MÓDULO 2

Funcionamiento

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

Módulo 2: Funcionamiento

En este módulo veremos distintos esquemas criptográficos y su aplicación al manejo de la información.

También estudiaremos cómo es el funcionamiento básico de la firma digital y el proceso de firma digital de un documento electrónico.

Además veremos la necesidad de utilizar certificados de clave pública, del rol que cumplen las Autoridades Certificantes y la necesidad de establecer jerarquías de certificación.

Definiremos qué es un certificado, una Autoridad Certificante y una Infraestructura de Firma Digital.

Por último veremos algunas consideraciones respecto del uso de los certificados.

Consideraciones preliminares

Para explicar el funcionamiento de la firma digital es necesario hablar sobre criptografía, ya que esta constituye una herramienta fundamental en el uso de sistemas de firma digital.

Antes de comenzar con el tema haremos una observación, si bien cuando vimos los conceptos básicos dijimos que firmar y encriptar son procedimientos independientes uno del otro, también dijimos que al momento de firmar digitalmente se le iba a agregar una marca al final del documento electrónico, tal como en el caso del papel, agregamos una marca al final del documento que es nuestra firma hológrafa.

Esta marca que vamos a agregarle al documento digital será generada a partir de criptografía, por tal motivo para entender el funcionamiento de la firma digital es necesario que hablemos de criptografía pero, a pesar de esto, se mantiene lo observado anteriormente, o sea que cuando firmemos digitalmente el documento electrónico, su contenido no se encriptará, sino que solo agregaremos una marca al final de este que será la firma digital del mensaje, y que será generada por medio de criptografía.

Por lo tanto en las próximas diapositivas, vamos a dejar de lado la firma digital y vamos a hablar únicamente de criptografía y confidencialidad, luego más adelante retomaremos el tema de firma digital.

Criptografía

El objetivo principal de la criptografía siempre fue el asegurar el secreto o confidencialidad de la información, o sea, proteger información sensible de la vista de terceros no deseados.

A pesar de que la criptografía se ha vuelto bastante popular en estas últimas décadas, no es una ciencia moderna, en la época del César ya se la utilizaba para proteger las comunicaciones de Estado.

El origen de la palabra ***criptografía*** proviene del griego que significa “escritura oculta”, y **se define como el arte y la ciencia que estudia la transformación (encripción) de información legible (texto plano) en otra que no se puede leer directamente por estar en un formato ilegible (texto cifrado).** En este proceso la información es codificada (cifrada) para evitar que sea leída por terceras personas. La información cifrada será ilegible para todo aquel que no tenga capacidad de descifrarla. Esta encripción protegerá la confidencialidad de la información tanto al ser transmitida como al ser archivada.

El cifrado y descifrado requieren una fórmula matemática o algoritmo y una clave, para convertir los datos "en claro" a datos cifrados y viceversa.

Dentro de la criptografía disputan permanentemente dos ramas: los criptógrafos, dedicados a inventar algoritmos, y los criptoanalistas, dedicados a romper dichos algoritmos. Esta puja permanente brinda seguridad respecto de la potencia de los algoritmos de encripción. “Durante dos mil años, los creadores de cifras han luchado por preservar secretos, mientras que los descifradores se han esforzado por revelarlos. Ha sido siempre una carrera reñida….. La invención de la criptografía de clave pública y el debate político en torno al uso de criptografía potente nos traen al momento presente, y es evidente que los criptógrafos están ganando la guerra de la información.” (SINGH; 2000: 317).

En general a lo largo de la historia, la criptografía siempre fue utilizada con fines bélicos o diplomáticos, recién en el último siglo la criptografía se empieza a aplicar tanto a las comunicaciones como al comercio electrónico.

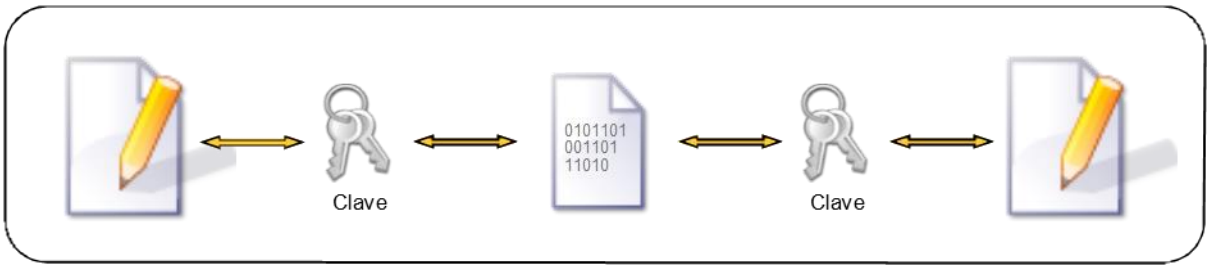
En principio para nuestro objeto de estudio podemos decir básicamente que los sistemas criptográficos pueden dividirse en dos categorías: **los sistemas simétricos, y los sistemas asimétricos o de clave pública.**

Criptografía Simétrica

Los sistemas criptográficos simétricos son los más antiguos y funcionan por medio de la utilización de una clave secreta arbitraria la cual consta letras y números, y que es elegida por el emisor para proteger la información.

En estos esquemas se utiliza la misma clave para encriptar y desencriptar la información, debido a eso es que este esquema recibe el nombre de criptografía simétrica.

Más abajo podemos observar un diagrama con este concepto, básicamente hay un programa en una computadora que recibe dos entradas: el documento y la clave. El programa ejecuta una fórmula matemática con el fin de cifrar o encriptar la información del documento y, como resultado el programa nos devuelve el documento encriptado, o sea el documento es estropeado utilizando la fórmula mencionada de manera tal que quede completamente ilegible. En la figura que está más abajo se observa, sobre la izquierda, el documento original sin encriptar (texto plano), el cual es cifrado con la clave y el algoritmo para obtener el documento encriptado el cual aparece representado con ceros y unos en el medio de la figura.



El documento encriptado se envía a través de un medio inseguro (por ejemplo internet, línea telefónica, ondas de radio, etc.) y, en caso de que un tercero no deseado intercepte el documento mientras se transfiere del emisor al receptor, el tercero no podrá ver leer su contenido ya que el mismo está encriptado, o sea completamente ilegible.

El destinatario al recibir el documento encriptado, utiliza la misma clave y el programa o algoritmo antes mencionado para desencriptar el documento, o sea lo que hace el programa es revertir el proceso de estropeado recuperando el documento tal cual se encontraba originalmente, a este proceso se lo denomina desencriptación o descifrado del mensaje. Siguiendo el ejemplo de la figura de arriba, el destinatario recibe el documento encriptado (el que tiene ceros y unos) y, utilizando el algoritmo y la contaseña el emisor puede desencriptar el mensaje obteniendo el documento original representado en la parte derecha de la figura. De esta forma, el receptor se hace el documento original pero en forma segura ya que la trasmisión del documento goza de confidencialidad debido a que el documento se envió encriptado.

Así la criptografía simétrica nos permite enviar información segura a través de canales inseguros, y de esta manera se aseguraba la confidencialidad de la información y, como ya dijimos, debido a que se utiliza la misma clave para encriptar y desencriptar el documento, este esquema recibe el nombre de criptografía simétrica.

Si bien utilizando este mecanismo se resolvían muchos problemas presentes en el traspaso de información sensible, este esquema poseía también ciertas limitaciones derivadas de la necesidad de que, para desencriptar el mensaje, el receptor necesitaba conocer la contraseña con la cual el mensaje fue encriptado, esto a su vez nos plantea un dilema:

¿Cómo hace el emisor para comunicar en forma segura la contraseña al receptor?

Esta pregunta que en principio a muchos les parecerá ingenua, en realidad no lo es, esto a su vez nos plantea los mismos problemas que teníamos para el documento, pero que ahora los tenemos que resolver para el envío de la contraseña en forma segura al destinatario. Debido a estas limitaciones es que aparece un nuevo esquema criptográfico el cual veremos a continuación.

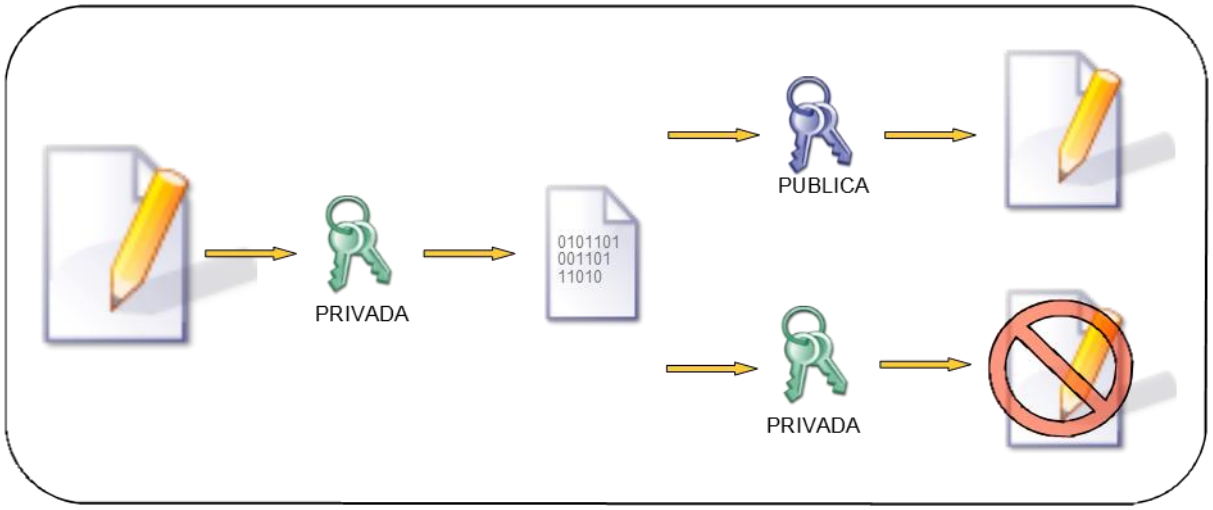
Criptografía asimétrica o de clave pública

Para resolver las limitaciones de la criptografía simétrica, un grupo de tres matemáticos (Rivest-Shamir-Adleman) implementaron en 1977 el primer esquema criptográfico asimétrico. Así la criptografía asimétrica, o también llamada criptografía de clave pública, venía a resolver varias de las limitaciones presentes en la criptografía simétrica.

En el esquema asimétrico, para encriptar y desencriptar se utilizan dos claves distintas en lugar de una, estas claves son numéricas y reciben el nombre de clave privada y clave pública. Vamos a ver que estas claves cumplen ciertas propiedades entre sí, la primera y más importante consiste en que dado un documento, podemos encriptarlo usando la clave privada, obtener así el documento encriptado, y solamente lo vamos a poder descifrar utilizando la otra clave, la pública, y si en lugar de la pública intentamos desencriptar el documento utilizando la clave privada, como en el caso simétrico, no vamos a obtener el documento original.

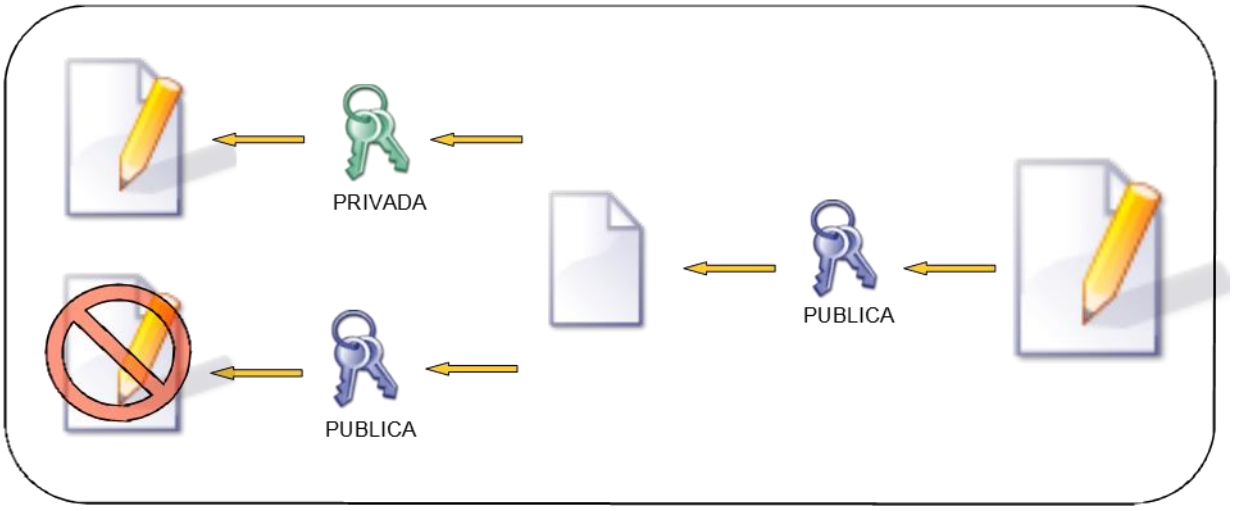
Esta situación es representada en la figura que está más abajo, nuevamente sobre la izquierda tenemos el documento original (texto plano), paso seguido el algoritmo asimétrico utilizando la clave privada encripta el documento, nuevamente en el medio de la figura aparece el documento encriptado representado con ceros y unos. En la parte superior derecha podemos observar la situación en que se desencripta el mensaje usando el algoritmo mencionado y la clave pública, así se obtiene el documento original representado sobre la parte superior derecha de la figura.

