Firma Digital

Carlos G. Figuerola, Angel Francisco Zazo Rodríguez, José Luis Alonso Berrocal
Universidad de Salamanca
e-mail: [figue | afzazo | berrocal]@gugu.usal.es

La proliferación de documentos de todo tipo en soporte electrónico es un hecho. La facilidad de creación de documentos electrónicos de calidad y, especialmente, las extraordinarias prestaciones en cuanto a su transmisión y difusión que ofrecen las redes de ordenadores, hacen que cada vez en más ámbitos sea frecuente la utilización del soporte electrónico. Esto plantea, entre otras cosas, el problema de la autentificación de esta clase de documentos. Hasta no hace mucho, aunque un documento era producido –e incluso también archivado- a través de medios electrónicos, era normal trasladarlo a papel o imprimirlo, y una vez impreso firmarlo autógrafamente, ponerle sellos, registrarlo de salida, enviarlo físicamente por medios convencionales, registrarlo de entrada, etc. Es decir, convertirlo a documento convencional en papel para poder aplicarle los métodos convencionales de autentificación bien conocidos y aplicados desde antiguo.

El advenimiento de las redes de ordenadores (como Internet) ha cambiado radicalmente este panorama. En efecto, la facilidad e inmediatez de los envíos de documentos a través de la red, o la posibilidad de acceso a documentos depositados en otros ordenadores, independientemente de su ubicación geográfica, hacen que ese paso intermedio (la conversión a documento-papel) aparezca como una especie de lastre que frena la comunicación entre personas e instituciones de todo tipo. ¿Para qué imprimir un documento, meterlo en un sobre y transportarlo mediante correo convencional, mensajero o lo que sea, si técnicamente es posible y fácil –incluso más barato- hacerlo llegar en cuestión de segundos o minutos a su destinatario?

Una de las razones para tener que someterse al dichoso paso intermedio es, precisamente, la autentificación del documento, en cualquiera de sus vertientes: en lo que se refiere a la autoría del mismo, en lo que toca a la

integridad de su contenido (incluso de sus aspectos formales), y también a cuestiones como la fecha de emisión y la adecuada recepción por parte del destinatario. En efecto, cuando tratamos con documentos electrónicos resulta técnicamente sencilla su manipulación (alterando su contenido, haciendo figurar un nombre distinto como su autor, etc), y además resulta fácil hacerlo sin dejar huella: a diferencia de lo que ocurre con un documento sobre papel, aquí los borrados, enmiendas y demás no se notan.

Se han propuesto diversos sistemas y técnicas para afrontar esta cuestión, y claramente puede decirse que hoy es, todavía, materia de investigación abierta. Sin embargo, parece que se asienta un tipo de solución basado en la criptografía, cuyo uso se está difundiendo rápidamente, y que, incluso, recibe sanción o reconocimiento legal en numeroso países (entre otros, el nuestro). Esta solución es lo que se conoce como firma digital, y cuyo esquema de funcionamiento vamos a tratar de exponer.

Firma Digital

A mediados de los años 70 unos investigadores diseñaron una serie de técnicas destinadas a resolver los problemas de la confidencialidad y autenticidad de los documentos electrónicos. Tales técnicas se conocen en la actualidad de forma genérica como Criptografía de Clave Pública; el modelo más difundido es conocido como RSA, por las siglas de sus diseñadores: Rivest, Shamir y Adelman. Básicamente, consiste en lo siguiente:

Mediante un sencillo programa de ordenador se generan parejas de números o claves. Estos números son por lo general muy grandes (cada uno ocupa una larga lista de dígitos) y están matemáticamente relacionados con su pareja. Uno de ellos se conoce como Clave Privada y el otro como Clave Pública. La generación de ambas claves es siempre pareja, y están, como se ha dicho, matemáticamente relacionadas; de tal forma que si dos claves públicas son distintas, también lo será sus correspondientes claves privadas, y viceversa.

Cuando alguien desea utilizar o aplicar firma digital, debe estar provisto de su pareja de claves, la pública y la privada. La clave privada debe guardarse en secreto, mientras que la pública, como su propio nombre indica, se difunde

libremente, utilizando incluso servicios o directorios diseñados expresamente para ello.

Una vez elaborado el documento a firmar, un programa aplicará un algoritmo criptográfico que, tomando los bytes de ese documento y la clave privada del autor, elaborará lo que se conoce como huella digital de ese documento. Como esta huella se produce a partir de los bytes del fichero que contiene el documento, dos documentos diferentes producirán huellas distintas, aunque el autor (y su clave privada, obviamente) sea el mismo. La huella se incorpora al documento y se transmite con él.

