



La firma digital, siempre a mano

El DNI electrónico será una realidad en España a finales del año 2003

Otras novedades del borrador

El borrador del anteproyecto introduce otras novedades. Una de ellas hace referencia a la emisión de certificados a nombre de personas jurídicas. Con ello, según el ministerio, se dota a estas entidades de mayor flexibilidad y se establece el régimen aplicable a la actuación de las empresas como firmantes. El nuevo texto también otorga mayor protagonismo al sector privado y favorece la autorregulación de la industria.

Alfonso Pérez

EN poco tiempo, el DNI digital será algo tan cotidiano como lo es la versión convencional. Esta semana el Ministerio de Ciencia y Tecnología (MCYT) ha dado un paso más para hacerlo realidad. En estrecha colaboración con los ministerios de Economía, Interior, Justicia y Administraciones Públicas, el MCYT ha concluido el segundo borrador del Anteproyecto de Ley de Firma Electrónica.

Los internautas que se dirijan a la web ministerial comprobarán que el nuevo anteproyecto incorpora las bases para la regulación del DNI electrónico. Éste se perfila como una tarjeta equivalente al DNI actual, que asegure la identificación en las relaciones *online* con cual-

quier Administración Pública, particulares y empresas. Y además de servir de instrumento identificador, el anteproyecto prevé la posibilidad de que el documento personal contenga la tecnología necesaria para que todos los ciudadanos dispongan de firma electrónica.

Este último aspecto ha creado recelo entre diversas autoridades de certificación, entidades que emiten un certificado que identifica al usuario con su firma digital. Estas empresas afirman que tal situación podría acabar con el mercado privado. El ministerio recién estrenado por Josep Piqué, lejos de entrar en polémicas, insiste en que el DNI digital representará un avance sustancial en el desarrollo de la Administración y comercio electrónico. Pero sobre todo,

explica el ministerio, "generalizará el uso de la firma electrónica como herramienta de seguridad de las transacciones".

De hecho, el DNI digital incrementará la disponibilidad, utilidad y accesibilidad de la firma electrónica. Según fuentes del sector, "será como llevarla en la cartera, teniéndola siempre a mano". Antes, el anteproyecto deberá seguir los trámites legales para su aprobación. De cumplirse los plazos, ya podremos usar esta modalidad de DNI a finales de 2003. *(sigue en la página 3)*

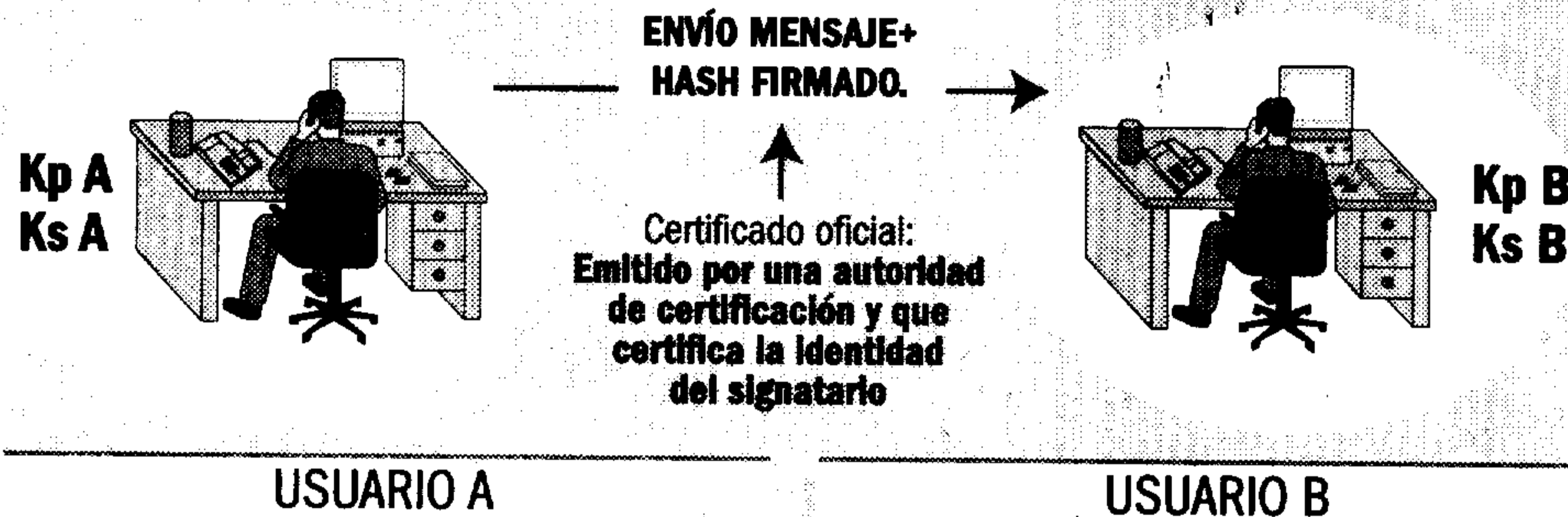
Diez cuestiones para comprender la firma digital

