MÓDULO 1

Conceptos básicos de firma digital

Curso: Autoridades de Registro de Firma Digital Remota (AC MODERNIZACION PFDR)

Módulo 1: Conceptos básicos de firma digital

En este módulo estudiaremos los **problemas que se presentan al trabajar** con documentos digitales y el porqué de la necesidad de utilización de la tecnología de firma digital sobre tales documentos.

Definiremos qué es una firma digital y veremos qué propiedades debe cumplir.

Compararemos la firma digital con otras tecnologías de autenticación y analizaremos sus ventajas.

Por último, veremos **qué cosas vamos a poder firmar digitalmente** y cuáles son las **diferencias entre encriptación y firma digital** de documentos.

Problemática actual

En el escenario actual, podemos observar un notable incremento en el uso de los medios electrónicos en la vida cotidiana. Trámites para los que antes era necesario el uso del papel, como enviar una carta o llenar un formulario en papel, hoy en día pueden ser realizados a través de medios electrónicos, como por ejemplo el correo electrónico o los formularios web.

Los documentos electrónicos o digitales son una herramienta fundamental para el uso de la tecnología digital y, como resultado de este avance, están reemplazando gradualmente al papel en su uso como soporte de la información. Si bien los documentos electrónicos han cumplido esta tarea con eficacia, no permiten reemplazar totalmente al papel.

Tomemos como ejemplo un correo electrónico, dado que Internet no es un medio seguro, cada vez que enviamos un correo electrónico, el contenido de dicho correo puede ser visto y accedido por cualquier persona. Como consecuencia de esto, el destinatario no tiene forma de saber si el contenido del mensaje recibido pudo haber sido alterado, esto significa que no puede saber si el mensaje es íntegro, o sea el destinatario no puede tener certeza de que el mensaje que le llegó está intacto o íntegro tal como fue producido por el emisor.

Por otra parte el destinatario tampoco puede saber con certeza el origen de dicho correo electrónico, ya que a pesar de que en el campo "De:" (o "From:") de dicho correo figura la cuenta de correo desde la cual proviene dicho mensaje, de igual forma a lo anterior, es posible que un tercero modifique este dato, sin que sea posible detectar dicha alteración.

Como consecuencia de esto, un documento electrónico puede ser repudiable, esto quiere decir que podemos enviar un correo electrónico al destinatario y luego desconocer el contenido de ese correo, o sea repudiarlo, y aun así no tener ningún tipo de apremio legal, ya que podríamos alegar que ese mensaje no es de nuestra autoría, o que su contenido pudo haber sido alterado durante su transmisión.

Esto hace que un documento electrónico, como por ejemplo el correo electrónico, no goce del mismo valor legal y probatorio que tiene un documento firmado en papel.

En función del análisis anterior podemos concluir que un documento electrónico puede ser digno de repudio por lo que no constituye una prueba legal, esto hace que un documento electrónico no pueda reemplazar a un documento en papel en los casos que ese documento en papel está firmado hológrafamente (firma manuscrita).

Objetivo de la firma digital

Nuestro objetivo es poder resolver esta desventaja que poseen los documentos digitales respecto del papel, es decir que, así como tenemos documentos en papel y los marcamos con nuestra firma hológrafa y eso nos identifica y le da valor legal y probatorio al papel, desearíamos poder hacer lo mismo con un documento digital, hacerle una marca al documento digital de manera tal que la misma nos identifique, y le otorgue valor probatorio del mismo modo que lo hace el trazo de una firma hológrafa en papel. En resumen, buscamos que una firma digital sobre un documento electrónico o digital, permita reemplazar a una firma hológrafa en soporte papel, eliminando de esta manera los problemas que se presentan al tratar con documentos digitales.

En resumen, queremos poder lo mismo que hacemos en un papel firmando hológrafamente pero ahora sobre un documento digital firmándolo digitalmente.

Ahora bien: **¿Qué Necesitamos para hacer este reemplazo de firma hológrafa por firma digital?**

Para ello en principio necesitamos poder resolver los dos problemas antes planteados:

- Poder atribuir el documento a su autor, una persona, en forma fehaciente de manera de poder identificar a su autor.
- Verificar la no alteración del contenido del documento luego de que fue firmado (*integridad del contenido*).

- De esta manera vamos a poder garantizar el *no repudio,* o sea que ese documento tenga carácter probatorio.

Si bien aún no dimos una definición formal de qué es una firma digital, es claro que, si un documento "firmado digitalmente" me garantizará a través de la firma quién es su autor, y que su contenido es íntegro, o sea no fue modificado desde su firma, entonces ese documento podría ser utilizado como prueba legal ya que el mismo no podría ser repudiado. El análisis anterior nos permite esbozar entonces una idea de cómo definir una firma digital, no a partir de que es, sino de qué debería cumplir.