Por último, en la parte inferior derecha se observa que sucedería si se intenta desencriptar el documento utilizando la misma clave con la que se cifró, o sea la privada en este caso, así podemos ver como resultado que no se obtiene el documento original, situación que es representada en la figura sobre la parte inferior derecha.



Otra de las ventajas de esta tecnología es que el esquema es reversible, o sea que podemos encriptar el documento con la clave pública, en lugar de la privada, obtener el documento encriptado, y solamente vamos a poder desencriptar el documento con la otra clave, la privada, y si en lugar de la privada intentamos desencriptar el documento con la clave pública, como en el esquema simétrico, no vamos a obtener el documento original.

Nuevamente podemos ver esta situación representada en la figura que está más abajo, el documento original (texto plano) ahora está sobre la parte derecha de la figura (se invierte el sentido del dibujo respecto del anterior), el documento encriptado aparece en el medio representado con ceros y unos, en la parte superior izquierda tenemos el documento original que fue desencriptado con la clave privada, mientras que en la parte inferior izquierda se representa la situación en que se intenta desencriptar el documento con la misma clave que se encriptó, ahora la pública, y sin embargo esto no permite obtener el documento original.



Otra característica es que, en general, dada una clave privada existe una única clave pública capaz de desencriptar todo lo que encripta la privada y viceversa, o sea dada una pública existe una única privada que puede desencriptar todo lo que encripta la pública.

Resumiendo lo anterior tenemos que, si encriptamos el documento con una de las claves, la única posibilidad de recuperar el documento es desencriptándolo con la otra clave.

Por este motivo no es posible realizar la elección de cada clave al azar, ya que si elijo un número al azar para que funcione como clave pública, entonces la privada ya no la puedo elegir al azar, porque hay una sola clave privada que funciona para esa pública, además de que no cualquier número funciona como una clave pública o privada.

En general, un par de claves está biunívocamente asociado, o sea que a una clave privada le corresponde una única pública, y a una pública le corresponde una única privada.

No obstante hay programas que se encargan de generar este par de claves, a continuación veremos cómo es el proceso de generación de este par de claves tal como lo haría una computadora.

Esquema RSA

El esquema RSA es el primer esquema asimétrico implementado, para la generación del par de claves se utilizan dos números primos (o sea que no se pueden descomponer), en este caso **p** y **q** serían ambos números primos, la multiplicación de estos dos números dará lugar a la clave pública, en este caso **n** (observar que n no es primo porque se puede descomponer como p por q). La clave privada se

obtiene por medio de una fórmula matemática a partir de la clave pública generada y de un segundo número (**e**). La clave pública está formada por el par **(n,e)**, si bien el número **e** se puede elegir al azar dentro de un cierto rango de valores, en general este valor está prefijado, con lo cual podemos decir en cierta forma que la clave pública es un número, aunque en realidad como recién dijimos consta de dos números y no uno.

ESQUEMA RSA: p y q ambos primos

p = 13069322402100655460372905860955471125556555722027918271400496820543230709995361923026449726342667352298135532444657556071721709079499346407281185886210303

q = 11543291706304854991282053266556482345340381283249361938035635072123140767619879947055794171558788310769886218818788832735309305386367311381911622872283337

CLAVE PÚBLICA:

n = p * q

n = 15086300089119274131984091466854446446751437178443907045057674491932959261191279542290348151510881966475744276056713725950587892510033530853501868579592504144361617020329924154972675296548181769150525685509454985696883348370874436275471921524194533073145498569688334837087443627547192152419453307314
e = 5

CLAVE PRIVADA:

d = e^{-1} mod ((p-1)(q-1))
d = 60345200356477096527936365867417785787005748713775628180230697967731837044765118169161392606043527865902977104226854903802351570040134123414007474318370006732400824719115515957907050181411338717827300631125736168334776326934906699005139653199216332874216683347763269349066990051396531992163328742

Como podemos observar la generación de ambas claves se realiza en un único proceso, además existen infinitos pares de claves que se pueden generar tan grandes como uno desee, cuanto más dígitos tengan las claves más seguras estas serán.

Una consideración importante a mencionar es que, si una persona conoce el programa que generó el par de claves, y además también conoce una de las claves, la pública, entonces como la privada es única para esa

pública, en teoría sería posible para esa persona conocer también cuál sería esa clave privada, pero en la práctica esto resulta muy difícil al punto que podríamos decir que es prácticamente imposible.

O sea que si solo conozco la clave pública de alguien, deducir cual es la clave privada sólo conociendo la clave pública es prácticamente imposible.

Concluimos entonces que el conocimiento de una de las claves, la pública, no implica el conocimiento de la otra, la privada, o sea que yo puedo conocer la clave pública de un tercero y aun así nunca voy a poder saber cual es su clave privada.

En resumen la clave pública de una persona puede ser pública, o sea puede ser conocida por todos, mientras que su clave privada continuará siendo secreta, o privada como ya dijimos.

Este esquema de clave privada y pública, utilizado en un principio para encriptar mensajes, también nos va a servir para firmar digitalmente un documento, pero es importante mencionar que para firmar digitalmente el firmante va a necesitar poseer una clave privada y la pública correspondiente. Debido a esto, es fundamental que ninguna otra persona posea una copia de las claves del firmante, ya que sino podría firmar digitalmente como si fuera el firmante, es por esta razón que la ley argentina establece que cada persona deberá generar su propio par de claves.

Para que una persona pueda firmar digitalmente deberá generar un par de claves privada-pública, la generación deberá ser hecha por el titular de la firma ya que así lo establece la ley con el fin de evitar falsificaciones.

En la práctica lo que sucederá es que la persona que desea firmar digitalmente deberá conectarse a través de su celular a la Plataforma de Firma Digital Remota donde allí generará su propio par de claves. De esta manera, y de acuerdo con la ley argentina, usando la plataforma de firma digital remota cada persona podrá generar su propio par de claves privada y pública al azar, con lo cual cada par de claves será distinto de la que haya generado otra persona, y de esta forma cada persona firmará digitalmente en la plataforma usando el par de claves que allí generó, esto a su vez asegurará también que no haya un tercero que posea una copia de las claves del firmante.

A partir de ahora entonces dejamos de lado la criptografía y retomaremos nuestro tema principal que es la firma digital, así que a continuación veremos a grandes rasgos cómo es el proceso de firma y como el firmante utilizará las claves para firmar digitalmente un documento electrónico.

Uso de claves para firmar digitalmente

A continuación explicaremos el esquema general de cómo utilizará sus claves el firmante para firmar.

