Criptografía, certificado digital y firma digital. Guía básica de supervivencia

(adaptación de información extraída de http://www.cert.fnmt.es/popup.php?o=faq)

En Internet nadie sabe quién está al otro lado

A lo largo de la historia el ser humano ha desarrollado unos sistemas de seguridad que le permiten comprobar en una comunicación la identidad del interlocutor (ej. tarjetas de identificación, firma), asegurarse de que sólo obtendrá la información el destinatario seleccionado (ej. correo certificado), que además ésta no podrá ser modificada (ej. notariado) e incluso que ninguna de las dos partes podrá negar el hecho (ej. Notariado, firma) ni cuándo se produjo (ej. fechado de documentos).

En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que se contrasta con el documento de identidad.

Actualmente cada vez mayor número de actividades se está trasladando al mundo electrónico a través de Internet. Se hace, por lo tanto, necesario trasladar también los sistemas de seguridad a este contexto en el que el principal problema reside en que no existe contacto directo entre las partes implicadas. Necesitamos un documento digital que ofrezca las mismas funcionalidades que los documentos físicos con el plus de ofrecer garantías aún sin presencia física.

¿Cómo se resuelve este problema? Gracias a mecanismos criptográficos siendo los dos elementos fundamentales el certificado digital y la firma electrónica.

Con estos elementos se consigue:

- Comprobar en una comunicación la identidad del interlocutor (**autenticación**)
- Asegurarse de que solo obtendrá la información el usuario seleccionado (**confidencialidad**)
- Asegurarse de que la información no ha sido modificada después de su envío (**integridad**)
- Asegurarse de que el emisor no puede desdecirse de su propio mensaje (**no repudio en origen**)

Una solución con solera: la criptografía.

Para comprender correctamente conceptos como firma electrónica y certificado digital es necesario partir de los conceptos más básicos sobre criptografía.

Como ya hemos dicho, a lo largo de la historia siempre ha habido necesidad de proteger la información. Así, la criptografía tiene su origen durante el Imperio Romano, en la época del Emperador Julio César. César utilizó un esquema criptográfico simple pero efectivo para comunicarse con sus generales. El esquema de César consistía en desplazar cada letra del alfabeto un número determinado de posiciones. Por ejemplo, la letra "A" podría ser codificada como "M", la "B" como "N", la "C" como "O" ... así sucesivamente. En este caso, el número que se sumaría a cada letra para realizar la codificación sería el 13.

Así pues, el mensaje "ATAQUEN HOY AL ENEMIGO" podría transformarse en "MFMCGQZ TAK MX QZQYUSA", sin poder ser reconocido por el enemigo.

El método de cifrado introducido por Julio César introduce el concepto de "clave criptográfica". El "desplazamiento de 13 letras" es la clave que se utiliza por César para cifrar el mensaje, necesitándose la misma clave para descifrarlo. El ejemplo de César muestra un criptosistema de *clave simétrica* en el que se utiliza la misma clave para cifrar y descifrar el mensaje.

Por supuesto hoy en día los sistemas criptográficos que se emplean en Internet son mucho más complicados, aunque la base es la misma. No lo olvide: una clave cifra el mensaje. A continuación veremos su aplicación al mundo de las telecomunicaciones.

El cifrado digital.

El cifrado digital ya ha sido introducido con el ejemplo del Emperador Julio César. El concepto de cifrado es muy sencillo: dado un mensaje *en claro*, es decir, mensaje reconocible, al que se le aplique un algoritmo de cifrado, se generará como resultado un mensaje *cifrado* que sólo podrá ser descifrado por aquellos que conozcan el algoritmo utilizado y la clave que se ha empleado.

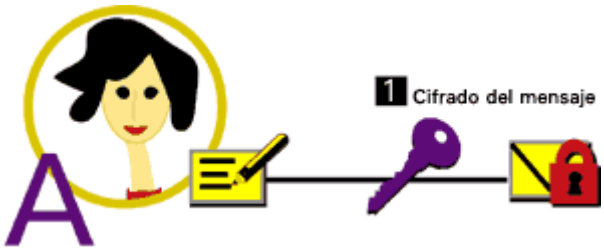
Dentro del cifrado digital encontramos dos opciones básicas: el cifrado de clave simétrica y el de clave asimétrica. Vamos a ver a continuación en qué consiste cada uno de ellos.

Criptografía de Clave Simétrica.

Se emplea una sola clave para cifrar y descifrar el mensaje. Este sería el caso que acabamos de ver con Julio César.

Proceso:

Ana ha escrito un mensaje para Bernardo pero quiere asegurarse de que nadie más que él lo lee.
Por esta razón ha decidido cifrarlo con una clave.
Para que Bernardo pueda descifrar el mensaje, Ana deberá comunicarle dicha clave.



Bernardo recibe el mensaje y la clave y realiza el descifrado.

El **beneficio** más importante de las criptografía de clave simétrica es su velocidad lo cual hace que éste tipo de algoritmos sean los más apropiados para el cifrado de grandes cantidades de datos.

El **problema** que presenta la criptografía de clave simétrica es la necesidad de distribuir la clave que se emplea para el cifrado por lo que si alguien consigue hacerse tanto con el mensaje como con la clave utilizada, podrá descifrar el mensaje.

Por esta razón se plantea el uso de un sistema criptográfico basado en claves asimétricas, como veremos a continuación.

Criptografía de Clave Asimétrica.

En este caso, cada usuario del sistema criptográfico ha de poseer una pareja de claves:

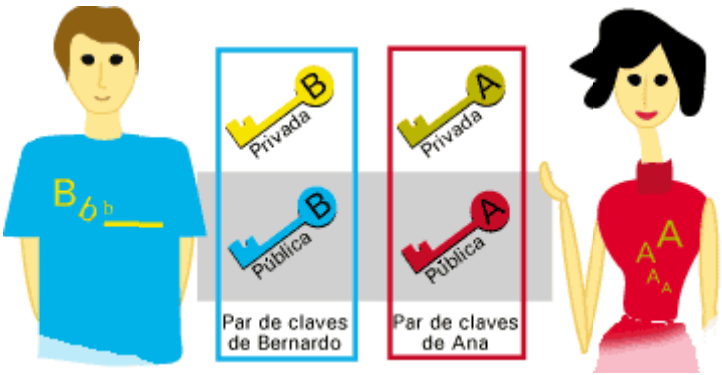
Clave privada: será custodiada por su propietario y no se dará a conocer a ningún otro.

Clave pública: será conocida por todos los usuarios.

Esta pareja de claves es complementaria: **lo que cifra una SÓLO lo puede descifrar la otra y viceversa**. Estas claves se obtienen mediante métodos matemáticos complicados de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de la otra.

Proceso:

Ana y Bernardo tienen sus pares de claves respectivas: una clave privada que sólo ha de conocer el propietario de la misma y una clave pública que está disponible para todos los usuarios del sistema.



Ana escribe un mensaje a Bernardo y quiere que sólo él pueda leerlo. Por esta razón lo cifra con la clave pública de Bernardo, accesible a todos los usuarios.

Se produce el envío del mensaje cifrado no siendo necesario el envío de la clave.

Sólo Bernardo puede descifrar el mensaje enviado por Ana ya que sólo él conoce la clave privada correspondiente.

El **beneficio** obtenido consiste en la supresión de la necesidad del envío de la clave, siendo por lo tanto un sistema más seguro.

El **inconveniente** es la lentitud de la operación. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública junto a uno de clave simétrica.

Criptografía de Clave Asimétrica. Cifrado de clave pública.

El uso de claves asimétricas ralentiza el proceso de cifrado. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es utilizar un algoritmo de clave pública junto a uno de clave simétrica. A continuación veremos cómo se produce el cifrado de un mensaje, mediante el cual obtenemos plena garantía de confidencialidad.

