Firma digital

Luego de una larga espera, nuestro país tiene su propio proyecto de firma digital, proceso capaz de ahorrar tiempo y costos tanto a la industria privada como al ámbito público. ¿Qué es una firma digital y cómo se genera? ¿Tiene validez legal? Fundamentos de esta tecnología, sus posibles aplicaciones y el marco normativo en el que debe utilizarse.

Hace ya varios años que se vienen implementando en el Sector Público Argentino iniciativas relativas a la digitalización de sus circuitos administrativos y a la utilización de la firma digital para dotar de seguridad a las comunicaciones internas.

A partir de la promulgación, en diciembre de 2001, de la *Ley N° 25.506* de Firma Digital, este proceso se ha consolidado.

¿Qué es una firma digital y cómo se genera? ¿Tiene validez legal? ¿Qué segmento del mercado podría beneficiarse con su utilización? Algunos de los muchos interrogantes que plantea esta tecnología que, por el momento, suena a desconocida por la mayoría

Firma digital

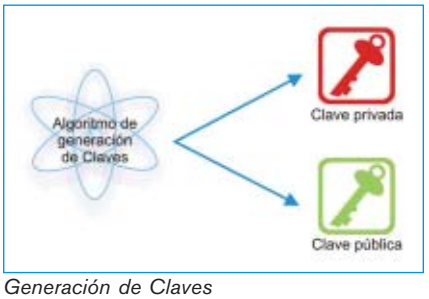
Uno de los principales desafíos que se plantea en la utilización de documentos electrónicos es determinar su autenticidad, es decir la capacidad de asegurar si una determinada persona ha manifestado su conformidad sobre el contenido del documento electrónico.

Este desafío es resuelto por lo que comúnmente se denomina como *"firma digital"*, que se basa en procedimientos criptográficos. Su función respecto de los documentos digitales es similar a la de la firma de puño y letra en los documentos impresos: ser el sello irrefutable que permite atribuir a una persona algo escrito o su conformidad en un documento. El receptor, o un tercero, podrán verificar que el documento esté firmado, sin lugar a dudas, por la persona cuya firma aparece en el documento y que éste no haya sufrido alteración alguna. El sistema de firma digital consta de dos partes: un método que haga imposible la alteración de la firma y otro que permita verificar que la firma pertenece efectivamente al firmante.

En resumen, la *firma digital* es la transmisión de mensajes telemáticos, un método criptográfico que asegura su integridad así como la autenticidad del remitente.

Obtención de claves

Mediante un algoritmo cualquier persona puede obtener un par de números matemáticamente relacionados, denominados claves. Una clave es un número de gran tamaño, que se puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes.



Generación de Claves

Cada persona genera un par de claves, una *pública* y una *privada*. La primera de ellas debe ser conocida por todos mientras que la segunda es mantenida en secreto por el usuario. Existen diversas formas de almacenar una *clave privada*: en un archivo en el disco rígido de una PC o en una tarjeta inteligente *(smartcard)*, por ejemplo.

Tanto la clave pública como la privada tienen características únicas, su generación es siempre en pareja y están relacionadas de tal forma que todo lo que sea encriptado por una de ellas sólo podrá ser desencriptado por la otra.

Para firmar un documento se aplica sobre el mismo una función unidireccional de resumen denominada función hash a través de la cual se obtiene un valor *hash*, que no es más que un resumen del documento.

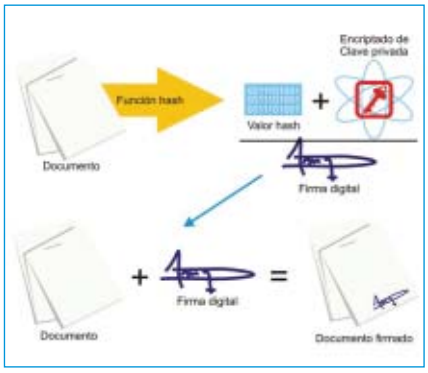
Para obtener la firma digital, se encripta el valor *hash* con la clave privada del firmante. La creación de la firma digital se lleva acabo a través de un algoritmo que combina los caracteres que conforman la clave privada con los caracteres del documento. De este modo se obtiene la *"firma digital"*. Juntos, el documento y la firma digital constituyen el documento firmado.

Es importante señalar que, a diferencia de la firma autógrafa, todas las firmas digitales generadas por una persona son diferentes entre sí. En otras

Continúa en página 148

Viene de página 144

palabras la firma digital cambia con cada documento firmado. Por otra parte, si dos personas firman un mismo documento, también se producen dos diferentes documentos firmados, ya que la clave privada utilizada por cada uno de los firmantes es diferente.

