La firma digital

Por Lic. Miguel Pérez[1]

Resumen:

Al mencionar la seguridad de la información en medios digitales se debe visualizar tanto su almacenamiento como su trasiego o comunicación. Este factor hoy en día ha tomado un papel preponderante. En este sentido se ha creado y desarrollado un método de seguridad al cual se le denomina “firma electrónica”, del cual un caso particular es la firma digital. Esta puede garantizar la confidencialidad, autenticidad e integridad de la información. Para esto se requiere de un ente externo a las partes, conocido como Autoridad Certificadora, que garantice la autenticidad de las firmas.

Palabras clave:

Firma electrónica / Firma digital / Seguridad informática / Criptografía asimétrica

Abstract:

When mentioning information security in a digital means, not only its storage should be visualized, but also its movement or communication. Today, this factor has played a very important role. In this sense a security method has been created and developed called "electronic signature", one particular case being the digital signature. It can guarantee confidentiality, information authenticity and integrity. For this, an external entity for the parties known as Certification Authority is required to guarantee the authenticity of the signatures.

Keywords:

electronic signature / digital signature / information security / asymmetric cryptography

Desde sus inicios, la humanidad ha confiado el registro y respaldo de la información a los medios físicos como la piedra, la madera, las pieles, el papiro, el papel y otros medios semejantes, y estos han evolucionado de acuerdo con el desarrollo de la tecnología con que se ha contado en cada una de las etapas de su existencia.

Al principio, no era necesario saber quién había realizado el grabado de la información, y por ello, no se puede determinar quién estampó los jeroglíficos de la mayoría de las estructuras egipcias, por ejemplo. Con el pasar de los años, la interrelación de los seres humanos, cada vez mayor, y el avance de la comunicación escrita trajeron consigo la necesidad de identificar al autor de los textos, más aun cuando estos implican algún tipo de obligatoriedad para alguna de las partes y mayor es la necesidad al crecer las sociedades de tener que compartir leyes, mandatos y toda clase de información. Para determinar al autor de un texto,

[1] Ingeniero en Sistemas y profesor de ULACIT.

primeramente se utilizaron sellos que identificaban a las personas que se responsabilizaban por la creación de los documentos, más adelante se empezaría a utilizar una rúbrica o firma que esencialmente solo su autor podría reproducir fidedignamente.

Dependiendo del ámbito de acción, puede que una sola firma no sea suficiente para establecer una responsabilidad, así por ejemplo, si se recibe un documento que incluye una firma que dice pertenecer a Leonardo Da Vinci (por citar cualquier nombre), a menos que se conozca plenamente esta firma o que se haya visto al autor estamparla, no habrá manera de establecer esa autoría; por esta razón es que, dependiendo de la formalidad y ámbito del documento, se requerirán algunas pautas para garantizar la autenticidad de una firma, como sellos y firmas de testigos que puedan ser identificables y quienes tengan la autoridad para realizar ese testimonio.

En la actualidad, la sociedad ha continuado evolucionando y uno de sus impulsores principales ha sido la tecnología. La humanidad busca en la tecnología formas de llevar a cabo acciones comunes de forma más eficiente, eficaz y segura, y el campo de los documentos no es la excepción.

Con el avance tecnológico nace también el registro de la información en documentos electrónicos, que no son otra cosa que la misma información, pero almacenada, ya no en papel y en medios tradicionales, sino en medios electrónicos, magnéticos, ópticos o, en definitiva, digitales.

Sería de esperar que la tecnología no solo permita almacenar mucha más información en menos espacio y con un tiempo de recuperación bastante menor al de los documentos tradicionales, abaratando significativamente el costo de producción almacenamiento, recuperación, mantenimiento, conservación y reproducción de la información, sino que también incremente sustancialmente su seguridad y preservación.

Al mencionar la seguridad de la información en medios digitales, se debe visualizar tanto en su almacenamiento como durante su trasiego o comunicación. Este factor fue dejado de lado en los albores de la computación y hoy en día ha tomado un papel preponderante.

La volatilidad y exposición tradicional de la información en medios magnéticos es alta, un ejemplo de ello es lo volátil que resulta la información almacenada en un disquete o lo insegura que puede ser en un disco duro de una computadora personal.

De esta manera, para que el documento electrónico sea funcional y práctico, se ha establecido que debe ser tanto o más confiable que un documento soportado en papel, para

lo cual se debe garantizar el fácil acceso para aquellas personas autorizadas, la permanencia o estabilidad de la información, de manera que su autor o propietario tenga plena confianza en que no perderá su información y que si eventualmente el medio físico se daña, se cuenta con procedimientos de recuperación de los documentos.

Por último, se debe garantizar que el documento no se pueda alterar sin el debido consentimiento de la persona responsable, y que aun con ese consentimiento, se pueda identificar al autor de las modificaciones y, de ser necesario, reestablecer los documentos alterados volviendo a las versiones anteriores a su modificación. La condición óptima sería que los documentos finales y oficiales no se puedan modificar del todo, lo cual garantizaría una vigencia de la información por un tiempo establecido, durante el cual ni siquiera se pueda eliminar el documento.

Todo lo anterior es posible con el uso de la tecnología; existen dispositivos y aplicaciones que garantizan que una vez almacenado un documento y establecidos los criterios de retención, nadie, incluyendo a los administradores y usuarios de mayor jerarquía tecnológica, pueda modificar o eliminar ese documento.

Una de las funciones principales de los documentos es su carácter probatorio, y esto no cambia cuando el medio en que se almacenen sea electrónico. Se debe poder establecer fehacientemente la autoría del documento, y que no ha sido alterado desde que fue estampada la firma de autor (o de quien lo respalda), de manera que el responsable no pueda repudiar su autoría.

Para cumplir con todos los requerimientos enumerados en los párrafos anteriores se ha creado y desarrollado un método de seguridad al cual se le denomina “firma electrónica” (no excluye los mecanismos de seguridad adicionales que se puedan establecer en el equipo o en sus aplicaciones, sino que se respalda y complementa con ellos). Este método consiste en agregar un conjunto de datos al documento electrónico original, de manera tal que se pueda garantizar la confidencialidad, autenticidad e integridad de la información.

Cabe destacar que una firma electrónica dista mucho, en su forma, de una rúbrica tradicional, pero en funcionalidad le suple y va mucho más allá.

Para implementar la firma electrónica de un documento, se debe recurrir a la criptografía, que consiste en tomar información en su estado natural y aplicar un procedimiento mediante el cual esa información es codificada, de manera que únicamente quien conozca ese mecanismo pueda reensamblar la información original.

De manera adicional, la firma electrónica de un documento requiere otro elemento, al que normalmente se le conoce como función “hash”, y consiste en un procedimiento matemático que obtiene, a partir del contenido de un documento electrónico, su respectivo resumen (de la misma longitud para cualquier documento).

El contenido de este resumen es diferente para cada documento en particular y a partir del resumen no se puede obtener ninguna información del documento original. Al producto de esta función se le conoce también como “digesto”.

Así las cosas, el proceso de firma de un documento electrónico podría verse, de una manera simplista, así:

- Ambas partes (emisor y receptor) se han puesto de acuerdo de antemano en el método criptográfico que utilizarán para “firmar” su información.
- El emisor aplica la función “hash” a su información y obtiene el digesto respectivo.
- Aplica el método criptográfico al digesto, con lo que obtiene un digesto codificado.
- Envía la información original y el digesto codificado al receptor.
- El receptor toma la información original y aplica el mismo método criptográfico que utilizó el emisor, con lo que obtiene un digesto de la información recibida.
- Aplica el método criptográfico para descodificar el digesto recibido.
- Compara el digesto que acompañaba la información original ya descodificado con el digesto calculado. Si son iguales, el mensaje no ha sido alterado y quien lo envía es quien conocía el procedimiento.
- De lo contrario, el documento ha sido modificado o ha sido creado por un tercero no autorizado.

El procedimiento anterior tiene varios inconvenientes: primero, funciona entre dos personas que se tuvieron que poner de acuerdo con anterioridad en la metodología, cualquiera que espiara un poco esa comunicación podría introducirse en los canales y falsear los medios y la información. Por lo anterior, se han creado métodos que solventan esas deficiencias y algunas otras aún más sofisticadas; estos métodos mucho más seguros, incluyen claves o llaves para llevar a cabo la codificación, las cuales son aplicadas en conjunto con los métodos criptográficos para crear documentos codificados virtualmente, imposibles de descifrar sin conocer las claves.

De acuerdo con la literatura, un caso particular de la firma electrónica es la firma digital, la cual se basa en el uso de dos claves: una llamada privada, que permanece confidencial en poder de quien emite o firma el documento electrónico, y la otra clave es conocida como llave pública, la cual debe ser conocida por cualquier persona que desee verificar el origen e integridad del documento electrónico. Ambas llaves constituyen un par único, con cualquiera de ellas que se codifique la información, se requiere la otra y solamente con esa se podrá aplicar el procedimiento inverso para obtener el mensaje original, esto es, que la misma llave no puede descodificar lo que ha codificado. Con base en la clave pública no se puede deducir ninguna información de la clave privada. A esto se le conoce como criptografía asimétrica.