Proceso:

Ana y Bernardo tienen sus pares de claves respectivas.

Ana escribe un mensaje a Bernardo. Lo cifra con el sistema de criptografía de clave simétrica. La clave que utiliza se llama clave de sesión y se genera aleatoriamente.

Para enviar la clave de sesión de forma segura, esta se cifra con la clave pública de Bernardo, utilizando por lo tanto criptografía de clave asimétrica..

Bernardo recibe el mensaje cifrado con la clave de sesión y esta misma cifrada con su clave pública. Para realizar el proceso inverso, en primer lugar utiliza su clave privada para descifrar la clave de sesión.

Una vez ha obtenido la clave de sesión, ya puede descifrar el mensaje.

Con este sistema conseguimos:

Confidencialidad: sólo podrá leer el mensaje el destinatario del mismo.

Integridad: el mensaje no podrá ser modificado.

Pero todavía quedan sin resolver los problemas de autenticación y de no repudio. Veamos cual es la solución.

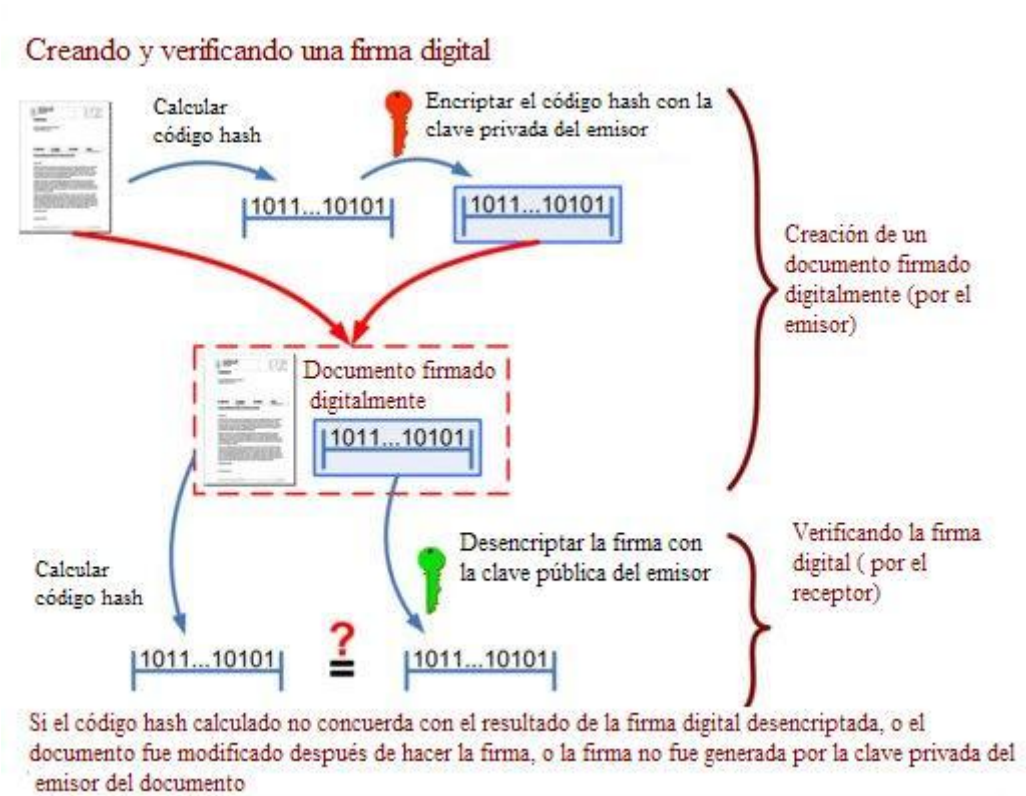
Criptografia de Clave Asimétrica. Firma digital.

Una de las principales ventajas de la criptografía de clave pública es que ofrece un método para el desarrollo de *firmas digitales*. La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación. De este modo, la firma digital ofrece el soporte para la *autenticación* e *integridad* de los datos así como para el *no repudio* en origen, ya que el originador de un mensaje firmado digitalmente no puede argumentar que no lo es.

