La firma electrónica es un sistema de acreditación que permite verificar la identidad de las personas con el mismo valor que la firma manuscrita, autentificando las comunicaciones generadas por el firmante. Esta herramienta, en cuya utilización el COITT ha sido pionero en España, permite, por ejemplo, el visado en los Colegios profesionales y las transacciones económicas seguras.

LA FIRMA ELECTRÓNICA

José Manuel Huidobro, *Ingeniero de Telecomunicación*

Cada día resulta más habitual realizar todo tipo de trámites y operaciones por vía telemática. En este entorno electrónico se plantea la necesidad de idear algún mecanismo que sustituya a la firma manuscrita, ya que muchos de estos trámites pueden llegar a tener consecuencias importantes para los implicados, tal como una transferencia bancaria. Este mecanismo recibe el nombre de *firma electrónica*. Sin embargo, dadas las peculiaridades de la tramitación electrónica, se requiere, además, un modo de garantizar que esa firma electrónica y los datos que la acompañan sean fiables y esta es, precisamente, la misión del certificado digital y la infraestructura de clave pública o PKI (*Public Key Infraestructure*).

La firma electrónica se utiliza en comunicaciones en las que no existe una confianza inicial total entre los comunicantes para autentificar mensajes, para validar compras por Internet, para realizar transferencias de fondos bancarios y para otras transacciones de negocios.

La firma electrónica debe ser:

— Única, pudiéndola generar solamente el usuario legítimo.

— No falsificable, el intento de falsificación debe llevar asociada la resolución de un problema numérico intratable.

— Fácil de autenticar, pudiendo cualquier receptor establecer su autenticidad aún después de mucho tiempo.

— Irrevocable, el autor de una firma no puede negar su autoría.

— Barata y fácil de generar.

Otra característica que han de tener las firmas electrónicas es que deben depender tanto del mensaje como del autor. Esto debe ser así porque en otro caso el receptor podría modificar el mensaje y mantener la firma, produciéndose así un fraude. La idea que subyace en la firma electrónica es que solamente el emisor la pueda producir y además se pueda demostrar que, efectivamente, es él quien la produce. Representa por tanto, un control más fuerte que la autenticación.

Reciente se ha lanzado en España el DNI electrónico que, entre otros objetivos, tiene el de impulsar el empleo de la firma electrónica, pues incorpora Certificado de autenticación y Certificado de firma electrónica reconocida. Permitirá realizar y firmar acciones y asumir compromisos de forma electrónica, pudiéndose comprobar la integridad de los documentos firmados por el ciudadano haciendo uso de los instrumentos de firma incluidos en él.

La Ley 59/2003, de 19 de diciembre, de firma electrónica regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

El proceso de firma electrónica consta de dos partes bien diferenciadas:

— **Proceso de firma.** El emisor (A) encripta el documento con su llave privada, enviando al destinatario (B) tanto el documento en claro como el encriptado.

— **Proceso de verificación de la firma.** El receptor (B) desencripta el documento cifrado con la clave pública de A y comprueba que coincide con el documento original, lo que atestigua de forma total que el emisor del mismo ha sido efectivamente A.

El método de la firma electrónica no sólo proporciona autenticidad al mensaje enviado por A, sino que también asegura el no repudio, ya que sólo el dueño de una llave privada puede encriptar un documento de tal forma que se pueda desencriptar con su llave pública, lo que garantiza que ha sido A y no otro el que ha enviado dicho documento. Asimismo proporciona integridad de datos, ya que si el documento fuera accedido y modificado en el camino, el resumen del documento cambiaría también.

Modelo de Certificado Digital.

FIRMA ELECTRÓNICA Y CIFRADO

La firma electrónica se construye sobre la base del cifrado asimétrico, uno de cuyos algoritmos más empleados es RSA. En este tipo de cifrado, cada usuario dispone de dos claves: una pública y otra privada. La primera se utiliza para descifrar los mensajes cifrados con la segunda, de manera que un usuario cifrará sus mensajes con su clave privada (que sólo conoce él) y el receptor los descifrará con la clave pública asociada al originador del mensaje.