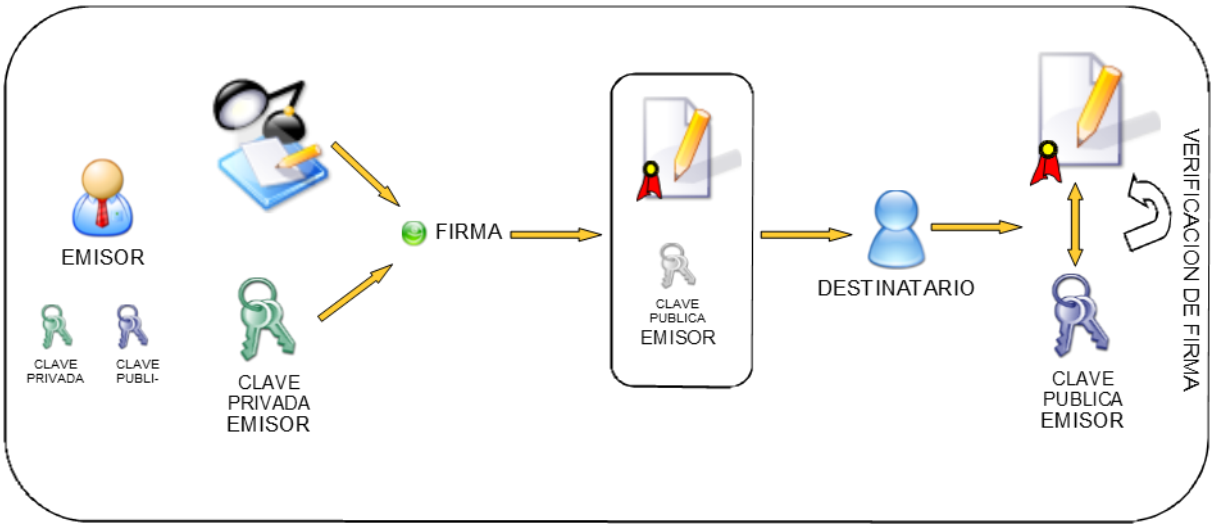
Anteriormente dijimos que cada firmante generará su propio par de claves (pública y privada) usando la Plataforma de Firma Digital Remota, esto lo hará una única vez y con estas claves podrá firmar digitalmente todos los documentos que desee.

El procedimiento consistirá en que el emisor utilizará su clave privada para firmar digitalmente el documento, esta clave será secreta ya que él mismo la generó y no la divulgará a terceros, esto a fin de asegurarse que sólo sea conocida por él, lo que a la vez garantizará que sólo él sea capaz de producir esa firma digital usando su clave privada. Por este motivo es importante que nadie, salvo el emisor conozca su clave privada, ya que para ley todo lo que este firme con su clave privada privada estará firmado por él y no podrá ser desconocido.

Una vez que el emisor generó la firma digital, se enviará al destinatario el documento junto con la firma digital y la clave pública del emisor. El destinatario recibirá el documento, la firma digital y la clave pública del emisor y utilizará esta última para verificar que la firma digital recibida es válida.

Podemos observar más abajo un diagrama ilustrativo de toda la secuencia recién mencionada, sobre la izquierda aparece el emisor con su par de claves repesentadas por sendas llaves, a la derecha en el siguiente paso aparece el documento redactado por el emisor quien utiliza su clave privada para firmarlo digitalmente, así el documento firmado aparece representado en el medio de la figura, la escarapela que se le agrega al documento sobre el margen izquierdo representa la firma digital del emisor.

La computadora del emisor envía al destinatario el documento, la firma digital y la clave pública del emisor tal como aparece representado en el medio de la figura, la computadora del destinatario recibe estas tres cosas y utiliza la clave pública recibida para validar la firma digital del documento, esta situación es representada en la parte derecha de la figura como se ve a continuación.



Resumiendo entonces, el esquema básico de uso de claves consiste en:

- **El emisor firma digitalmente sus mensajes utilizando su clave privada, envía al destinatario el mensaje junto con la firma digital agregada y su clave pública.**
- **El destinatario utilizará la clave pública recibida para verificar la firma digital y, si la firma es válida, entonces tendrá certeza de que el mensaje no fue modificado, o sea que es íntegro, y que la firma fue hecha efectivamente por el emisor.**

Cabe observar que ahora cobra sentido el uso de los términos clave privada y clave pública, la clave privada sólo será conocida por el firmante lo que permitirá que sólo él pueda firmar digitalmente usando esa clave privada. En cambio la clave pública, será conocida por todo aquel que reciba el documento con el fin de verificar su firma, o sea que será públicamente conocida. Anteriormente dijimos que, a partir de una clave pública no se puede conocer cuál es la privada asociada, así que no importa que otras personas conozcan la pública del emisor, ya que eso no implica que puedan firmar como lo hace este porque para eso necesitarían conocer su clave privada.

En resumen la clave privada del emisor debe ser secreta o privada para que nadie más pueda firmar en su nombre, mientras que su clave pública tiene que ser pública de manera que los demás puedan verificar todo lo que él firme.

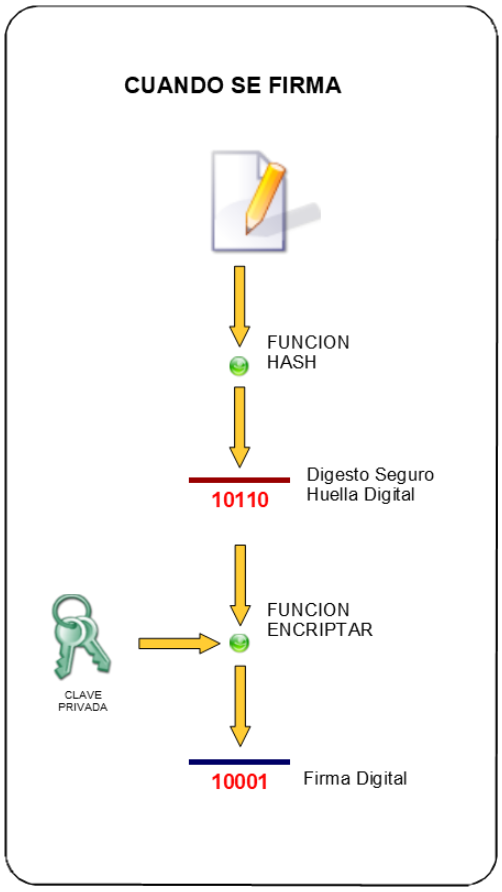
A continuación vamos a explicar este proceso que acabamos de ver con más detalle, pero como dijimos anteriormente, el usuario firmará sus documentos utilizando la plataforma de firma digital remota por medio de las claves que allí mismo generó, todo el procedimiento que se explicó, y el explicado a continuación, será realizado por la plataforma de firma digital remota, y para el usuario este proceso será totalmente automático.

Proceso de firma digital

Nuevamente partimos de que el emisor ya generó su par de claves asimétricas, y que ya tiene el documento en formato PDF que desea firmar a través del firmador web de la Plataforma de Firma Digital Remota.

Cuando la persona le indique a la plataforma que desea firmar digitalmente un documento, esta realizará la siguiente secuencia de operaciones.