Una firma digital está destinada al mismo propósito que una manuscrita. Sin embargo, una firma manuscrita es sencilla de falsificar mientras que la digital es imposible mientras no se descubra la clave privada del firmante.

La firma digital se basa en la propiedad ya comentada sobre que un mensaje cifrado utilizando la clave privada de un usuario sólo puede ser descifrado utilizando la clave pública asociada. De tal manera, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la privada. La firma digital, por tanto, es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública.

Sin embargo ya se ha comentado el principal inconveniente de los algoritmos de clave pública: su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar éste problema, la firma digital hace uso de funciones *hash*. Una función hash es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado *resumen* de los datos originales, de tamaño fijo e independiente el tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico.



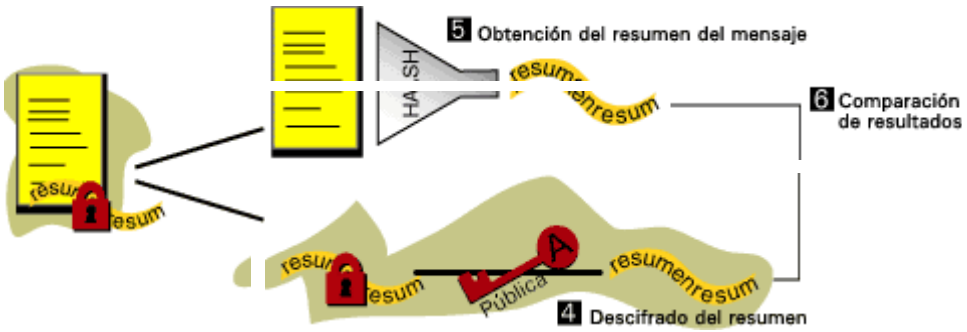
Proceso:

Ana y Bernardo tienen sus pares de claves respectivas.

Ana escribe un mensaje a Bernardo. Es necesario que Bernardo pueda verificar que realmente es Ana quien ha enviado el mensaje. Por lo tanto Ana debe enviarlo firmado:

1. Resume el mensaje mediante una función hash.
2. Cifra el resultado de la función hash con su clave privada. De esta forma obtiene su firma digital.
3. Envía a Bernardo el mensaje original junto con la firma.

Bernardo recibe el mensaje junto a la firma digital. Deberá comprobar la validez de ésta para dar por bueno el mensaje y reconocer al autor del mismo (integridad y autenticación).



4. Descifra el resumen del mensaje mediante la clave pública de Ana.
5. Aplica al mensaje la función hash para obtener el resumen.
6. Compara el resumen recibido con el obtenido a partir de la función hash. Si son iguales, Bernardo puede estar seguro de que quien ha enviado el mensaje es Ana y que éste no ha sido modificado.

Con este sistema conseguimos:

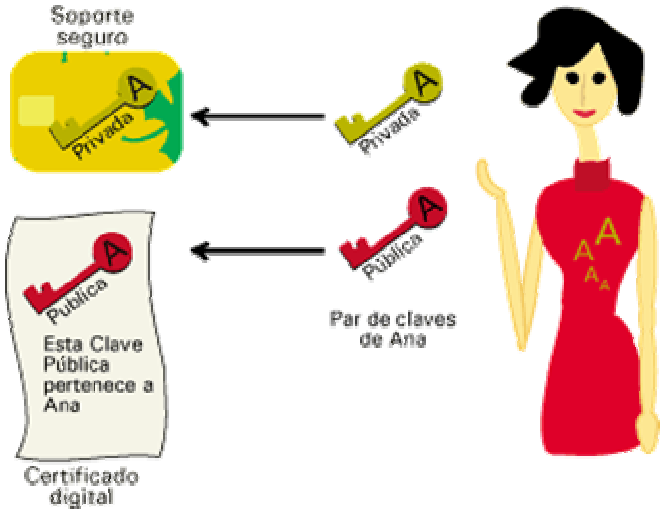
Autenticación: la firma digital es equivalente a la firma física de un documento.

