FIRMA ELECTRÓNICA

Agustín Cernuda del Río

Universidad de Oviedo

EUITIO – C/ Calvo Sotelo, S/N (Oviedo)

guti@lsi.uniovi.es

RESUMEN

A medida que la informática se incorpora a más aspectos de la vida cotidiana, muchos trámites que tradicionalmente se realizaban en papel pasan a efectuarse de manera electrónica. Esto representa una ventaja para el tratamiento de la información.

Sin embargo, la propia naturaleza física del papel y la escritura ha sido utilizada también con ciertos fines. La dificultad de alterar un medio físico de representación de la información sirve como medida de seguridad contra las falsificaciones. La firma manuscrita, por otra parte, puede asociarse a su autor con un alto grado de certeza y sirve, por tanto, para acreditar su consentimiento, conocimiento o autorización en relación con la información escrita. Lógicamente, esto resulta fundamental en todo tipo de acuerdos, transacciones comerciales, etc.

Puede pensarse que los procedimientos electrónicos, en principio, no ofrecen estas posibilidades. En este documento se ofrece una somera introducción al funcionamiento de la firma electrónica y en qué medida permite que las transacciones electrónicas sustituyan a las manuscritas sin tener que renunciar a ninguna de sus ventajas.

CRIPTOGRAFÍA DE CLAVE ASIMÉTRICA

Antes de entrar en la aplicación específica a la firma electrónica, conviene conocer el fundamento de la misma: la criptografía de clave asimétrica.

Es conocido que cuando se transmite información el mensaje puede ser interceptado por terceros, que tendrían acceso a dicha información de forma no autorizada. Para evitarlo, se utiliza la encriptación. El emisor altera (de manera reversible) el mensaje original mediante el uso de una clave; el mensaje alterado (y por tanto ilegible) se transmite a salvo de intromisiones, y el receptor aplica la clave para devolver el mensaje a su estado original.

Este proceso plantea dos requisitos: uno, que sea imposible (a efectos prácticos) recuperar el mensaje original a partir del alterado si no se posee la clave. Otra, que el emisor y el receptor dispongan de la clave, pero el espía no.

Existen métodos de criptografía lo suficientemente avanzados que garantizan la imposibilidad práctica de *adivinar* la clave de cifrado. Pero existe un problema si la misma clave se utiliza para cifrar y para descifrar: si el emisor y el receptor no disponían de la clave de antemano (cosa habitual en transacciones electrónicas, en las que las partes nunca se han visto), tendrán que enviársela, y este envío compromete la seguridad.

