uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora Curso: **-Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

LECCIÓN 7: FIRMA ELECTRÓNICA

Elaborado por Prof. Dr. Carlos Galán Pascual (PhD)

Profesor Área Derecho Administrativo// Departamento de Derecho Público
Profesor Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz
Universidad Carlos III de Madrid
Agencia de Tecnología Legal, S.L.

SUMARIO:

II. FUNDAMENTOS TECNOLÓGICOS

1. La firma digital

2. La confianza

3. Los Prestadores de Servicios de Certificación

4. Los certificados digitales

5. Clases de certificados

II. FUNDAMENTOS TECNOLÓGICOS

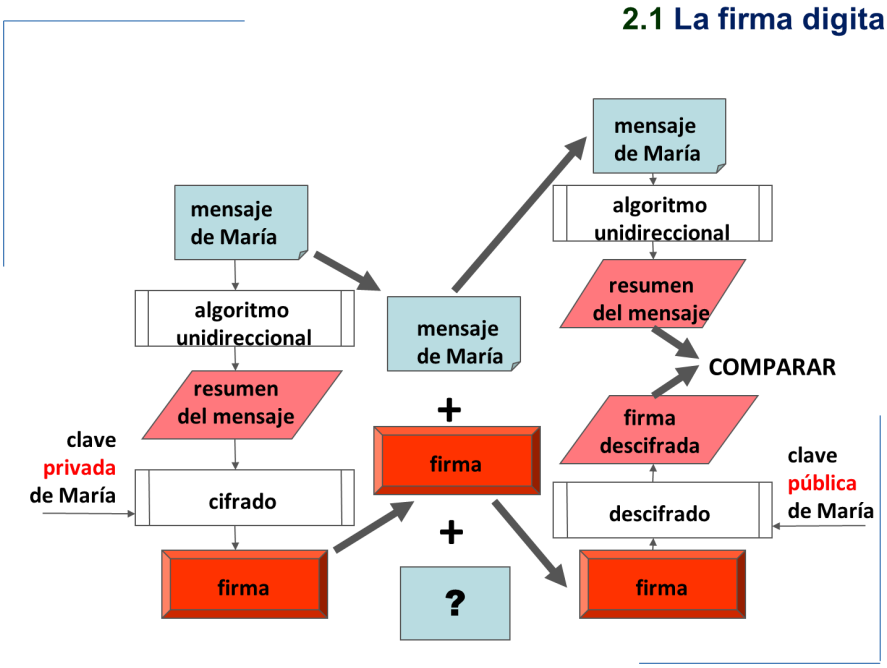
El tipo más importante de firma electrónica (y el que confiere mayor garantía jurídica) está sustentado en mecanismos criptográficos, en concreto en la llamada criptografía de clave pública o criptografía asimétrica. Este método se fundamenta en la utilización de una pareja de claves, llamadas *pública* y *privada*, que poseen la siguiente peculiaridad: Un mensaje que sea cifrado con la clave pública sólo podrá ser leído con la correspondiente clave privada y viceversa.

Este novedoso método, desarrollado a mediados de los años 70, se basa en la existencia de un algoritmo -susceptible de ser trascrito a programa de ordenador- que, mediante avanzadas teorías matemáticas fundamentadas en las propiedades de los grandes números primos, es capaz de generar una pareja de números (claves) de vinculación no computable (es imposible, conociendo uno de ellos, obtener el otro) con las características dichas más arriba.

Naturalmente, cuando un usuario utiliza la criptografía asimétrica, la clave privada debe permanecer siempre bajo su exclusivo control –de ahí su denominación de *privada*-, mientras que la clave pública puede –y debe, como veremos- ser conocida públicamente.

La criptografía de clave pública es la base tecnológica de la firma digital. Se hace necesario, por consiguiente, profundizar en su funcionamiento.

1. La firma digital



Esquema de funcionamiento de la firma digital

La firma digital, o *digital signature* como se la conoce en el mundo anglosajón, permite, mediante el uso de la criptografía de clave pública, identificar indubitadamente al firmante (autor o remitente, por ejemplo) de un mensaje electrónico.