Primero procesará el documento a firmar con un programa que se conoce como función de hash, lo que hace este programa es resumir toda la información del documento en un número. Este número recibe el nombre de digesto o huella digital del documento, y podemos decir que ese número es un resumen del documento original.



Una característica de estos algoritmos de hash es que son funciones matemáticas, esto significa que para un mismo documento este programa siempre va a calcular el mismo número de digesto, pero si en cambio el documento variase, aunque difiera en un bit por ejemplo, entonces el digesto que va a calcular esta función como resultado va a ser completamente distinto del anterior.

Una vez obtenido el número de digesto, la computadora lo encriptará utilizando la clave privada del emisor, en este preciso momento es cuando el emisor firma el documento con su clave privada y así genera la firma digital del documento.

Tenemos entonces que la firma digital es la huella digital del documento encriptada con la clave privada del firmante.

Cabe observar que esta firma digital depende de dos variables: primero del firmante a través de su clave privada, y segundo del documento que se está firmando a través de su número de digesto. O sea que si la persona que firma es otra, entonces firmará con otra clave privada, y aunque firme el mismo documento, si bien el digesto será el mismo, sucederá que la firma digital producida será distinta que la del primer firmante. Que la firma de un documento cambie con la persona que firma suena lógico ya que, al igual que sucede con la firma hológrafa, esto nos permite identificar al autor de la firma del documento.

Pero por otra parte, también dijimos que si el firmante firmase otro documento, aunque lo firme usando la misma clave privada, al cambiar el documento el hash también cambiará, y aunque se cifre con la misma clave privada, la firma digital también cambiará.

De esta forma la firma digital del documento cambiará, no solo con la persona que firma, sino también con el documento que firma la persona.

Volviendo a lo último dicho, recordemos que necesitamos no solo identificar al firmante, sino también asegurar la integridad del documento, con lo cual de alguna manera, también necesitamos identificar al documento, pero esto es justamente lo que está haciendo la firma digital, o sea que si el documento o el firmante cambian entonces cambia la firma, de esta manera a través de la firma digital se está estableciendo una vinculación lógica entre el firmante y el documento que este firma.

Así el firmante será responsable por aquello que él exactamente consintió con su firma, y no por cualquier otra modificación posterior del documento que no tenga su consentimiento.

En este punto la plataforma generará un paquete de datos que consistirá en: el documento, la firma digital y la clave pública del firmante, y este paquete es el que se enviará al destinatario. Veremos a continuación cómo es el proceso de verificación de una firma digital en la computadora del destinatario pero antes haremos algunas aclaraciones.

Algunas alcaraciones antes de seguir:

Como dijimos en el primer módulo, cabe observar que el documento firmado no está encriptado, lo que se encriptó fue el resumen del documento, el digesto, pero no el documento en sí, por lo que si un tercero intercepta el documento firmado podrá ver el contenido del mismo. Nuevamente recordemos que lo que nos interesa es asegurar la autoría e integridad del documento y no su confidencialidad.

Otra consideración importante es que, es muy común cuando se ve esta explicación por primera vez, se confunda la clave privada con la firma digital como si se tratasen de una misma cosa, pero esto no es así. Como dijimos la clave privada se utiliza para generar la firma digital del documento, si hacemos una analogía con la firma hológrafa, la clave privada es como si fuera la mano del firmante la cual permite realizar o generar el trazo de su firma hológrafa, mientras que la firma digital es como si fuera la firma hológrafa. Ahora bien es claro que la mano del firmante y su firma hológrafa no son la misma cosa, de igual forma no son lo mismo la clave privada del firmante y la firma digital del documento. Otro punto para reforzar esta última idea es que, recordemos, la firma digital variaba con el documento a firmar mientras que la clave privada no, la clave privada es siempre la misma independientemente del documento que se vaya a firmar.

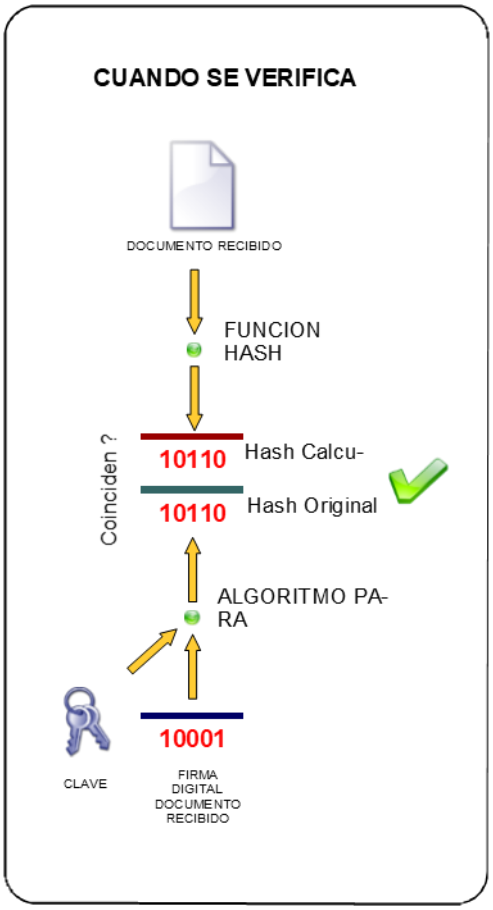
Por último y siguiendo la analogía recién planteada, se puede pensar que el algoritmo de hash y el algoritmo de encripción, los cuales en conjunto se utilizan para generar la firma digital a partir de la clave privada del emisor, vendrían a ser en este caso como la lapicera del firmante. Así cada una de estas tres cosas: clave privada, algoritmos y firma digital, son cada uno conceptos distintos entre sí, y cada uno de ellos ocupa un rol específico en el proceso de firma del documento digital.

- Clave privada = Mano del firmante
- Algoritmos (de hash y de encriptación) = lapicera del firmante
- Firma digital = firma hológrafa

Veremos a continuación cómo es el proceso de verificación de una firma digital en la computadora del destinatario.

Proceso de verificación de la firma digital

Para el proceso de verificación de una firma digital, el destinatario recibe el documento, la firma digital y la clave pública del emisor. La computadora del recpetor procederá a verificar la firma para lo cual desencriptará la firma digital con la clave pública recibida del emisor, obteniendo de esta forma el número de digesto original producido por el emisor. Recordemos que siempre que se encriptaba algo con la clave privada solamente se podía revertir el proceso desencriptando con la clave pública, pero como la firma digital es el digesto encriptado con la clave privada del emisor, al desencriptarlo con la clave pública de este se volverá a obtener el digesto que calculo el emisor antes de firmar el documento.



Por otra parte a partir del documento recibido, la aplicación del receptor calculará el digesto del documento recibido utilizando el mismo algoritmo de hash que uso el emisor. En este punto el receptor posee dos números de digesto: el que se obtuvo de la firma digital y que fue producido por el emisor antes de enviar el documento, y el digesto del documento recibido que fue calculado por la aplicación del receptor.