Si se utiliza el algoritmo RSA para conseguir secreto y como firma electrónica, entonces es preferible que cada usuario use claves distintas para cada uno de los dos propósitos. De esta forma, cada usuario tendría asignada una clave en el directorio público de claves de cifrado y otra distinta en el directorio público de firma digitales. Esta separación es útil para dos propósitos. En primer lugar, ayuda a evitar el problema que surge cuando el módulo del emisor es mayor que el del receptor. En segundo lugar, dado que el RSA es débil frente a algunos ataques con texto escogido, tales ataques pueden verse facilitados si se utiliza la misma clave para ambos fines, y en consecuencia es preferible evitarlo.

El criptosistema RSA presenta algunos inconvenientes para las firmas digitales parecidos a los que presentaba como sistema de cifrado. En particular, podría resultar fácil falsificar firmas digitales para algún mensaje dado después de haber visto las firmas digitales auténticas de varios mensajes parecidos. Lo visto anteriormente sugiere que podría resultar más favorable para diseñar esquemas de firmas electrónicas el empleo de sistemas probabilísticos, en vez de los sistemas de clave pública.

CERTIFICADO DIGITAL

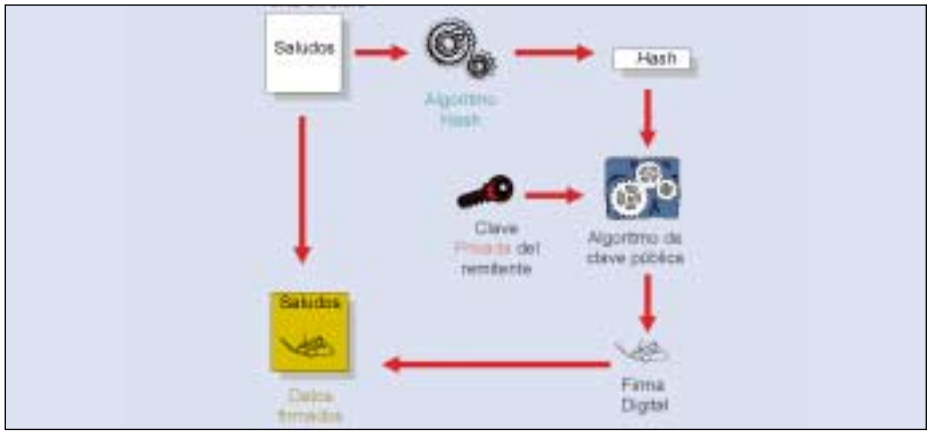
La firma electrónica asegura que el mensaje únicamente pudo ser originado por el poseedor de la clave pública con que se cifró el mensaje. Sin embargo, todavía queda por resolver el problema de la suplantación, ya que en ningún momento se comprueba que el remitente es el correcto. Este problema queda resuelto con la utilización de un certificado digital.

Un certificado digital contiene los datos de identificación de un individuo, empresa o Administración y, en general, de una entidad que dispone de una determinada clave pública y que garantiza que dicha clave pública pertenece a ese individuo, empresa o Administración durante un cierto periodo de validez. En realidad, un certificado digital está constituido por una clave pública a la que se adjunta el testimonio de alguna entidad que ha comprobado su validez y que dispone de la credibilidad necesaria para que dicha comprobación sea considerada válida. Esta entidad externa recibe el nombre de autoridad de certificación (CA, *Certification Authority*).

Sin embargo, el empleo de certificados digitales no está exento de problemas. El más importante de ellos es la distribución de los certificados. La solución más sencilla es la distribución manual por parte del administrador del sistema, que lo entrega a sus usuarios en soporte informático (por ejemplo, un disquete). Sin embargo, si el número de usuarios es muy elevado se vuelve inviable. Por tanto, es necesario algún mecanismo automático que facilite la distribución.

