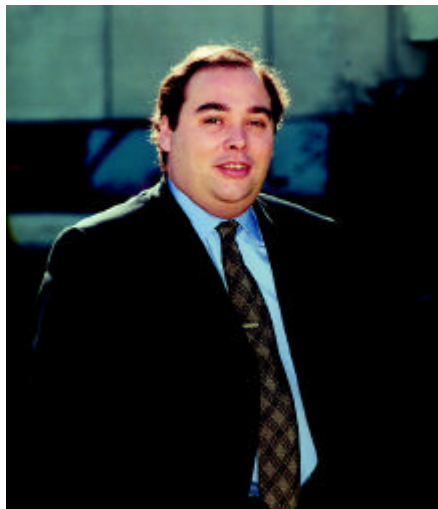


Rodolfo Lomascolo, Director General de IPS Certification Authority

«Ya va siendo hora de que las entidades de comercio electrónico en España se decidan a meter certificados en sus servidores 'web'»

El pasado mes de marzo, IPS, compañía que desde 1995 ha sido pionera en España en la provisión de servicios de certificación electrónica, PKI, consultoría y formación, decidió fundar una filial especializada en los distintos mercados de la seguridad y la confianza: ipsCA. Rodolfo Lomascolo, su Director General, expresa en esta entrevista los planes de la entidad y aporta su personal visión del presente y del futuro de la aplicación de la firma electrónica autenticada en los entornos empresariales y de comercio electrónico.



– ¿Por qué decidieron ustedes fundar ipsCA?

– Tras la publicación del Real Decreto-ley sobre firma, punto de partida para la conformación de un mercado real para la confianza, decidimos separar de IPS, que es la compañía matriz, aquellas actividades propias de tal mercado y, en consecuencia, creamos ipsCA, Internet Publishing Services Certification Authority, en marzo de 2000.

– ¿Quiénes participan en su capital social?

– En un 95% es propiedad de IPS; el resto corresponde a socios que nos apoyaron en el lanzamiento comercial de la empresa, la cual, debido a los derroteros actuales y previsibles de su sector de actividad, tiene una extraordinaria proyección y rentabilidad. Por este motivo, y en línea con lo que están haciendo otras compañías, vamos a dar entrada en el capital social a una entidad que nos permita crecer a las velocidades de mercado, aportándonos imagen y nuevas vías de comercialización. Al día de hoy tenemos muy avanzadas las conversaciones con algunos grupos de inversión y con compañías dedicadas al almacenamiento y transporte de información y documentos.

– ¿Cuál es el abanico de servicios y propuestas de ipsCA?

– Seguimos dos líneas fundamentales. La primera se centra en la provisión de servicios de certificación electrónica. Las posibilidades de negocio como AC son razonables, pero tengo claro que nadie hará dinero vendiendo certificados únicamente, aun siendo como es una actividad estratégica para tomar cuerpo en el mercado. En la actualidad tenemos una base de 25.000 certificados electrónicos emitidos. La segunda línea está constituida por nuestras pro-

puestas de PKI, aplicaciones de firma electrónica autenticada, servicios profesionales en el contexto y formación.

– ipsCA también ofrece consultoría en materia de tratamiento de datos personales...

– Esta era una línea exclusiva de IPS; digo era porque desde hace dos meses en ipsCA también se aborda este nicho de mercado. ¿Por qué? Pues porque los mismos clientes con los que estábamos colaborando para diseñar e implantar soluciones de cifrado y autenticación, nos solicitaban también consultoría en materia de tratamiento legal de datos personales. Y visto desde una perspectiva coherente, hay que reconocer que en ciertos entornos algunos mandatos de la LOPD y sobre todo del Reglamento de Medidas, tienen una solución elegante y con niveles de confidencialidad y autenticación más que óptimos aplicando adecuadamente la criptografía moderna.

La protección de datos personales tiene también un componente jurídico esencial, por ello tenemos acuerdos con algunos bufetes de abogados que ofrecen servicios legales en la materia: Pinto y Asociados, y Omnia. Con este último, ubicado en Mallorca, además hemos trabajado para implantar una AC que le proporcione seguridad interna y en los tratos telemáticos con sus clientes, concretamente en lo que concierne a la contratación electrónica segura.

– En el contexto del mercado empresarial, ¿a quién se dirige ipsCA?

– Nuestro objetivo es la empresa mediana y mediana-grande: Inizia, Catsa... No vamos, por ahora, a las grandes organizaciones: banca, 'telcos'..., aun- que algunas nos han llamado.

– ¿En qué tecnologías se basa ipsCA para ofrecer sus servicios en el entorno de la PKI?

– Por una parte nos basamos en la PKI incorporada en Windows 2000, que es interesante para entornos pequeños y medianos. Ahí ya tenemos clientes importantes con los que estamos trabajando, como por ejemplo Infotel. La solución de Microsoft puede presentar limitaciones en la gestión si hablamos de escenarios con miles o decenas de miles de usuarios; sin embargo tiene sus ventajas: permite empezar de una forma sencilla y con inversiones no superiores a los 5 ó 6 millones de pesetas. No se trata de un sistema de PKI 'pesado', como puedan ser los de Baltimore o Entrust. Además, no todas las organizaciones están en disposición de gastarse varias decenas de millones de pesetas en un software de PKI.

Por otra parte, y para clientes que puedan necesitar, digamos, unos 80.000 certificados, nos decantamos por la solución de Safelayer, porque es flexible y robusta, con independencia de que el interfaz pueda estar más o menos elaborado, cosa que se reduce a una simple cuestión de tiempo. La tecnología de este fabricante va a evolucionar muy bien, sin problemas ni complicaciones.

No obstante, nuestra obligación es conocer todas propuestas de mercado. Por ejemplo, estamos trabajando con Entrust en proyectos no para clientes directos nuestros. Un caso: intervenimos en el proyecto de subasta de deuda pública del Tesoro, la certificación la proporciona la FNMT-RCM, pero el desarrollo de firma electrónica ha correspondido a ipsCA. Y trabajamos para el cliente Entrust y en el entorno Entrust con las herramientas de la FNMT-RCM.

– Y como autoridad de certificación, ¿en qué tecnologías se apoya ipsCA?

– Esta es una línea de negocio distinta y puramente comercial, que se reduce a la venta de certificados. Por razones históricas trabajamos con nuestro propio software, y ocasiones con Windows 2000. El problema de nuestro software es que hay que mantenerlo y evolucionarlo, lo que para nosotros representa una carga, ya que no estamos por la labor de vender software comercial de PKI. Probablemente en un par de meses nuestra estructura de certificación comercial descansa en la plataforma de Safelayer.

La actividad de la certificación comercial tiene la ventaja de que te permite introducir la firma electrónica y los certificados en los entornos de las empresas para luego pasar a mayores. Se da mucho el caso de clientes que no se planteaban hasta hace poco usar el mecanismo de firma electrónica, pero por haber dispuesto de certificados nuestros para algunos de sus usuarios, le han visto las posibilidades y han emprendido proyectos de más amplias miras. Tenemos un caso interesante en el sector de tasaciones hipotecarias.

– Para el desarrollo de la actividad de autoridad de certificación, ipsCA tiene una ventaja poco común en España frente a otros proveedores: que está reconocida en el visor web de Microsoft. ¿Cómo es posible?

– Para las estructuras PKI empresariales, este hecho no es tan importante como para una entidad dedicada a la certificación comercial. El hecho de que los navegadores y los sistemas operativos reconozcan el certificado raíz de tu CA es fundamental.

En 1995 hablamos con Microsoft y con Netscape, que en aquel tiempo llevaba la delantera. Conseguimos entrar en el programa de socios de Netscape, nos

reconocieron como AC, pero, posteriormente, los procesos de cambio y evolución de esa entidad hicieron que nos quedáramos fuera en 1998. Precisamente en ese año, en el que empezaba a despuntar Explorer, teníamos muy adelantadas nuestras gestiones con Microsoft en EE.UU. y tras los exámenes pertinentes: auditorías, documentación, prácticas de certificación..., conseguimos ser reconocidos por esta multinacional. Con todo, esperamos volver a estar reconocidos en el navegador de Netscape en su versión 6, aunque no sabemos si en la *release* primera o segunda. Teleformix, nuestro socio en EE.UU., nos ha ayudado mucho en este asunto. Esto es importante, ya que los administradores de servidores utilizan Netscape mayoritariamente.