Si los números de digesto o hash coinciden esto quiere decir que el documento no fue alterado, puesto que si hubiese sido alterado durante su transmisión, el hash del documento recibido calculado por la computadora del receptor diferiría del original enviado por el emisor y obtenido como resultado de la desencripción de la firma digital.

De esta manera se corrobora la integridad de un documento firmado digitalmente mientras que su autoría también se valida por este mismo proceso, ya que si sabemos positivamente que la clave pública recibida es del emisor, la única posibilidad entonces es que esa firma digital verificada haya sido producida con la única clave privada que se corresponde con esa pública, sino el proceso de verificación de la firma no se validaría debido a que ambos números de digesto no coincidirían. De esta manera sabemos también que el emisor es el único capaz de producir esa firma digital ya que pudo ser verificada con su clave pública en la computadora del receptor.

Dado que este proceso de verificación puede ser realizado tantas veces como sea necesario, es factible demostrar ante un tercero que una persona en particular firmó un documento determinado, y garantizando de esta manera el no repudio de la firma, así el documento cuya firma fue verificada tiene carácter

probatorio. Por último el requisito de exclusividad reside en el secreto de la clave privada, la única persona que posea la clave privada será capaz de producir esa firma digital.

De esta manera hemos encontrado una tecnología, la criptografía asimétrica, que cumple con las mismas características de seguridad que posee una firma hológrafa.

Ahora bien, antes de proseguir con el desarrollo del curso cabe acotar que en el relato anterior hay una sutil omisión que se ha cometido en forma deliberada. Si volvemos hacia atrás, durante el proceso de validación de la autoría del documento dijimos que:

“si sabemos positivamente que la clave pública recibida es del emisor”

La cuestión fundamental en la línea de razonamiento anterior reside en:

¿Cómo sabe el receptor que la clave pública que recibió del emisor junto con el documento firmado realmente es del emisor?

¿Qué sucede si el receptor al recibir el documento firmado con la clave pública cree equivocadamente que pertenece al emisor y lo da por válido cuando en realidad ese documento fue firmado por otra persona? Y por otra parte: ¿quién es el emisor?

Como se dijo anteriormente la clave pública es un número, pero en ningún momento nadie me asegura que ese número pertenezca al emisor del mensaje, o mejor dicho la cuestión es: ¿cómo sabe el receptor que esa clave pública que recibió junto con el mensaje firmado es la misma que el emisor generó al azar en la plataforma? Por este motivo no puedo considerar esta información como válida ya que el receptor no puede estar seguro de a quién pertenece esa clave pública recibida.

En este punto es donde empiezan a aparecer las Autoridades Certificantes o también denominados Certificadores.

Proceso de verificación de firma digital con certificado de clave pública

Supongamos por un momento que estamos dictando este curso por primera vez en forma presencial, así que el docente tiene un listado de personas por nombre, apellido y número de documento, sólo aquellas personas que están en ese listado pueden ingresar al aula donde se dictará este curso. Así las personas llegan al aula y le dicen al docente a viva voz su número de documento, el docente verifica que ese número aparezca en el listado y, si aparece entonces esa persona puede ingresar al curso.

La pregunta es: ¿el docente está identificando a las personas que ingresan al curso? ¿Puede estar seguro de que la persona que acaba de ingresar realmente es la que figura en el listado? La respuesta es claramente NO.

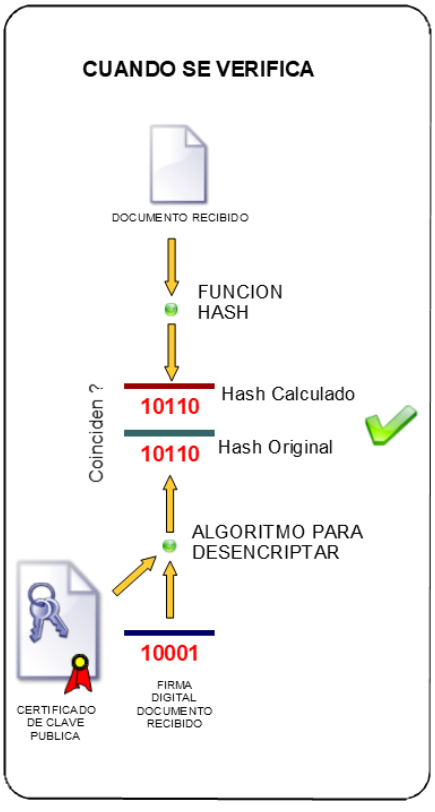
Lo correcto sería que las personas que van a ingresar al curso le presenten al docente su documento de identidad, si la foto del DNI coincide con la persona que lo presenta y el número de DNI coincide con el del listado, recién entonces el docente estaría identificando a la persona que está por ingresar.

De igual forma el emisor al enviar al destinatario el documento con su firma y su clave pública, le está indicando al receptor, "a viva voz" siguiendo la analogía, cuál es su clave pública. Así como los ingresantes al curso deben exhibir un certificado de identificación (que se llama documento de identidad), de igual forma el receptor debería enviarle al destinatario, no solamente su clave pública, sino en su lugar, su certificado de clave pública. Siguiendo esta idea, así como el Registro Nacional de las Personas emite certificados de identificación única llamdos DNI, y cada persona se identifica a un tercero exhibiendo su DNI, de igual forma debe haber alguien que se encargue de certificar que una clave pública pertenece a una cierta persona, ese alguien se va a llamar Autoridad Certificante.

De esta forma aparece la Autoridad Certificante la cuales será una tercera parte confiable que se encargará de certificar la vinculación entre una clave pública y su propietario.

¿De qué manera el certificador va a dar fe de que una clave pública pertenece a una persona determinada?

Por medio de certificados de clave pública, por lo tanto no bastará con que el emisor al firmar en la plataforma incluya su clave pública junto al documento firmado digitalmente; en lugar de ello, la plataforma deberá adjuntar el certificado de clave pública del emisor, el cual deberá previamente ser emitido por una Autoridad Certificante válida, ahora esta tercera parte en confianza es la que asegurará al receptor que esa clave pública pertenece positivamente al firmante.



Así la computadora del receptor obtendrá la clave pública del certificado, el cual fue emitido por un certificador válido, y la utilizará con total seguridad durante el proceso de verificación de firma, de esa manera el receptor sabrá que el documento fue firmado por la persona que figura en el certificado de clave pública avalado por la Autoridad Certificante.

De esta manera así como en un documento firmado de puño y letra,

la aclaración de la firma hológrafa es la que le indica al receptor quién es la persona que firmó, en un documento firmado digitalmente es el certificado de clave pública el que funciona como la aclaración de la firma digital, ya que únicamente en el certificado es donde el receptor encontrará los datos del firmante.

Resumiendo lo anterior, tenemos que es imprescindible la utilización de los certificados de clave pública como herramienta para identificar al autor de la firma digital de un documento, ya que como dijimos anteriormente, el autor de una firma digital sólo podrá determinarse obteniendo sus datos del certificado de clave pública asociado a esa firma.

A continuación veremos entonces qué es un certificado de clave pública.

Certificados de clave pública

Cabe entonces preguntarnos **¿Qué es un certificado de clave pública?**

Un certificado de clave pública es un archivo digital donde una Autoridad Certificante o Certificador, da fe de que a una determinada persona le corresponde una determinada clave pública. Para ello la Autoridad Certificante (AC) asocia los datos de identidad del emisor como ser: nombre, apellido, CUIL, otros datos de identidad relevantes de ser necesarios, y la clave pública que el emisor generó.

Por cuestiones de seguridad los certificados incluyen además un número de serie identificatorio, y fechas de emisión y caducidad del mismo a fin de indicar su período de validez, toda esta información a su vez está firmada digitalmente con la clave privada de la AC, de esta forma se puede saber quién fue el que certificó dicha clave y a la vez asegurarse también de poder detectar cualquier alteración de la información posterior a la firma del certificado.

Con el fin de verificar un documento firmado, la computadora del receptor va a poder obtener la clave pública del emisor en forma segura a través de su certificado de clave pública y, si el proceso de verificación de la firma digital es válido, entonces el receptor sabrá que la firma verificada pertenece realmente a la persona identificada en el certificado.

Ahora bien, cabe observar que en el esquema de verificación de la firma digital, el receptor recibe en realidad dos documentos firmados digitalmente, el primer documento original firmado por el emisor mientras que a la vez recibe también un segundo documento firmado digitalmente, el certificado de clave pública del emisor, el cual no está firmado por el emisor sino por la propia Autoridad Certificante que certificó esa clave pública.

Siguiendo la observación anterior, el receptor recibe dos documentos firmados digitalmente, el documento firmado por el emisor y certificado del emisor firmado por la AC, pero hasta ahora la computadora del receptor solamente válido la firma del emisor pero: ¿la firma digital del certificado no debería también ser validada?

La respuesta a esta pregunta dará lugar a lo que llamaremos **Jerarquía de Certificación**.

Jerarquía de certificación

Establecimos la necesidad de que un tercero en confianza de fe de que una clave pública pertenece a una cierta persona, esto se hace por medio de un certificado de clave pública firmado digitalmente por una Autoridad Certificante. De esta manera sabemos que la firma del documento pertenece realmente a la persona que figura en el certificado. Ahora bien, cabe preguntarnos:

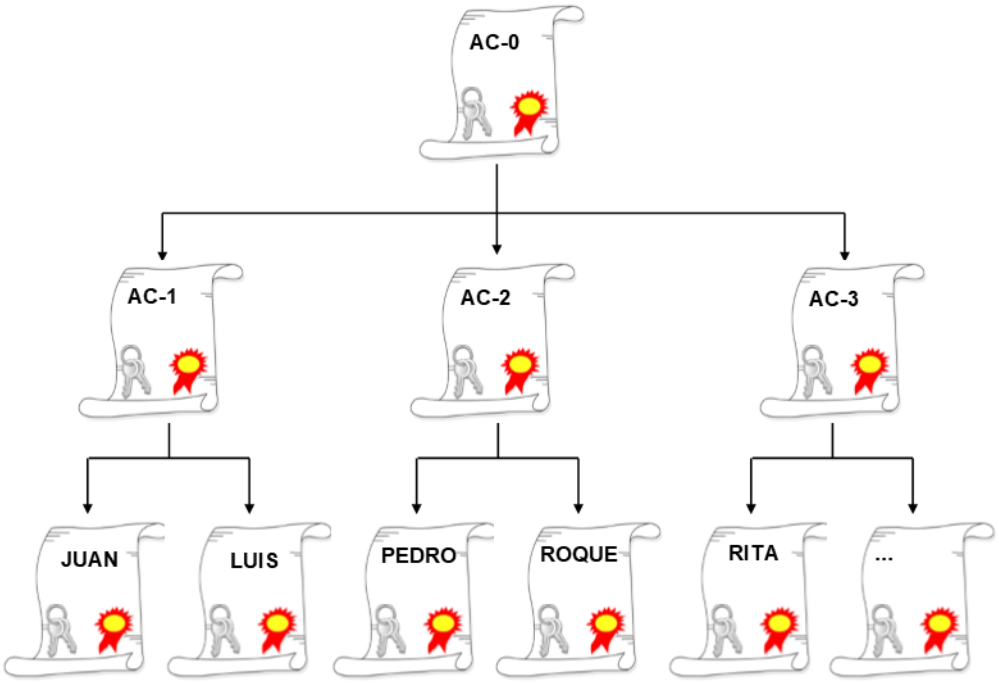
¿Cómo sabemos que la información del certificado es válida?

Para asegurarnos que la información del certificado no haya sido alterada, así como verificamos la firma del documento del emisor usando la clave pública del certificado de este, también debemos verificar la firma digital del certificado del emisor utilizando la clave pública de la Autoridad Certificante (AC) que fue la que lo firmó.

Sin embargo esto nos plantea a su vez un nuevo problema: ¿Cómo sé que la clave pública que estoy utilizando para verificar la firma del certificado pertenece realmente a esa Autoridad Certificante? Recordemos que el problema original empezó porque no podíamos dar por válida la clave pública del emisor si esta no estaba certificada, pero ahora necesitamos usar la clave pública de la AC (que no está certificada) para validar la firma del certificado del emisor.

Siguiendo la misma línea de razonamiento, podemos poner la clave pública de la AC dentro de otro certificado de clave pública firmado por otra AC que certifique la clave pública de la primera AC. De esta manera se va a formar una cadena de certificación con distintas jerarquías de Autoridades Certificantes, donde una AC de mayor nivel certifica a otra de menor nivel, y así sucesivamente hasta llegar al certificado del emisor tal como se observa en la figura que está más abajo. Sin embargo en este punto es evidente que podríamos seguir indefinidamente el proceso de certificación y el problema continuaría sin resolverse.

Lo que va a suceder es que en algún punto va a ser necesario cortar la cadena de certificación de manera que quede una única Autoridad Certificante en la cima de la jerarquía (AC-0 en el dibujo), esta AC se llamará Autoridad Certificante Raíz. La característica distintiva de esta AC es que no tendrá su certificado firmado por otra AC, sino que ella misma se firmará su propio certificado con el fin de cortar este proceso de certificación en cadena que, de otra forma sino continuaría indefinidamente.



La Autoridad Certificante Raíz emitirá su certificado de clave pública y lo autofirmará con su propia clave privada, esta autocertificación no es una certificación real en sí, ya que las certificaciones siempre deben ser realizadas por un tercero y no por el mismo que se está certificando. Ahora bien tenemos que todas las claves públicas de la jerarquía están certificadas salvo la raíz que está autocertificada.

