos; es un concepto fundamentalmente técnico.
- **Firma electrónica:** es un término mucho más amplio y hace referencia a cuestiones legales, organizativas, técnicas, entre otros.

En términos generales la firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma hológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Teniendo en cuenta lo anterior, una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar

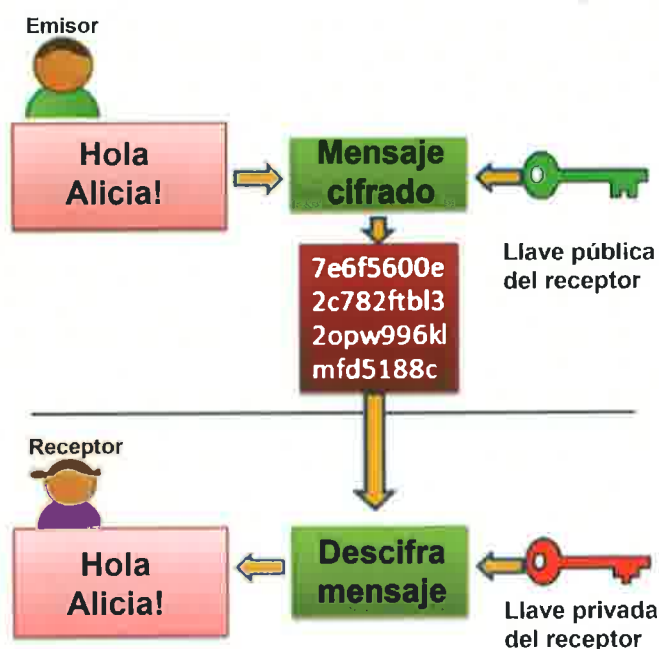


que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).. Dicha firma puede aplicarse en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos, por ejemplo documentos electrónicos o software, ya que proporciona una herramienta para detectar y evitar la suplantación, falsificación y manipulación del contenido.

Criptografía

Vocablo que proviene de la palabra griega kriptos, secreto. El diccionario de la Real Academia Española lo define como: "El arte de escribir en clave secreta o de un modo enigmático". La criptografía aplicada a los documentos digitales consiste en la disciplina de las matemáticas, que basada en modelos de difícil solución ofrece explicaciones de rigor matemático a los problemas de seguridad y confidencialidad en este tipo de documentos.

El siguiente esquema ilustra el funcionamiento del cifrado y descifrado en la criptografía.



El emisor envía al receptor el mensaje cifrado con la llave pública del receptor. El receptor descifra el mensaje con su llave privada para poder ver el mensaje en claro (textopano)

Principios Generales

El uso de la firma digital debe satisfacer los siguientes principios o aspectos de seguridad:

- *Autenticidad del origen del mensaje, con lo cual se garantiza que el mensaje es confiable.*
- *Integridad de la información, otorga certeza de que los datos recibidos por medios electrónicos no han sido modificados en su tránsito desde el iniciador hasta el destinatario.*
- *Confidencialidad, garantiza al iniciador y destinatario que los mensajes electrónicos no serán conocidos por terceras personas, sin su expresa autorización.*
- *Equivalencia Funcional, consiste en observar en los documentos archivados y comunicados de manera electrónica, aquellos requisitos que son exigidos en los documentos presentados por escrito y consignados en papel.*
- *No Repudiación del origen, garantiza que cuando un mensaje ha sido suscrito con firma electrónica certificada, no puede ser repudiada su autoría por la persona del iniciador.*

Certificados Digitales

Es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.

El certificado digital es válido principalmente para autenticar a un usuario o sitio web en internet, por lo que es necesaria la colaboración de un tercero confiable (Autoridad Certificadora) para cualquiera de los participantes en la comunicación.

Autoridad Certificadora (CA, por sus siglas en inglés) Entidad de confianza que crea, emite y revoca los certificados digitales, junto con las llaves privadas y públicas; básicamente, dicha Autoridad se encarga del manejo del ciclo de vida de los certificados digitales; asimismo, mantiene una lista digital de los certificados que han sido revocados.

Autoridad Registradora (RA, por sus siglas en inglés) Entidad de confianza de la Autoridad Certificadora que realiza el proceso de validación de quién aplica al certificado, concretamente, realiza el esfuerzo de asegurar la identidad de los titulares que recibirán un certificado digital. Cabe mencionar que una CA puede realizar la función de RA, pero por lo general se apoya en una tercera autoridad de confianza.