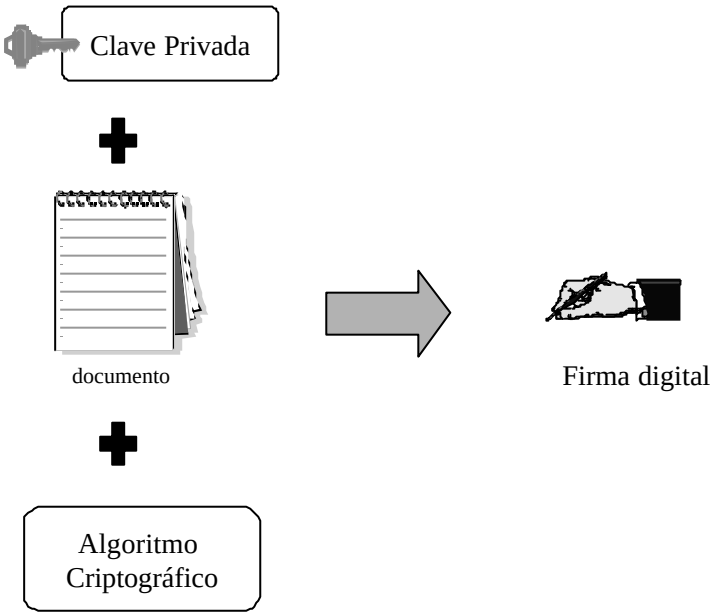

Ilustración 1 . Firma digital de un documento

Cuando se desea verificar la autenticidad de un documento firmado de esta manera, un programa puede comprobar, mediante el documento y la clave pública de quien dice ser autor, si la huella o firma es correcta. Si una clave pública autentifica la firma de un documento, esto quiere decir que ese documento fue firmado con la clave privada pareja o correspondiente a esa clave pública. Esto quiere decir también que el documento no ha sido

modificado desde que se firmó, y que no lo ha sido en lo más mínimo: ni un solo byte.

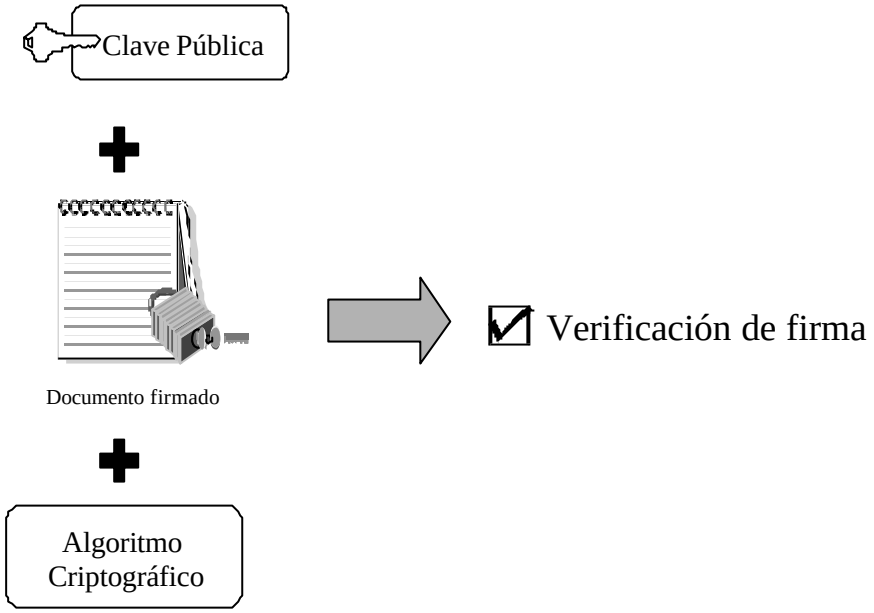

Ilustración 2. Verificación de la firma digital

En realidad, la criptografía lo único que nos asegura aquí es que la clave pública utilizada para verificar la firma es la pareja auténtica de la clave privada usada para firma el documento; pero en absoluto garantiza que esa pareja de claves pertenezcan a quien dice ser su propietario: cualquiera podría hacerse pasar por otra persona y dar a conocer (en Internet, por ejemplo) una determinada clave pública como correspondiente a esa otra persona, sin serlo. Es preciso, pues, algún sistema que garantice que las claves públicas (y, por consiguiente, las correspondientes privadas) pertenecen realmente a quienes dicen se sus propietarios. Ésta es la función, precisamente, de lo que se conoce como Autoridad de Certificación.

