tecnimap 2002
www.tecnimap.com
VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
Ponencias

Los PSC como generadores de confianza en los ciudadanos y PKI como herramienta para la gestión interna de las AAPPs

Javier Jarauta Sánchez.

Responsable Preventa para las Administraciones Públicas del Grupo SIA.

1. INTRODUCCIÓN

Sin más que dar un vistazo al lema y temario de Tecnimap'2002: "Jornadas sobre Tecnologías de la Información para la Modernización de las Administraciones Públicas – Administración Electrónica: Transformando el Servicio Público" nos encontramos con los dos aspectos esenciales que a los que se pretende dar solución con la incorporación de las nuevas tecnologías en las AAPP:

- Servicio Público, de cara al ciudadano y a las empresas en sus relaciones con las administraciones.
- Modernización, entendiéndola desde el punto de vista interno, modernizando cada organismo y la relación entre las diferentes administraciones.

Es un hecho sobre el que no vamos a insistir, que una de las tecnologías que más está aportando actualmente y puede aportar en el futuro, para el cumplimiento de dichos objetivos son las Infraestructuras de Clave Pública (PKI). Dicha tecnología ha de considerarse como una herramienta más, en la construcción de la eAdministración y su utilización puede abarcar igualmente los dos ámbitos mencionados:

- Herramienta principal para construir la confianza en la eAdministración de cara al ciudadano, utilizada por los Prestadores de Servicios de Certificación (PSC)
- Herramienta interna para la modernización de los procesos de la Administración, fundamental para aumentar la productividad y competitividad de las AAPP

Las necesidades de cada uno de los entornos son diferentes, y si bien ambas se pueden abordar con tecnologías PKI, ha de realizarse con enfoques diferentes.

En la presente comunicación se presentan modelos de utilización de las PKI y recomendaciones para las AAPP, basadas en experiencias concretas y reales tanto del sector público como del privado, con objeto de que sirva como guía para lograr los objetivos que se identifican en estas VII jornadas.

El hecho de haber implantado y puesto en producción más de 80 PKIs, que abarcan sistemas públicos y privados, nacionales e internacionales, de diferentes tamaños y para múltiples aplicaciones de Internet e Intranet, avalan al Grupo SIA para disponer de una visión global, de las necesidades de las Administraciones Públicas en proyectos de certificación digital y dar una visión del futuro que nos espera, la cual queremos compartir en Tecnimap 2002.

2. PASADO PRESENTE Y FUTURO DE LAS TECNOLOGÍAS PKI

Los avances en las tecnologías PKI se han venido desarrollando desde la aparición en 1976 de la criptografía de clave pública, y del concepto de certificados digitales a finales de los 80, hasta que actualmente podemos considerarla una tecnología madura que está incluso empezando a ser integrada en la gran mayoría de las aplicaciones comerciales que van apareciendo en el mercado.

Su evolución ha sido lenta pero imparable de tal modo que podemos decir que esa lentitud ha servido para confirmar y afianzar a la tecnología PKI como estratégica para abordar la implantación de la Sociedad de la Información.

A principios de la década de los 90 se comenzó a acuñar el término PKI (Infraestructura de Clave Pública) apareciendo los primeros productos comerciales estables hacia 1993. A mitad de la década comenzaron a aparecer las Autoridades de Certificación o Prestadores de Servicios de Certificación que básicamente utilizan la tecnología PKI y una

serie de procedimientos y normas de buen uso para crear las condiciones de confianza y seguridad entre terceras partes, priorizando su utilización en las AAPP para aplicaciones de cara al ciudadano.

Ha sido a principios de ésta nueva década donde se ha empezado a considerar la importancia de ésta tecnología, no solamente de cara al ciudadano, sino también de cara a la modernización interna y optimización de los procesos administrativos.

En resumen, en más de 25 años de existencia de la tecnología de clave pública, se ha pasado de unos inicios incipientes en los que solamente se le veía como una tecnología de nicho, a una expansión quizá excesiva por la aparición de demasiados fabricantes de la misma al hilo de las grandes e irreales perspectivas del comercio electrónico.

Actualmente, la situación se ha estabilizado y van quedando solamente los fabricantes, integradores y prestadores de servicios de certificación que realmente están afianzados y realizando proyectos con contenidos y con tecnología madura. Se están encontrando proyectos de utilización de las PKI en las Intranets, quizá no tan espectaculares como un PSC, pero seguramente más reales y efectivos y en los que se está sacando todo el partido que sin duda tiene todavía ésta tecnología.

El futuro de la tecnología, de unos pocos fabricantes e integradores está garantizado y su utilización masiva por parte de las Administraciones, empresas, empleados y ciudadanos, está igualmente garantizado.

Quizá sea aventurado decirlo, pero seguramente la tecnología PKI tal como la entendemos actualmente, desaparecerá para la próxima década. Estará tan integrada en los sistemas operativos, software de base, aplicaciones, bases de datos, etc. que no nos daremos cuenta de su utilización y pasará a ser una herramienta más de los Sistemas de Información.

No se consumirá tanto tiempo como el que actualmente se le dedica para la motivación y justificación de su implantación, se le habrá perdido el miedo a las implicaciones legales de su utilización y a la posible complejidad de explotación, y será una herramienta más, casi invisible para los usuarios pero con una implantación masiva, como puedan ser actualmente cualquier software de base de datos.

3. LOS ACTORES QUE INTERVIENEN EN LA ADMINISTRACIÓN ELECTRÓNICA

En el teatro de la Sociedad de la Información, existen múltiples escenarios y actores que conviene identificar, analizando su papel, que si bien hace unos años era difuso, actualmente está muy claro y es primordial que se entienda y que cada uno lo ejecute con precisión.

- **Fabricantes de tecnología PKI.** Existen fabricantes especializados o generalistas. La elección de uno u otro ha de estar basada principalmente en su solidez y experiencia tecnológica, estandarización, solidez comercial e implantación local.

  Tras el estallido de hace unos años donde aparecieron una enorme cantidad de fabricantes, se ha llegado a una madurez del mercado, donde solo los grandes y estables o los que disponen de elementos diferenciadores se mantienen. La madurez de una tecnología implica competencia, que ha sido muy dura en los últimos años, pero que finalmente ha situado a cada uno en el lugar que le corresponde. La situación actual es una consolidación de dos o tres tecnologías sólidas, interoperables y con estricto cumplimiento de los estándares.

  El reto actual de los fabricantes es lograr precisamente dicha interoperabilidad entre ellos, lo cual ya está básicamente conseguido, y a su vez posibilitar que la gran mayoría del software comercial pueda trabajar de forma nativa con certificados digitales.

- **Prestadores de Servicios de Certificación (PSC).** La elección de un PSC vendrá dada por los niveles de confianza, seguridad y servicio que aporta, así como su capacidad de despliegue y universalidad de soluciones.

  Al igual que con los fabricantes, hace unos años comenzaron a aparecer múltiples organizaciones y entidades dispuestas a proporcionar éste servicio. La promulgación de la ley de firma electrónica así como el nuevo anteproyecto, abren un mercado de PSC, donde la competencia y el saber posicionarse en el sector apropiado, hará que solamente prevalezcan muy pocos, eso si operando de modo competitivo en cuanto a servicios.

Las tendencias de los PSC están orientadas a proporcionar exclusivamente servicios de autenticación y firma, pero no de cifrado de la información almacenada, cuyo tratamiento (imprescindible en muchos casos) corresponderá a las organizaciones propietarias de dicha información.

- **Consultores e integradores.** La elección de un Integrador es uno de los aspectos más críticos de cualquier proyecto de certificación digital. Existen igualmente especializados o generalistas, cada uno con sus pros y contras. Necesitan disponer de amplios conocimientos de la tecnología PKI en general y específicamente del fabricante seleccionado. Necesitan conocer en detalle las necesidades y requisitos específicos de los usuarios y de las organizaciones y por último disponer de la experiencia y especialización apropiadas en la implantación de proyectos de certificación, tanto externos como internos.

  El papel de los consultores e integradores puede considerarse transcendental en el buen desarrollo e implantación de este tipo de proyectos. Un diseño fuera de la realidad o sin tener en cuenta los requisitos tecnológicos y organizativos de las AAPP, pueden derivar en que el proyecto no se lleve a su fin, o que se quede en un simple piloto.

- **Administraciones.** Ya se ha comentado la gran importancia del papel que juegan las administraciones públicas en el desarrollo de proyectos de firma electrónica. Lo que deben hacer las administraciones es definir las necesidades, tanto internas como externas, identificando las aplicaciones de negocio susceptibles de implantar firma electrónica y que permitan facilitar el acceso a los ciudadanos y optimizar los procesos de sus empleados. Igualmente han de plantear los requisitos que deben cumplir tanto la tecnología PKI como el(los) posible(s) PSC y el integrador del proyecto.

  Las tendencias en cualquier organización son desarrollar sus aplicaciones de tal forma que sean independientes del PSC que se seleccione y de la tecnología asociada. De hecho, lo normal es que las aplicaciones importantes de negocio acepten certificados de múltiples PSC, actuales o futuras, con objeto de no depender de uno solo.

- **Empleados (funcionarios).** Las necesidades de los empleados vienen siempre priorizadas en la facilidad de uso de las herramientas. El objetivo principal de implantación de firma en un proyecto interno es que facilite la labor de los funcionarios, optimizando en tiempo, papel y dinero los procesos administrativos internos. De igual o mayor importancia es el proporcionar herramientas para la confidencialidad de la información que se procesa, restringiendo su uso a los que no tienen derechos y limitando los riesgos de fugas de información.

- **Usuarios (ciudadanos).** El objetivo de los ciudadanos es disponer de una Administración más cercana y ágil, que le facilite todos los procesos administrativos evitando desplazamientos y pérdidas de tiempo frente a múltiples ventanillas. El éxito de cualquier proyecto de cara al ciudadano vendrá dado por la incorporación de un valor añadido importante de la aplicación con firma, frente a lo que se ofrece por los procedimientos normales.

4. EL MERCADO DE LOS PSC Y DE LA TECNOLOGÍA PKI

Toda la legislación sobre firma electrónica tanto nacional como europea, va encaminada a crear un mercado de servicios de certificación, en el que existan múltiples PSC y en el que los ciudadanos, empresas y administraciones puedan seleccionar dicho prestador en un mercado de competencia.

En nuestro país la Administración es la que ha tomado el papel preponderante en la Sociedad de la Información. Los certificados emitidos por FNMT para los ciudadanos que les facilita sus relaciones con las AAPP, así como los futuros DNI electrónicos que permitirán una masiva utilización de firma electrónica son la respuesta de las AAPP de cara a los ciudadanos.

Los PSC pueden actualmente seleccionar una o varias tecnologías PKI e implantarlas de forma integrada para prestar sus servicios. Las tendencias para grandes PSC, sobre todo en la Administración es utilizar multi-tecnología, con objeto de aprovechar las ventajas que aporta cada una de ellas y no depender de un solo fabricante. Hace poco esto parecía imposible dada la competencia existente entre fabricantes, mientras que en la actualidad, la estandarización ha permitido que este tipo de proyectos sea perfectamente abordable.

Por otra parte, las tendencias de mercado en cuanto a PSC a nivel europeo es la utilización de una identidad digital basada en certificados cualificados (RFC 3039) que disponen de un certificado para autenticación y otro para firma (no repudio).

Aunque las tecnologías PKI actualmente amplían la utilización en un certificado más por usuario para realizar el cifrado de la información (3 certificados por usuario, autenticación, firma y cifrado) es un aspecto que ninguno de los PSC actuales o futuros tiene contemplado.

El certificado de cifrado se deja normalmente para las propias organizaciones que son las propietarias de la información, dada la necesidad de realizar backup y gestión de las claves de dicho certificado, aunque la tecnología PKI lo permita, no es una función propia de los PSC.

5. REQUISITOS Y NECESIDADES INTERNAS Y EXTERNAS DE LAS AAPP

Es indudable las diferentes necesidades que existen en la AAPP en cuanto a la implantación de firma electrónica si se trata de proyectos internos o externos. Hasta el momento, la gran difusión de la firma electrónica viene por parte de los proyectos de cara al ciudadano, pero ha llegado el momento de modernizar la Administración por dentro, para lo cual la tecnología PKI juega un importante papel.

Los requisitos para proyectos de cara al ciudadano vienen fundamentalmente dados por la sencillez en la utilización de los certificados y la utilización de un solo certificado para toda la tramitación administrativa. La realidad de la situación actual o futura es que cada ciudadano va a disponer de varios certificados diferentes para realizar sus trámites frente a las diferentes administraciones (FNMT, Autonomías, etc.) hasta que se utilice el DNI electrónico como identidad digital común. Estos certificados pueden considerarse más como un derecho de los ciudadanos y que las administraciones han de proporcionarle.