Definición y propiedades características de la firma digital

Siguiendo el razonamiento anterior, si deseamos que una firma digital pueda reemplazar a una firma hológrafa, vamos a necesitar entonces que ésta cumpla por lo menos, con las mismas características técnicas de seguridad, legales y funcionales que posee una firma hológrafa. Para ello, necesitamos entonces abstraer las propiedades que caracterizan a una firma hológrafa en esencia, y vamos a pedirle a una firma digital que también las cumpla. A continuación enumeraremos tales características, y comprobaremos que estas propiedades son equivalentes a las que cumple una firma hológrafa.

- **Autoría:** poder atribuir el documento a su autor en forma fidedigna, de manera de poder identificarlo. Al igual que en el caso de la firma hológrafa, cada individuo posee un modo de firmar que es único y puede ser identificado a través de ella.

- **Integridad:** que esté vinculada a los datos del documento digital poniendo en evidencia su alteración luego de que fue firmado. De igual forma, si un documento firmado en papel es modificado, el mismo pierde validez, por eso cuando un médico escribe una receta y, posteriormente la modifica, vuelve a firmarla aclarando que la modificación posteriormente introducida también es válida.

- **Exclusividad:** garantizar que la firma se encuentra bajo el absoluto y exclusivo control del firmante. Al pensar esto en términos de firma hológrafa, esta característica se vuelve un poco más difícil de interpretar, pero podría suceder por ejemplo, que alguien nos obligue a firmar un documento mediante el uso de la coerción, en ese caso perderíamos la capacidad de exclusivo dominio sobre nuestra propia firma hológrafa. Salvo casos específicos como el mencionado, una firma es de exclusivo dominio de su autor y éste, tiene plena capacidad de firmar lo que desee en el momento que considere oportuno. En el caso de la firma digital, su autor debe tener la misma capacidad, al igual que en el caso de la firma hológrafa, de tener acceso exclusivo a su firma a voluntad y en el momento en que lo desee.

- **No repudio:** Garantizar que el emisor no pueda negar o repudiar su autoría o existencia. Debe ser susceptible de verificación ante terceros, en resumen, poder demostrar ante terceros que una persona determinada firmó exactamente ese documento. En el caso de una firma hológrafa en papel se puede realizar una pericia caligráfica a la firma para determinar su autoría, a la vez que se puede peritar el papel a fin de verificar que el mismo no haya sido alterado. De esta manera una vez que una persona firma un documento este no podrá desconocer su autoría.

Definición: en adelante cuando hablemos de firma digital nos vamos a estar refiriendo a una tecnología que me garantice estas cuatro propiedades que, como vimos recién, son las mismas que me garantiza una firma hológrafa.

Cabe aclarar que, por lo anterior, no debería quedarnos duda de que la firma digital nos otorga las mismas garantías que nos otorga la firma hológrafa ya que ambas cumplen con las mismas cuatro propiedades.

Por último antes de seguir, una observación interesante es que el requisito de "No repudio" que le exigimos a una firma digital que cumpla en realidad siempre se va a cumplir, esto debido a que es una consecuencia de la autoría e integridad, ya que a través de ambas propiedades me permiten probar ante un tercero quién firmó (autoría) y qué firmó (integridad).

Qué no es una Firma Digital

Ahora veamos, en función de la definición anterior, qué tecnologías no constituyen una firma digital ya que no cumplen con alguno de los cuatro requisitos que recién pedimos.

Firma digitalizada: es una firma manuscrita escaneada; en ningún caso esta firma garantiza que haya sido producida por su autor, ya que, al tratarse de una imagen, esta puede replicarse con facilidad sin necesidad de contar con su consentimiento.

Contraseña (password): sirven como mecanismos de identificación o autenticación, pero en general no cumplen con la propiedad de exclusividad. Tomemos como ejemplo un sistema de redes con usuarios que acceden a la red por medio de su nombre de usuario y contraseña, en ese caso si bien el usuario es el único que conoce su contraseña, en todo sistema de redes debe haber un administrador que administre las contraseñas de los usuarios, y si bien este no conoce la contraseña del usuario, si tiene la posibilidad de blanquearla o denegar acceso al usuario al sistema. Nos encontramos entonces ante la situación de que al usuario le puede ser bloqueada su contraseña por el administrador, de esta forma el usuario no está en control exclusivo del uso de su contraseña.

Sistemas biométricos: consisten en la identificación de personas a partir de ciertos rasgos característicos como ser la voz, las huellas dactilares, el iris del ojo, entre otros. Estos sistemas comparan la información biométrica obtenida a partir de una persona contra registros almacenados en una base de datos, esto hace que esa información biométrica no sea de exclusivo control del propietario, ya que nuevamente al haber administrador, este podría ganar acceso a la información, podría replicarla sin consentimiento del autor, o simplemente bloquear el acceso al sistema. Al igual que en el caso anterior esta tecnología no garantiza la exclusividad de la información biométrica.

