METODOS DE AUTENTICACION Y FIRMA EN ENTORNOS ELECTRONICOS

Ivan Dario Marrugo Jimenez

En las tecnologías de la información y las comunicaciones y en la ciencia informática se han puesto a punto diversos medios para vincular la información en forma electrónica a personas o entidades concretas, con objeto de garantizar la integridad de dicha información o de permitir que las personas demuestren su derecho o autorización para obtener acceso a un determinado servicio o depósito de información. Estas funciones suelen denominarse genéricamente métodos de "autenticación" electrónica o de "firma" electrónica. Estas expresiones aunque suelen usarse como sinónimas, por sus efectos y alcances, no se tratan de lo mismo. El empleo de la terminología de manera indistinta no sólo es poco sistemático, sino en cierta medida engañoso. En un entorno basado en el papel, las palabras "autenticación" y "firma" y los actos conexos de "autenticar" y "firmar" no tienen exactamente el mismo matiz en distintos ordenamientos jurídicos y poseen funciones que no tienen por qué corresponderse con el propósito y la función de los métodos electrónicos de "autenticación" y "firma". Además, en ocasiones se utiliza la palabra "autenticación" de forma genérica en relación con el aseguramiento de la autoría y la integridad de la información, pero cabe la posibilidad de que algunos ordenamientos jurídicos establezcan distinciones entre esos elementos. No obstante lo anterior, debemos entender que para efectos del presente Articulo, tales expresiones se utilizarán para referirse en su conjunto a las técnicas o mecanismos de autenticación y firmas electrónicas.
Tradicionalmente para el derecho, se suele interpretar que los vocablos de "autenticación" y "autenticidad" se refieren a la génesis de un documento o la información plasmada en él, o sea, que el escrito es el soporte "original" de la información que contiene, en la forma en que se transcribió y sin ninguna alteración.

Por su parte, la firma cumple tres funciones básicas en el ambiente impreso: las firmas permiten identificar al signatario (función de identificación); las firmas otorga certidumbre sobre la participación personal de ese individuo en el acto de la firma (función probatoria); y las firmas relacionan al individuo con el contenido de un documento (función de atribución). Entonces podemos afirmar que las firmas pueden cumplir asimismo otras funciones, según cual sea el entorno del documento firmado. A manera de ejemplo, podemos mencionar: La intención de una persona de resguardar la autoría de un texto (declarando así su conciencia de que del acto de su firma puede suponerle consecuencias jurídicas) o la del hecho de que una persona estuviera en un lugar determinado en un momento determinado.

No obstante lo anterior y aunque a menudo se presume la autenticidad por existir una firma, la firma por sí sola no "autentica" un escrito. Puede inclusive que los dos elementos se puedan disgregar, de acuerdo a las circunstancias. Una firma puede mantener su "autenticidad" aun si el documento en el que está puesta se ha alterado posteriormente. De igual forma, un documento podrá ser "auténtico" aunque la firma que contiene sea falsa.

En este escenario, independientemente de la tradición jurídica (Romana o Anglosajona) de que se trate, la firma - con limitadas excepciones - no es válida por sí sola. Su efecto

jurídico dependerá de la relación existente entre la firma y la persona a la que se atribuye la firma.

Ahora, si bien una firma manuscrita es una forma tradicional de "autenticación" (Validación o comprobación de la identidad del autor o generador del documento) y sirve para documentos de transacción, en diversas situaciones comerciales y administrativas una firma manuscrita es relativamente insegura. Para ello, la mayoría de los ordenamientos jurídicos describen procedimientos o requisitos específicos creados para refrendar la fiabilidad de las firmas autógrafas. Algunos de estos pueden ser de obligatoria observancia para que determinados documentos tengan efectos jurídicos. También pueden ser facultativos y ser utilizados por las partes que quieran tomar medidas para descartar posibles evidencias sobre la autenticidad de determinados instrumentos. Entre los más conocidos encontramos: Sellos y Atestaciones.

En algunos casos, se emplea la expresión "autenticación electrónica" para referirse a unas técnicas que, según el contexto en que se utilicen, pueden suponer varios elementos, como la identificación de personas, la confirmación de la autoridad de una persona (por lo general para actuar en nombre de otra persona o entidad) o sus prerrogativas (por ejemplo, la pertenencia a una institución o su suscripción a un servicio) o una garantía sobre la integridad de la información.

