Curso de Introducción a la Historia Clínica Electrónica

Firma Digital

Material elaborado por equipo docente - 2017

Tabla de contenido

Conceptos generales sobre la Firma Digital

Cuando una persona firma un documento en papel, realiza trazos con características tales que sólo esa persona puede realizarlos. De esa manera se deja constancia de que sólo ese individuo es el responsable de lo que dice el documento. Además, se firma al final del contenido para dejar constancia de que lo que se refrenda no ha sido modificado, firmando posteriormente cada modificación o escritura posterior que haya sido realizada en el mismo. De esta manera, se garantiza la autoría o acuerdo con el contenido e integridad de la información. Esto es lo que denominamos **Firma Manuscrita.**

Lo que se conoce como "**Firma Digital",** "**Firma Electrónica Avanzada**" o "**Firma Electrónica Reconocida**" es una herramienta tecnológica que permite garantizar la autoría y la integridad de los documentos digitales, utilizando la tecnología de claves asimétricas (Public Key Infrastructure - PKI -). Es un conjunto de datos asociados a un documento, también conocido como hash o digesto, que no implica asegurar la confidencialidad del mensaje, ya que al igual que cuando se utiliza la firma manuscrita, un documento firmado digitalmente puede ser visualizado por otras personas. La firma electrónica, electrónica avanzada, o digital (dependiendo el país puede adquirir diferentes nombres) es una de las estrategias propuestas para permitir verificar que un documento electrónico no fue alterado, y que el autor (o la última persona que lo modificó) es quien dice ser.

Criptografía

La criptografía es la ciencia de mantener en secreto los mensajes. El texto original, o texto puro es convertido en un equivalente en código, llamado criptotexto (ciphertext) vía un algoritmo de encriptación. El criptotexto es decodificado (desencriptado) al momento de su recepción y vuelve a su forma de texto original. La criptografía tiene su origen en la Grecia Antigua cuando los ejércitos utilizaban un método para "esconder un mensaje" (encriptarlo). Utilizaban un pequeño báculo de madera al cual le enredaban un listón

delgado, de tal manera que quedara forrado (Figura 2). Finalmente, sobre el báculo forrado por el listón, escribían el mensaje a ser enviado al ejército aliado. Posteriormente, el listón era desenrollado y en él quedaba escrito un mensaje indescifrable a simple vista que era enviado a otro ejército de manera "segura".

Figura 2: Criptografía de la Grecia Antigua

Para poder leer el mensaje encriptado, era necesario que el ejército aliado tenga un báculo idéntico para desencriptar el mensaje. Esto es conocido como criptografía simétrica o tradicional, dónde si el destinatario tiene la "clave" puede leer el mensaje. Podemos transpolar este ejemplo tradicional a las contraseñas actuales.

La **criptografía tradicional** evolucionó hacia la **criptografía asimétrica, o** Infraestructura de Clave Pública, también llamada de clave asimétrica (PKI) que usa un par de claves (pública y privada) para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona (o directamente estar disponible en cualquier lugar), la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Es importante no confundir el par de claves pública y privada con una contraseña, las claves están compuestas por cientos (o miles) de caracteres, dependiendo de la tecnología criptográfica utilizada, y en general se almacenan electrónicamente (pendrives, disco rígido, tarjetas chip, etc.).

Necesidad de una Firma Digital

La digitalización de los documentos y las transacciones han aportado una gran comodidad a la vida actual, mejorando los procesos y logrando que las distancias no impidan la realización de trámites y operaciones. Pero esto acarreó la pérdida de la posibilidad de firmar físicamente los documentos, como se hacía tradicionalmente. La utilización de simples firmas electrónicas, como uso de "usuario y contraseña", no cumple con todos los requisitos necesarios para reemplazar la firma manuscrita en todos los usos posibles.

La firma digital es una herramienta tecnológica, un conjunto de datos asociados a los documentos digitales que permiten garantizar la autoría e integridad de los mismos. O sea que sólo se pueden firmar digitalmente documentos digitales.

Un documento digital es la "representación digital de actos o hechos", es decir, cualquier archivo digital, de computadora, no importa si es un texto, una foto, una base de datos, un correo electrónico, entre otros.

El CDA (de la familia de estándares HL7) es un ejemplo de un documento clínico que puede ser firmado. De hecho, incluye en su código XML la posibilidad de que varios actores firmen un documento con distintos fines (1). Por ejemplo, si hablamos de un informe de una radiografía de tórax, éste puede contener la firma del residente de guardia que generó el pre-informe, del médico especialista que revisó y realizó el informe definitivo (y, una nueva versión del documento, claro), una autoridad responsable de la institución (Director Médico, Jefe de Servicio), y el responsable de mantener la base documental (Jefe de Tecnología, Administrador de Bases de Datos, etc.