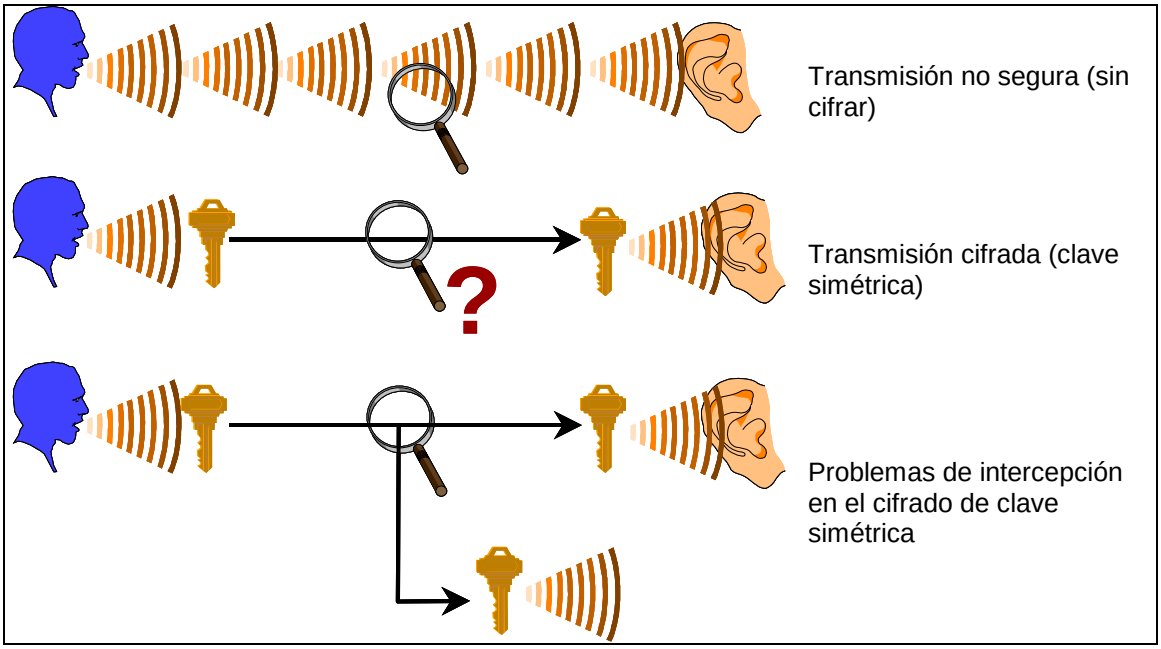

Ilustración 1. Criptografía de clave simétrica

Los métodos de criptografía de clave asimétrica se basan en el uso de dos claves. Ambas sirven para cifrar y para descifrar, pero lo que se cifra con una sólo se puede descifrar con la otra, y viceversa. De este modo, una persona dispone de dos claves; una de ellas será pública, y la otra privada. Cualquiera que desee enviarle un mensaje confidencial puede usar la clave pública para cifrarlo; de este modo el mensaje viajará seguro, y el receptor utilizará su clave privada para descifrarlo. No necesita darle su clave privada a nadie ni arriesgarse a que alguien la *escuche*; la clave pública, por su parte, permite a todo el mundo enviarle mensajes cifrados, pero es inútil para descifrarlos.

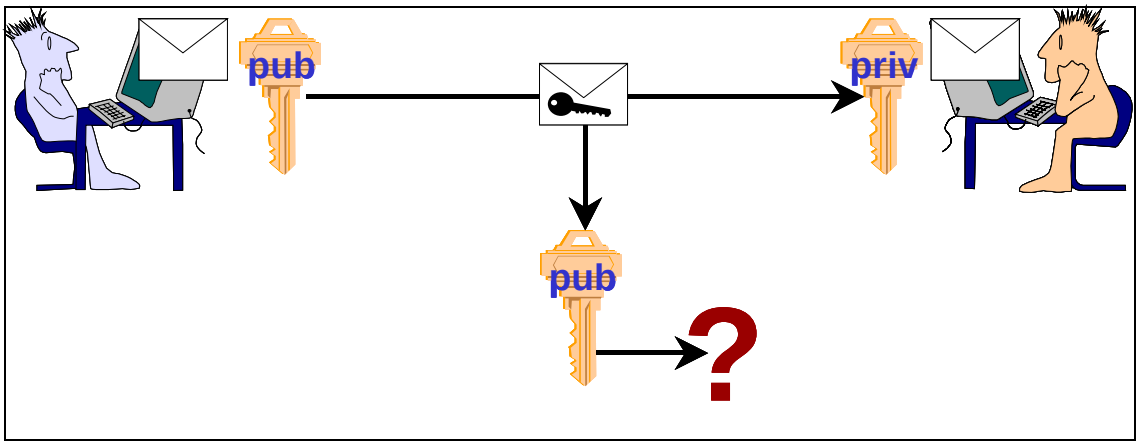

Ilustración 2. Criptografía de clave asimétrica

FUNDAMENTOS DE LA FIRMA ELECTRÓNICA

¿Qué relación tiene el cifrado de mensajes con la firma electrónica? El problema de los documentos electrónicos es que, a priori, su falsificación resulta técnicamente más sencilla que en los documentos físicos. Puesto que un documento electrónico contiene únicamente información, no ligada a ningún soporte ni acción física concreta, la información podría alterarse sin dejar huella física alguna. Evidentemente, esto abre las puertas a muchos tipos de fraude: falsificación de mensajes y cartas, modificación

maliciosa de las condiciones de los contratos, o suplantación de personalidad, por citar sólo algunos.

El cifrado puede utilizarse como elemento de apoyo para la firma electrónica. Lo que pretende la firma es, esencialmente, lo siguiente:

- Acreditar la validez de un documento, de modo que no pueda ser alterado o sustituido por otro.
- Vincular un documento a una persona o entidad.

La criptografía de clave asimétrica permite ambas cosas. Para *firmar* un documento, bastaría acompañarlo de una versión cifrada del mismo, que el firmante ha cifrado con su clave privada. Como ya se ha dicho, es imposible a efectos prácticos generar tal versión cifrada sin disponer de la clave, que el firmante conserva en su poder y no comunica a nadie. Además, los métodos de cifrado garantizan que cualquier mínima alteración en el documento original producirá una versión cifrada notablemente distinta.

El receptor puede tomar ambos documentos, el original y el cifrado (que es la *firma* que lo acompaña), y usando la clave pública del firmante (que es conocida por todos) descifrar dicha firma. Si el resultado coincide con el documento, efectivamente sabemos que este no ha sido alterado y además el firmante es quien dice ser, ya que sólo él tiene la clave privada y sólo con esa clave se puede haber cifrado el documento.

El método no es matemáticamente infalible. Por ejemplo, ¿cómo estar seguros de que la clave pública es la del firmante y nadie nos ha engañado? Para eso existen las llamadas autoridades de certificación, que son entidades que garantizan la asociación entre una persona física y su clave pública. En cualquier caso, aunque en teoría es posible la suplantación, la fiabilidad del método es suficiente para su uso práctico; al fin y al cabo, la firma manuscrita tampoco está a salvo de falsificaciones.

