Identificación y análisis en torno a PKI: Infraestructura de clave publica y su relacion con los certificados digitales y la firma electrónica avanzada

Por Javier Areitio Bertolín y Gloria Areitio Bertolín

El Prof. Dr. Javier Areitio Bertolín es Catedrático de la Facultad de Ingeniería. ESIDE y Director del Grupo de Investigación de Redes y Sistemas de la Universidad de Deusto
jareitio@eside.deusto.es

La Prof. Dra. Gloria Areitio Bertolín trabaja en el Laboratorio de Informática Aplicada de la Universidad del País Vasco (UPV / EHU)
ebparbeg@bs.ehu.es

En el presente artículo se identifica y analiza a la PKI (Public Key Infrastructure) sistema completo que engloba algo mas que una simple tecnología o producto se trata de un amalgama de tecnologías, personas, servicios, procesos y políticas diseñados para gestionar el ciclo de vida de las claves de usuario operando con criptografía de clave pública. También se identifican las PMI (Privilege Management Infrastructure) y AAI (Authentication and Authorization Infrastructure), estas últimas basadas de la combinación de PKI y PMI..

La firma electrónica avanzada permite la identificación del signatario y ha sido creada por medios que esté mantiene bajo su exclusivo control. Signatario es la persona, etc. que cuenta con un dispositivo de creación de firma. Se pueden identificar dos tipos de dispositivos: de creación de firma y de verificación de firma.

El certificado digital vincula unos datos de verificación de firma a un signatario y confirma su identidad. A efectos jurídicos, la *firma electrónica* avanzada, siempre que esté basada en un *certificado reconocido* y que haya sido producida por un *dispositivo seguro de creación de firma* tendrá:

- El mismo valor jurídico que la firma manuscrita.
- Será admisible como prueba en juicio.
- Valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Se entiende por certificados reconocidos:

- Identificación única.
- Identificación de la autoridad certificadora (VeriSign, Ceres (con la Fábrica Nacional de Moneda y Timbre), Izenpe-País Vasco, etc.).
- Identificación del sujeto reconocido: nombre y apellidos o seudónimo; si representa o actúa en nombre de otro.
- Período de validez.
- Límites de uso del certificado, si se prevén.
- Límites del valor de las transacciones para las que puede utilizarse, si se establecen.

Así mismo, los dispositivos seguros de creación de firma:

(a) Garantizan que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto, por ejemplo claves privadas.
(b) Exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación, por ejemplo tecnología de clave pública.
(c) Los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros, por ejemplo una tarjeta inteligente con un "cripto-chip".
(d)El dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que este se muestre al signatario antes del proceso de firma, o sea "homologados".

La Ley 59/2003 – BOE de 19 Diciembre del 2003 sobre Firma Electrónica, regula el uso de las firmas electrónicas, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.

Definición de PKI. Papel de las PKI. PMI. AA. AAL.

Una PKI (Public Key Infrastructure) es el conjunto de políticas, personas, procesos, tecnologías y servicios que hacen posible desplegar y gestionar la utilización de la criptografía de clave pública y de los diferentes certificados digitales X509v3 (de identidad y de atributos, estos últimos relacionados con la especificación del control de acceso y los permisos de acceso de personas físicas, jurídicas, máquinas de computación, etc.) a gran escala.

Otra definición, en este caso del IETF (Internet Engineering Task Force), señala que una PKI es el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública. Entre las aplicaciones de las claves se puede destacar:

(a) Claves para llevar a cabo intercambios confidenciales.
(b) Claves para firmar electrónicamente documentos de usuario.
(c) Claves para autenticación e identificación de clientes.
(d) Claves para que las autoridades de certificación firmen CRLs (Listas de Revocación de Certificados) y certificados, etc.

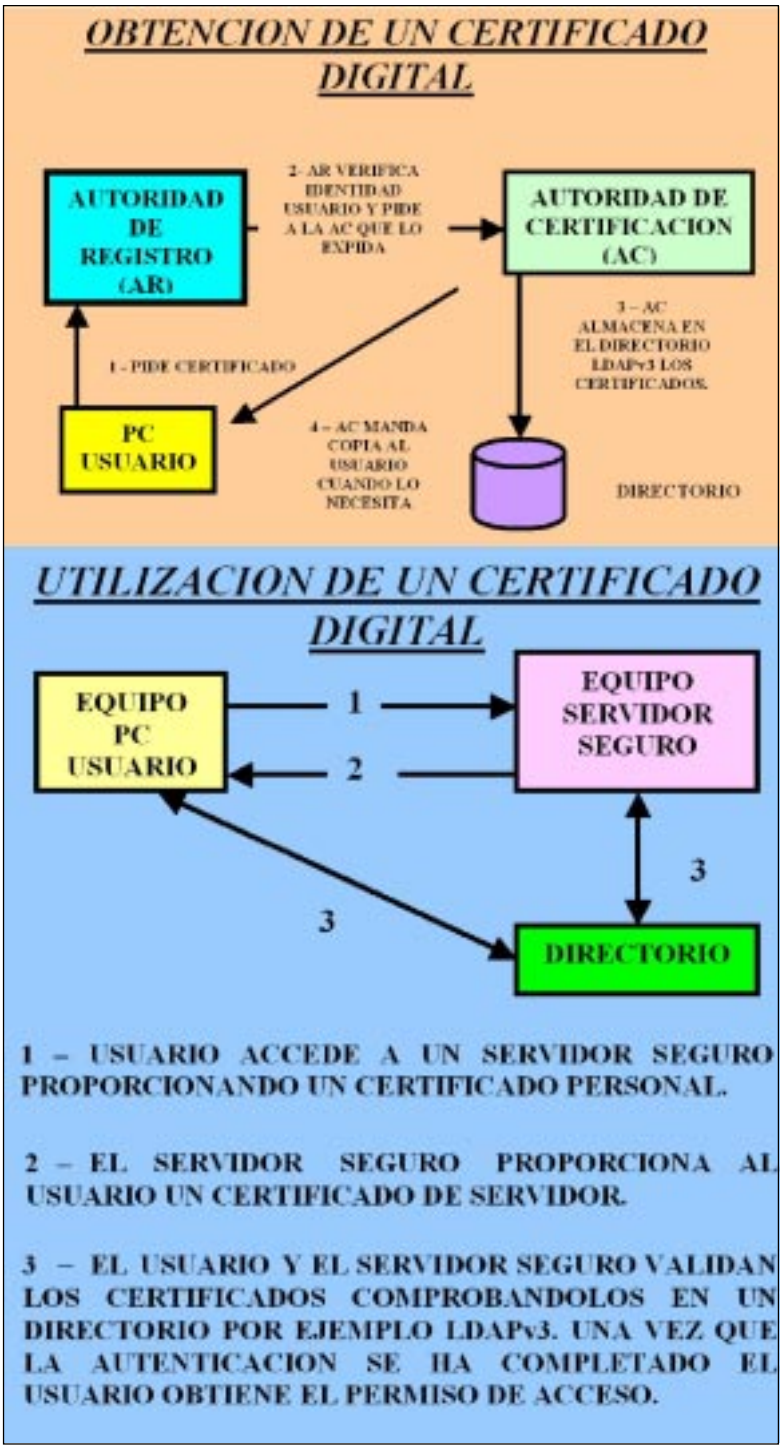
Entre los principales modelos de revocación que utilizan las PKI se encuentran:

(a) CRLs (Certificate Revocation Lists), es el modelo tradicional soportado por Entrust, VeriSign y la mayoría de Autoridades de Certificación.
(b) OCSP (On-line Certificate Status Protocol), es un protocolo de gestión de certificados propuesto por el IETF e introducido por VeriSign permite verificar en tiempo real los certificados desde el punto de vista de su posible revocación.

Otros protocolos de gestión de certificados son LDAP para la recuperación de certificados y PKCS#10 para la petición de certificados (implementado en navegadores, define el mensaje que se puede enviar por correo electrónico a una Autoridad de Certificación, incluye baja seguridad, necesita protección adicional). El papel de una PKI es:

- Gestionar las claves criptográficas del usuario (ciclo de vida de la clave).
- Proporcionar confianza dando lugar a entornos de seguridad de alto nivel.
- Soporte para la política de la organización específica.
- Soporte en diferentes aplicaciones.

Las PKI para atributos se denominan PMI (Privilege Management Infrastructure). Se necesita un emisor reconocido por el que vaya a utilizar el atributo; se necesita CRL (Lista de Revocación de



certificados) para terminar atribuciones, si es de muy corta duración, puede no haber CRL. Los atributos para controlar si un atributo es delegable son:

- ¿A quién?.
- ¿Durante qué período?.
- ¿Con que restricciones?.

La mecánica es:

a) Identificarse, por ejemplo mediante un certificado de identidad emitido por una autoridad confiable para el validador, o bien demostrando conocer la clave secreta o bien cualquier cosa que me reconozca como beneficiario.

b) Aportar atributos, emitidos por una AA (Autoridad de Atributos) capacitada, en el caso mas complejo proporcionar una cadena de atributos. Existen dos modelos: en el primero el cliente aporta AC; en el segundo el servidor reclama AC de un repositorio.

Por tanto, el control de acceso se puede hacer de dos formas:

a) El objeto accedido sabe quién le puede acceder y con qué derechos; este método es difícil de mantener y poco ágil.

b) El objeto accedido sabe de quién puede fiarse, el que accede aporta sus atributos; este método es ágil y fácil de mantener. Cuando se habla de atributos se puede hacer referencia a tipos de privilegios como: pertenencia a un grupo, identificación de cargos, valores límite de transacciones, hora de acceso a ciertas operaciones, límites temporales, etc.

Una AA (Autoridad de Atributos) es responsable de asignar o delegar privilegios a los usuarios finales o a otras AAs. Antes de que una AA pueda delegar un privilegio es necesario que tenga posesión del mismo. Esto significa que bien se le ha delegado el privilegio con anterioridad o bien es la fuente del privilegio en si mismo. La AA puede tener restringida la capacidad de delegar un privilegio a otra AA, y sólo tener permitido delegar privilegios a los usuarios finales.

LA SOA (Fuente de Autoridad) es una AA y su papel es análogo al de una Autoridad Raíz en las PKI. Una AAI (Authentication and Authorization Infrastructure) es una infraestructura que proporciona soporte conjunto para servicios de autenticación y autorización y se puede

desarrollar a partir de una PKI. Existen diferentes opciones de AAIs basadas en PKI:

- PKI + PMI.
- PKI + Extensiones de los certificados de identidad.
- PKI + Gestión de la información de autorización utilizando un DBMS (Sistema de Gestión de Base de Datos).

Ventajas de la PKI

La criptografía de clave pública se esta convirtiendo en una herramienta de negocio vital para cualquier organización que busque proteger sus activos de información en entornos de red potencialmente no confiable como Internet que utiliza para soportar sus comunicaciones la pila de protocolos TCP/IP. La utilización de la criptografía de clave pública hace posible:

- Cifrar las comunicaciones, por ejemplo cuando se envía correo electrónico, ficheros, etc. de forma confidencial sobre una red no confiable.
- Detectar cambios no autorizados en los datos transmitidos sobre las redes, utilizando por ejemplo firmas electrónicas.
- Identificar y autenticar positivamente a usuarios remotos sobre redes, por ejemplo cuando se necesita proporcionar acceso a sistemas sensibles, por ejemplo utilizando tecnología VPN (Virtual Private Network).
- Firmar digitalmente información, por ejemplo cuando se autorizan servicios electrónicamente y donde el valor de las evidencias es muy importante (de cara a análisis forenses).
- Asegurar que los usuarios no puedan repudiar sus acciones realizadas posteriormente, por ejemplo cuando se necesita confirmar la identidad del usuario específico que envió un mensaje o instrucción concreta sobre una red no segura; para garantizar el no repudio de envío, recepción, etc. es necesario la existencia de una tercera parte confiable intermedia (ó TTP) entre emisor y receptor que opere como fedatario ó notario electrónico con valor probatorio ante posibles disputas.

Problemas que plantea la utilización de PKI

Existen algunos problemas prácticos asociados con la utilización de criptografía de clave pública que si no se tratan adecuadamente sirven para socavar las capacidades anteriormente señaladas y a sembrar la duda en la confianza de cualquier sistema que lo utilice. Así, se pueden destacar la gestión de claves criptográficas en donde una carencia de control podría conducir a una:

- Incapacidad para actualizar o renovar claves.
- Incapacidad para recuperar datos cifrados con una clave antigua.
- Utilización continuada de una clave que se ha visto comprometida o esta caducada.

Otras consideraciones que surgen como resultado de utilizar criptografía de clave pública son:

- Proteger las claves públicas de suplantación y falsificación.
- Hacer la criptografía de clave pública disponible a un amplio número de usuarios de una manera que sea consistente y fiable.
- Hacer la criptografía de clave pública transparente a los usuarios finales.

Modo de proporcionar gestion y control a una PKI

Una PKI trata estas cuestiones de gestión y control mediante la:

- Gestión de claves a lo largo de su ciclo de vida.
- Utilización de certificados digitales X.509v3 para proteger y asegurar la autenticidad de las claves públicas.
- Provisión de una infraestructura escalable, consistente, fiable y digna de confianza para el uso de criptografía de clave pública.

Proporcionando un entorno para el uso fiable de autenticación, confidencialidad, integridad y servicios de no repudio, una PKI puede ayudar a proporcionar la confianza que es necesario para llevar a cabo los negocios en entornos de red no seguros.

Generaciones de PKI

Primera generación. Sólo generación de claves centralizada. Registro y certificación se combina en una función. Restringida a una aplicación.

Segunda generación. Separación entre certificación y registro., mas funciones como revocación, recuperación de claves, etc.

Tercera generación. Soporta múltiples dominios de aplicación. Permite interoperabilidad. Soporta políticas dinámicas. Incorpora mas funciones como por ejemplo marcas de tiempo, notarización, etc.

Componentes de una PKI

Una PKI consta básicamente de siete componentes:

- Certificados digitales (ó certificados de clave pública ó certificados X.509v3 – ITU-T). Un certificado digital es una estructura de datos firmada que vincula uno o mas atributos a una entidad con su correspondiente clave pública. Al estar firmada por una autoridad confiable y reconocida (es decir, la Autoridad de Certificación) un certificado digital proporciona garantía de que una clave pública concreta pertenece a una entidad específica y que esa entidad posee la correspondiente clave privada.

- Autoridad de Certificación (AC). Las autoridades de certificación son las personas, procesos y herramientas que son responsables de la creación,

expedición y gestión de los certificados de clave pública que se utilizan dentro de una PKI.

• Autoridad de Registro (AR).L a s autoridades de registro son las personas, procesos y herramientas responsables de autenticar la identidad de nuevas entidades (usuarios (personas físicas y jurídicas), dispositivos de computación (servidores, etc.)) que necesitan certificados de las ACs. Las ARs adicionalmente mantienen datos de registro locales e inician procesos de renovación o revocación para certificados viejos o redundantes. Las ARs actúan como agentes de las ACs y en ese aspecto pueden llevar a cabo, si se necesita, algunas de las funciones de una AC.

• Repositorio de certificados. Una base de datos u otro tipo de almacenamiento que este accesible a todos los usuarios de una PKI dentro del que pueden soportarse los certificados de clave pública, información de revocación de certificados e información de política.

• Software del cliente PKI. Se necesita el software del lado del cliente para asegurar que las entidades de la PKI pueden hacer uso de la clave y servicios de gestión de certificados digitales de una PKI, por ejemplo, creación de la clave, refresco y actualización automática de la clave.

• Aplicaciones que permite la PKI. Las aplicaciones software deben ser permitidas por la PKI antes de que se puedan utilizar dentro de una PKI. Normalmente esto implica modificar una aplicación para que pueda entender y hacer uso de los certificados digitales, por ejemplo, para autenticar un usuario remoto y autenticarse la PKI a un usuario remoto.