En un registro electrónico se usa la firma digital para firmar, entre otros, evoluciones, indicaciones (Fármacos/Estudios), reportes de estudios complementarios o

imágenes DICOM. La aplicación de la firma digital al registro médico electrónico permite el **cumplimiento de los requisitos básicos para su legalidad:**

- Que permita verificar la autoría de su contenido
- Que permita verificar la secuencia cronológica de sus entradas
- Que permita asegurar que no se modificó el contenido con posterioridad al ingreso

El proceso de la Firma Digital

Requiere dos elementos básicos: el documento digital a firmar y la información del usuario firmante. El **documento digital** puede ser cualquier tipo de archivo de computadora. La **información del firmante** es equivalente a la firma manuscrita, ese trazo personal e irreproducible es reemplazado por un complejo sistema de claves informáticas que, al no ser compartido por el usuario, le otorgan la misma funcionalidad de la firma tradicional.

La Firma Digital otorga **presunción de autoría**, es decir, que se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma. Podemos establecer, entonces, que un documento firmado digitalmente fue firmado por quien dice la firma hasta que se demuestre lo contrario. También otorga **presunción de integridad**: si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume que este documento digital no ha sido modificado desde el momento de su firma, nuevamente, salvo que se demuestre lo contrario.

El **No Repudio** implica que la persona que firma un documento no puede decir que no lo ha hecho. Esto, que a simple vista suena poco agradable, se logra gracias a la existencia de certificados digitales que, como veremos más adelante, es otorgado por entes certificantes, logrando lo que se conoce como “cadena de confianza”. En la elaboración de una firma digital y en su correspondiente verificación se utilizan complejos procedimientos

matemáticos basados en **criptografía asimétrica**, también llamada criptografía o infraestructura de clave pública.

En un sistema criptográfico asimétrico, también llamado “de clave asimétrica”, cada usuario posee un par de claves propio. Estas dos claves, llamadas clave privada y clave pública, poseen la característica de que, si bien están fuertemente relacionadas entre sí, no es posible calcular la primera a partir de los datos de la segunda, ni tampoco calcular una a partir de los documentos cifrados con la otra. Como su nombre lo indica, la clave pública está disponible para todo el mundo, y la privada sólo la usa el usuario firmante.

La utilización de la firma digital involucra dos procesos:

- Proceso de Firma
- Proceso de Comprobación

Proceso de Firma Digital

El proceso de la firma digital comienza con una función matemática al documento digital, que permite obtener el **HASH** (a veces llamado “huella digital”). El HASH es una secuencia de caracteres de una longitud fija, que es única para cada documento y que no puede utilizarse para generar el documento original. La **utilidad** del HASH es específicamente comparar documentos: si dos documentos tienen el mismo HASH (misma huella digital), son idénticos. Para generar el HASH no se usan las claves privadas o públicas. El proceso de firma continúa con la combinación del HASH con la clave privada, para obtener la versión cifrada o encriptada del HASH (HASH cifrado). El HASH cifrado es la firma y se distribuye junto con el documento.

Proceso de Comprobación de la Firma

Para comprobar la firma se aplica nuevamente la función de HASH del documento. Luego, se descifra el HASH cifrado (firma) original utilizando la clave pública del supuesto autor. Si el HASH obtenido del documento es igual al obtenido al descifrar la firma del

documento, la comprobación es exitosa (es decir, se utilizó el par de claves, público y privado de una misma persona), por lo tanto, el documento fue firmado originalmente por el propietario de la clave pública y la firma es válida.

Hay casos en que la comprobación no es exitosa, esto puede ser debido a:

- Error de Autoría: el documento no fue firmado por el propietario de la clave pública
- Error de Integridad: el documento fue modificado luego de la firma

Aquí se ve la utilidad extra de la firma digital sobre la firma tradicional, no sólo comprueba la autoría de la firma, sino que comprueba que el contenido firmado esté igual que en el momento de la firma. El cambio de sólo un carácter en una evolución o de un solo píxel en una radiografía digital desencadenaría en un HASH (o huella digital) diferente, por lo que la firma perdería validez.

Normativas de Implementación

Queda claro, según lo que vimos hasta ahora, que si un documento está firmado con una clave privada podemos comprobar la autoría e integridad de la firma. De este concepto surgen algunas preguntas lógicas:

- ¿Cómo sé que la clave pública y, por ende, su par privado pertenecen a una persona determinada?
- ¿Cómo sé que el certificado que me muestra esa persona es válido?
- ¿Quién otorga las claves?
- ¿Quién administra las claves públicas?

Todo esto está contemplado en las normativas de implementación de estos procesos. Los **componentes de los procesos** son los siguientes:

- Certificados Digitales
- Autoridades Certificantes
- Ente Licenciante

- Cadena de Confianza

Para vincular una clave pública con un individuo (o entidad) existen pequeños documentos digitales llamados "**certificados digitales**". Estos dan fe de este vínculo y permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona. El certificado digital, en su forma más simple, contiene una clave pública y un nombre. Para garantizar que este certificado pueda ser leído o escrito por cualquier aplicación, su formato está definido por un estándar internacional.