El DNI electrónico permite identificar al emisor de un documento y evitar que suplanten su identidad en las relaciones *online*

El proceso de la firma digital

Clave pública (Kp): El emisor conoce la clave pública del destinatario del mensaje para poder enviarle un mensaje cifrado

Clave privada (Ks): El receptor del mensaje utiliza su clave privada para descifrar el mensaje cifrado (Las dos claves del usuario están insertadas en la tarjeta)



El usuario firma el mensaje con su clave privada

- 1.- Generar un resumen del mensaje hash
- 2.- Cifrar ese hash con clave privada del remitente
- 3.- El emisor envía el mensaje+hash encriptado (hash firmado)

El receptor debe comprobar la validez del mensaje firmado.

- 1.- Descifrado del hash y del mensaje con clave pública del remitente
- 2.- Generar un resumen del mensaje recibido
- 3.- Comparar resumen del mensaje obtenido con el hash recibido para comprobar autenticidad

mensaje firmado con su clave privada a María, quien sabría que es realmente Juan quien se lo envía. Imagínese que ambos no se conocen, quién garantizaría a María esa firma corresponde con la de Juan. En este caso, es aconsejable la intervención de una autoridad de certificación.

4. ¿Qué son las autoridades de certificación?

Son entidades de libre crea-

ción que suministran certificados que garantizan la identidad del firmante, ya sea una persona física o jurídica (empresas). Podrían asemejarse a un notario.

5. ¿Para qué sirve el certificado digital?

En la práctica, mediante un certificado electrónico su titular podrá identificarse ante terceros, firmar documentos electrónicamente asegurando su procedencia y au-

toría, evitar la suplantación de la identidad o encriptar la comunicación de manera que sólo el destinatario pueda verla. Éste certificado puede instalarse en el disco duro del ordenador, y cada vez que se remita un documento que necesita la firma digital lo adjunta.

6. ¿Cuál es la validez de las firmas y los certificados?

Legalmente, la firma digital tiene "el mismo valor jurídi-

co que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio". Así lo refleja el art. 3 del Real Decreto-Ley 14/1999 sobre Firma Electrónica. Técnicamente, puede de-

mostrarse que la firma digital ofrece más garantías que la firma real, ya que no puede duplicarse ni puede ser imitada.

Por su parte, la validez y reconocimiento de un certificado dependerá fuertemente de la credibilidad de la autoridad de certificación que lo emite.

7. ¿Qué tipos de certificados se emiten en Internet?

Hay tantos como usos se puedan imaginar: certificados que garantizan la titularidad de una tarjeta de crédito, o la pertenencia a un club, o la afiliación a un determinado entorno, etc. No obstante, se suele hablar de tres tipos de certificado, en función de la calidad: seguridad baja, media y alta. En

los primeros no existe ninguna comprobación de los datos que se aportan, no tiene valor probatorio, y su uso es meramente promocional. Los certificados de seguridad media van dirigidos al uso interno de las empresas y asociaciones. Los últimos, los de seguridad alta, se pueden usar más o menos como prueba irrefutable de la identidad.

8. ¿Cuánto cuesta un certificado digital?

Las tarifas varían según el tipo de certificado. El precio puede ir desde los 60 euros de los más sencillos hasta los 300 que cuesta un certificado de servidor seguro.

9. ¿En qué soporte se guarda el certificado?

En una tarjeta chip similar a las tarjetas monedero o de Telefónica. En esta tarjeta se almacena la identidad del usuario, al igual que su capacidad de firma. Como ocurre con los teléfonos móviles, sólo podrá acceder su propietario cuando introduzca su número de identificación

personal (PIN).

10. ¿Qué leyes regulan la firma electrónica?

Además del mencionado Real Decreto, esta modalidad está regulada, principalmente, por: la Directiva Europea sobre Firma Electrónica; la Ley SB761 de los Estados Unidos y la Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la Firma Electrónica.

Las autoridades de certificación garantizan la autenticidad de los firmantes

La firma digital tiene el mismo valor jurídico que la versión manuscrita