Pongamos que María desea enviar un mensaje; por ejemplo, un correo electrónico para el que desea identificarse plenamente, es decir, hacer llegar la certeza al destinatario de que es ella quien envía el mensaje. En otras palabras, que nadie le ha suplantado.

Para ello, después de escribir el mensaje que desea hacer llegar al receptor, lo hace pasar –de manera automática- por un algoritmo unidireccional que reduce

el mensaje a un resumen de pequeño tamaño. Las características de este algoritmo unidireccional son las siguientes:

- Se le conoce como *función hash*.
- Es unidireccional, esto es, sólo funciona en el sentido descrito, nunca al contrario.
- El *resumen* obtenido es pequeño y de longitud estándar; esto es, sea cual sea el tamaño del mensaje original el resumen siempre posee el mismo tamaño.
- Cada carácter del mensaje original es relevante para la creación del resumen; esto es, la mera alteración de un solo carácter del mensaje original daría como resultado un resumen distinto y
- Es prácticamente imposible realizar todos los cambios necesarios en el mensaje original para que se obtenga un mismo resumen.

Como se verá, la existencia del resumen obtenido a partir del mensaje original mediante el algoritmo unidireccional es relevante sólo a efectos prácticos, sin que su presencia venga a alterar en modo alguno la filosofía de la firma digital.

En el paso siguiente María *firma* el resumen así obtenido –lo cifra- utilizando su clave privada que, como recordaremos, es aquella que nunca deberá salir de su exclusivo control.

El resumen firmado así obtenido se denomina *firma digital* o, simplemente, *firma*.

Esta firma digital presenta respecto de la tradicional firma manuscrita que todos conocemos, la semejanza de que, en ambos casos, identifica al autor del mensaje, y la diferencia en que si la firma manuscrita es siempre la misma, la firma digital, como acabamos de ver, será diferente para cada mensaje distinto que se envíe.

No cabe hablar, por tanto, de *nuestra firma digital* –porque, en general, será siempre distinta- y sí de *nuestra clave privada* –que, con las precisiones que veremos más adelante, será siempre la misma si usamos el mismo certificado.

Hecho esto –que, en el caso del correo electrónico, tiene lugar de manera instantánea y automática en el ordenador que envía- las informaciones que pasan al canal de comunicaciones son: el mensaje original de María y la firma electrónica de tal mensaje. Ambas informaciones circularán a través de la red y llegarán al destino –por ejemplo, al buzón del correo electrónico del destinatario.

Ha de hacerse notar que, en este momento, estamos tratando sólo de la *firma* de los mensajes (aquella que proporciona autenticación, integridad y no-repudio), no así la *privacidad* de la información transmitida puesto que, como se ve, el mensaje original circula en claro.

Cuando el receptor recibe el mensaje de María, le llegan dos ficheros de datos: por un lado, el mensaje propiamente dicho –mensaje en claro, como se ve en la figura- y, por otro, la firma digital. El proceso que se sigue en el ordenador del receptor se describe seguidamente.

En primer lugar, el mensaje original escrito por María se hace pasar por el mismo algoritmo unidireccional que utilizara el emisor, con lo que, si el mensaje no ha sufrido alteración en el trayecto, el resumen obtenido será también el mismo.

En paralelo, la firma de María se verifica –descifra- con la única clave que puede hacerlo; esto es con la clave pública de María que, puesto que es pública, está disponible para cualquiera que la necesite.

Pues bien, si el mensaje no ha sufrido alteración durante la transmisión –integridad- y si efectivamente ha sido María quien lo ha firmado –autenticación-, entonces y sólo entonces la firma descifrada de María y el nuevo resumen así obtenido deberán ser idénticos.

Si no lo son sólo puede deberse a dos razones -ambas igualmente importantes para la seguridad de las comunicaciones-: que el mensaje ha sido alterado en el trayecto y/o que el mensaje no ha sido firmado con la clave privada de María.