Los certificados digitales son emitidos por una **Autoridad Certificante** y cuentan con una fecha de expiración, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del mismo. Para poder emitir certificados esta entidad tiene que ser un "certificador licenciado", esto quiere decir que tiene que contar con la aprobación del Ente Licenciante o de una Autoridad Certificante Superior. **El Ente Licenciante es una organización que se encarga de licenciar a las Autoridades Certificantes, se lo llama también "Autoridad Certificante Raíz".** Como vemos, existe una cadena de certificados, ésta comienza con el certificado de clave pública del autor del documento digital, y se denomina **Cadena de Confianza**. En la cúspide de esta jerarquía de certificados, se tiene a una Autoridad Certificante de más alto nivel, que es el Ente Licenciante, en la que se confía sin necesidad de ninguna otra certificación probatoria. La cadena sigue con las autoridades certificantes involucradas, hasta la que otorgó la clave pública del autor. La comprobación de la firma requiere la validación de toda la cadena de certificados. Este sistema permite una administración descentralizada de los certificados digitales.

Time Stamping

Un punto no cubierto hasta ahora es el **control de la cronología**, es decir, podemos verificar quién firmo algo, y si mantuvo su integridad, pero no podemos saber cuándo fue

firmado. Para esto se usa la técnica de **Time Stamping certificado**. Un servidor de Time Stamping certificado firma digitalmente un documento al que incluye la hora y fecha actual. La validez de esta hora y fecha están respaldadas por la cadena de confianza de los certificados de la entidad que provee el servicio. Disponer de la fecha y hora confiable de la utilización de la firma, y por lo tanto del documento, provee una gran ventaja, ya que la validez de una firma puede estar determinada por el momento en que fue utilizada.

Características técnicas y normativas de la Firma Digital

La firma digital cuenta con ciertas características técnicas y normativas, ya que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen. También existe lo que se denomina "cadena de confianza", cada certificado (y par de claves) es firmado digitalmente por el ente que lo otorga, y los certificados digitales de éste a su vez, también están firmados digitalmente por un ente superior, y así sucesivamente.

Utilizando la clave privada, el emisor genera un hash (un control, a modo resumido, como un dígito verificador) de un documento digital. Al recibir este documento, el receptor utiliza la clave pública del emisor y verifica que el documento no fue alterado y lo envió la persona que firma. Este mecanismo es válido tanto para la firma electrónica como la digital, de hecho, pueden no existir diferencias tecnológicas entre una y otra, y la diferencia práctica radica en que la firma digital (en argentina por lo menos) cumple con los requisitos regulatorios establecidos en la Ley Nº 25.506 (2,3).

El HIBA aplicó la tecnología PKI para realizar firma electrónica en el 2008. Contar con certificados válidos otorgados por entes certificantes oficiales (que mantengan la cadena de confianza) para todos sus profesionales significaría una inversión no justificada. Si fuera necesario, podría adquirirse una firma digital (cuando existan entes certificantes para tal fin) y se firmarían digitalmente todos los registros con una única firma hospitalaria. En cambio, con validez interna (nuestra propia cadena de confianza), pero careciendo de la

figura legal de firma digital, los profesionales utilizan un certificado y par de claves generados por los sistemas HIBA, aplicando en este caso la firma electrónica.

Desde un punto de vista legal, la diferencia entre *firma electrónica* y *firma digital* radica en el **valor probatorio** atribuido a cada uno de ellos. Concretamente, en el caso de la "Firma Digital" existe una presunción "iuris tantum" en su favor; esto significa que si un documento firmado digitalmente es automáticamente verificado como correcta se presume, salvo prueba en contrario por parte del demandante, que proviene del suscriptor del certificado asociado y que no fue modificado. Es decir, **adquiere características de documento público**, a pesar de ser privado. La "Firma Electrónica", se invierte la carga probatoria, y en caso de ser desconocida la firma, corresponde a quien invoca su autenticidad acreditar su validez.

Si bien la *firma digital* no garantiza la seguridad de la información (solo autoría e integridad), es posible valerse de esta herramienta para encriptar la información, y garantizar que sólo un determinado destinatario pueda acceder al contenido de un documento. Esto se conoce como firma invertida, en la que el remitente firma digitalmente con la clave pública del destinatario, garantizando que solo el poseedor de la clave privada que corresponda a esa clave pública acceda a dicha información.

Resumiendo: la firma electrónica-digital es un mecanismo que se vale de la tecnología de encriptación asimétrica (PKI) para crear un juego de claves digitales únicas (una pública y otra privada) y un certificado digital, que en conjunto permiten que la comunicación electrónica cuente con los siguientes elementos de seguridad: integridad, autoría y no repudio y privacidad.

Referencias

1. González Bernaldo de Quiros F. Interoperability and Security: Design and Development of a Clinical Documents Repository Digitally Signed using CDA Standard. In: Medinfo 2007. Brisbane, Australia: IOS Press; 2007. p. 2406.
2. Pública S de G. Proyecto Firma Digital de la República Argentina [Internet]. 2001. Available from: http://www.pki.gov.ar
3. Ley 25506. Firma Digital. Bolentin Oficial de la República Argentina 2001.