La Ley Modelo de la CNUDMI sobre Comercio Electrónico y la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, no utilizan la expresión "autenticación electrónica", habida cuenta del diferente significado de "autenticación" en diversos ordenamientos jurídicos y la posible confusión con procedimientos o requisitos de forma concretos. La Ley Modelo sobre Comercio Electrónico utiliza en cambio la noción de "forma original" para aportar los criterios de la equivalencia funcional de la información electrónica "auténtica". Según el artículo 8 de la Ley Modelo, "*cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos: a) Si existe "alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma*[1]*;" y b) De requerirse que la información sea presentada, si dicha información "puede ser mostrada a la persona a la que se deba presentar".*

En cuanto a la firma electrónica, gran parte de la bibliografía la describe como el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante[2] o autor de la información. La definición de "firma electrónica" en los textos de la CNUDMI es premeditadamente amplia, para que abarque todos los métodos de "firma electrónica" existentes o futuros. Siempre que el método utilizado "es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos," a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente, se deberá considerar que cumplen las prescripciones legales en materia de firma. Los textos de la CNUDMI relativos al comercio

[1] Art. 8 Ley Modelo CNUDMI sobre Firmas Electrónicas.
[2] ESPAÑA. MINISTERIO DE JUSTICIA. Ley 59/2003, de 19 de diciembre, de firma electrónica, Art 3.

electrónico, así como un gran número de otros textos legislativos, se basan en el principio de la neutralidad tecnológica y por lo tanto pretenden dar cabida a todas las formas de firma electrónica. Así pues, la definición de firma electrónica dada por la CNUDMI abarcaría todo el abanico de técnicas de "firma electrónica", desde los altos niveles de seguridad, como los sistemas de garantía de la firma basados en criptografía asociados a un sistema de PKI.

En el curso de los años han aparecido una serie de distintas técnicas de autenticación electrónica, teniendo por objetivo atender a distintas necesidades y proporcionar distintos niveles de seguridad. También entraña diferentes requisitos técnicos asociados a los factores de autenticación empleados en el proceso que busca asegurar que la persona que se está identificando en un sistema es realmente quien dice ser.

Los métodos de autenticación están clasificados en función de los elementos (factores) que se usan para validar la identidad de una persona y podrían agruparse en tres grandes categorías, a saber:

1. Aquellos que se apoyan en lo que el usuario o el receptor sabe. Por ejemplo: Contraseñas, números de identificación, PIN (Personal Identification Number), respuestas a preguntas, etc.
2. Los fundados en las características físicas del usuario o en actos involuntarios del mismo. Por ejemplo: Biometría (verificación de voz, de escritura, de huellas, de patrones oculares)
3. Los que se apoyan en la posesión de un objeto por el usuario. Por ejemplo: Tarjetas de coordenadas, Tokens OTP, Token criptográficos u otra información almacenados en una tarjeta magnética.
4. En una cuarta clase se podría incluir diversas tipologías o métodos de autenticación y firma que, aunque no pertenecen a ninguna de las citadas arriba. Pueden utilizarse también para indicar el creador de un mensaje electrónico (Un facsímil de una firma manuscrita o un nombre mecanografiado en la parte inferior de un mensaje electrónico).

Por lo general, el uso de un determinado método de autenticación esta ligado a la seguridad que requiera la operación o transacción asociada al mismo. Se debe tener presente que el compromiso de alguno de los factores de autenticación (Robo del token OTP, copia del password, etc) podría desencadenar en suplantaciones de identidad y acceso no autorizado a información confidencial. En un esfuerzo por hacer más seguro el proceso de autenticación, se han ideado mecanismos que requieren dos o más de estos factores para validar la identidad del usuario. Un caso puntual es la autenticación que realizan los cajeros automáticos del sector financiero, en donde se valida la identidad del usuario a través de una tarjeta magnética (Algo que se tiene) y el PIN (Algo que se sabe).

Ahora bien, entre las tecnologías que mas se utilizan en la actualidad para la aplicación de los Métodos de Autenticación, podemos encontrar las siguientes:

1. *Certificados Digitales:* Esta tecnología usa certificados digitales X.509 existentes emitidos por una entidad de certificación dentro de un ambiente PKI. Los certificados se pueden almacenar de forma local o en dispositivos seguros como tarjetas inteligentes o tokens de USB. Durante el proceso de autenticación se selecciona el certificado asociado al usuario y se le solicita el PIN o password que protege las llaves criptográficas asociadas a este.
2. *Dispositivos biométricos.* Estos dispositivos permiten identificar a una persona por sus rasgos físicos o de comportamiento intrínsecos. Los rasgos que pueden utilizarse para el reconocimiento biométrico son el ADN, las huellas dactilares, el iris, la retina, la geometría de las manos o el rostro, el termograma facial, la forma de la oreja, la voz, el olor corporal, la configuración de los vasos sanguíneos, la letra, el modo de andar y la forma de mecanografiar.
3. *ID y Contraseñas.* Para controlar el acceso a cierta información o servicios y para "firmar" mensajes electrónicos pueden usarse nombres de usuario (ID) y contraseñas. Aunque este método supone el riesgo de poner en entredicho el código o contraseña si se transmite en mensajes no cifrados, el conjunto de ID y contraseña corresponden al método de "autenticación" más utilizado con el fin de controlar el acceso y la verificación de la identidad en muchas operaciones, incluidas casi todas las financieras online, el retiro de dinero en cajeros automáticos y las compras con tarjeta de crédito.
4. *Token OTP (One Time Password).* Estos dispositivos ofrecen un password dinámico diferente cada vez que un usuario se autentica ante un sistema. Esta tecnología funciona con base a un algoritmo semilla (Confidencial del fabricante) que se asocia a las cuentas de usuario y permiten posteriormente validar su identidad.
5. *Grilla o Tarjeta de coordenadas.* Es un elemento de autenticación que contiene números o caracteres en un formato de filas y columnas o posiciones, que se usan para validar la identidad del usuario (Asociada al poseedor de la tarjeta). En el inicio de sesión, se les presenta a los usuarios una pregunta acerca de coordenadas o posición, la que se debe responder usando la información correspondiente en las celdas de la tarjeta de cuadrícula única que poseen.
6. *Preguntas y Respuestas:* Como su nombre lo indica, este método de autenticación valida la identidad del usuario basándose en preguntas de carácter confidencial.
7. *Soluciones Híbridas.* Estas están basadas en la combinación de distintas tecnologías, como por ejemplo en el caso del uso combinado de contraseñas y sistemas TLS/SSL (Secure Socket Layer), que es una tecnología en la que se utiliza una combinación de cifrados de clave pública y encripcion simétrica. Un claro ejemplo de este caso es la autenticación de los usuarios de sistemas operativos Unix a través de SSH, utilizando un ID-Password y una llave asimétrica que asegura el contenido de la transmisión.

En cuanto a la firma, también se pueden identificar algunas tecnologías o mecanismos que permiten su implementación:

1. *Firmas digitales.* Se conoce por "firma digital" a la que se obtiene mediante aplicaciones tecnológicas en que se utiliza el tipo de criptografía asimétrica, también denominada sistemas de clave pública, para asegurar la autenticidad de los mensajes electrónicos, la integridad de su contenido y el no repudio.

2. *Firmas manuscritas escaneadas o Firma facsímil*. Este método de firma le incorpora al documento una imagen electrónica de la firma manuscrita (Imagen escaneada) o un sello que hace referencia a la misma para relacionarlo con el firmante o autor. Este tipo de firma es usada principalmente en comunicados que no requieren un alto nivel de seguridad, ya que las imágenes utilizadas pueden ser duplicadas (copiadas) fácilmente.
3. *Firmas realizadas por medio de un lápiz digital*. Este tipo de firma asocia la imagen producto de firmar con un lápiz digital a un documento en particular.
4. *CheckBox*. Este termino hace referencia a los botones o casillas de selección del tipo de "sí" o "aceptar" o "acepto". Normalmente se usan cuando se necesita dar constancia de la aprobación o conciencia del usuario ante algún compromiso o responsabilidad expresado en un ambiente electrónico. Al reunir los datos generados por la aplicación donde se da constancia del acto a través de este mecanismo, se constituye un a firma electrónica.

Ahora bien, debemos reconocer que se puede utilizar varias tecnologías para "autenticar" una operación electrónica. En una operación específica se pueden usar varias de ellas o diversas versiones de la misma. Por ejemplo, la dinámica de la firma a efectos de autenticación puede conjugarse con criptografía para ratificar la integridad del mensaje.

Los modelos de autenticación arriba citados reportan un elemento de confusión frente al uso técnico de las expresiones tradicionales para documentos en papel ya que su equivalente en medios electrónicos con ofrecen afinidad con el entorno jurídico. Cada uno de los métodos de Autenticación y firma tienen distintos usos y finalidades, así por ejemplo para proceder con la firma de un documento electrónico puedo utilizar un procedimiento en el que accedo a un sistema informático por medio de un usuario y contraseña (Correos electrónicos por ejemplo) así mismo ese uso inicial que hice de ese usuario y contraseña también fue un mecanismo de autenticación frente a ese sistema (p ej. Hotmail o gmail). En el ejemplo expuesto la contraseña o password se utiliza como mecanismo de comprobación de identidad mientras que en el segundo caso (Autenticación ante un sistema) se usó como una credencial.

Ahora bien, para ilustrar un poco mas el desfase de la terminología en el ámbito electrónico tenemos el caso de las firmas digitales: "*La firma digital se considera una tecnología concreta para "firmar" documentos electrónicos. No obstante, como mínimo puede ponerse en duda que, desde un punto de vista jurídico, la aplicación de la criptografía asimétrica con fines de autenticación se califique como "firma" digital, ya que sus funciones trascienden de las funciones típicas de una firma manuscrita. La firma digital ofrece medios para "verificar la autenticidad de mensajes electrónicos" así como de "garantizar la integridad de su contenido". Además, la tecnología de la firma digital "no determina simplemente el origen o la integridad respecto de personas como es necesario a efectos de firma, sino que también puede autenticar, por ejemplo, servidores, sitios de Internet, programas informáticos, o cualesquiera otros datos que se distribuyan o*

almacenen de forma digital", lo que confiere a las firmas digitales "una utilización mucho más amplia que la de alternativa electrónica de las firmas manuscritas"[3]

[3] Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónicas. CNUDMI, Viena 2009.