Autoridades de Certificación y Certificados Digitales

Las Autoridades de Certificación son instituciones cuya misión es mantener un registro de claves públicas. Naturalmente, para cada clave pública se registra o almacena también la identidad de su propietario. La Ley, en los países donde la firma digital está regulada, establece las formas en que se acredita debidamente esta identidad; pero lo habitual es que el registro de una clave pública requiera la presencia física de su propietario, y que éste acredite su identidad debidamente. La función principal de cualquier Autoridad de Certificación es, precisamente, certificar que determinada clave pública pertenece a determinada persona, ya sea física o jurídica.

En este punto hay que decir que pueden existir múltiples Autoridades de Certificación; de hecho, en España, la legislación deposita esta función en la iniciativa privada, de manera que se prevé que diferentes empresas ofrezcan esta clase de servicios. Igualmente, hay que indicar que las Autoridades de Certificación sólo necesitan registrar las claves públicas (además de los datos personales: nombre, dirección postal, etc.); para nada precisan de las claves privadas, puesto que para comprobar una firma sólo es preciso la clave pública. La privada sigue siendo secreto privativo de su propietario, y no es preciso cederla o comunicarla a nadie para que el sistema funcione.

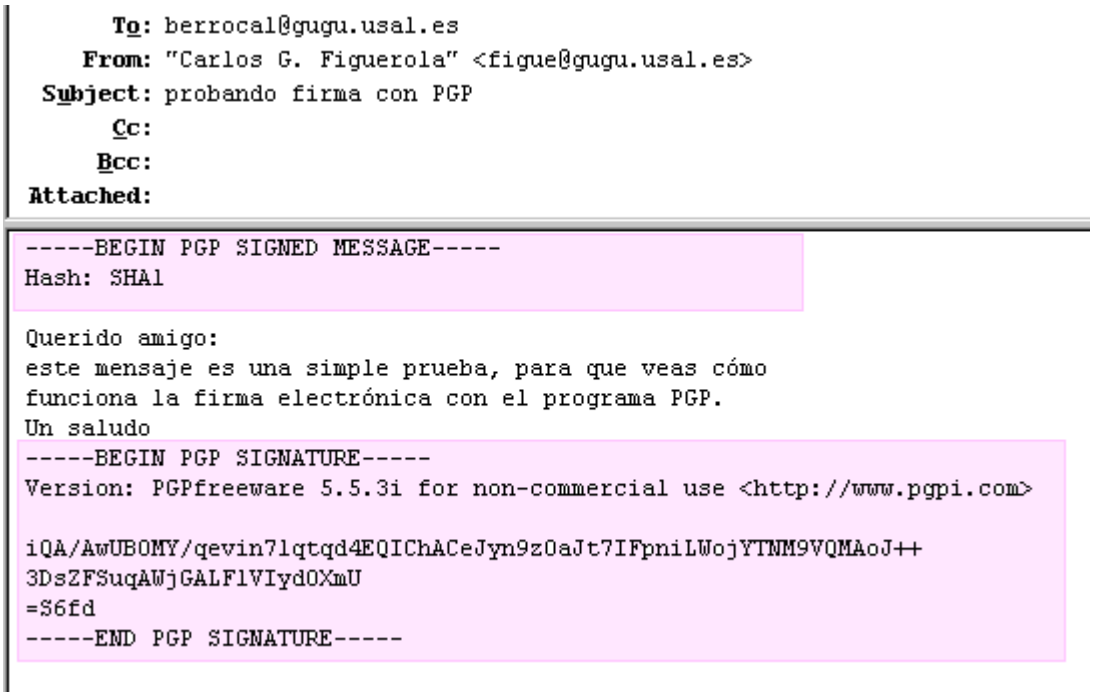

Ilustración 3. Mensaje firmado: las partes coloreadas corresponden a la firma digital

La existencia de múltiples Autoridades de Certificación plantea la cuestión de a cuál de ellas nos dirigimos cuando queremos verificar una firma digital. La forma de solventar esta cuestión es a través de lo que se conoce como Certificados Digitales.

