COMUNICACIÓN PARA TECNIMAP 2000 PRESENTADA POR SIA, SISTEMAS INFORMÁTICOS ABIERTOS.

Correspondiente al punto del temario:
Aspectos tecnológicos de la Administración Electrónica.- Infraestructura tecnológica en materia de seguridad para las transacciones con las Administraciones Públicas.
Documento realizado en **Word 6.0- MS Office 97**

Persona de contacto para Comunicaciones y evento Tecnimap 2000: Magdalena de Salazar Serantes (Dtora. Marketing). msalazar@sia.es
Tel: 91-307 79 97 / Fax: 91-307 79 80
C/ Gobelas 47-49 28023 MADRID

TÍTULO: INFRAESTRUCTURAS DE CLAVE PÚBLICA COMO GARANTÍA DE SEGURIDAD EN LAS TRANSACCIONES CON LA ADMINISTRACIÓN ELECTRÓNICA

AUTOR:
Enrique Palomares del Amo
Director General
SIA, SISTEMAS INFORMÁTICOS ABIERTOS, S.A

RESUMEN DE LA COMUNICACIÓN

El factor seguridad se ha convertido en el principal protagonista de las transacciones electrónicas, tanto para la Administración Pública como para las empresas privadas. En la presente comunicación se presenta la solución de Infraestructura de Clave Pública o PKI de Entrust como arquitectura completa que posee todos los elementos necesarios para asegurar la privacidad y la autenticidad de los datos en un momento en el que, con el desarrollo de Internet, Las Administraciones Públicas se han abierto al exterior a la hora de intercambiar información con ciudadanos, empresas y organismos gubernamentales.

BREVE HISTORIAL PROFESIONAL: Enrique Palomares del Amo

Licenciado en Ingeniería de Telecomunicaciones por la ETSIT de Madrid.
Socio fundador y Director General de SIA desde 1989, cuenta con una dilatada experiencia en sector de las Tecnologías de la Información.

INTRODUCCIÓN

El progresivo empleo de la informática en la actualidad ha motivado una indiscutible sensibilización tanto por parte de la Administración Pública como por las empresas privadas de la implantación de medidas de seguridad electrónicas para asegurar la confidencialidad de toda aquella información transmitida por la red.

Poner la información administrativa a disposición del ciudadano, establecer nuevos canales de relación, facilitar la tramitación administrativa, eliminar papeles, olvidar el *"vuelva usted mañana"* Todas las frases hechas, tan frecuentemente utilizadas, empiezan a ser una realidad. Se han ido eliminando, paulatinamente, las barreras que dificultaban el desarrollo de la Administración telemática. La tecnología aporta todos los elementos necesarios, siendo además cada vez más accesible desde el punto de vista económico. Del mismo modo, la normativa legal está suficientemente desarrollada como para dar marco de legalidad a proyectos de este tipo.

La accesibilidad a la información es una de las premisas que busca el usuario a la hora de consultar cualquier documento, público o privado, pudiendo convertirse en un arma de doble filo. Con el fin de evitar posibles filtraciones en una información transmitida por la red se han creado métodos de seguridad que la intentan proteger al máximo. La visión de mantener una defensa electrónica, en la propia empresa o institución, debe extenderse a todos los componentes del sistema, haciéndose imprescindible la dotación de procedimientos que determinen su seguridad.

AUTORIDADES DE CERTIFICACIÓN

Es imprescindible la creación de una Autoridad de Certificación (CA), primer paso para dotar de seguridad a las comunicaciones electrónicas. La funcionalidad de una Autoridad de Certificación es comparable con la de un organismo gubernamental encargado de emitir Certificados Digitales, permitiendo establecer relaciones de confianza entre diferentes grupos o usuarios. Se trata, en definitiva, de verificar la identidad del propietario a través de la Agencia de Certificación, del mismo modo que el pasaporte es un documento que certifica que el ciudadano es efectivamente quien dice ser y nadie duda de ello.

PKISs O INFRAESTRUCTURAS DE CLAVE PÚBLICA

La Autoridad de Certificación no puede considerarse como algo aislado, se requiere la existencia de las denominadas Infraestructuras de Clave Pública. Se conoce como Infraestructura de Claves Públicas o su acrónimo en inglés PKI (Public Key Infrastructure), al sistema global necesario para proveer a una Organización de los servicios

de cifrado y de firma digital basada en claves públicas.

Una PKI puede definirse como una entidad de certificación electrónica más lo necesario para su funcionamiento, fundamentalmente una estructura de directorio. Su propósito es gestionar claves y certificados para que una organización mantenga un entorno de red fiable.

Hay que destacar que una PKI ofrece confianza en las relaciones mantenidas en tres diferentes escenarios claramente delimitados: entre Administraciones Públicas (correo o boletín oficial), entre ciudadanos y las Administraciones Públicas (registros de la propiedad), y entre las compañías y las Administraciones Públicas (impuestos corporativos, trámites de la sociedad, etc.). En cualquiera de los tres supuestos los beneficios de las nuevas tecnologías conllevan una *mejora en la provisión de los servicios públicos* adecuándolos a los tiempos modernos, *incrementando la productividad* y, a gran escala, la *coordinación internacional*. En realidad tal oportunidad supone un trabajo. Es necesario entender que no sustituimos una tecnología por otra, lo que estamos haciendo es añadir algo más. Se trata, en definitiva, de poner en manos del

ciudadano las aplicaciones informáticas necesarias para mecanizar sus acciones con la Administración.

Desde el punto de vista del usuario final, las relaciones con la Administración Pública se mantienen de la manera más fácil y cómoda posibles. En este recién inaugurado siglo, realizar un trámite administrativo ha dejado de ser una odisea para convertirse en una gestión más. La revolución de las tecnologías de la información y el desarrollo de la infraestructura de comunicaciones está haciendo cambiar significativamente las relaciones entre individuos y organizaciones tanto en España como en todo el mundo.

Partiendo de la base de que un documento emitido en soporte electrónico y firmado digitalmente es igualmente válido que un documento firmado en papel y está sometido a la Ley y a la directiva sobre Firma electrónica, cualquier trámite administrativo tiene la misma fiabilidad tramitado a través de transacciones electrónicas que si acudiéramos a la sede para gestionarlo personalmente. Con este avance, los usuarios se beneficiarán de un amplio abanico de ventajas. El poder realizar las operaciones electrónicas desde cualquier PC, empleando las correspondientes claves, hace que el usuario no se vea en la necesidad de desplazarse para ejecutar sus trámites, ni alejarse de su propio hogar o lugar de trabajo. Paralelamente se produce la consiguiente reducción de costes y tiempo por ambas partes, ampliando el servicio durante las 24 horas del día los 7 días de la semana.

La utilización de los certificados digitales se va empleando cada día más y, en breve, los usaremos para casi todo, siendo aún mayor su utilidad. Debemos de tener en cuenta que se pueden almacenar en una tarjeta inteligente, por supuesto protegidos por un PIN. En este sentido, la Fábrica Nacional de Moneda y Timbre está trabajando actualmente en lo que en un futuro cercano será nuestro nuevo carnet de identidad. Con un chip inteligente, seremos capaces de firmar cheques, letras, enviar correo electrónico certificado y hasta votar. Todo esto hace pensar en un futuro muy digital y mucho más rápido gracias al sistema de la criptografía.

Un claro ejemplo de lo explicado anteriormente, es el proyecto desarrollado por la Agencia Tributaria para posibilitar la entrega de la Declaración de la Renta a través de Internet, habiéndose emitido más de 20.000 certificados personales por parte de la FNMT. Además, se han puesto en marcha nuevas aplicaciones telemáticas para empresas, como la declaración de IVA, retenciones a cuenta,

importaciones, exportaciones, etc; que también requieren los servicios de certificación como garantía de seguridad. En este aspecto, requiere una mención especial el proyecto puesto en marcha con la Dirección General de Tesoro, que facilitará la contratación de deuda pública a través de Internet.

Un avance importante es la posibilidad de poder realizar los trámites en determinadas oficinas en el caso de que el ciudadano no disponga de ordenador personal ni de acceso a Internet, y que no conozcan lo suficiente su funcionamiento o que simplemente deseen utilizar los medios públicos.

Todas estas facilidades permitirán el acercamiento de los servicios públicos tanto a ciudadanos como a empresas, de manera que se podrá conseguir transformar un PC en una auténtica ventanilla de 24 horas.

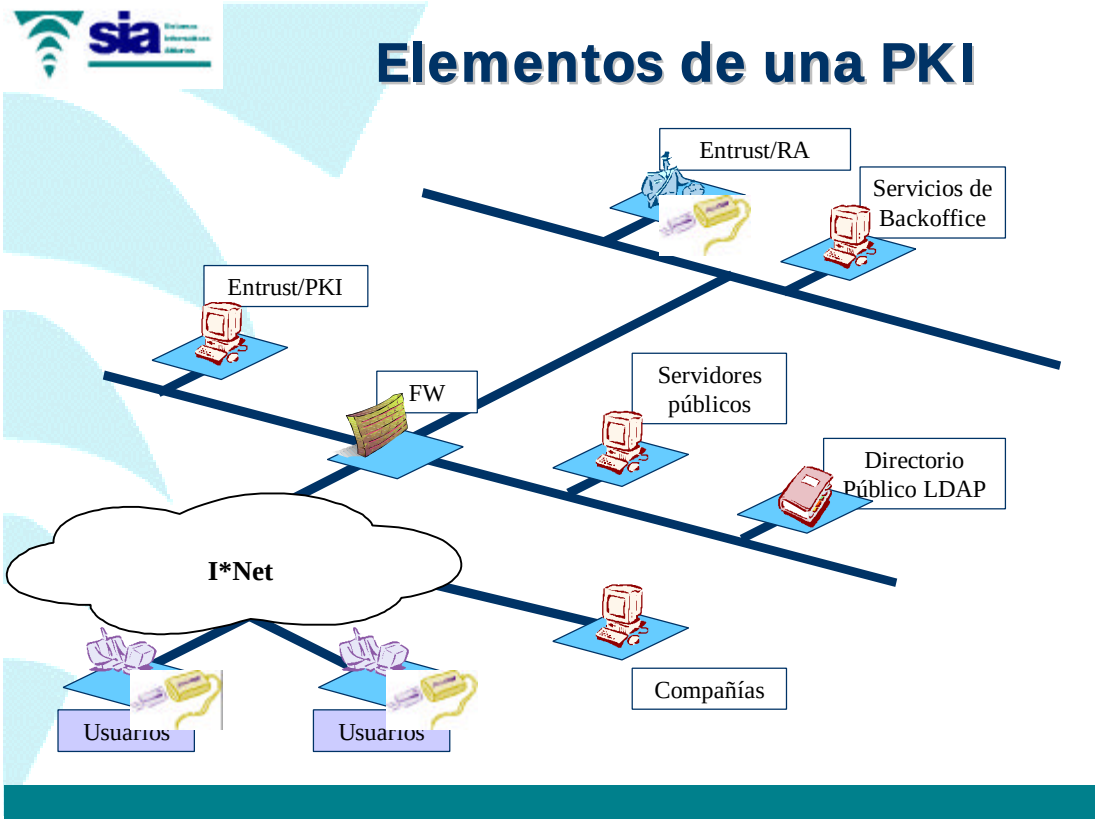
PARADIGMAS DE SEGURIDAD

Una PKI ofrece un marco de seguridad único, cumpliendo los cuatro paradigmas de **autenticación**, **confidencialidad**, **integridad** y **no repudio.** Paradójicamente se trata de reconocer la identidad de la persona o usuario dándole, al mismo tiempo, acceso a la información. Por otro lado, se asegura que la información es también auténtica, sin haber experimentado ningún tipo de modificación.