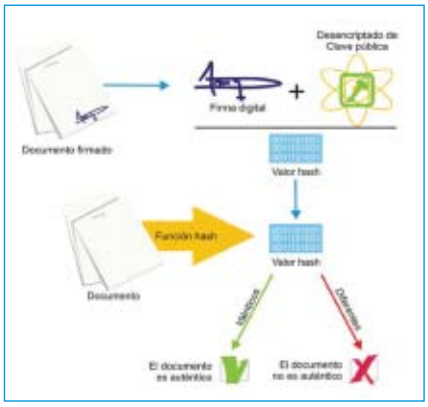


Firmado de documentos digitales

Validación

Para validar la autenticidad de un documento firmado, el receptor del documento debe crear un valor *hash* del documento transmitido y también debe desencriptar la firma digital con la clave pública del firmante. Una vez que obtiene los dos valores *hash*, los compara para determinar la autenticidad del documento firmado.

Si el documento o la firma es modificada, aunque sea ligeramente, el procedimiento de autenticación indicará que el documento firmado no es auténtico.



Autenticidad de documentos firmados

Si dos personas deciden reconocer legalmente la validez de la firma digital en los documentos electrónicos emanados de su intercambio electrónico de información, deben intercambiar sus claves públicas para que ambos puedan autenticar documentos firmados por ellos. Si estos individuos quisieran reconocer formalmente la validez de la firma digital, en caso de que no exista un marco legislativo que regule su aplicación, tendrían que suscribir un acuerdo formal, con firma autógrafa, donde se acepten las técnicas a utilizar y sobre todo donde conste el reconocimiento y aceptación de sus respectivas claves pública.

Certificado digital

Es claro que una persona, en el proceso de autenticar un documento firmado digitalmente debe contar con un archivo que contenga la clave pública del supuesto firmante. Es decir que para autenticar un documento firmado por 10 personas se deberá contar con 10 archivos o con una base de datos conteniendo las 10 claves públicas de los posibles firmantes. Si este número aumenta a 100, 1000 o a un 1.000.000 el problema crece en forma considerable. Por otra parte, es sumamente importante determinar con seguridad la identidad del titular de cada clave pública. Una solución a este problema de manejo de claves se basa en el concepto conocido como *Certificado Digital.*

El *Certificado Digital* es en sí un documento firmado digitalmente por una persona o entidad denominada *Autoridad Certificante (AC)*, mediante el cual se atestigua que una clave pública pertenece a un determinado individuo o entidad. En general, contiene la identidad de la persona (nombre), su clave pública y el nombre de la AC. Todos estos datos son previamente validados por la AC, asegurando de esta forma la veracidad de la información.

La idea es que cualquiera que conozca la clave pública de la AC puede autenticar un *Certificado Digital* de la misma manera que se auténtica cualquier otro documento firmado.

Si el Certificado es auténtico y confiamos en la *AC*, entonces, podemos confiar en que el sujeto identificado en el Certificado Digital posee la clave pública que se señala en dicho certificado. Los certificados ayudan a evitar que alguien utilice una clave falsa haciéndose pasar por otro.

Así, si una persona firma un documento y anexa su certificado digital, cualquiera que conozca la clave pública de la AC podrá autenticar el documento.

Aplicaciones

- Invitación electrónica
- Dinero electrónico
- Notificaciones judiciales electrónicas
- Voto electrónico
- Decretos ejecutivos (gobierno)
- Créditos de seguridad social
- Contratación pública
- Sellado de tiempo

Proyección

Si bien el uso de la firma digital es casi ilimitado, en el mercado no se espera una gran demanda de autorizaciones por parte del mercado minorista o la pequeña y mediana industria ya que un certificado *-según quien lo emita y el grado de complejidad de la operación-* cuesta actualmente entre $25 anuales sin límite de uso hasta US$ 250 por firma, si bien existen algunos gratuitos. Por este motivo los entendidos coinciden en que el sistema no será masivo.

Según señalara *Jorge Linskens*, subdirector de Sistemas de la AFIP, por sus costos, "*esta tecnología se aplicará sólo en trámites o procedimientos aduaneros o impositivos donde la ley exige una firma manual*". Es decir, donde exista un beneficio concreto. Porque la AFIP, el año pasado, recibió 30 millones de declaraciones juradas, el 90% de ellas por Internet, sin firma digital y sin controversias.

¿Cuáles son los mercados potencialmente consumidores de este servicio?

El sector financiero, por el manejo de grandes volúmenes de dinero. Por su parte, distintos especialistas aseguraran que el sistema de firma digital impactará fuerte en el Estado, en especial la Justicia: sólo con notificaciones electrónicas el tiempo de los procesos judiciales podrían reducirse a la mitad.

PKI

En nuestro país se denomina "*Infraestructura de Firma Digital*" al conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes como Internet.

Realmente, esta definición es conocida mundialmente con las siglas **PKI,** que significan *Public Key Infraestructure* o Infraestructura de Clave Pública.

¿Qué valor legal tiene la firma digital?