Los requisitos de modernización interna de las administraciones requieren la utilización de firma electrónica por parte de los funcionarios. Aquí viene la pregunta, ¿es razonable que un funcionario, o el secretario de estado de un determinado ministerio, utilice su certificado FNMT con el que presenta su declaración de la renta, para firmar o cifrar documentos de procesos internos del ministerio al que pertenece? Parece que la respuesta debe ser negativa. Desde el punto de vista de las AAPP, para procesos internos han de cumplir al menos los siguientes requisitos:

- Poder controlar las políticas de registro, y de seguridad de sus funcionarios y sus procesos, que serán diferentes para cada administración
- Poder controlar la información que se cifra con el certificado de un funcionario, con capacidad de recuperarla, aún si dicho funcionario ha perdido el certificado.

- Poder revocar certificados de funcionarios que cambian de posición, abandonan el ministerio, que hacen mal uso del certificado, etc.
- Disponer del concepto de "usuarios vivos" es decir, poder reutilizar los certificados dentro de la organización.
- Poder disponer de un sistema de Single Sign On a las aplicaciones internas, con autenticación fuerte de los usuarios
- Poder definir en los certificados extensiones específicas para la organización, como puesto del funcionario, capacidad o nivel de firma que posee, correo electrónico oficial del funcionario, etc.

En general, todas estas funciones no pueden realizarse con los certificados que cada funcionario dispone por ser ciudadano, además (y legalmente hay que tratar con mucho cuidado) no se deberían de mezclar los aspectos personales con los profesionales. Imitando al modelo físico actual, todos como ciudadanos disponemos de un DNI, pero a su vez disponemos de un identificador específico de la organización a la que pertenecemos (tarjeta de funcionario, etc.) que utilizamos en el entorno laboral. Cuando se requiere se utiliza el DNI, pero a efectos de que nos emitan una nueva identificación.

Las anteriores consideraciones nos llevan a la conveniencia de utilizar un sistema de certificación digital interno para cada organización, y específicamente diseñado y configurado para sus necesidades particulares, que diferirán de las de otras administraciones.

El hecho de que dichos servicios de certificación se realicen por un PSC externo a la administración en cuestión, o por una PKI interna explotada por la propia administración (puede ser en modo de Insourcing o Intasking) es una decisión a tomar en cada caso.

6. LA PKI COMO HERRAMIENTA PARA LA GESTIÓN INTERNA

Una vez identificada y justificada la necesidad de las administraciones públicas de utilizar múltiples PSC para sus relaciones de cara al ciudadano, y una PKI interna para la optimización de sus procesos internos, trataremos de argumentar las ventajas de implantar su propia PKI en lugar de acudir a un PSC para proyectos de certificación digital en sus aplicaciones de negocio.

En primer lugar es difícil que un PSC se adapte a los diferentes requisitos de cada administración, y que sea capaz de prestar el nivel de servicio que se requiere para los procesos de negocio. Ya se ha dicho que por ejemplo la capacidad de cifrado y recuperación de la información, no es un servicio que presten los PSC. Las organizaciones son dinámicas y requieren actuaciones y reconfiguraciones rápidas que se realizan internamente.

Varios han sido los aspectos que han frenado las implantaciones de la tecnología PKI internamente en las organizaciones y que trataremos de desmitificar:

- Las implicaciones legales del uso de la firma electrónica. El nuevo anteproyecto de ley de firma clarifica totalmente las responsabilidad de uso de firma en procesos internos, facilitando así su implantación para la modernización de las Administraciones y organizaciones privadas.
- La complejidad en la implantación y explotación de la PKI. Dada la madurez actual de la tecnología, y basándose en un integrador experimentado, la implantación de una PKI no es más compleja que cualquier software de base de datos, portales o servidores de aplicaciones. Respecto a la explotación, actualmente el software PKI está tan automatizado y preparado para grandes cantidades de usuarios, que se requiere una mínima intervención de personal interno a tiempo parcial para su explotación, y con una formación que fácilmente pueden proporcionar los integradores.
- La falta de estándares e interoperabilidad del software PKI. Actualmente todos los fabricantes cumplen estrictamente los estándares e interoperan entre sí y con las aplicaciones que admiten certificados digitales, como lo demuestran proyectos actualmente en producción.

En resumen, deberíamos de considerar el software PKI como una herramienta más de los Sistemas de Información, no siendo ni más fácil ni más difícil de ¡mplantar y gestionar que el resto de las herramientas. La PKI es la herramienta básica para los Prestadores de Servicios de Certificación, pero las Administraciones han de considerar la utilización tanto de dichos PSC, como de la herramienta propiamente dicha para cubrir todas sus necesidades.