¿Pero entonces de qué manera nos vamos a poder asegurar de la validez de ese certificado?

La forma será verificar su validez por algún medio alternativo y seguro a fin de asegurarnos que esa clave pública realmente pertenece a esa Autoridad Certificante Raíz.

Una manera alternativa y segura de obtener el certificado raíz sería descargarlo directamente desde un sitio web seguro de un organismo público. Este requisito es fundamental ya que, del mismo modo que cuando realizamos una compra por Internet debemos verificar que el sitio web desde donde realizamos la compra sea un sitio seguro, esto mismo debemos hacer cuando descargamos un certificado raíz. Para verificar que el sitio es seguro debemos visualizar en la barra de direcciones del navegador web desde el cual haremos la descarga, que aparezca el protocolo **https** en lugar del protocolo no seguro **http** (por ejemplo **https://argentina.gob.ar** en lugar de **http://argentina.gob.ar**), de esa manera descargando e instalando el certificado raíz desde un sitio web seguro de un organismo público podemos asegurarnos de la autenticidad de dicho certificado raíz.

Una vez que el receptor descargó el certificado raíz de un sitio seguro de un organismo público, se aseguró de esta forma que ese certificado raíz realmente es válido, así la aplicación del receptor encargada de validar la firma digital del documento recibido estará en condiciones de validar todos los certificados que se encuentran en la cadena de certificados a la cual el emisor pertenece.

Vamos a dar un ejemplo utilizando la figura que está más arriba, si el receptor recibe un mensaje firmado digitalmente por Juan, una vez que la computadora del receptor validó la firma del documento utilizando el certificado de Juan, también deberá verificar la firma del certificado de Juan utilizando el certificado de la Autoridad Certificante AC-1 que fue la que lo firmó. A su vez la computadora del receptor también verificará la firma digital del certificado de AC-1 para lo cual deberá utilizar el certificado de la Autoridad Certificante Raíz AC-0, por último validará la firma del certificado de AC-0, pero en este caso como el certificado está autofirmado, utilizará el mismo certificado de AC-0 para validar su firma. Si en cambio el receptor validara un documento firmado por Pedro entonces deberá tener instalado el certificado AC-2 y el certificado raíz de AC-0 y, si alguno de estos dos certificados no estuviese instalado la aplicación, entonces la computadora del receptor arrojará un error informando tal situación y que la firma digital del emisor no puede ser validada debido a esto.

Es importante aclarar que el receptor del mensaje firmado digitalmente deberá tener instalados en su computadora todos los certificados que aparecen en la cadena de certificación.

De esta manera realizando la validación de la clave pública de un único certificado raíz, la computadora del receptor puede determinar la autenticidad de todos los certificados que descansan debajo de la jerarquía de certificación.

Vamos a dar a continuación las definiciones de los conceptos introducidos.

Definición de certificado de clave pública y autoridades certificantes

A continuación daremos algunas definiciones de los conceptos recientemente vistos.

Los certificados de clave pública son documentos digitales firmados digitalmente por una Autoridad Certificante, que vinculan la clave pública de una persona a sus datos de identidad.

Una Autoridad Certificante o Certificador es una tercera parte confiable que da fe de la veracidad de la información incluida en los certificados que emite.

Es importante que toda la información que incluye el certificado haya sido previamente validada antes de ser emitido ya que sino la Autoridad Certificante (AC) no tiene razón de ser, así la AC deberá certificar la vinculación entre la identidad del titular del certificado y su clave pública.

Para ello la Autoridad Certificante deberá validar toda la información que contendrá el certificado, principalmente la identidad del titular como así también que ese titular es el que generó la clave pública que contendrá ese certificado.

Consideraciones para usuarios de la Plataforma de Firma Digital Remota

- **La clave privada debe ser generada, almacenada y utilizada por el titular del certificado a través de la Plataforma de Firma Digital Remota:** la Autoridad Certificante no tendrá acceso al proceso de generación de las claves por parte del titular en la plataforma.
- **Se debe proteger la clave privada:** esto se hará por medio de tres factores de autenticación, la contraseña de usuario, el PIN de acceso a la clave privada y un código OTP (One Time Password).
- **No se necesita el uso de token para firmar digitalmente:** los suscriptores disponiendo de una conexión internet a través de su celular o computadora pueden firmar digitalmente desde cualquier lugar conectandose al firmador web de la plataforma.

- **La Autoridad Certificante (AC) NO tiene forma de acceder a la clave privada del titular:** por tal motivo la AC no puede restaurar la misma si se pierde; en este caso el titular deberá revocar su certificado.

- **No es necesario un certificado por cada documento a firmar digitalmente:** con la clave privada y el certificado de clave pública correspondiente el titular puede firmar digitalmente todos los documentos que necesite siempre en formato PDF.

- **Un documento con firma digital impreso no posee valor legal** ya que el mismo no está firmado digitalmente.

Sistema de Firma Digital: Actores

Finalmente tenemos que en un sistema de firma digital hay cuatros actores principales:

- El **emisor o titular** del certificado (también denominado **suscriptor**).
- El **receptor** o también llamado **tercer usuario**.
- El que testimonia que una firma digital pertenece a una cierta persona, en este caso el **certificador o autoridad certificante**.
- Una **entidad auditante** de todo el sistema.

Debe existir una cuarta entidad que se encargue de controlar el sistema de firma digital. Así como el banco central controla la gestión de los bancos, los entes reguladores la gestión de las empresas de servicios, etceterá; es necesaria una cuarta entidad que controle la gestión de las autoridades certificantes.

Por ejemplo, que verifique que antes de emitir un certificado de clave pública el certificador realiza todos los procedimientos de verificación de identidad necesarios, que sus sistemas cuentan con la debida seguridad física, lógica entre otros aspectos.

Toda la estructura antes desarrollada junto con el agregado de la parte legal que veremos en el próximo módulo dará lugar a una última definición general que engloba a todos los conceptos antes vistos.

Infraestructura de Firma Digital (PKI)

Por último daremos una definición formal de este concepto que contiene y engloba a todos los conceptos que recién vimos.

Podemos definir el concepto de **Infraestructura de Firma Digital**, o también llamada **Infraestructura de Claves Públicas** (PKI - Public Key Infraestructure), como el conjunto de leyes, normativa legal, jerarquía de autoridades certificantes, entidades auditantes, hardware, software, bases de datos, redes, estándares tecnológicos, personal calificado y procedimientos de seguridad, entre otros, que permiten que distintas entidades, individuos u organizaciones, mediante el uso de firma digital y certificados de clave pública como herramienta, se identifiquen entre sí de manera segura al realizar transacciones en redes, especialmente Internet, permitiendo además dotar de autoría e integridad a los documentos digitales.