Un Certificado Digital no es más que un documento electrónico emitido por una Autoridad de Certificación, en el cual se da fe de que una determinada clave pública pertenece a una determinada persona (física o jurídica). Para garantizar la autenticidad de un Certificado Digital, éste va firmado (digitalmente, claro está) por la Autoridad de Certificación que lo emite. Existe un estándar aceptado internacionalmente para Certificados Digitales, recogido en la norma X.509 de la CCITT. Las legislaciones suelen prever un registro de Autoridades de Certificación, en el cual consta la clave pública de cada una de ellas.

De manera que cuando uno quiere firmar digitalmente un documento electrónico, genera la firma de la forma ya vista, y añade un Certificado Digital que, previamente, habrá tenido que solicitar a la Autoridad de Certificación con la que tenga contratados este tipo de servicios.

Hay otra cuestión que también resuelven los Certificados Digitales. Las claves caducan o se vuelven obsoletas por diversas razones: por motivos de seguridad, cuando se sospecha que la clave privada ha podido ser vulnerada; pero también por causas muy diferentes (tutores de menores que se hacen mayores, representantes legales que dejan de serlo, etc.).

Por ello, se asume que los Certificados Digitales tienen una vigencia temporal. Debido a esto, las Autoridades o Agencias de Certificación producen y publican lo que se conoce como Listas de Certificados Revocados. En ellas figuran los números de serie identificativos de cada certificado expedido y revocado posteriormente por la Autoridad de Certificación de que se trate, junto con la fecha de revocación de cada uno de ellos. Esta fecha, por cierto, viene expresada en el formato conocido como Tiempo Universal Coordinado y recoge el año, mes, día, hora, minutos y segundos referidos el meridiano de Greenwich. Esto evita posibles problemas derivados de las diferencias horarias, toda vez que las operaciones con documentos electrónicos a través de las redes de ordenadores pueden realizarse en tiempo casi real entre puntos geográficos muy diferentes.

Así pues, la verificación de una firma digital necesita, adicionalmente, la comprobación de que la clave utilizada para producir dicha firma pertenece a quien dice ser su propietario; y esto se consigue a través de un Certificado Digital que acompañe a dicha firma. Y el Certificado Digital, a su vez, requiere también la comprobación de que la clave certificada está en vigor y no ha sido revocada. Gracias a las redes de ordenadores, esta operación puede efectuarse de forma automática por programas informáticos.

El futuro de la firma digital

Parece claro que existe una necesidad, en muchos casos apremiante, de disponer de algún mecanismo que permita autentificar documentos electrónicos. El sistema descrito brevemente hasta aquí, es el que, en la actualidad, resuelve mejor esta necesidad, hasta el punto de que, como se ha dicho, las legislaciones de numerosos países lo regulan ya, y confieren a este tipo de firma el mismo valor legal que a la firma autógrafa de los documentos sobre papel.

Sin embargo, esto no significa que este sistema de firma carezca de puntos débiles. En primer lugar, los algoritmos criptográficos utilizados; existen varios algoritmos diferentes basados en parejas de claves públicas y privadas, y cualquiera de ellos puede ser utilizado. En general, puede considerárselos extraordinariamente seguros desde el punto de vista criptográfico; desde este punto de vista exclusivamente técnico, su seguridad depende de dos factores: el tamaño o número de dígitos de las claves, y que se trate de un algoritmo público o no.

El primer punto es obvio: cuanto más largas sean las claves, más difícil es romperlas o 'reventarlas'. Sin embargo, dado que estos algoritmos no sólo se emplean para firmar, sino que también pueden usarse para cifrar documentos, no son pocos los países que limitan a través de su legislación el tamaño de las claves, alegando cosas como las posibles 'escuchas' o interceptaciones de comunicaciones entre bandas de crimen organizado, terroristas y cosas así. Ésta es una intensa polémica que no cabe en este artículo, pero debe saberse que, por precepto legal, por condiciones de exportación o por motivos de índole

parecida, muchos programas de firma y cifrado trabajan con claves de tamaño limitado.

El segundo punto puede parecer paradójico: un algoritmo criptográfico debe ser público, perfectamente conocido, para ser considerado fiable. Lo que ofrece privacidad en un sistema criptográfico es la clave utilizada, que debe permanecer secreta. Que el algoritmo sea público, y que el código consiguiente de los programas que lo aplican sea abierto nos aseguran que el mecanismo de encriptación sea realmente el que se nos dice que es, y también que los programas que usamos para llevar a cabo la firma (o la encriptación, en su caso) no tienen puertas falsas.