De esta manera, ambos, emisor y receptor, utilizan el mismo procedimiento para obtener el digesto de la información original; de hecho, este procedimiento constituye un estándar de la industria que es utilizado en forma generalizada.

Luego, el emisor codifica el digesto obtenido de su información original con su clave privada, y lo envía al receptor conjuntamente con la información original (sea en su estado natural o codificada con su clave privada). El receptor descodifica el digesto con su clave pública (y el mensaje si viniese codificado también, esto se haría para obtener confidencialidad en el medio de transporte de la información). Una vez que tiene el digesto descodificado, calcula el digesto sobre la información original y realiza la comparación. Si ambos digestos son iguales, la firma es auténtica y el mensaje no ha sido alterado y se puede garantizar que quien envía la información es quien posee la clave privada.

Cuando la práctica de enviar información firmada digitalmente tiende a generalizarse y podemos recibir información de personas con quien no hemos hecho ningún arreglo previo, y además se desea tener certeza de que quien firma el documento electrónico es quien dice ser, se debe recurrir a un tercero, en el cual ambas partes (emisor y receptor) puedan confiar. Si se hace una analogía con las cédulas de identidad, se puede deducir que, de no ser por una entidad que avala la autenticidad de ese documento a nivel nacional (el Tribunal Supremo de Elecciones), ese pedazo de plástico, con nuestra foto y firma estampada en él, no tendría ninguna validez para un tercero que no nos conozca.

En el mundo virtual, la situación es igual; se requiere de ese “ente” externo a las partes que garantice la autenticidad de las firmas. Esta entidad se conoce como “Autoridad Certificadora”. Este ente emite lo que se conoce como un “certificado digital” a cada persona física que lo

requiera. Este certificado equivaldría a la cédula de identidad en el mundo virtual y debe ser entregada en forma personal y cumpliendo una serie de requerimientos de seguridad para garantizar que quien la recibe es quien dice ser, y que a partir de ese momento solo esa persona puede utilizar ese certificado ("cédula de identidad virtual") para firmar sus documentos electrónicos, y para llevar a cabo cualquier otro trámite que requiera de seguridad a través de su certificado y por ende de sus claves.

Este certificado quedará registrado en la Autoridad Certificadora y cualquiera podrá consultar ahí su autenticidad. Al usuario se le entregará algún medio con información de su certificado y sus claves privada y pública, para que sean utilizadas cada vez que así lo requiera. El usuario debe garantizar el buen uso de ese certificado, así como extremar las condiciones de seguridad para que no caiga en manos de terceros que puedan utilizarlo de forma inadecuada. Si el certificado se llegara a extraviar (al igual que cualquier otro documento de identificación en otros medios, por ejemplo la cédula de identidad), el propietario deberá reportar de inmediato a la autoridad certificadora el incidente, para que el certificado y todo lo relativo a él sean inhabilitados con la mayor brevedad posible.

La forma física del certificado que se le entrega al usuario puede ser un "token", similar a una memoria USB (también conocida como "llave maya"), una tarjeta inteligente (con un chip, similar a una tarjeta de crédito con monedero), un disco compacto o simplemente se puede instalar en su microcomputador. Adicionalmente, se puede incrementar la seguridad en el uso del certificado para firma de documentos electrónicos, mediante la incorporación de un "pin" similar al de las tarjetas utilizadas en los cajeros automáticos, el cual se deberá digitar cada vez que se utilice el certificado para firmar digitalmente un documento electrónico.

Cuando se recibe información que ha sido firmada digitalmente, el programa respectivo por medio del cual la estemos visualizando (llámese MS Outlook, MS Word, etc.) nos desplegará alguna indicación que nos advierta que viene con una firma digital, por lo general esta misma indicación nos brindará información adicional de quién firma la información y quién la autoriza.

Es conveniente que la persona que recibe información firmada digitalmente guarde copia de esta de manera original (esto es, sin alterar, para que su firma digital no pierda validez) con el propósito de que la pueda utilizar en el momento en que se requiera como prueba que incluya la autoría de su creador. Esto implica que se puedan guardar cuantos originales idénticos se quiera, siempre y cuando no sean

modificados y cada uno de ellos conserve la firma digital original de su creador.

Como se ha podido observar, el concepto de la firma digital no difiere mucho de la filosofía tradicional de firma de un documento, utilizada para garantizar su integridad, validez y autoría. También se ha podido establecer que el proceso de firma digital no es un proceso complicado y que su uso viene a reducir costos y tiempos en el trámite de documentos, además de que aumenta la seguridad y permanencia de la información.