Autenticación: los mecanismos de autenticación sirven para permitir que una persona específica gane acceso a un determinado recurso, los dos ejemplos anteriores constituyen casos particulares de mecanismos de autenticación. Que en un documento electrónico se pueda identificar al autor no es condición suficiente para decir que está firmado digitalmente, puesto que además de esto es necesario que el documento goce de integridad. Para ello es necesario que exista una conexión lógica entre el firmante y el contenido del documento que éste firma, de manera tal que si la información firmada es posteriormente modificada entonces pueda detectarse la alteración.

Firmas electrónicas: La Ley de firma digital establece dos clases de firmas, la firma electrónica y la firma digital. Ambos son conceptos diferentes y más adelante veremos en qué consiste la firma electrónica y cuáles son sus diferencias respecto de la firma digital, por ahora sólo diremos que no son lo mismo.

Encriptación o cifrado: la encriptación de datos es un proceso que permite otorgarle características de confidencialidad a la información, de manera tal que ésta solamente pueda ser vista por el destinatario y, si durante su transmisión la información es interceptada por un tercero, éste no podrá interpretar su contenido ya que el mismo no será legible. Cabe observar que la confidencialidad no figura entre las propiedades que debe poseer una firma digital que antes enumeramos, recordemos que el objetivo de la firma digital es que permita reemplazar a la firma hológrafa, por lo tanto, dado que un documento con firma hológrafa no goza de esta propiedad, no le corresponde a la firma digital tampoco añadirle tal característica a un documento, lo que queremos decir es que un documento firmado digitalmente no me va a asegurar la confidencialidad de su contenido.

Qué se puede Firmar Digitalmente

Entre los documentos electrónicos que se pueden firmar digitalmente podemos mencionar varios ejemplos:

- Datos enviados a través de un formulario Web.
- Una imagen, fotos o música.
- Una base de datos.

- Un disco rígido, un CD o un DVD.
- Una página o un sitio de Internet.
- Una transacción electrónica o un e-mail.
- Una hoja de cálculo o un documento de texto.
- El código fuente de un programa o un software.
- Uno o varios archivos en general.

Cualquier información que esté en uno o varios archivos digitales se podrá firmar digitalmente, independientemente del medio de almacenamiento de la información en sí. Todos los ejemplos antes listados, son archivos que pueden estar almacenados en un computadora, dispositivos de almacenamiento, un correo electrónico que circula por Internet, etc.

En el caso particular de la **Plataforma de Firma Digital Remota (PFDR)** es importante observar que la misma **sólo permite firmar digitalmente documentos en formato PDF.**

Es importante mencionar que **es posible integrar la Plataforma de Firma Digital Remota con otros sistemas** propietarios**, en ese caso será posible firmar digitalmente cualquier tipo de documento electrónico** si el desarrollo del sistema propietario lo permite (para más información sobre el tema acceder a https://firmar.gob.ar/integrar.html).

Medidas de Seguridad

Dijimos antes que la confidencialidad es una característica de seguridad complementaria, la cual no es satisfecha por la firma digital, siendo la primera totalmente independiente de las características de seguridad que ésta cumple.

En virtud de esto cabe observar que un documento electrónico puede:

- **No estar ni firmado digitalmente ni encriptado:** en ese caso el documento no posee ningún tipo de protección, como sucede con un correo electrónico tal como fue planteado al inicio de este módulo.

- **Estar firmado digitalmente pero no encriptado:** en ese caso goza únicamente de las características de seguridad de la firma digital: autoría, exclusividad, integridad y no repudio; pero la información si es interceptada por un tercero podría ser visto su contenido.

- **Estar encriptado pero no firmado digitalmente:** se puede proteger un documento de la vista de terceros por medio del uso de una contraseña, así el contenido del documento es codificado de tal

manera que dicho documento sólo pueda ser visto por aquellos que, reciben el documento codificado y poseen la contraseña capaz de decodificar el mismo. La información de los documentos protegidos de esta manera gozan de confidencialidad, y si en cambio el documento es interceptado por un tercero este no podrá acceder a su contenido si no conoce la contraseña con la cual se codifico. Sin embargo este mecanismo de confidencialidad, no le otorga ninguna de las características de autoría, integridad y no repudio que garantiza un documento con firma digital. De esta forma si el documento fuera interceptado por un tercero, podría ser alterado, sin que sea posible para el destinatario, al recibirlo, detectar que el mismo pudo haber sido modificado.

- **Estar firmado digitalmente y encriptado:** en ese caso la información goza de confidencialidad junto con las propiedades otorgadas por la firma digital. En este caso la información no podrá ser revelada a terceros, además se tendrá certeza del autor y de la integridad del contenido del documento.

En función de lo expuesto, podemos observar entonces que firmar digitalmente un documento y encriptarlo, son procesos completamente distintos e independientes uno de otro. Teniendo en cuenta las características de seguridad que el documento requiera, se deberá evaluar la necesidad de firmarlo, o encriptarlo, o de efectuar ambos procedimientos conjuntamente.