La solución tecnológica a la distribución de certificados depende del ámbito de validez de dicho certificado. Es decir, si se desea que la validez se limite únicamente a entornos privados, es posible emplear un servidor de certificados que los entregue a sus usuarios bajo demanda. Sin embargo, en este caso los certificados expedidos no suelen tener validez fuera del entorno privado, por lo que no resulta válida en ámbitos públicos (tramitación electrónica de documentos oficiales, pago de facturas por Internet, etc.).

Los entornos públicos exigen la participación de una entidad externa que dote a las comunicaciones del máximo nivel de seguridad a la vez que actúe de intermediario transparente entre los implica-



Proceso de firma electrónica (digital).

dos en la comunicación. Esta entidad externa es la autoridad de certificación, que genera los certificados y los firma digitalmente con su clave privada.

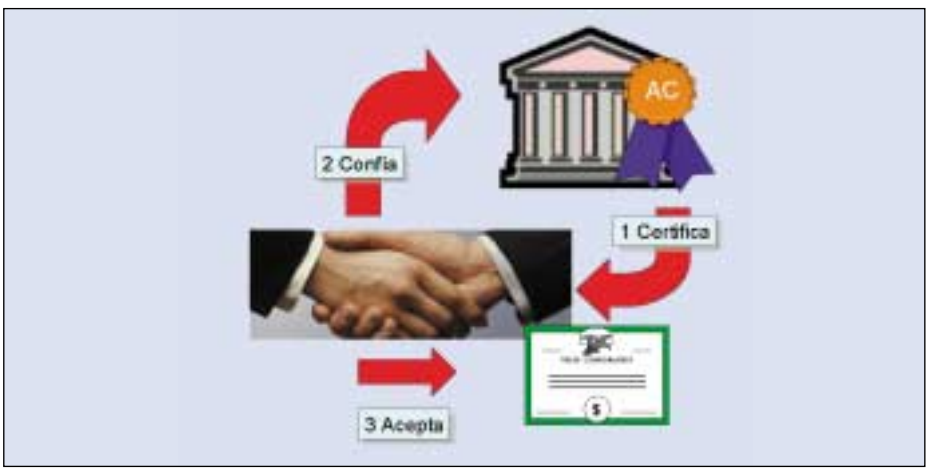
Utilizando la clave pública de la CA, disponible al mundo entero, cualquiera puede comprobar la autenticidad y la integridad del certificado emitido. Sin embargo, los certificados tienen asociadas funciones de gestión de los mismos (expedición, revocación, etc.) de las que suelen encargarse unos organismos llamados autoridades de registro (RA, *Registry Authority*).

AUTORIDADES DE CERTIFICACIÓN

Una de las iniciativas puestas en marcha por la Administración española es el denominado proyecto CERES (CERtificación ESpañola) que lidera la Fábrica Nacional de Moneda y Timbre (FNMT), y que, en líneas generales, consiste en establecer una Entidad Pública de Certificación, que permita autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación. Además de esta iniciativa, existen otras.

Las posibilidades de CERES cubren todas aquellas relaciones entre las distintas Administraciones (Central, Autonómica y Local) y los ciudadanos que necesiten ser securizados en términos de garantía de identidad, confidencialidad e integridad, con el objetivo de que CERES facilite al máximo sus relaciones a través de las nuevas redes de comunicaciones.

La tarjeta CERES está especialmente diseñada para infraestructuras de clave pública en las que se requiere autenticación de una entidad, integridad, confidencialidad de datos y el no repudio en origen.



Modelo de Confianza

Mantiene el material sensible criptográfico siempre interno a la tarjeta y protege su uso mediante control de acceso. De esta manera, se obtiene una considerable ventaja en términos de seguridad y portabilidad sobre las soluciones software.

Las características de los procesadores utilizados, en conjunción con el escrupuloso diseño del sistema operativo, consigue una herramienta eficaz que dificulta ataques basados en fuerza bruta y análisis diferencial. Un rasgo diferenciado es la posibilidad de que las claves RSA sean generadas por el emisor y almacenadas en un estado inactivo. Así, se asegura que las claves no son operativas hasta que un usuario en conocimiento de una clave de activación desencadene el proceso interno de descifrado.