– **¿Qué importancia le confiere ipsCA al capítulo de formación?**

– Es una línea esencial para incrementar la cultura tecnológica, pieza básica para generar un mercado dinámico y avanzado, y, además, constituye una actividad mercantil interesante. IPS e IpsCA ofrecen formación en el contexto de la firma electrónica, la PKI y las VPN. A la postre, la formación es un método de evangelización, una necesidad de mercado, un negocio en sí, y un procedimiento para conseguir clientes por la vía legítima de demostrar que entiendes de lo que hablas. En lo que llevamos de 2000 hemos formado a un centenar de personas. Para que se haga una idea, la formación representa entre un 20% y un 30% de nuestra facturación.

– **¿Cuántos clientes tiene ipsCA y qué facturación alcanzó en 1999?**

– Alrededor de cincuenta empresas. El año pasado las facturaciones de IPS y de ipsCA estaban mezcladas. Pero en todo caso podemos hablar de unos 80 millones de pesetas. Este año, nuestra previsión se sitúa en 200 millones de pesetas, y en 2001 preveimos multiplicar estas cifras por ocho o diez.

– **¿No le parece esta previsión para 2001 excesivamente optimista?**

– No. Hasta hace poco no ha habido un mercado real para la confianza. La explosión empieza ahora. A día de hoy, ipsCA tiene ofertas planteadas por valor de 1.000 millones de pesetas, y algunos de los proyectos de aquí a fin de año se mueven en el entorno de entre 100 y 150 millones.

– **¿Se percibe como cara la seguridad?**

– Sí cuando no sabes para qué la quieres. Ahora bien, ¿es cara? Pues todo depende de lo que puedes perder si no la tienes. Al margen de esta explicación ortodoxa, entiendo que no es barata:

los servicios profesionales cuestan dinero, los técnicos bien formados y con conocimientos de estructuras y requisitos de negocio también, el *outsourcing* no es gratis... Tenemos clientes pequeños, por ejemplo despachos de abogados, que han invertido entre 5 y 10 millones de pesetas en una PKI, porque han tenido claro para qué les servía intraempresarialmente y cara al trato con sus clientes. En el caso concreto al que me estoy refiriendo, la PKI la gestiona el propio cliente: no le ha interesado que le prestemos el servicio de externalización, cosa que también entra en nuestra oferta.

– **¿Va a entrar ipsCA en la guerra de la firma electrónica avanzada y los certificados reconocidos?**

– Esa guerra está aún por empezar. Nadie dispone hoy de certificados reconocidos por la sencilla razón de que esa parte del Reglamento de prestadores y de determinados productos de firma está sin desarrollar. Ahora no vamos a gastar cartuchos en eso, aunque a medio plazo iremos en ese sentido. Uno de

los objetivos de la inversión de capital que estamos planteando es, precisamente, estar en disposición de poder asumir los costes de trabajar con firma avanzada y certificados reconocidos. No obstante, quiero que quede claro que las legislaciones europea y la española confieren valor legal a la firma electrónica sin apellidos. La firma electrónica avanzada es un tipo concreto de firma electrónica, y en el fondo, todo se reduce a unos requisitos técnicos y a un problema de prueba.

– **¿Qué opina de los otros actores que configuran el mercado español de prestación de servicios de certificación?**

– FESTE, ACE, FNMT-RCM empezaron hace ya bastante tiempo, cada con un enfoque diferente: Fábrica se orientó hacia las administraciones públicas (ya



«ipsCA dará entrada en su capital a una entidad que le permita crecer a la velocidad de mercado. Están muy avanzadas las conversaciones con grupos de inversión y con compañías dedicadas al almacenamiento y transporte de información y documentos»

veremos como acaba), Feste lo hizo más hacia el registro, ACE a los medios de pago, ispCA al entorno puramente comercial... Ahora surgen iniciativas que copian algunos de estos esquemas, porque nadie quiere perder una parte del pastel. Habrá que ver cómo se va desarrollando Camerfirma, aunque digno es reconocer que la relación de las empresas con las Cámaras de Comercio no es muy fluida. Quizá el asunto, al final, se reduzca a un problema de precios.

– **No cabe duda: la firma, los certificados, las autoridades de certificación, de registro... están de moda. Pero, de pronto, comienzan a aflorar otras TTPs: sellado de tiempo, validación, notariación, almacenamiento y transporte seguro de documentos... ¿No cree que esto causa cierto desconcierto en muchos usuarios?**

– En el escenario de comercio-e que se nos propone, la certificación tiene sentido a efectos de autenticación y firma; y cargando las tintas en la segunda, su uso implica servicios de transporte y almacenamien-

to seguro y perdurable, registro, validación, y alguien tiene que dar esos servicios. Por ejemplo, en el apartado de almacenamiento, qué vamos a pretender, ¿qué todas las tiendas que tienen hoy un certificado de servidor monten un entorno de almacenamiento seguro de documentos por detrás! No, no es razonable. Parece mejor solución, en ese contexto, que existan prestadores que ofrezcan este y otros servicios críticos: son necesarios, y o se los monta uno o los tendrá que contratar. Sería bueno, no obstante, que hubiera estándares definidos, cosa que no ocurre ni en validación ni en sellado de tiempo. Tampoco disponemos de legislación sobre notaría electrónica.

Alrededor del mercado de la confianza hay un gran campo de actividad, especialmente en el terreno de la validación, y no sólo me refiero a la validación de la identidad y de atributos. Por ponerle un caso: con nuestro cliente Infotel estamos hablando de necesidades que van más allá de la autenticación de usuarios/clientes; además de saber quién es quién, interesa conocer qué hay detrás de él, qué poderes tiene, si todavía pertenece a la empresa a la que dice que pertenece, hasta cuánto puede comprar, qué nivel de riesgo tengo con él, qué cuantía de crédito le puedo dar, qué historia tiene... Estos parámetros pueden ir cambiando minuto a minuto, y es necesario conocerlos en tiempo real. Infotel, como le digo, tiene iniciativas al respecto en España, al igual que en EE.UU., principalmente, las tiene Equifax.

Por el contrario, la validación de certificados en línea es un problema técnico que aún no está solucionado completamente. No hay un estándar definido y sí algunas soluciones de fabricante. Es un problema de compatibilidad preocupante, porque incluso lo que hay no termina de funcionar.

– **¿Cuál es el proyecto de certificación más ilusorio en el que ipsCA ha participado?**

– El que iniciamos con Infotel. Tengo que reconocer que no paramos de pensar en cosas para hacer juntos. Este proyecto, rentable para nosotros, consistió en la creación de un entorno de seguridad e implantación de una PKI a la que ipsCA presta confianza, lo que permite a Infotel quedar encadenada a la jerarquía de certificación de Microsoft.

– **Tienen ustedes un importante cliente en USA. ¿De quién se trata?**

– Se trata de Teleformix, un ASP vinculado con *call centers* y tarjetas de fidelización, que ha decidido usar nuestros certificados, en vez

de los de Verisign, para vincularlos con sus entornos de fidelización, entornos de miles de usuarios con tarjeta: Amoco, Texaco... Ésta ha sido nuestra entrada en USA, un mercado inmenso y durísimo.

– **¿Cuáles son sus planes más inmediatos de promoción?**

– Tenemos dos muy interesantes. El primero lo denominamos Servicio de Garantía de Servidores *Web Seguros*, y es gratuito. El segundo lo llamamos Programa de Pilotos de Firma Electrónica. Mediante este programa, ipsCA pone a disposición de las empresas que se adhieran, en unas condiciones económicas muy ventajosas, un sistema completo y los servicios correspondientes (formación, consultoría...) para que puedan realizar internamente proyectos de firma. El lema es: «la forma más sencilla de que una empresa vea las aplicaciones prácticas de la firma electrónica es que las pruebe». **■**

Texto: **José de la Peña Muñoz**

Fotografía: **Jesús A. de Lucas**