• Política (Política de certificados y declaración de prácticas de certificación). La CP (Certificate Policy) y la CPS (Certification Practice Statement) son documentos de política que definen los procedimientos y prácticas a emplear para el uso, administración y gestión de certificados dentro de una PKI.

Bajo ciertas circunstancias también se pueden necesitar otros componente PKI como:
a) Servicio confiable de marca de tiempos (ó TSS, Time Stamping Service), por ejemplo, cuando es importante mantener un registro preciso de la hora concreta de los eventos.
b) Autoridad de validación, por ejemplo donde se necesita la validación en tiempo real automática de certificados, por ejemplo en sistemas altamente críticos.
c) Servicio de Notario Electrónico, por ejemplo en donde es importante asegurar los registros precisos de todas las transacciones que se depositan y mantienen de una manera segura, por ejemplo en donde las implicaciones de un usuario de la PKI que repudie sus acciones podrían ser perjudiciales y / o costosas.

Además de los componentes anteriores una PKI debe operar dentro de una infraestructura de Tecnologías de la Información, es decir, una red con maquinas de computación servidores y clientes. Esta infraestructura debe poder soportar las demandas de procesamiento, resiliencia y rendimiento de una PKI.

Los componente de una PKI se pueden agrupar en tres grupos:
1) Componentes del servidor:
• Autoridad de Certificación (AC), responsable de generar objetos de clave como los certificados, CRLs, etc.
• Autoridad de Recuperación de Clave ó KRA (Key Recovery /Escrow Authority), responsable del procedimiento de copia de seguridad / restauración de claves en el sistema.
• Sistema de Directorio (SD), responsable de publicar los objetos de clave PKI (certificados, CRLs, etc.).
• Autoridad de Marcas de Tiempo ó (TSA, Time Stamping Authority), responsable de un mecanismo de reloj seguro.
• Sistema de Expedición de Tarjeta ó CIS (Card Issuing System), responsable de los dispositivos hardware de personalización utilizados para funciones criptográficas.
• Otros Servicios de Aplicación: "CodeSigning", servidor de certificados de atributos, etc.
2) *Componentes de administración:*
• Autoridad de Registro (AR), responsable del registro de los aspectos principales del ciclo de vida de la clave, por ejemplo, añadir nuevos usuarios, revocación de usuarios, etc..
• Autoridad de Registro Local ó LRA (Local Registration Authority), AR de segundo nivel.
• Autoridad de Notarización (AN), responsable de la validez de las firmas digitales.
3) Componentes del cliente:
Agentes de Usuario, la aplicación que es responsable de los aspectos principales del ciclo de vida de la clave en el cliente, por ejemplo el navegador.

Funcionalidades principales de una PKI

La principal función de una PKI es gestionar las claves criptográficas y los certificados. Sin embargo debe permitir las funciones siguientes:
• Registrar nuevos usuarios, verificando sus credenciales para asegurarse que son aspirantes genuinos.
• Generar-Crear pares de claves pública-privada, centralizada o des-centalizadamente.
• Proporcionar mecanismos para proteger la clave privada, por ejemplo autenticación para control de acceso para la clave privada.
• Crear y expedir certificados de clave pública para usuarios de PKI legítimos.
• Hacer los certificados de clave pública disponibles para uso por parte de otros usuarios de PKI.

• Soporte de verificación de revocación para que los certificados que dejan de ser válidos sean fácilmente identificados.
• Soporte del no repudio, por virtud de generar y proteger el par de claves de firma.
• Periódicamente actualizar los pares de claves, para reducir el riesgo de verse comprometida la clave.
• Gestionar las historias de claves para que el contenido cifrado en el pasado pueda aún recuperarse.
• Proporcionar un mecanismo para recuperar claves de cifrado.
• Soporta certificación cruzada lo que permite a los usuarios de una Autoridad de Certificación utilizar los certificados en otra AC.
• Gestión de las claves maestras del sistema (claves de la AC Raíz).
• Gestión del Sistema de directorio.
• Gestión del ciclo de vida del dispositivo y de la clave (creación, actualización, revocación de certificados, recuperación, etc.)