ASPECTOS LEGALES DE LA FIRMA ELECTRÓNICA

Los poderes públicos están promoviendo el desarrollo de la llamada *sociedad de la información* mediante diversos planes de actuación [1], y la firma electrónica resulta de gran importancia en la consecución de este objetivo. Una vez presentados los fundamentos técnicos que posibilitan la firma electrónica, cabe preguntarse por su uso práctico, así como por el valor legal de la firma electrónica.

Marco normativo

Existen diversos códigos legales que afectan al uso de la firma electrónica. Existe una Directiva Europea 1999/93/CE, del 13/12/1999 [2], que afecta a los países miembros de la Unión y debía aplicarse antes del 19 de julio de 2001; no obstante, España se adelantó a la promulgación de esta directiva con el Real Decreto-Ley 14/1999 sobre firma electrónica [3], promulgado el 17 de septiembre de 1999.

Posteriormente, se publicó el Reglamento de Acreditación en forma de Orden Ministerial [4], el 21 de febrero de 2000. Se aplica a los prestadores de servicios de certificación, es decir, a las entidades que ofrecen productos de firma electrónica y garantizan la asociación entre las claves y las personas.

Se pretendía tramitar el R.D.L. 14/1999 como Proyecto de Ley, a fin de que el debate parlamentario permitiera perfeccionarlo. No obstante, la legislatura terminó en marzo de 2000, por lo que se pospuso tal tramitación.

En 2002 surge una nueva iniciativa para perfeccionar algunos aspectos de la Ley, y se presentan sendos Borradores de Anteproyecto de Ley de Firma Electrónica, el primero en enero de 2002 y el segundo en julio [5]. Esa es la situación en el momento actual (noviembre de 2002).

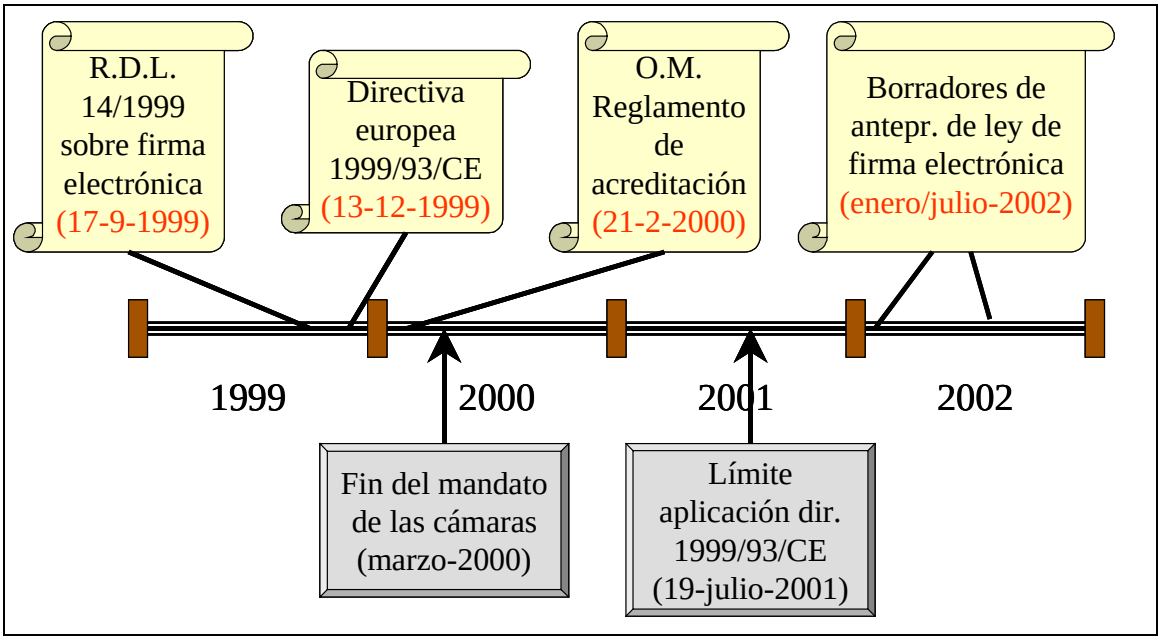

Ilustración 3. Legislación sobre firma electrónica

Validez legal de la firma electrónica

La legislación vigente en España sigue las directrices de la norma europea ya mencionada. Básicamente, la denominada firma electrónica *avanzada* tiene para los documentos electrónicos la misma validez que la firma manuscrita para los documentos en papel. Por ello debe aceptarse como prueba en un juicio, y en caso de que el firmante alegue error o falsedad, el juez decidiría previa intervención de los peritos correspondientes. Es decir, lo mismo que se aplica a la firma manuscrita. Existe, además, una presunción de validez de la firma si el prestador de servicios de certificación implicado está *acreditado* (la ley detalla en qué consiste esta *acreditación*).