Adicionalmente, el uso de algoritmos públicos nos garantiza una mayor compatibilidad de programas: una firma generada a través de un algoritmo propietario probablemente sólo podrá ser verificada utilizando un programa determinado. Por el contrario, la mayor parte de los programas de firma digital existentes pueden reconocer y manejar firmas generadas con los algoritmos públicos más usuales.

Con todo, probablemente el elemento que aporta más problemas de seguridad es el mantenimiento en secreto de la clave privada. Como se ha visto, todo el sistema descansa sobre esta presunción, y es, desde luego, responsabilidad del propietario de la clave mantener ésta a buen recaudo. Sin embargo, cualquier clave privada es una lista más bien larga de caracteres, aparentemente sin sentido, difícil o prácticamente imposible de memorizar. Naturalmente, puede escribirse en papel, y guardar este papel en un lugar seguro; dejando de lado el hecho de que la fiabilidad de una firma dependería de lo realmente seguro que fuese ese lugar, el hecho es que la mayor parte de la gente guarda dicha clave en un fichero en su ordenador. La mayor parte de los programas de firma digital esperan encontrar dicha clave en un fichero determinado del ordenador en que se trabaja, y el nombre y localización de ese fichero suele ser conocido. De otra parte, si la clave ha de introducirse manualmente cada vez que hace falta, resulta innegable que es mucho más fácil hacerlo usando las posibilidades de copiar y pegar que ofrecen los ordenadores actualmente; mucho más si tenemos en cuenta que es fácil confundirse al teclear los caracteres que conforman cualquier clave.

Así, bien mediante acceso físico a nuestro ordenador, o a través de las redes, si estamos conectados, alguien podría obtener nuestra clave privada. El problema aquí está en que difícilmente podríamos percatarnos de que alguien se ha adueñado de dicha clave: la copia, o la simple lectura, de un fichero informático no deja huellas.

De otro lado, como habrá podido apreciarse, el sistema de firma digital descrito es tan complejo en su uso, que cabe preguntarse si realmente llegará a generalizarse entre el gran público. Por eso se comentaba más arriba que la firma digital es un tema en el que todavía se investiga, por lo que su asentamiento como mecanismo de autentificación de documentos electrónicos está aún por ver.

Resulta indudable que el sistema es lo suficientemente eficaz como para resolver esas necesidades que existen ya actualmente, y que hay personas e instituciones que la utilizan, y con cobertura legal. Pero no está claro que éste sea el sistema que en un futuro más o menos próximo se generalice como instrumento de autentificación. Y, si no es éste, ¿qué pasará dentro de algunos años con los documentos firmados ahora, y, sobre todo, con los Certificados Digitales expedidos ahora? ¿Seguirán existiendo las Autoridades de Certificación y se archivarán en algún sitio y de forma fiable las Listas de Certificados Revocados?

Para saber más sobre la Firma Digital:

Una introducción básica, pero rigurosa puede encontrarse en el trabajo de Ignacio Mendívil: El ABC de los documentos electrónicos, que es, a su vez, un documento electrónico que puede obtenerse en la dirección http://www.seguridata.com [consultado el 26/08/1999]

Manuales asequibles sobre criptografía y sus aplicaciones: Fusté Sabater, A. y Otros: Técnicas criptográficas de protección de datos, Madrid, Ed. RA-MA, 1997 y Pastor Franco, J. y Sarasa López, M.A.: Criptografía digital: fundamentos y aplicaciones, Zaragoza, Prensas Universitarias, 1998.

Una dirección de red especialmente interesante es la de Kriptópolis (http://www.kriptopolis.com). Aunque especialmente centrado en la criptografía, como su propio nombre indica, este colectivo tiene también otras áreas de interés relacionadas; una de ellas es la firma digital, pero otras tienen que ver con la protección de la intimidad en Internet, la seguridad en la red, etc. Además de información técnica, pueden encontrarse informaciones y artículos que abordan estos temas desde una perspectiva legal, política o sociológica. Editan un boletín electrónico con noticias y novedades especialmente interesante.

RedIris mantiene una serie de páginas web sobre seguridad en la red, y también sobre firma digital, incluso con un servicio experimental de certificación. Además de abundante documentación, es posible descargar de ahí programas de cifrado y firma digital. La dirección es: http://www.rediris.es/cert/

Legislación:

Directiva Comunitaria: Proposal for a European Parliament and Council Directive on common framework for electronic signatures COM(1998)297/2

Decreto-Ley español 14/1999 de 17 de septiembre (BOE 224) sobre firma electrónica

Orden ministerial de 21 de febrero de 2000 (BOE 45) por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación