

# La ley de firma digital abre el camino hacia el futuro DNI electrónico

El Ministerio de Ciencia y Tecnología ha colgado en Internet el proyecto de Ley de Firma Electrónica. Durante un mes el público incorporará sus sugerencias. En principio, la opinión de las autoridades de certificación es positiva

ANA PANTALEONI

España tomó la iniciativa. Pasó por delante de la Unión Europea e incluso de Estados Unidos para aprobar con urgencia un decreto ley de firma electrónica. Era septiembre de 1999. Dos años y tres meses después, el Gobierno ha reformado ciertos aspectos del texto y lo envía al Par-

lamento para tramitarlo como ley. Dos años y tres meses después, la firma electrónica, ese sello que otorga reconocimiento jurídico a las personas que operan en Internet, sigue siendo un tema incipiente. El borrador de anteproyecto de ley de firma electrónica se presentó en el último Consejo de Ministros del año 2001, el 27 diciembre.

“La novedad de este texto radica en que crea un marco legal para el desarrollo del DNI electrónico. La firma es un elemento de seguridad en Internet. El DNI electrónico tiene que acreditar, como el físico, la identidad de una persona en la red. Ése es un primer peldaño; pero luego se realizan actividades en Internet que requieren otro tipo de

certificados. Se trata de otorgar distintos grados de seguridad a distintas actividades”, explica Borja Adsuara, director general para el Desarrollo de la Sociedad de la Información.

El borrador regula el DNI electrónico como una tarjeta equivalente al documento de identidad actual, que incorporará firma electrónica y podrá ser utilizada en las relaciones con cualquier Administración Pública y con particulares y empresas.

Autoridades como CERES, Feste, ACE o Camerfirma han expresado su satisfacción por la inclusión del DNI. “Es importante porque se ofrece un marco legal específico para el DNI; no puede ser una más. Tiene que ser la firma electrónica para la Administración”, dice Sergio Ramón Ruiz Mahillo, de CERES, autoridad pública de certificación.

“¿Cuántos certificados necesitas?”, se pregunta Mahillo. “Yo quiero una cartera con una sola tarjeta para mi relación con la Administración”. Para Ignacio Alamillo, de la Agencia de Certificación Electrónica (ACE), “la inclusión del DNI supone el fomento de nuestra actividad como autoridades certificadoras”.

# Las autoridades de certificación apoyan la futura ley sobre la firma digital

El Gobierno se ha visto obligado a reformar el texto para adaptarse a las novedades surgidas en dos años. El documento regula con mayor detalle la labor de las autoridades y establece sus responsabilidades

El nuevo texto legal de firma electrónica "es bueno porque clarifica cosas que en el real decreto no se habían definido bien o quedaban ambiguas", explica Rodolfo Lomascolo, director de ipsCA, entidad certificadora creada en 1995 y que ha emitido 26.000 certificados. Aunque creen que es mejorable, las diferentes entidades que emiten certificados electrónicos en España están satisfechas con el borrador del Ministerio de Ciencia y Tecnología. Un texto que se verá sometido a debate hasta el 31 de enero.

El director general para el Desarrollo de la Sociedad de la Información Borja Adsuara subraya que, junto a la inclusión del DNI electrónico, otra de las mejoras es un mayor equilibrio en el sistema de responsabilidades. Las autoridades certificadoras se quejaban de que recaía sobre ellas demasiado peso.

Ahora la autoridad puede limitar su responsabilidad definiendo el alcance del uso del certificado. "El borrador intenta hacer algunos retoques sin menoscabar las garantías del usuario", afirma Adsuara.

Desde la Fundación Feste, autoridad vinculada al consejo general del notariado, califican el documento de acertado. "El anteproyecto da carta de naturaleza al DNI digital, lo que supondrá un espaldarazo importante al desarrollo de la firma digital en nuestro país. Además, se hace hincapié en la comprobación previa y simultánea de la identidad y de otras circunstancias personales de los solicitantes. Hay que reforzar el rigor en la identificación de las personas a las que se les dispensa la firma digital", reconoce César Belda, secretario de Feste.

Otra de las novedades es el debate que se abre sobre los certificados de personas jurídicas. El texto reconoce las prácticas que se producen en Internet, donde es habitual que las empresas utilicen su propia firma para fines diversos.

El certificado de persona jurídica no ha sido del agrado de



SUSANNA SÁEZ

## Clave pública y clave privada

El manejo de claves públicas y privadas en la firma digital es distinto al del cifrado de un texto. El poseedor de la firma digital tiene dos claves. Una pública, que comunica a terceros y que puede ser conocida por todos porque es consultable y acompaña al certificado, y una privada, que sólo conoce él. Cuando uno pretende firmar digitalmente un documento, lo ha-

ce con su clave privada, y quien lo recibe lo abre con la clave pública que va unida al certificado. El programa, antes de enviar el documento, le aplica un algoritmo que lo comprime; cuando el documento llega al destinatario, el programa coteja éste con el texto comprimido para comprobar que no ha habido modificaciones durante el envío.

todas las autoridades. Adsuara considera que lo que pretende es generar el debate para después decidir.

## Frenos para su implantación

De forma progresiva, la firma electrónica trata de hacerse un hueco en el día a día del ciudadano. En el último año, varias empresas han optado por instalar el sistema. Sin embargo,

existen ciertos obstáculos que frenan su implantación. Para Rodolfo Lomascolo (ipsCA), "el principal freno reside en que no hay un uso generalizado de Internet por parte de los españoles". Para Ignacio Alamillo (ACE, en la que participa Telefónica), "el problema es que todo el mundo parece estar tan centrado en el concepto de la firma, que no piensan dónde y

cómo utilizarla. Por ejemplo, todo contexto donde emplearíamos un documento escrito es ideal para la firma electrónica, como por ejemplo, las facturas electrónicas, los contratos, los trámites administrativos...". Para Juan Luis Iturralde (Camerfirma, autoridad de las Cámaras de Comercio), "el freno está en la falta de información sobre sus utilidades". César Belda (Feste) explica: "Proyectos como el DNI electrónico me hacen pensar que en muy breve plazo la firma digital va a formar parte de nuestro entorno cotidiano, aunque nos pueda parecer tan rara como en su día lo fueron el fax".

ACE: [www.ace.es](http://www.ace.es)

ipsCA: [www.ipsca.com](http://www.ipsca.com)

CAMERFIRMA: [www.camerfirma.com](http://www.camerfirma.com)

EUROCIBER: [www.eurociber.es](http://www.eurociber.es)

PROYECTO CERES: [www.cert.fnmt.es](http://www.cert.fnmt.es)

FESTE: [www.feste.com](http://www.feste.com)

MCyT: [www.mcytes](http://www.mcytes)

SAFELAYER: [www.safelayer.com](http://www.safelayer.com)

SGL: [www.sgi.es](http://www.sgi.es)

# Un mercado que crece poco a poco

**MERCÈ MOLIST**

A pesar de que aún crece lentamente, el mercado de PKI (Infraestructura de Clave Pública) en España subirá a un ritmo de casi el 100% durante los próximos años hasta llegar, en 2006, a un volumen de negocio de unos 120 millones de euros, según los datos que maneja Safelayer Secure Communications, empresa española que crea tecnología de certificación. Nacida entre Madrid y Barcelona, en mayo de 1999, con 10 personas en plantilla, hoy son 60 y piensan llegar a la

rentabilidad en 2002, mientras abren oficinas en Roma, Múnich, París, Londres y Brasil. "Montar una autoridad de certificación normalita cuesta entre ocho y doce millones", asegura Adrián Moure, de Safelayer, quien considera que "hay poco cliente aún" por desconocimiento y ausencia de reglamentación.

