Colaboraciones

Francisco González-Calero Manzanares. *Abogado*

Hacia una Ley sobre firma electrónica

La normativa aplicable sobre firma electrónica la componen el Real Decreto Ley 14/1999 de 17 de septiembre sobre firma electrónica y la Directiva 1999/93/CE sobre firma electrónica. Actualmente se está tramitando en el Parlamento un Proyecto de Ley que, en caso de ser aprobado, sustituirá al mencionado Real Decreto Ley.

Lo primero que debemos hacer es diferenciar la firma electrónica de la firma digital. Así, la primera actúa como firma en un documento electrónico, sustituyendo a la firma autógrafa o manuscrita, y la segunda añade otros requisitos, como la confidencialidad, el origen y la integridad del mensaje. Al tener el mismo valor probatorio que la firma manuscrita, se abren múltiples posibilidades de uso. Así, por ejemplo, un administrador de fincas puede remitir documentos oficiales a la Administración sin tener que desplazarse a sus oficinas, con el consiguiente ahorro de tiempo y dinero. Los ministerios que actualmente tienen más desarrollada la materia son el de Trabajo, el de Economía y el de Hacienda.

También podría dar las altas y las bajas en la Seguridad Social de los empleados del despacho o las comunidades. Piénsese que a la hora de solicitar una subvención o presentar cualquier otro tipo de solicitud ante la Administración referente a una comunidad de propietarios podemos hacerlo sin salir del despacho. O el ahorro de costes al incorporar la factura electrónica (basada en un sistema de firma electrónica u otro mecanismo de intercambio electrónico de datos equivalente) a nuestro proceso de gestión de negocio, en sobres y sellos, así como los oportunos desplazamientos a correos dejarán de ser necesarios. O el valor añadido que podemos dar a nuestros clientes, evitándoles tener que desplazarse a los despachos para firmar simples documentos.

La firma se crea por medio de mecanismos técnicos tales como la utilización de un lápiz especial que recoge ésta en la pantalla, la analiza y la convierte en un conjunto de caracteres numéricos, o por otros mecanismos como la utilización de un número PIN, el uso de tarjetas inteligentes, y *passwords*, o los métodos biométricos que recogen características anatómicas o fisiológicas del firmante, como la huella digital, el reconocimiento del iris o la pupila.

CRIPTOGRAFÍA

Creada ésta, se utiliza la criptografía para generar un certificado, que

no es otra cosa que el cifrado del mensaje de datos que se quiere transmitir, utilizando algoritmos que convierten a éste en formas aparentemente ininteligibles, para devolverlos con posterioridad a su forma habitual, es decir, el cifrado actúa como el sobre postal, impidiendo su interceptación y avisando al receptor en caso de que ésta se haya producido. Existen dos modelos de firmas: uno basado en criptosistemas simétricos, el cual utiliza una clave privada única para cifrar y descifrar el mensaje, y otro asimétrico, que utiliza dos claves diferentes, una pública y otra privada, de manera que una cifra el mensaje y la otra lo descifra y verifica la firma. El sistema simétrico es bastante fiable, pero plantea un inconveniente: que las dos partes han de conocer la clave, con lo cual se plantea un problema cuando se tienen que mandar muchos mensajes cifrados a diferentes personas, con lo que o mucha gente conoce tu clave privada o dispones de gran multitud de ellas, una para cada persona, e imaginémonos qué ocurriría si se trata de un comerciante, aunque este extremo es rebatido en base a que, por ejemplo, los supermercados o grandes almacenes proporcionan gran multitud de tarjetas de crédito distintas, una por cada cliente. No obstante, el método más utilizado es el de clave pública, ya que sólo requiere la emisión de dos claves. Este sistema está basado en el empleo de funciones algorítmicas que generan dos claves diferentes, pero matemáticamente relacionadas entre sí por el empleo de números primos. Aunque estas dos claves estén matemáticamente relacionadas entre sí, el diseño y la ejecución de un criptosistema asimétrico hace virtualmente imposible que las personas que conozcan la clave pública puedan adivinar la privada.

A principios de 2004 se pondrá en marcha el DNI electrónico

CLAVES

Por lo dicho anteriormente, la clave privada se utiliza sólo por el firmante para crear una firma numérica y la clave pública que, de ordinario conocen más personas, sirve para verificar (ésta también incluye, además de la identidad y la confidencialidad, la integridad del mensaje, es decir, que no ha sido modificado) y descifrar la firma numérica. Por tanto, es necesario que la clave privada se mantenga en secreto, e incluso no es necesario que la conozca, porque puede accederse a ella, como se indicó antes, a través de una tarjeta inteligente, número PIN o método biométrico (reconocimiento de características físicas).

Por poner un ejemplo, si A quiere mandar un mensaje a B, utilizaría la clave pública de B para cifrar el mensaje, y una vez recibido por B, éste utilizaría su clave privada para descifrarlo. También cabe la operación inversa. Mas aún, partiendo del mismo supuesto, si B quiere tener certeza de que es realmente A quien le manda el mensaje, en ese caso A debería cifrar el mensaje con la clave pública de B, más la clave privada de A, y para descifrarlo, B utilizaría su clave privada, más la clave pública de A.

Pero aún no tenemos cerrada la problemática que afecta a esta materia. Pensemos por un momento que un impostor se quiere hacer pasar por A, con lo cual crea una clave privada de A, con su correspondiente clave pública. Las personas, al ver que con la clave pública se descifra el mensaje de datos, creerán realmente que es A quien les ha enviado el mensaje. Para evitar esto se utiliza la denominada PKI (*public key infraestructure*), que basa su funcionamiento en los denominados terceros de confianza, entidad certificadora o prestador de servicios de certificación, que además de crear la clave privada y pública del solicitante, se aseguran que es realmente quien dice ser. Esto se produce por la emisión de un certificado, por parte de este tercero de confianza, en el que se indica que los datos en él consignados son ciertos, por eso es vital para el éxito de este sistema que se aplique a nivel internacional la regla del reconocimiento mutuo a los certificados.

A principios del año que viene se estima que se pondrán en marcha los primeros documentos nacionales de identidad electrónicos, a raíz de la habilitación que recoge el Proyecto. La creación de este documento no será incompatible con la tenencia de otras firmas electrónicas. La otra gran novedad es la habilitación a las personas jurídicas para utilizar estos medios, que en la actualidad les está vedada. ■