Existen otros tipos de firma electrónica, que al no cumplir todos los requisitos establecidos por la ley no se calificaría como *avanzada*. En el caso de la firma *simple* o *no avanzada*, la ley garantiza cuando menos que dicha firma no se rechazará de plano como prueba por el mero hecho de ser electrónica.

La firma electrónica no sustituye las funciones de los fedatarios públicos. Cuando un notario interviene en una escritura pública no sólo verifica la identidad de los firmantes, sino que también enjuicia su capacidad para contraer las obligaciones correspondientes, y la firma digital es inútil para esto.

Aspectos comerciales

Según la legislación europea, no se necesita autorización previa para prestar servicios de certificación, si bien es cierto que el proceso de acreditación (que tiene efectos legales) sí está regulado y además existe un Registro de Prestadores donde deben inscribirse obligatoriamente estas entidades.

La legislación europea establece también la igualdad entre los proveedores de los estados miembros; de lo contrario, las transacciones comerciales internacionales se

verían gravemente afectadas. En consecuencia, la firma electrónica de un prestador de servicios reconocido en un estado miembro de la UE es automáticamente válida en los demás estados miembros.

Respecto a países ajenos a la UE, los proveedores de servicios de firma electrónica serán igualmente reconocidos en la UE si se adhieren a un programa de acreditación de un país miembro, si cuentan con el aval de un proveedor de un país miembro, o bien en virtud de acuerdos específicos bilaterales o multilaterales.

Los Borradores de la futura ley española que sustituirá al RDL 14/1999 permiten el uso de la firma electrónica por parte de personas jurídicas, aunque siempre a través de una persona física que actúe como representante legal que se hará responsable por el eventual uso inadecuado de dicha firma.

Ilustración 4. Plan de implantación del DNI electrónico(fuente: [7])

Iniciativas estatales

Existen diversas iniciativas en España para la implantación de la firma electrónica, pero la más relevante quizás sea la auspiciada por la Fábrica Nacional de Moneda y Timbre. El proyecto CERES (CERtificación ESpañola) pretende establecer una autoridad de certificación de carácter público. Ya ofrece diversos servicios de certificación y firma electrónica.

Una novedad del Borrador es la incorporación de capacidades de firma electrónica al D.N.I. [7] Se prevé que el D.N.I. sea una tarjeta con los dispositivos electrónicos necesarios para la firma electrónica; utilizando ordenadores dotados de dispositivos lectores adecuados, el usuario podría utilizar dicho D.N.I. como medio de identificación y como medio de firma electrónica. El plan de implantación de esta medida contempla su adopción definitiva a finales de 2003, de modo que entre en vigor en 2004.

CONCLUSIONES

La transición de la gestión física de la información a un modelo electrónico exigía medios de firma similares a los existentes tradicionalmente, a fin de garantizar la confidencialidad, autenticación, integridad y no repudio que se veían comprometidas en el ámbito digital. La criptografía de clave asimétrica ofreció una solución técnica sobre la cual puede edificarse un nuevo conjunto de relaciones electrónicas; para ello sólo se necesitaba un marco jurídico que ya está, en gran medida, desarrollado, y la difusión de la firma digital entre el gran público hasta el punto de convertirse en algo cotidiano, cosa que también parece que se logrará en un futuro cercano. El DNI electrónico puede ser un paso decisivo en esa dirección.

REFERENCIAS

1. Plan Info XXI del Ministerio de Ciencia y Tecnología. http://www.info21.es
2. Diario Oficial de las Comunidades Europeas, 19 de enero de 2000. http://europa.eu.int/eur-lex/pri/es/oj/dat/2000/l_013/l_01320000119es00120020.pdf
3. Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica. http://www.sgc.mfom.es/legisla/internet/rdley14_99.htm
4. Orden Ministerial de 21 de febrero de 2000, por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados dispositivos de firma electrónica (BOE nº 45, de 22 de febrero). http://www.boe.es/boe/dias/2000-02-22/pdfs/A07732-07737.pdf
5. Borrador de Anteproyecto de Ley de Firma Electrónica. Ministerio de Ciencia y Tecnología, Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Dirección General para el Desarrollo de la Sociedad de la Información. http://www.setsi.mcyt.es/inic_legisla/firma260702.pdf
6. Autoridad Pública de Certificación Española. Proyecto CERES. http://www.cert.fnmt.es/
7. DNI electrónico. Acción código INT001 del Ministerio del Interior en el marco del Plan de Acción Info XXI. http://www.info21.es/acciones/mostraraccion.asp?cod=INT001