Otro problema es la desorganización, las iniciativas son como reinos de taifas que no hablan entre ellos. Para Roberto López, responsable técnico del Área de Infraestructuras de Clave Pública en SGI Solucio-

nes Globales Internet, no debería ser así: "Una PKI es una estructura jerárquica con una raíz de confianza. Lo ideal sería tener una única raíz, pero nadie se pone de acuerdo en quién está habilitado para ejercer como tal. Por lo tanto, se forman iniciativas diferentes, con lo que el usuario termina teniendo diferentes certificados para hacer cosas muy similares, en ámbitos distintos. Aunque técnicamente esta única raíz es posible, existen dificultades burocráticas y administrativas".

Otro punto débil, que preo-

cupa a los expertos, es la inseguridad de los soportes donde se almacenan los certificados, sean navegadores, tarjetas inteligentes, teléfonos móviles o asistentes personales (PDA). La falta de información técnica sobre los programas de PKI dificulta la tarea de los informáticos que los integran en soluciones de seguridad, como Jorge Hurtado: "Lo mejor sería que los fabricantes proporcionasen el código fuente de sus productos, de forma gratuita o no, para que el resto de la comunidad pudiese verificar la no existencia de puertas traseras".

# Una norma de última hora contempla el papel de los notarios

R. C.

Antes de que el Gobierno presentara el borrador del anteproyecto de ley sobre la firma electrónica en el Consejo de Ministros, introdujo en el dictamen de la Comisión del Senado al Proyecto de Ley de Medidas Fiscales, Administrativas y de Orden social, una serie de modificaciones de la Ley Hipotecaria, del Código de Comercio y de la Ley del Notariado, entre otras, que afectan a las funciones y al funcionamiento de los registradores de la propiedad, mercantiles y de bienes muebles así como a los notarios.

Entre las novedades más destacables de este documento se cuentan la introducción de la escritura electrónica y la obligatoriedad de uso de la firma electrónica avanzada.

La ley exige a todos los notarios y a los registradores que dispongan de sistemas telemáticos para la emisión, transmisión, comunicación y recepción de información, siendo obligatorio para todos ellos a la hora de tomar posesión de una nueva plaza obtener una firma electrónica avanzada.

A efectos prácticos, la normativa permite la generación de lo que se conocen como documentos públicos electrónicos o escrituras electrónica que serán intercambiadas entre notarios y registradores, lo que permitirá la firma de cualquier documento en cualquier notaría e incluso obtener de manera electrónica la tan pesada "unidad de acto" a pesar de no coincidir físicamente en la misma notaría.

Para la abogado Paloma Llana esta ley mantiene el papel de los notarios.

Por ejemplo, en el caso de acreditar los poderes de un empleado para suscribir un contrato, en lugar del problemático camino de la triangulación a través de la autoridad de certificación, si el notario remite una copia digital de los poderes de este empleado, este documento se adjunta en el contrato y solventa el problema.