Integridad: el mensaje no podrá ser modificado.

No repudio en origen: el emisor no puede negar haber enviado el mensaje.

Certificados digitales.

Según puede interpretarse de los apartados anteriores, la eficacia de las operaciones de cifrado y firma digital basadas en criptografía de clave pública sólo está garantizada si se tiene la certeza de que la clave privada de los usuarios sólo es conocida por dichos usuarios y que la pública puede ser dada a conocer a todos los demás usuarios con la seguridad de que no exista confusión entre las claves públicas de los distintos usuarios.



Para garantizar la unicidad de las claves privadas se suele recurrir a soportes físicos tales como tarjetas inteligentes o tarjetas PCMCIA que garantizan la imposibilidad de la duplicación de las claves. Además, las tarjetas criptográfica suelen estar protegidas por un número personal sólo conocido por su propietario que garantiza que, aunque se extravíe la tarjeta, nadie que no conozca dicho número podrá hacer uso de ella.

Por otra parte, para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los *certificados digitales*. Un certificado digital es un documento electrónico que asocia una clave pública con la identidad de su propietario.

Adicionalmente, además de la clave pública y la identidad de su propietario, un certificado digital puede contener otros atributos para, por ejemplo, concretar el ámbito de utilización de la clave pública, las fechas de inicio y fin de la validez del certificado, etc. El usuario que haga uso del certificado podrá, gracias a los distintos atributos que posee, conocer más detalles sobre las características del mismo.

Terceras Partes de Confianza.

Una vez definido el concepto de certificado digital se plantea una duda: ¿cómo confiar si un determinado certificado es válido o si está falsificado?. La validez de un certificado es la confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado. La validez del certificado en un entorno de clave pública es esencial ya que se debe conocer si se puede confiar o no en que el destinatario de un mensaje será o no realmente el que esperamos.

La manera en que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la confianza en terceras partes.

La idea consiste en que **dos usuarios puedan confiar directamente entre sí, si ambos tienen relación con una *tercera parte* ya que ésta puede dar fé de la fiabilidad de los dos**.

La necesidad de una Tercera Parte Confiable (TPC ó TTP, Trusted Third Party) es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es impensable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada. Además, la mejor forma de permitir la distribución de los claves públicas (o certificados digitales) de los distintos usuarios es que algún agente en quien todos los usuarios confíen se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

En conclusión, se podrá tener confianza en el certificado digital de un usuario al que previamente no conocemos si dicho certificado está avalado por una tercera parte en la que sí confiamos. La forma en que esa tercera parte avalará que el certificado es de fiar es mediante su firma digital sobre el certificado. Por tanto, podremos confiar en cualquier certificado digital firmado por una tercera parte en la que confiamos. La TPC que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave púbica se conoce con el nombre de Autoridad de Certificación (AC).

Infraestructura de clave pública.

El modelo de confianza basado en Terceras Partes Confiables es la base de la definición de las Infraestructuras de Clave Pública (ICPs o PKIs, Public Key Infrastructures).

Una infraestructura de Clave Pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.

Algunos de los servicios ofrecidos por una ICP son los siguientes:

- Registro de claves: emisión de un nuevo certificado para una clave pública.
- Revocación de certificados: cancelación de un certificado previamente emitido.
- Selección de claves: publicación de la clave pública de los usuarios.
- Evaluación de la confianza: determinación sobre si un certificado es válido y qué operaciones están permitidas para dicho certificado.
- Recuperación de claves: posibilitación de recuperar las claves de un usuario.

Las ICPs están compuestas por distintas terceras partes en los que todos los demás usuarios de la infraestructura confían:

- Autoridad de Certificación
- Autoridad de Registro
- Otras Terceras Partes Confiables como por ejemplo las Autoridades de Fechado Digital.