Funcionamiento Firma Digital¹

El procedimiento utilizado para firmar digitalmente un mensaje es el siguiente: el emisor crea un mensaje determinado y le aplica una función hash² y así obtiene un resumen del mensaje; el emisor cifra dicho mensaje utilizando su clave privada, el emisor le envía al receptor un correo electrónico con los siguientes elementos:

- El cuerpo del mensaje (sin cifrar o cifrado, por medio de la clave pública del receptor)
- La firma del mensaje, que se compone de:
 - El hash o mensaje cifrado con la clave privada del emisor.
 - El certificado digital del emisor con todos sus datos y que está cifrado con la clave privada del Prestador de Servicios de Certificación.

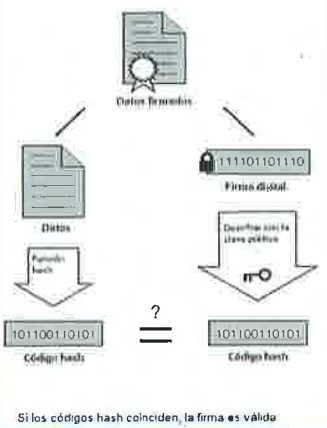
- El hash o mensaje cifrado con la clave privada del emisor.
- El certificado digital del emisor con todos sus datos y que está cifrado con la clave privada del Prestador de Servicios de Certificación.

Para realizar la verificación del mensaje, el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que no hubo alteración y que el firmante es quien dice ser.

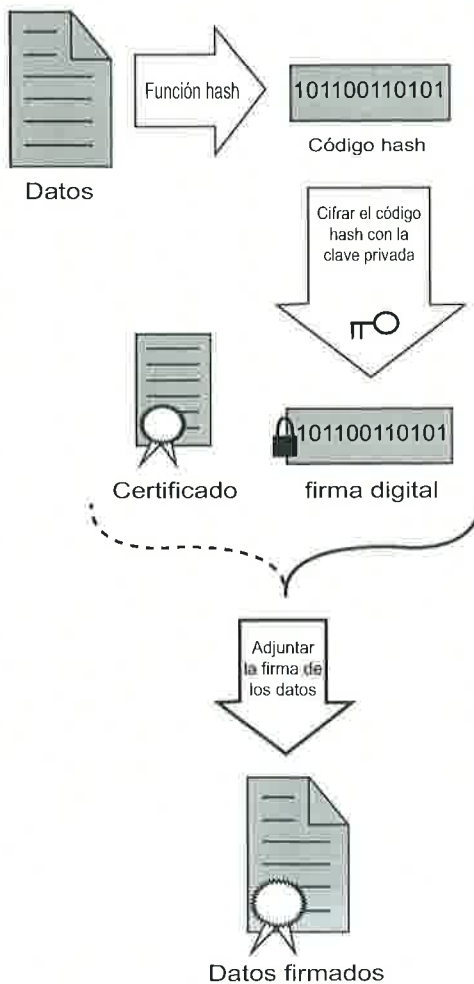
Algunos de los atributos más representativos de la firma digital son:

- Es única
- Es verificable
- Está bajo control exclusivo del iniciador
- Está ligada a la información del mensaje.

Comprobación de una Firma³



Firma Digital³



III. IMPLEMENTACIÓN DE LA FIRMA DIGITAL PARA OPERACIONES DE COMERCIO EXTERIOR

El Sistema Económico Latinoamericano y del Caribe (SELA), en su documento de investigación denominado: "Panorama Digital de los Trámites de Comercio Exterior en América Latina y el Caribe. Propuesta de acciones a nivel regional", con la finalidad de realizar un análisis detallado del tema en cada uno de sus Estados Miembros, así como de los Estados no Miembros del SELA que son parte de la región en el cual se incluye a El Salvador, establece entre los aspectos legales y tecnológicos previos a la digitalización de los trámites de Comercio Exterior, la necesidad de que los países cuenten con instrumentos legales y tecnológicos compatibles con la firma digital entre los que se incluyeron los siguientes aspectos:

- Existencia de ley de comercio electrónico o similar.
- Existencia y funcionamiento de la firma digital
- Existencia y funcionamiento de la factura Electrónica.
- Emisión de certificados de origen por medios electrónicos.

Asimismo, la Secretaria Permanente del SELA, en el documento de consulta denominado: "Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe", diagnosticó que en El Salvador no existe una legislación especial que regule el comercio electrónico, sin embargo existen normas que habilitan su uso en diferentes disciplinas del derecho.

También, dentro la legislación aduanera, en el Código Aduanero Uniforme Centroamericano (CAUCA), en su Capítulo III, acerca del uso de los sistemas informáticos, se establecen normas relacionadas a la firma electrónica o digital certificada (Art. 32), valor probatorio (Art. 33), certificadores (Art. 34), prueba de los actos realizados en sistemas informáticos (Art. 35), entre otros.

¹ Rojas, Suarez, Meneses (2010) Firma digital: instrumento de transmisión de información a entidades financieras.

² Es una clave simétrica estándar internacional, que sirve para garantizar la integridad de los textos, se utiliza en el área de la criptografía.

³ Imágenes del sitio <http://fontana-analia.blogspot.com/2011/11/firma-electronica-y-firma-digital.html>

⁴ Enlace de consulta de documentos citados:

<http://www.sela.org/a-tach/258/EDQCS/SRed/2010/04/T023600004015-0-Panorama-Digital-Tramites-de-Comercio-Exterior.pdf>

⁵ http://www.sela.org/attach/258/default/DI-Z-12_Fundamentos_Firma-Digital_y_su_Estado_Arte_en_ALC-Final.pdf



El Sistema Integrado de Comercio Exterior (SICEX) y el Sistema de Importaciones (SIMP) ambos bajo administración del CIEX El Salvador, cuentan a la fecha con un mecanismo de autenticación electrónica a través de claves y contraseñas generadas mediante los sistemas antes citados, y enviados mediante correo electrónico a los diferentes usuarios autorizados, lo cual posibilita la autorización de las operaciones, sean estas de exportaciones o importaciones, pero carece de un mecanismo electrónico que reemplace la firma autógrafa para los documentos que se emiten o incorporen en cualquier formato digital.

Si bien es cierto que los servicios están en línea y en ambiente 7x24, siempre se exige que los clientes presenten los documentos físicos en cualquier punto fronterizo, aeropuerto internacional, puerto de embarque, zonas francas, etc., para formalizar sus trámites.

Entre las de normas alternas que facultan y regulan el uso de la firma digital o electrónica, se encuentra la Ley de Creación del CIEX El Salvador, que en el Art. 8, en el apartado relacionado con el Intercambio Electrónico de Datos, establece que las transacciones que se realicen a través del CIEX El Salvador podrán utilizar:

- a. Firma digital, entendiéndose por ésta aquella que se obtiene mediante aplicaciones tecnológicas en la que se utiliza criptografía asimétrica, también denominada sistemas de cifrado de clave pública, para asegurar la autenticidad de los mensajes electrónicos y garantizar la integridad de su contenido.
- b. Firma electrónica, que son los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

Con base en su ley de creación, el CIEX El Salvador está trabajando en el proyecto para implementar la firma digital, en la autorización de la transacción, en los documentos emitidos o digitalizados y que se transmitan electrónicamente a través del Sistema

Integrado de Comercio Exterior (SICEX) y el Sistema de Importaciones (SIMP), ambos del Banco Central de Reserva de El Salvador por la Ventanilla Única. Asimismo, es importante mencionar que la firma digital que implemente en el proceso de comercio exterior tendrá validez probatoria de los participantes. En dicho proyecto participarán todas las instituciones del Estado que autorizan y emiten los documentos vinculados al comercio internacional, de conformidad con sus competencias y que forman parte del CIEX El Salvador.

III. CONCLUSIÓN

La firma digital es un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico; asimismo, da al destinatario seguridad de que el mensaje fue creado por el remitente y que no fue alterado durante la transmisión.

Por lo tanto, la firma digWital es una herramienta que permite resguardar la confidencialidad de los documentos; permite disminuir los costos de operación, de recursos; simplifica los procesos de las empresas y además representa mejoras en el tiempo de respuesta al exportador y al importador, lo cual convierte a la firma digital en un tópico relevante y necesario de desarrollar para mejorar los trámites relacionados al comercio de mercancías.

Entre algunas ventajas que podría ofrecer la firma digital, son:

- Mayor seguridad e integridad de los documentos. El contenido del documento electrónico firmado no puede ser alterado, por lo que se garantiza la autenticidad del mismo y la identidad del firmante.
- Se garantiza la confidencialidad, el contenido del mensaje solo será conocido por quienes estén autorizados a ello.
- Eliminación del papel, lo que implica una disminución del almacenamiento en espacio físico y reducción de gastos en los procedimientos de administración de archivos.
- Se evitan desplazamientos y traslados.
- Disminución del tiempo en la ejecución de procesos (se evitan colas y se reducen los procedimientos manuales).

CONTÁCTENOS:

CENTRO DE TRÁMITES IMPORTACIONES Y EXPORTACIONES (CIEX EL SALVADOR)

Alameda Juan Pablo II, entre 15 y 17 Av. Norte, San Salvador

Teléfonos 2281-8085 y 8090, FAX 2281-8086

Sección Exportaciones

Sección importaciones

2281-8087, 8088, 8287, 8467, 8513, 8538 y 8551

2281-8539, 8089, 8131, 8507, 8514, 8532 y 8754

ciexportaciones@bcr.gob.sv y cieximportaciones@bcr.gob.sv

www.centrex.gob.sv y www.centrexonline.com