Profundizando en estos términos debemos de explicar que la *autenticación* implica que el usuario se puede identificar de una forma fiable a otros usuarios y servicios en una red, sin necesidad de enviar información secreta sin tener que enviarse información secreta como password. Gracias a la *integridad,* el receptor puede determinar si un mensaje ha sido alterado desde que fue firmado por el emisor, a través de la comprobación de la digital del origen. La *confidencialidad* o *privacidad* implica que la información que viaja por la red se encuentra cifrada de forma que no puede ser vista por una tercera persona no confiable. Por último, no debemos de olvidarnos del paradigma de *no repudio,* asegurando que el sistema tiene los medios necesarios para que se pueda demostrar fehacientemente la identidad de los usuarios que ha firmado un mensaje, sin posibilidad de que este pueda negarlo.

Son muchos los elementos que ha de poseer una PKI, como por ejemplo su capacidad de soportar un sistema de copia de seguridad y recuperación de las claves privadas de descifrado en el caso de que algún usuario perdiera el

acceso a su información cifrada. Para ello, la organización debe de estar prevista de un sistema de almacenamiento de claves de cifrado bajo unas estrictas normas de seguridad y poder recuperarlas según las necesidades.



La actualización de las claves, públicas o privadas, debe de realizarse de manera automática y transparente para que el usuario no tenga en mente la obligación de renovar los códigos con el riesgo de que le sea denegado de servicio porque sus claves no sean válidas.

Siguiendo esta línea, la aplicación debe de estar segura de que el certificado, al igual que la clave, es válido en el momento de usarlo, siendo, los que no son fiables, renovados por la Autoridad de Certificación. Como aspecto de suma importancia es necesario mantener lo que se denomina una confianza en tres bandas. A la hora de crear certificados, la Autoridad de Certificación actúa como un agente de confianza dentro de la PKI y sólo en la medida en que los usuarios confíen en la Autoridad de Certificación, podrán confiar en los certificados emitidos por la misma.

La importancia radica en que el usuario dedique el menor tiempo posible para mantener actualizadas sus

claves y, poder así, realizar transacciones electrónicas, al igual que no es necesario el requerimiento de un amplio conocimiento tecnológico para dicho fin.

Un informe de la compañía IDC, confirma la tendencia al alza en el uso de estas tecnologías. Según se desprende del estudio, el software de PKI, a escala mundial, pasará de mover un total de 132,2 millones de dólares en 1999, a 586,3 en el 2003. Por su parte, los servicios de certificación, según este mismo estudio, pasarán en este mismo periodo de 30,2 millones de dólares a 726,4. Se desprende una clara concienciación por parte de las empresas entrevistadas a la evolución que está sufriendo actualmente este tipo de infraestructuras.

¿Qué es una Infraestructura de Claves Públicas Efectiva? La PKI de Entrust Technologies

La criptografía de la Clave Pública se ha convertido en la misión a seguir por las grandes compañías del sector Tecnológico. La tecnología Entrust®PKI combina las capacidades de encriptación y firma digital con una gestión de ciclo de vida de la clave, totalmente automatizada, configurándose como una solución de seguridad completa a través de plataformas múltiples para sobremesas, redes corporativas, Intranets e Internet.

Además de la transparencia para el usuario final, una PKI efectiva debe contemplar los siguientes puntos:

- *Autoridad de Certificación*

Como mencionábamos anteriormente, para que la criptografía basada en claves públicas sea utilizable se debe disponer de medios para asegurar de forma fiable la identidad de los participantes en el sistema. Todos los usuarios de una PKI deben tener registrada su identidad. Estas identidades se almacenan en un formato electrónico conocido como Certificado Digital de clave pública. La Autoridad de Certificación firma digitalmente este certificado, asegurando la integridad del mismo y certificando la relación existente entre la clave pública contenida y la identidad del propietario de la misma.

- *Repositorio de certificados escalable*

El papel de la Autoridad de Certificación (CA) es la de actuar como tercera parte confiable emitiendo los certificados para los usuarios. Estos certificados, a su vez, deben ser distribuidos a los usuarios para ser utilizados en las aplicaciones. Los repositorios de certificados almacenan los certificados, de tal forma que las aplicaciones puedan recuperar los mismos en nombre del

usuario. El término *repositorio* se refiere a un servicio de red que permite el almacenamiento y la distribución de los certificados de una PKI.

A lo largo de los últimos años, se ha llegado a un consenso dentro de la industria de las Tecnologías de la Información en que la mejor herramienta para implantar el repositorio de certificados son los sistemas de directorios compatibles LDAP (Lightweight Directory Access Protocol). LDAP define un protocolo estándar para el acceso a sistemas de directorio.

- *Revocación de certificados*

Además de verificar la firma digital de la CA en los certificados, el software cliente debe asegurarse que el certificado es todavía fiable en el momento del uso. Los certificados que dejan de ser fiables deben ser revocados por la CA.

Hay numerosas razones por las cuales un certificado necesite ser revocado antes del final de su período de validez. Por ejemplo, la clave privada (eso es, la clave de firma digital o la de descifrado) correspondiente a la clave pública del certificado puede verse comprometida. En algún otro caso, la política de seguridad de la organización puede establecer que los certificados de los empleados que dejan la Empresa han de ser revocados. En estas situaciones de revocación los usuarios del sistema deben ser informados que el uso de dichos certificados revocados no se consideran fiables a partir de ese momento.

Antes de utilizar cualquier certificado se ha de comprobar su estado de revocación, por lo que la PKI debe incorporar un sistema escalable de gestión de certificados revocados. La Autoridad de Certificación debe permitir la publicación de información fiable sobre el estado de cada certificado en el sistema. El software de cliente debe, en nombre del usuario, verificar las listas de revocados antes de utilizar un certificado. La combinación de la publicación de listas de revocados y la verificación automática del estado de revocación de los certificados por parte del software en el cliente, constituyen un sistema de revocación completo, que toda PKI operativa debe disponer.

Las aplicaciones integradas con la PKI deben interactuar con un solo sistema de revocación de certificados. Debido a que la revocación de certificados es un elemento central para la confianza en el sistema. el software del cliente debe interactuar con el sistema de revocación de certificados de una forma consistente para todas las aplicaciones integradas con la PKI.

- *Copia de seguridad y recuperación de claves*

Un organismo gubernamental no se puede permitir perder información cifrada por los usuarios. Ya que los usuarios se olvidan frecuentemente de la palabra de paso de acceso a sus claves privadas, o que el contenedor (fichero, tarjeta,..) de las mismas se puede corromper, la organización a la cual el usuario pertenece necesita un sistema que permita realizar copias de seguridad y recuperación de las claves privadas de descifrado de los usuarios. Y se debe permitir, en su caso, la recuperación de las mismas por parte del usuario.

- *Soporte de "no repudio"*

El repudio sucede cuando una persona rechaza haber participado en una transacción. Por ejemplo, cuando alguien notifica que una tarjeta de crédito le ha sido robada, esto significa que rechaza toda la responsabilidad sobre las transacciones que se puedan realizar después de dicha notificación. No repudio significa que se puede demostrar fehacientemente que una persona ha participado en una transacción sin que dicha persona puede rechazarlo. En el mundo basado en papel, las firmas manuscritas son una herramienta legalmente reconocida utilizada para demostrar la participación de una persona en cualquier transacción (como cargos en tarjetas, contratos, recepción de suministros, etc.). Mediante esta firma se asegura que la persona no puede negar su participación en la transacción, y por tanto el no repudio. En el mundo electrónico, el papel de la firma manuscrita lo realiza la firma digital. Toda clase de comercio electrónico requiere el uso de firmas digitales para poder asegurar el no repudio de las transacciones.