Para la legislación argentina los términos "*Firma Digital*" y "*Firma Electrónica*" no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada uno de ellos, dado que en el caso de la "*Firma Digital*" existe una presunción "*iuris tantum*" en su favor. Esto significa que si un documen-

Continúa en página 152

Viene de página 148

to firmado digitalmente es verificado correctamente, se presume, salvo prueba en contrario, que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la *firma electrónica*, de ser desconocida por su titular, corresponde a quien la invoca acreditar su validez.

Por otra parte, para reconocer que un documento ha sido firmado digitalmente se requiere que el certificado digital del firmante haya sido emitido por un certificador licenciado (o sea que cuente con la aprobación del Ente Licenciante).

Actualidad

La legislación actual establece como obligación del Estado Nacional la utilización de esta tecnología en su ámbito interno y en sus relaciones con los administrados, estableciendo un plazo máximo de cinco años para que la misma sea aplicada a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas del Sector Público Nacional *(Ley N° 25.506, arts. 47 y 48).*

A fin de fortalecer y apoyar a los organismos del Sector Público Nacional, la *Oficina Nacional de Tecnologías de Información (ONTI)* participa en las iniciativas de despapelización, proveyendo certificados digitales a agentes y funcionarios públicos actuando como Autoridad Certificante.

Estos certificados digitales son administrados de manera centralizada por la *ONTI*, la cual delega en las jurisdicciones respectivas las funciones de Autoridad de Registro.

De este modo se logra mayor eficiencia en el proceso de emisión y administración de los certificados ya que el procedimiento de validación de identidad de los suscriptores se realiza directamente en cada organismo, evitando desplazamientos y demoras.

Esta función ha sido asignada a la *ONTI* por el *Decreto N° 1028/03*, el cual establece como una de sus responsabilidades primarias "*Asistir al Subsecretario de la Gestión Pública... actuando como Autoridad Certificante en los organismos del Sector Público Nacional*" y dentro de sus acciones "*Entender, asistir y supervisar en los aspectos relativos a la seguridad y la privacidad de la información digitalizada y electrónica del Sector Público Nacional*".

Aval oficial para el proyecto

En noviembre de 2001 el Congreso de la Nación sancionó la *ley 25.506*, referida a la implementación del proyecto de Firma digital aunque recién un año después fue reglamentada. El pasado 12 de febrero, con la publicación en el Boletín Oficial de las normas para otorgar y revocar licencias a empresas y organismos públicos y privados para operar como autoridades de certificación, se puede decir que la firma digital tiene plena vigencia. No es un hecho menor: Las certificadoras habilitadas tendrán la responsabilidad de garantizar la autoría e integridad de cada documento firmado digitalmente. De todas maneras, cada operación tendrá una réplica en el centro de cómputos de la AFIP.

En Junio de 2006, el Presidente Kirchner recorrió el Centro de Cómputos de la AFIP, junto Alberto Abad, Administrador Federal de ese organismo, comprobando el sistema en el que estarán a resguardo copias de cada operación realizada con firma digital.

Marco Normativo

El marco normativo de la República Argentina en materia de Firma Digital está constituido por la *Ley N° 25.506 (B.O. 14/12/2001), el Decreto N° 2628/02 (B.O. 20/12/2002), el Decreto N° 724/06 modificatorio del anterior (B.O. 13/06/06)* y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

Este conjunto normativo conforma una *Infraestructura de Firma Digital* de alcance federal integrada por:

• **Autoridad de Aplicación:** Según el *Decreto N° 409/2005*, la Subsecretaría de la Gestión Pública actuará como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital establecida en la *Ley N° 25.506* y en las funciones de entidad licenciante de certificadores, supervisando su accionar.

• **Comisión Asesora para la Infraestructura de Firma Digital:** Funciona en el ámbito de la Subsecretaría de la Gestión Pública, emitiendo recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la Infraestructura de Firma Digital. A través del *Decreto N° 160/2004,* el Poder Ejecutivo Nacional ha designado a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la *Ley N° 25.506.*

• **Ente Licenciante:** Es el órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad.

• **Certificadores licenciados:** Son aquellas personas de existencia ideal, registro público de contratos u organismo público que obtengan una licencia emitida por el ente licenciante para actuar como proveedores de servicios de certificación en los términos de la *Ley N° 25.506* y su normativa complementaria.

• **Autoridades de Registro:** Son entidades que tienen a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por el certificador licenciado.

• **Sistema de Auditoría:** Será establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.

Este marco normativo deroga el *Decreto N° 427/98*, cuya aplicación era específica para el Sector Público, por cuanto cubre sus objetivos y alcance.

Firma Electrónica: Conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada firma digital.

Firma digital: Resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control, susceptible de verificación identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma.

Documento Digital o Electrónico: Representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento archivo.

Certificado Digital: Documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

Certificador Licenciado: Persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

Política de Certificación: Conjunto de criterios que indican la aplicabilidad de un certificado.

Fuentes: *Subsecretaría de la Gestión Pública, Jefatura de Gabinete de Ministros www.pki.gov.ar, Diario Clarín, Revista Next IT Specialist y www.confirma.com.ar*