Plataforma de Certificación Digital de la Generalitat Valenciana

Autores:
Enrique Vall Muñoz
Jefe del Servicio de Sistemas y Telecomunicaciones
Joaquin Galeano Senabre
Responsable de Sistemas del Servicio de Sistemas y Telecomunicaciones

OBJETIVO :

Conseguir una infraestructura de Clave Pública que de cobertura en este tipo de tecnologias a todo el entorno administrativo de la Generalitat Valenciana, proporcionando la base de conocimientos suficiente a desarrolladores y administradores para modificar los aplicativos existentes y realizar los nuevos desarrollos con esta plataforma.

1. Introducción

La evolución de los sistemas de información y de las telecomunicaciones está posibilitando el cambio de las relaciones entre individuos y organizaciones en todo el mundo. Estas nuevas formas de relación abren una serie de posibilidades, tanto para ciudadanos como para empresas, a la hora de comercializar productos y servicios de una forma rápida, cómoda y económica. La implantación de servicios consumidor-empresa y empresa-empresa es ya una realidad cada vez más asumida y adoptada por todos. De forma similar, la relación entre el Ciudadano y la Administración Pública se puede beneficiar de este tipo de tecnología.

A parte del hecho de posibilitar no sólo nuevas formas de dar los servicios sino también de posibilitar nuevos servicios, la diferencia introducida por este cambio en los comportamientos de relación comercial o administrativa viene dada por la sustitución del soporte papel por soportes electrónicos. Este cambio de soporte ha provocado la transposición de algunos mecanismos de garantía, tanto desde el punto de vista legal como del comercial, necesarios para equiparar efectivamente las nuevas formas de relación con las clásicas: los documentos típicamente contienen firmas y fechas, necesitan protegerse de posibles falsificaciones o revelaciones de contenido.

Aunque la garantías necesarias dependen del contexto de la organización y del tipo de información implicada, las más destacables son las siguientes:

- El remitente de la transacción ¿es realmente quien dice ser? (**autenticación / control de acceso**)

- La información recibida, ¿es igual a la que fue enviada? (**integridad de la información**)

- La información enviada, ¿habrá podido ser espiada por un tercero? (**confidencialidad de la información**)

- ¿Podrá el remitente negar que la ha enviado, o el destinatario que la ha recibido? (**no repudio**).

1.1. Fundamentos de la firma electrónica

La solución a los problemas que puede plantear el disponer de esta serie de garantías pasa por la utilización de mecanismos criptográficos. Estos mecanismos se basan en funciones matemáticas empleadas para cifrar y descifrar la información. Cifrar es el proceso de transformar la información de tal manera que sólo sea inteligible por su destinatario; por otro lado, descifrar es el proceso por el cual se hace inteligible la información cifrada.

Con la mayoría de los métodos actuales de criptografía, la seguridad no se basa en el secreto del algoritmo criptográfico empleado, que suele ser ampliamente conocido, sino en un parámetro de dicho algoritmo llamado **clave**, que se emplea para cifrar, para descifrar o para ambas cosas, dependiendo del tipo de algoritmo criptográfico empleado.

1.1.1. Certificación digital

Las garantías de seguridad anteriormente descritas son necesarias para poder transponer determinados procedimientos de negocio o administrativos. No obstante, la utilización de la criptografía de clave pública sin más plantea un importante problema de base que hemos obviado deliberadamente hasta este momento: se ha partido de la premisa de que todos los usuarios conocen todas claves públicas y que saben a qué usuario pertenece cada clave pública.

Es necesario establecer un mecanismo que garantice que una clave pública pertenece realmente a quien se supone que pertenece. Este problema se soluciona con la utilización de **certificados digitales**.

Un certificado digital puede definirse como el medio por el que se vincula cierta información correspondiente a una entidad (nombre, apellidos, NIF, etc.) con una clave pública. El certificado digital viene a ser un documento electrónico, firmado digitalmente por una tercera parte

confiable (Autoridad de Certificación; CA en adelante) en el que se establece la relación entre un sujeto y su clave pública.

1.2. La infraestructura de clave pública (PKI)

Una infraestructura de clave pública o PKI (de ***Public Key Infrastructure***) es el conjunto de elementos de seguridad y sistemas criptográficos que permiten el establecimiento de los más altos niveles de seguridad de una forma flexible y con un coste de gestión razonablemente bajo. Gestionando claves y certificados a través de una PKI, una organización posibilita la utilización de servicios de firma electrónica y cifrado en una amplia variedad de aplicaciones y establece y mantiene un entorno de red seguro.

1.2.2. Funciones y usos de una PKI

El objeto final de una PKI es securizar las transacciones electrónicas de una organización con su entorno. La implantación de una PKI permite a una organización proporcionar, entre otros, los siguientes servicios:

- Tecnología para firmar digitalmente y/o cifrar documentos.

- Ofrecer la plataforma para que los servidores puedan ser certificados y garantizar así la autenticidad de éstos y la confidencialidad e integridad de los datos.

- Servicios de acreditación fuerte para el acceso de usuarios a servidores (por ejemplo acreditación de cliente mediante SSL sobre redes IP o WTLS sobre redes WAP).

- Plataforma para firma de código (generación de código software confiable).

- Certificación temporal o generación de sellos de tiempo.

En muchos casos la implantación de una PKI en determinadas organizaciones puede resultar casi obligada para poder afrontar las obligaciones y las garantías de seguridad de los datos exigidas por la Ley (por ejemplo el Real Decreto 994/1999, de 11 de junio).

1.3. Marco legal

En España, en lo que a Infraestructuras de Clave Pública se refiere, el marco legal viene determinado por el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica y a nivel europeo por la Directiva del Parlamento Europeo sobre firma electrónica.

El Real Decreto-Ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios de certificación en España. Se definen, entre otros, los conceptos de firma electrónica (“*conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que las recoge*”) y de firma electrónica avanzada (“*la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos*”).

Asimismo se establecen los requisitos para la existencia de un certificado reconocido, la vigencia de los certificados, las obligaciones de los prestadores de servicios de certificación, un régimen sancionador y las garantías para afrontar responsabilidades por daños y perjuicios.

Por otro lado, la Directiva europea tiene por finalidad garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, instituyendo un marco jurídico homogéneo y adecuado para la Comunidad

Europea, y definiendo criterios que fundamenten su reconocimiento legal.

En ambos documentos se recoge que, la firma electrónica avanzada, es aquella que siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba de juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

2. La Firma Electrónica en la Generalitat Valenciana

La Generalitat Valenciana, al igual que otras administraciones tanto autonómicas como locales, se encuentra actualmente en los inicios de la implantación de las tecnologías que posibilitarán el uso de los servicios de firma electrónica y el desarrollo de aplicaciones telemáticas que requieren de estos servicios para su correcto desarrollo.

El actual estado de la tecnología junto con la regulación de que ésta ha sido objeto forman un marco suficiente como para poder afrontar en este momento el desarrollo de aplicaciones destinadas tanto a la mejora de los procedimientos administrativos internos como a ofrecer nuevos servicios al Ciudadano o mejorar algunos que ya se están dando.

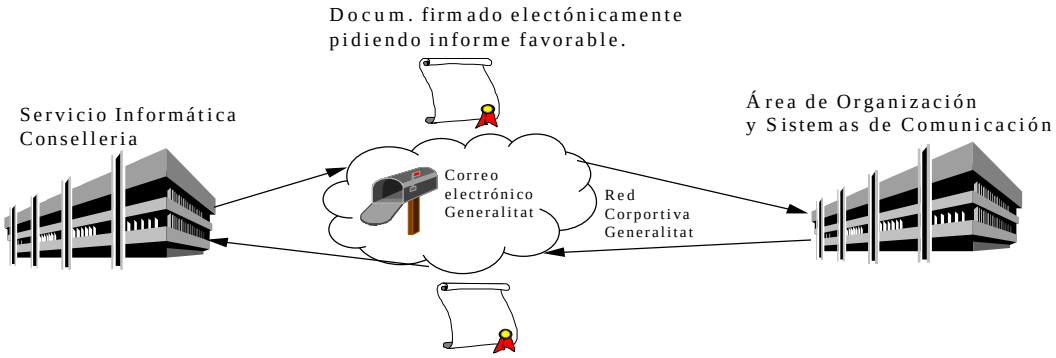
2.1. Experiencias y pilotos desarrollados

Desde la D.G. de Telecomunicaciones y Modernización se han venido estudiando las diferentes tendencias de las tecnologías criptográficas y, en menor medida, la normativa de soporte desde hace más de tres años. Durante este periodo de tiempo se han mantenido conversaciones con algunos prestadores de servicios de certificación, se ha estudiado la problemática en la aplicación de estas

tecnologías e incluso se han desarrollado algunas aplicaciones piloto.

El primero de estos pilotos fue desarrollado hace tres años y consistió en una aplicación que incorporaba firma electrónica con tecnología PGP para el Registro de Convenios. Esta aplicación piloto estuvo funcionando durante varios meses y sirvió para revelar la ventaja del uso de la firma electrónica frente a la tramitación en papel. El problema a resolver en este primer piloto consistía básicamente en la eliminación de los envíos de documentación en papel para agilizar las tramitaciones. Para ello debian darse las mismas garantias: **autenticidad** de los envíos, **integridad** de la información enviada y **conservación** de ésta. Esto se consiguió utilizando firma electrónica junto con una serie de mecanismos, transparentes al usuario, de almacenamiento seguro de la información que se remitía.

Experiencia piloto de transferencia electrónica de documentos de forma segura.



El mayor escollo que presentaba esta solución era la dificultad de gestión de usuarios/claves. Más adelante se vio que surgía una tecnología basada en certificados digitales que permitía flexibilizar la gestión de usuarios y mejorar los niveles de seguridad, por lo que se abandonó la vía de PGP a favor de la filosofía de "confianza centralizada", que es por la que actualmente se ha optado mayoritariamente.

En este sentido se llevó a cabo el desarrollo de una Autoridad de Certificación piloto (accesible en http://ca.gva.es y cuya página principal del interfaz web se muestra en la siguiente figura) que permitiera conocer

en detalle la tecnología, su forma de extensión a aplicaciones y los problemas que planteaba a la hora asimilar la confianza de las firmas manuscritas a los procesos sin papel con firmas electrónicas.

Esta Autoridad de Certificación piloto ha venido sirviendo desde entonces para probar la emisión de distintos tipos de certificados (certificados de cliente, certificados para distintos servidores web, etc), para probar el comportamiento de protocolos de securización de sesiones TCP (SSL para servicios web, FTP y telnet) e incluso llevar a cabo el desarrollo de aplicaciones con uso de tecnología de PKI.

De manera paralela se han ido revisando y modificando algunas estructuras de servicios para facilitar su adecuación a la PKI. Los que más repercusión han tenido han sido la introducción del servicio de mensajería Internet corporativa y la labor que se viene desarrollando para la integración de diversos directorios de la Generalitat y organismos con los que se colabora, destinada a la consecución de un directorio LDAP con información lo más completa posible y de calidad. Este directorio LDAP será, entre otras cosas, futuro soporte del repositorio de certificados digitales y base de la publicación de éstos.

Actualmente se están empleando certificados digitales emitidos por esta CA experimental en pilotos de envíos seguros entre organismos internos a la Generalitat con el correo electrónico como transporte (usando S/MIME) y también desde organismos externos a otros internos, permitiendo alcanzar el grado de confianza suficiente para enviar de forma electrónica por la red determinados envíos

de información crítica que antes se realizaban sin hacer uso de ningún medio telemático (mediante envíos de cintas o discos a través de empresas de mensajería), con el consiguiente ahorro de tiempo y dinero, y mejora del nivel de seguridad. De entre estos pilotos, el más destacable por el número de usuarios y por utilizar tanto firmado como cifrado es el de envíos de ficheros de información de liquidaciones desde más de 70 Oficinas Liquidadoras repartidas por toda la Comunidad.

2.2. Proyecto FIRMA

Ante la actual situación legal y de la tecnología y ante la demanda de servicios de PKI que desde otros proyectos se viene generando, se ha considerado adecuado desarrollar un proyecto de implantación formal de una PKI para, fundamentalmente:

- Poder ofrecer los servicios de certificación necesarios: se trata de disponer de todos los elementos de una PKI necesarios para la emisión de certificados, gestión de usuarios, control de revocados, etc. sin los cuales no es factible afrontar aplicaciones que hagan uso de mecanismos criptográficos.

- Ofrecer un conjunto homogéneo e interoperable de soluciones criptográficas: dar un entorno común a toda la Generalitat que facilite la gestión de recursos, reduzca costes de infraestructura y garantice la compatibilidad de las soluciones.

- Poder asesorar en cuanto a las diferentes soluciones disponibles ante los problemas que plantean otros proyectos: favorecer la incorporación de la tecnología de PKI en las aplicaciones a través del asesoramiento en aquellos proyectos que lo requieran e incluso colaborando en las fases de análisis e implementación inicial de aplicaciones. Esta labor se viene desarrollando hasta ahora de una forma muy limitada y siempre en base a pilotos.

2.2.1. Contratación de una plataforma de certificación

Con este proyecto, que se ha dado en llamar FIRMA, se pretende, pues, implantar una Infraestructura de Clave Pública en explotación y que cumpla con todos los requisitos legales. Esta pretensión pasa por la adquisición del equipamiento hardware/software y soporte necesario, para lo que, en breve, se publicará un concurso para este suministro.

Esta contratación tiene dos vertientes. Una destinada a la implantación de la PKI de la Generalitat Valenciana y otra, quizá más importante, destinada a dar soporte a proyectos relacionados con la firma electrónica y formación en estas nuevas tecnologías al personal que se considere conveniente.

La implantación de la PKI consistirá básicamente en:

- Instalación de servidores (hardware + software) para los elementos básicos de la PKI: CA, RAs, servidores OCSP para control transparente de revocados, TSA para procesos de fechado, etc. De manera paralela se intentará implantar un entorno de test-desarrollo muy similar al de explotación y que se destinará a tareas de pruebas y desarrollos.

- Instalación inicial de un número limitado de operadores de Autoridad de Registro y otros módulos de cliente.

- Establecimiento de las Políticas de Certificación y circuitos de gestión de usuarios/certificados.

En el caso de los pilotos actuales que se decida poner en explotación se realizarán las tareas de sustitución de certificados, redacción de los procedimientos de uso de los certificados, ámbito de aplicación, periodo de validez, etc. Eventualmente y por decisión de los responsables de esos pilotos, se reemplazarán los soportes de los certificados (actualmente en discos o disquetes) para pasarlos a tarjeta.

La otra parte de la contratación se destinará a dar a conocer la PKI y facilitar la integración de ésta en las aplicaciones. Esto se puede traducir en:

- Dar a conocer los servicios de PKI a los responsables técnicos de proyectos. Se plantea la formación completa en cuestiones de PKI de un grupo de asesoramiento, sin descartar la formación específica para responsables de aplicaciones y de sistemas.

- Ofrecer las herramientas de integración de aplicaciones sobre la PKI, tanto a nivel de módulos cerrados como a nivel de librerías de desarrollo. Se procurará disponer de un conjunto completo de herramientas para el desarrollo sobre PKI a fin de poder afrontar las fases de análisis y pruebas de las aplicaciones que se planteen.

- Soporte técnico para llegar, inicialmente, al desarrollo de módulos específicos y a medida por parte de la empresa adjudicataria.
Está fuera del objeto de esta contratación el desarrollar las aplicaciones que se planteen dentro de los distintos proyectos que surjan en la Generalitat, pero se pretende dar un fuerte soporte en las primeras aplicaciones o en las fases iniciales de éstas cuando sea necesario.

2.2.2. Desarrollo y cronograma previstos

Dada la complejidad de la implantación de una infraestructura completa de estas características que conlleva, a parte de la instalación de equipamiento, la formación de personal, la redacción de documentación de procedimientos de certificación y, posiblemente, el establecimiento de acuerdos con otros prestadores de servicios de certificación, se prevé que la implantación hasta la puesta en explotación definitiva se extienda durante varios meses. El cronograma que se está barajando es el siguiente:

Fase 1ª (mes 0- mes 4 / septiembre de 2000 – enero de 2001):

- formación de personal de gestión de la PKI

- diseño de la estructura básica
- redacción de documentación de prácticas de certificación
- implantación del entorno de test

Fase 2º (mes 4 – mes 10 / enero de 2001 – julio de 2001):

- implantación del entorno de explotación básico
- formación específica a desarrolladores y responsables técnicos
- puesta en explotación de pilotos existentes

Fase 3º (mes 10 en adelante / julio de 2001 en adelante):

- extensiones del entorno de explotación básico para la adecuación a proyectos que lo requerirán
- participación en fases iniciales de desarrollo de aplicaciones.

2.3. Conclusiones

Con el proyecto FIRMA se pretende introducir de manera formal y definitiva las tecnologías criptográficas necesarias para el soporte de la Firma Electrónica y sus servicios asociados. Con ello, se espera poder facilitar el camino del desarrollo de proyectos reales de teleadministración y de proyectos que agilicen multitud de tramitaciones internas de la Administración Valenciana.

Por otra parte, es necesario destacar que FIRMA no pretende cubrir el desarrollo de aplicaciones sino únicamente servir de punto de partida inicial, de base tecnológica común y de soporte para que los distintos departamentos de la Generalitat desarrollen sus proyectos sobre esta PKI e incluso, si se considera necesario, extiendan la PKI ellos mismos, llegando a disponer de sus propios servicios de Autoridad de Certificación y de Registro, sin perder de vista una estructura de certificación coherente a lo largo de toda la Generalitat Valenciana.