Si a la garantía de integridad del mensaje unimos la autenticación de su emisor, podremos igualmente probar que el emisor realizó tal comunicación (no-repudio en origen).

Como hemos visto en la explicación de la figura anterior, el mensaje de María circula en claro por la red. Si deseáramos, además, que el mensaje discurriera cifrado María debería cifrarlo con la clave pública del destinatario quien, a su vez, podría descifrarlo con su clave privada.

2. La confianza.

La criptografía y, en concreto, la criptografía de clave pública tiene su fundamento en las matemáticas. Son las matemáticas las responsables de la existencia de un algoritmo capaz de generar una pareja de claves pública-privada de las características antes citadas; son las matemáticas las responsables de la existencia de un algoritmo unidireccional capaz de resumir un mensaje de longitud variable en otro de longitud fija; son las matemáticas las responsables de diseñar mecanismos para cifrar y descifrar información..., etc. Estamos hablando, por consiguiente, de asuntos verificables matemáticamente. Esto es lo que hemos llamado seguridad.

Sin embargo, para que la estructura que sustenta la firma electrónica tenga sentido, es preciso incorporar al sistema un elemento de confianza al margen de las matemáticas.

Veámoslo con detalle.

Cuando un usuario accede a un determinado sitio web debe estar seguro de que, efectivamente, tal sitio web es quien dice ser. Esto puede lograrse si tal sitio web ha sido *certificado* por una Tercera Parte Confiable (*Third Trust Part* o *Prestador de Servicios de Confianza,* en la terminología del Reglamento eIDAS), organización que ha verificado previamente la autenticidad del lugar y proporciona copias certificadas de su correspondiente clave pública.

Lo mismo cabría decir de las claves públicas de las personas físicas. Cuando un usuario de criptografía asimétrica precisa de la clave pública de otro, necesita conocer fehacientemente que tal clave pública es precisamente de quien dice ser. La Tercera Parte Confiable certificará –*notarizará*, en terminología anglosajona- la autenticidad de la clave y la pertenencia a su titular.

3. Los Prestadores de Servicios de Certificación.

En la bibliografía estas organizaciones que se encargan de dar fe de la autenticidad de las claves públicas se las denomina Autoridades de Certificación (*Certification Authorities*) o, en la terminología del Reglamento eIDAS, *Prestadores de servicios de Confianza*, toda vez que certifican -mediante un instrumento especial que veremos más adelante llamado *certificado digital*- la identidad y correspondencia entre un determinado titular y su clave pública. De esta manera, cuando un tercero tiene acceso a la clave pública de una persona que le ha enviado un mensaje firmado, podrá comprobar quien está avalando tal correspondencia, tal identificación. De ahí la enorme importancia que tiene que tal Autoridad de Certificación sea capaz de generar la mayor confianza posible entre los usuarios.

Como más adelante estudiaremos, la normativa europea sobre la materia posibilita que puedan coexistir una multiplicidad de Terceras Partes de Confianza, tanto de naturaleza jurídica pública como privada. Entre las

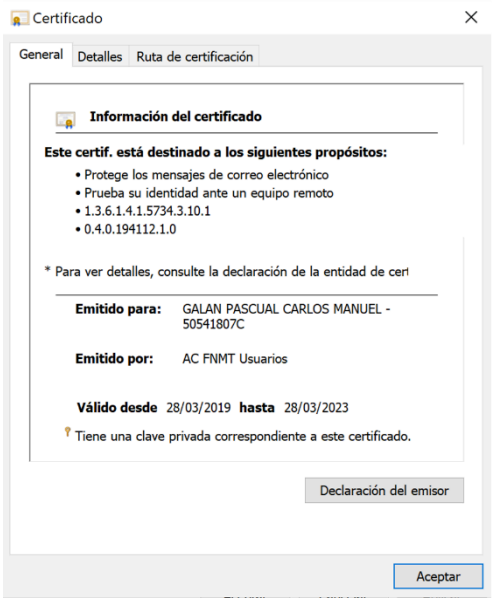
primeras cabe mencionar a la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, a través de su proyecto CERES, el organismo público por excelencia en la expedición de certificados digitales.