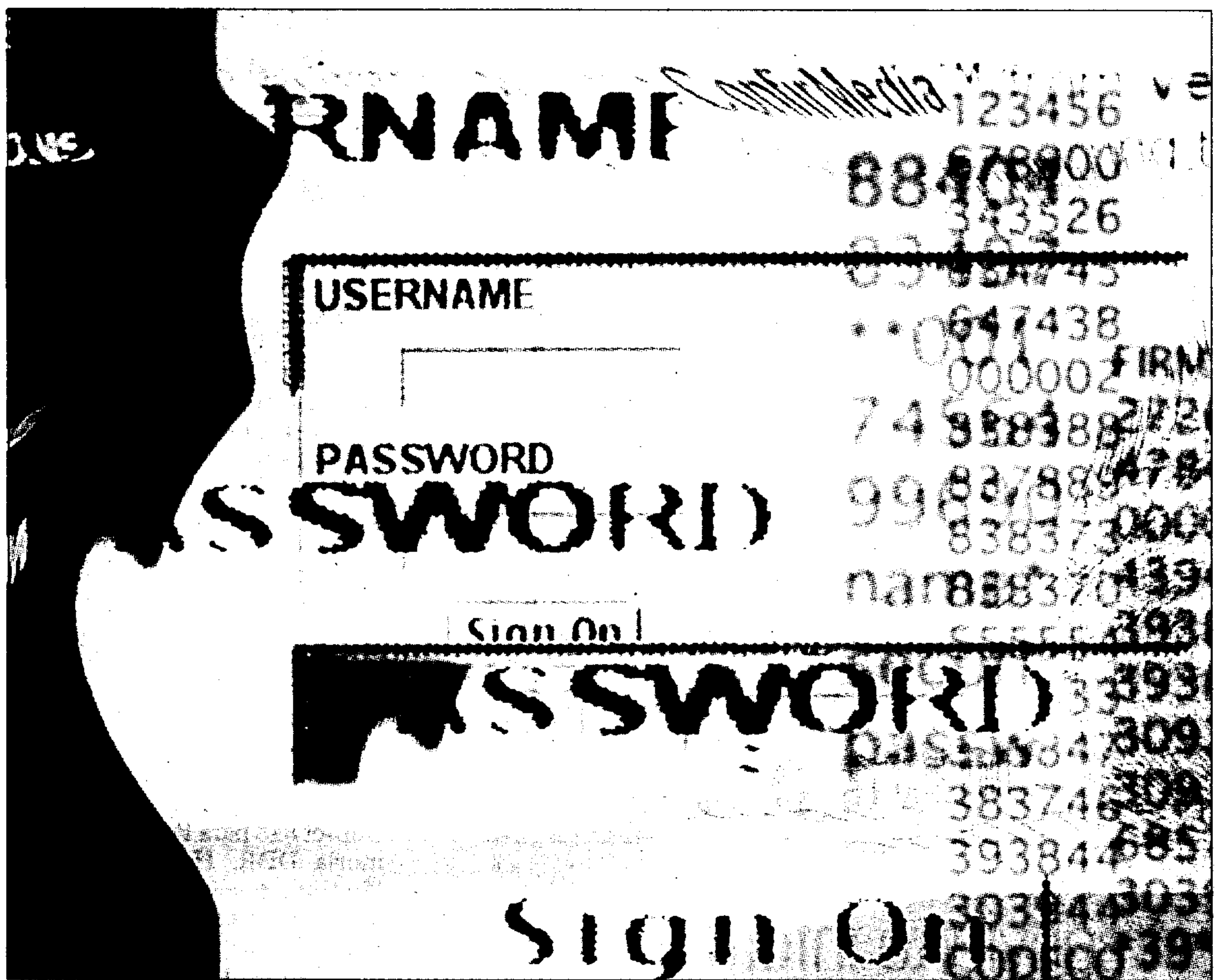
De esta manera, los notarios, que en un momento del proceso, temían perder competencias en favor de las autoridades de certificación, las conservan.

## **Alegría notarial**

Para César Belda, secretario de la Fundación Feste, autoridad de certificación vinculada al Consejo General del Notariado, "no cabe duda de que estamos avanzando. Sin ir más lejos, esta ley ha atendido a una demanda solicitada por el notariado español: dotar de firma digital a los notarios constituyendo al Consejo General del Notariado como entidad de certificación".

Belda explica que "hoy los notarios ya cuentan con el lector de tarjetas digitales y en unos meses todos estos profesionales dispondrán de firma digital".

La autoridad certificadora encargada de suministrar el certificado electrónico será Ceres, en colaboración con la Fundación Feste.



SUSANNA SÁEZ

# ¿Qué es una autoridad de certificación?

Cuestionario básico para aclarar los principales conceptos que se manejan

R. C.

Paloma Llaneza es abogada especializada en derecho informático y cada mes responde a un consultorio jurídico en la revista *Ciberp@ís Mensual*. Este suplemento le ha planteado las preguntas básicas para entender cómo funciona la firma digital.

## ¿Qué es la firma digital?

La firma es un sistema que permite identificar al emisor de un documento. Cuando hablamos de firma electrónica es para distinguir que no se genera manualmente, sino por medio de sistemas informáticos. Hay dos variedades: la firma electrónica simple y la avanzada; de hecho, cuando se habla de firma digital se entiende que hablamos de la avanzada. La simple consistiría, por ejemplo, en digitalizar tu firma manuscrita, conservarla en un archivo de imagen y adjuntarlo cuando remites un documento. No lleva aparejado ningún sistema de seguridad que garantice que el documento es de quien dice haberlo enviado. La firma digital (o electrónica avanzada), por el contrario, permite la identificación del signatario, consiste en un par de claves —la pública y la privada—, tiene que crearse por medios que el signatario mantiene bajo su exclusivo control y permite detectar si se han introducido modificaciones en el documento una vez ha sido enviado.

## ¿Cómo se genera una firma digital?

La firma digital, aunque la ley no lo dice para evitar tener que cambiarla si surgen nuevas tecnologías, se basa en un sistema de cifrado asimétrico con dos claves, una pública y otra privada. Las claves se generan con dispositivos de creación de firma.

## ¿Qué son las autoridades de certificación?

Son entidades de libre creación, aunque por ahora se les exige estar registradas, que suministren los certificados que identifiquen al usuario con su clave pública e, indirectamente, con la privada, con la que mantiene una re-

lación matemática. Los llamados certificados de atribución no sólo garantizan la identidad del firmante, sino que, por ejemplo, si tienen poderes de la empresa para concluir un determinado contrato comercial.

## ¿Es necesaria la intervención de una autoridad de certificación para obtener la firma?

No, basta con disponer del programa informático adecuado. Una empresa, un caso, puede organizar un sistema de firma

## Guerra de autoridades

### ¿Qué pasa si la otra parte contrata una autoridad de certificación distinta de la mía?

La Administración central sólo reconoce en sus relaciones con el ciudadano la autoridad de certificación de la FNMT. Hay que acudir a ella en las relaciones electrónicas con la Administración central. Las autonómicas están iniciando sus propios proyectos de autoridad de certificación, lo que puede conducir a un panorama casi feudal. Según vayan las cosas necesitaremos tantas firmas digitales como administraciones públicas con las que queramos tener relación, a no ser que se acuerden sistemas de reconocimiento mutuo, aunque con el DNI digital esta situación podrá atenuarse. En el caso de empresas particulares, en principio, las autoridades de certificación deberían reconocerse mutuamente. Si una empresa no admite otra autoridad que la que tiene contratada, entonces dependerá del interés de la otra parte en llegar a un acuerdo para que acuda a ella o no. Es una cuestión de poder en una relación bilateral.

digital de sus empleados para los trámites internos de la misma. Para la relación con terceros es más aconsejable obtener un certificado de una autoridad de certificación. Tras una gestión en persona, como en el caso de la FNMT, para cotejar la identidad del signatario, la autoridad emite un certificado que identifica al usuario con su firma digital (más bien con su clave pública). Este certificado puede instalarse en el disco duro del ordenador, y cada vez que se remita un documento que necesita la firma digital lo adjunta. Este sistema tiene un problema. Al estar depositados los datos en el ordenador, existe el peligro de que un pirata entre en él y los consiga. Es preferible conservar el certificado y las claves en una tarjeta electrónica que, a través de un lector, se introduce cuando se quiere firmar. De esta manera, los datos sólo son vulnerables a una intromisión en el instante de la firma.

## ¿Cómo trabaja una autoridad de certificación si se contrata que certifique atributos como, por ejemplo, que tengo poderes de la empresa?

Mientras que el documento con firma digital se envía directamente al destinatario, en este caso se debería acudir a un sistema de triangulación; es decir, en cada operación la autoridad de certificación habría de acudir a datos externos (como el registro mercantil o un colegio de abogados) para comprobar mis poderes. Este sistema está poco extendido ya que no están generalizados los convenios de las certificadoras con bases de datos de terceros. Algunos poderes de un empleado se inscriben en el Registro Mercantil, pero una empresa puede haberle retirado los poderes sin notificarlo al Registro, por lo que la consulta es inútil.

En otros casos, ni siquiera existe esta base de datos. Por ello no se acude a la triangulación. Cuando una empresa solicita una firma digital para uno de sus empleados se concreta el rango de la misma.