Para soportar el "no repudio", el software del cliente debe generar el par de claves de firma digital por sí mismo, y asegurar mediante password el acceso a la clave privada de firma. Además, el software del cliente debe asegurar que la clave privada de firma no abandonarán nunca su sistema, ni se realizarán copias de seguridad de la misma.

Para cubrir simultáneamente estos dos requisitos, recuperación de claves (exige backup centralizado de la clave privada de descifrado) y el no repudio (exige que la clave privada de firma no abandone el sistema del cliente), la PKI debe soportar el uso de *dos pares de claves por cada usuario*. Así, cada usuario debe poseer una par de claves de cifrado y descifrado y otro par de claves para firma digital y verificación de firma digital. El primer par se genera centralmente y se realiza un backup del mismo para permitir su recuperación, y el par de firma digital es

generado por el cliente y su clave privada no abandona nunca el sistema del usuario.

- *Renovación automática de los pares de claves*

Para asegurar la transparencia, el software del cliente debe iniciar automáticamente la renovación de los pares de claves del usuario. Esta actividad debe ser realizada de acuerdo con las políticas de seguridad de la Organización. Es de todo punto inaceptable que el usuario tenga que saber cuándo y cómo se ha de renovar sus claves y que tenga que gestionar el mismo la renovación de forma manual. En el caso de no hacer esta renovación automática, la Organización se expone a que se produzcan "deniegos de servicio" porque las claves del servidor o de los usuarios han expirado.

- *Gestión de la historia de las claves*

Al renovar las claves del usuario, se ha de mantener una historia de las claves privadas de descifrado. Esta historia de claves permitirá que los usuarios puedan acceder a cualquiera de sus claves anteriores para descifrar la información cifrada con la correspondiente clave. Para asegurar la transparencia, el software del cliente debe gestionar automáticamente la historia de las claves de cifrado.

Asimismo, la historia de las claves de un usuario ha de ser gestionada de forma segura por el sistema de copia de seguridad y recuperación de claves antes descrito. Esto asegura que la información cifrada se puede recuperar fiablemente, independientemente de que clave pública de cifrado se utilizó para firmar la misma (y, por extensión, independientemente de cuando se cifró la información).

- *Soporte de certificación cruzada*

La certificación cruzada de CAs extiende las relaciones de tercera parte confiable entre dominios de Autoridades de Certificación. Por ejemplo, dos personas con relaciones de negocio, cada una de ellas pertenecientes a CAs diferentes, pueden querer validarse sus certificados emitidos por la CA de la otra persona. Por otra parte, una gran empresa distribuida geográficamente, puede requerir implantar múltiples CAs en distintas regiones. La certificación cruzada permite establecer y mantener relaciones de confianza entre los usuarios de diferentes CAs.

El término "certificación cruzada" hace referencia a dos operaciones. La primera operación, que se ejecuta normalmente una sola vez, y es el establecimiento de relaciones de confianza entre dos CAs. En el caso de certificación cruzada bilateral, las CAs han de

intercambiar de forma segura sus claves de verificación. Estas son las claves utilizadas para verificar la firma de la CA en los certificados y CRLs. Para completar la operación, cada CA firma la clave de verificación de la otra CA creando un certificado especial llamado "certificado cruzado".

La segunda operación se realiza en el software del cliente. La operación, que se ejecuta frecuentemente, consiste en la verificación de la confiabilidad del certificado del usuario firmado por la CA con certificado cruzado. Esta operación se referencia frecuentemente como "navegar en la cadena de confianza". La "cadena" se refiere a la lista de validaciones de certificados cruzados por la que se ha de "navegar" desde la clave de la CA del usuario origen hasta verificar la clave de la CA del usuario destino.

Cuando se navega por la cadena de certificados cruzados, cada uno de ellos han de ser verificados para asegurar que todavía son fiables y no están revocados. Al igual que hay que posibilitar la revocación de los certificados de usuarios, se debe tener la posibilidad de revocar certificados cruzados entre CAs. Este requisito es frecuentemente omitido en discusiones sobre certificación cruzada de CAs.

La Infraestructura de Entrust permite establecer certificaciones cruzadas entre distintas CAs generando los certificados cruzados apropiados. Esta relación de confianza se realiza a nivel de administradores de las PKI. El software del cliente automáticamente verifica, cuando recibe un certificado de otra CA, si existe una relación de confianza entre las CAs a través de certificados cruzados y si este certificado no está revocado. Si esta verificación es correcta el certificado del usuario se da por válido. Toda esta operación se realiza de forma transparente al usuario final.

- *Sellado de Tiempo (Timestamping)*

A través de la firma digital se puede demostrar, siempre que el sistema asegure el no repudio, de una forma fehaciente y legal la autoría del origen de una transacción. En muchos casos, yo diría que en casi la totalidad de las transacciones comerciales, no sólo es importante a nivel de negocio, saber **quién** es el origen de la transacción, sino que es vital asimismo tener un mecanismo electrónico que demuestre sin posibilidad de duda **cuándo** se hizo la transacción. No tenemos que ir muy lejos para encontrar claros ejemplos de esta necesidad: compra de acciones en una fecha determinada, escrituras públicas, fecha de pago de un impuesto, etc. A través de la tecnología de clave pública también se puede resolver esta

necesidad utilizando una Autoridad de Sellado de Tiempo, en la que las partes confíen, y que realice un Sellado de Tiempo (Timestamping) de la transacción en cuestión.

La familia de PKI de Entrust dispone de un componente para implantar una Autoridad de Sellado de Tiempo (Entrust Timestamp Server) y las aplicaciones disponen de medios a través de los Toolkits existentes para pedir, en su caso, el Sellado de Tiempo para las transacciones que así lo requieran. Asimismo a través de los mismos Toolkits se puede verificar fehacientemente cuando se fechó una transacción con Sellado de Tiempo.

Cuando se discute sobre requisitos de una Infraestructura de Claves Públicas (PKI), generalmente se omiten los requisitos necesarios en la parte cliente (por ejemplo, frecuentemente se habla sólo de la Autoridad de Certificación). Sin embargo, no hay que perder de vista que el objetivo de cualquier PKI es habilitar a los usuarios para que firmen y cifren su información crítica. Por esta razón, la PKI debe incluir software de cliente que permita integrar las aplicaciones de usuario (como correo electrónico, acceso a Webs, etc..) de forma consistente y transparente con la Infraestructura. La existencia de software de cliente fácil de integrar con la PKI, reduce en gran manera los costes de operación de la misma.

Una de las principales ventajas de la solución Entrust es que aporta una extraordinaria flexibilidad y movilidad a los usuarios, ya que éstos pueden acceder a sus credenciales desde un directorio gestionado de forma centralizada, sin necesidad de recurrir a mecanismos adicionales.

Los años de experiencia de Entrust Technologies han hecho de la confianza del comercio electrónico su principal objetivo. La criptografía de Clave Pública se ha convertido en la misión a seguir por las grandes compañías del sector Tecnológico. La tecnología Entrust®PKI combina las capacidades de encriptación y firma digital con una gestión de ciclo de vida de la clave, totalmente automatizada, configurándose como una solución de seguridad completa a través de plataformas múltiples para sobremesas, redes corporativas, Intranets e Internet.

CONCLUSIÓN

En la actualidad la Administración Pública ha establecido planes estratégicos para la puesta en marcha de sistemas de gestión telemática. Ciertamente el factor seguridad se ha convertido en el principal protagonista de las transacciones electrónicas entre empresas, organismos

gubernamentales y ciudadanos. La solución PKI de Entrust posee todos los elementos necesarios para asegurar la privacidad y la autenticidad de los datos en un momento en el que, con el desarrollo de Internet, Administración se ha abierto al exterior ofreciendo información que anteriormente circulaba en su ámbito interno y cambiando los métodos de comunicación con ciudadanos y empresas.