Otro organismo de naturaleza pública-empresarial es la iniciativa Camerfirma avalada por el Consejo Superior de Cámaras de Comercio, Industria y Navegación español.

Los fedatarios públicos, notarios y corredores de comercio, agrupados bajo un mismo cuerpo, poseen también ANCERT, Agencia Notarial para la Certificación y el Consejo General del Notariado, una Autoridad de Certificación para sus colectivos.

En cuanto a la iniciativa privada conviene destacar a la Agencia de Certificación Electrónica ACE, que fue la primera Autoridad de Certificación privada en nuestro país que, entidad participada por Telefónica, Sermepa (Visa España), Sistema 4B y la Confederación Española de Cajas de Ahorros CECA, entidad de la que el firmante del presente documento fue Director General.

4 Los certificados digitales.



2.4 Los certificados digitales

Un certificado digital no es más que un pequeño fichero informático (una secuencia de bits, en último extremo) que, fundamentalmente, establece esa correspondencia entre clave pública y titular.

La figura siguiente muestra el contenido de un certificado digital conforme a la norma estándar x.509. Los campos del certificado digital están determinados por el antedicho estándar internacional, siendo los más importantes:

- **Versión del certificado y número de serie**. Que debe ser único para cada Autoridad de Certificación.
- **Nombre del Emisor**: Autoridad de Certificación (Prestador de Servicios de Certificación) que ha expedido el certificado.
- **Fecha de inicio/expiración**: Periodo de validez del certificado.
- **Nombre del titular**: Persona física (o jurídica) para la que se expide el certificado, titular de la clave pública.
- **Clave pública del titular**: Aquella que permitirá a un tercero verificar los documentos electrónicos que reciba firmados electrónicamente por el poseedor de la correspondiente clave privada. Asimismo, un emisor podrá utilizar tal clave pública para cifrar aquellos documentos que desee enviar a su titular.
- **Extensiones**: Campo suplementario para incorporar otros datos que puedan ser relevantes para la identificación completa, por ejemplo, permisos y poderes que posee el titular, empresa, cargo, etc.
- **Firma del Emisor**: Se trata de la firma digital de la Autoridad de Certificación (Prestador de Servicios d Certificación en la terminología de nuestra norma). Mediante esta firma, la Autoridad de Certificación avala que todos los datos anteriores son ciertos y se responsabiliza de su exactitud.

5 Clases de certificados.

Ya hemos dicho que no todos los certificados digitales son iguales ni sirven para lo mismo. Suelen distinguirse distintas clases. Una **clasificación tipo** podría ser la siguiente:

- *Clase 0*: *Sin identificación*. No existe identificación previa del titular, por lo que la utilidad práctica de este tipo de certificados es prácticamente nula.
- *Clase 1*: *Con registro previo*. La Autoridad de Certificación (o entidades colaboradoras) han procedido previamente a la identificación del titular.
- *Clase 2*: *Administración Pública*. Certificados digitales expedidos por órganos de la Administración Pública (por ejemplo, los anteriormente citados para la presentación telemática del impuesto de la renta de las personas físicas).
- *Clase 3*: *Fedatario Público*. Certificados digitales expedidos por personas con atribuciones de fe pública.
- *Clase 4*: *Militar*. Certificados circunscritos al ambiente militar.
- *Clase WEB*: *Certificado de servidor seguro*. Certificados emitidos generalmente a favor de una sociedad con presencia en Internet, de modo que cualquiera que acceda a su sitio web pueda tener la seguridad de que es quien dice ser.

Como hemos visto, la confianza que emana de los certificados digitales es la misma que los usuarios depositan en las Autoridades de Certificación, puesto que son éstas entidades las que han registrado –identificado- previamente al titular y las que han asociado tal titular a su clave pública.