Estas funciones son normalmente de cómo se debería establecer una PKI. Sin embargo, una de las complejidades de la PKI es que algunas funciones pueden llevarse a cabo por diferentes partes.

Para facilitar el uso y funcionamiento, es esencial que todas estas funciones se implementen y realicen tan transparentemente como sea posible para los usuarios finales.

Arquitecturas de conexión entre autoridades de certificacion. Ruta de certificacion

Dadas dos autoridades de certificación diferentes CA1 y CA2, éstas se pueden unir de diversas formas, por ejemplo:
• Ambas CA1 y CA2 pueden ser certificadas por una tercera autoridad de certificación denominada CA3 en una jerarquía. CA3 expendería certificados diciendo cuales son las claves públicas de CA1 y CA2. Estas se podrían verificar utilizando la clave pública de CA3.
• CA1 y CA2 pueden certificarse de forma cruzada entre sí. CA1 expendería un certificado diciendo cual es la clave pública de CA2 y CA2 expendería un certificado (digital X.509v3-ITU/TSS) diciendo cual es la clave pública de CA1.
• CA1 y CA2 pueden estar en diferentes niveles de certificación. En este caso (sin pérdida de generalidad) CA1 debería certificar a CA2 expidiendo un certificado que diga cual es la clave pública de CA2, pero CA2 no certificaría a CA1 ya que CA1 está más próximo a la raíz de la jerarquía.

Por "ruta de certificación" (visible desde los navegadores web cuando actúan con certificados digitales caso de https y ssl) se entiende un árbol en que al menos debe hacer una raíz y puede haber varios niveles.

Por ejemplo si una empresa (por ejemplo lenyt) monta una autoridad de certificación para su uso interno, por ejemplo para trabajar con ssl, en correo electrónico y acceso a sitios https de su intranet puede crear como ruta de certificación únicamente su propia autoridad de certificación como raíz (servidor de certificados de lenyt).

En cambio, otra empresa (por ejemplo resys) que desee dar servicio no sólo dentro de su intranet sino al exterior puede crear como ruta de certificación un árbol formado por una raíz Verign/RSA Secure Server CA y por debajo su sitio web (www.resys.net).

Consideraciones finales

Las PKI no son apropiadas para dotar de servicios de autorización a las aplicaciones de comercio electrónico que requieren algo mas que la simple autenticación.

Las infraestructuras de administración de privilegios PMI vienen a solucionar funcionando en paralelo con las PKI, el problema de la utilización de los certificados de atributos.

Las infraestructuras de autenticación y autorización AAI que surgen como combinación de PKI y PMI se sitúan en un lugar privilegiado para dar solución a muchos de los problemas del comercio electrónico, por ejemplo el control de acceso basado en roles y la delegación de privilegios y potestades. ❑

Bibliografía

- Adams, C. and Lloyd, S. "Understanding PKI: Concepts, Standards and Deployment Considerations". 2nd Edition. Addison-Wesley Pub. Co. 2002.
- Areitio, G. "Integración de las políticas de seguridad en los procedimientos de seguridad". SIC. Diciembre 1993.
- Areitio, J. "Transacciones Electrónicas Seguras: Consideraciones sobre Certificados Digitales, Autoridades de Certificación y Terceras Partes Confiables". Congreso Securmática'97. Madrid. 1997.
- Areitio, J. "Protocolos Criptográficos de No Repudio para el Comercio Electrónico". Congreso Turitec'99. Málaga. Septiembre 1999.
- Areitio, J. "A New Protection Mechanism for Computer Network". 8th European Conference on Information Systems Security, Control and Audit. Sweden. Septiembre 1993.
- Austin, T. "PKI: A Wiley Tech Brief". John Wiley & Sons Ltd. U.K. 2000.
- Feghhi, J. and Williams, P. "Digital Certificates: Applied Internet Security". Addison-Wesley Pub. Co. 1998.
- Grant, G.L. "Understanding Digital Signatures: Establishing Trust Over the Internet and Other Networks - CommerceNET". McGraw-Hill Professional Books. 1st Edition. 1997.