PKI - Infraestructuras de Clave Pública

En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

Propósito y funcionalidad

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

En una operación criptográfica que use PKI, intervienen conceptualmente como mínimo las siguientes partes:

1. Un usuario iniciador de la operación.
2. Unos sistemas servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación (autoridad de certificación, Autoridad de registro y sistema de Sellado de tiempo).
3. Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación (puede ser él mismo).

Las operaciones criptográficas de clave pública, son procesos en los que se utilizan unos algoritmos de cifrado que son conocidos y están accesibles para todos. Por este motivo la seguridad que puede aportar la tecnología PKI, está fuertemente ligada a la privacidad de la llamada clave privada y los procedimientos operacionales o Políticas de seguridad aplicados.

Es de destacar la importancia de las políticas de seguridad en esta tecnología, puesto que ni los dispositivos más seguros ni los algoritmos de cifrado más fuerte sirven de nada si por ejemplo una copia de la clave privada protegida por una tarjeta criptográfica (del inglés 'smart card') se guarda en un disco duro convencional de un PC conectado a Internet.

Usos de la tecnología PKI

- Autenticación de usuarios y sistemas (login)
- Identificación del interlocutor
- Cifrado de datos digitales
- Firmado digital de datos (documentos, software, etc.)
- Asegurar las comunicaciones
- Garantía de no repudio (negar que cierta transacción tuvo lugar)

Tipos de certificados

Existen diferentes tipos de certificado digital, en función de la información que contiene cada uno y a nombre de quién se emite el certificado:

- Certificado personal, que acredita la identidad del titular.
- Certificado de pertenencia a empresa, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- Certificado de representante, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- Certificado de persona jurídica, que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- Certificado de atributo, el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal. (p.ej. Médico, Director, Casado, Apoderado de..., etc.).

Además, existen otros tipos de certificado digital utilizados en entornos más técnicos:

- Certificado de servidor seguro, utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
- Certificado de firma de código, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

Componentes

Los componentes más habituales de una infraestructura de clave pública son:

- La autoridad de certificación (o, en inglés, CA, Certificate Authority): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la

relación de una clave pública con la identidad de un usuario o servicio.

- La autoridad de registro (o, en inglés, RA, Registration Authority): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.

- Los repositorios: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (o, en inglés, CRL, Certificate Revocation List) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

- La autoridad de validación (o, en inglés, VA, Validation Authority): es la encargada de comprobar la validez de los certificados digitales.

- La autoridad de sellado de tiempo (o, en inglés, TSA, Time Stamp Authority): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.

- Los usuarios y entidades finales son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.)

Consideraciones sobre PKI

Todo certificado válido, ha de ser emitido por una Autoridad de certificación reconocida, que garantiza la validez de la asociación entre el tenedor del certificado y el certificado en sí.

El poseedor de un certificado es responsable de la conservación y custodia de la clave privada asociada al certificado para evitar el conocimiento de la misma por terceros.

Las entidades de registro se encargan de la verificación de la validez y veracidad de los datos del que pide un certificado, y gestionan el ciclo de vida de las peticiones hacia las AC's.

El poseedor de un certificado válido puede usar dicho certificado para los usos para los que ha sido creado según las políticas de seguridad.

Toda operación que realice el poseedor de un certificado ha de realizarse de forma presencial por parte del poseedor del certificado y dentro del hardware de cliente (ya sea la tarjeta criptográfica o PKCS#11 u otro dispositivo seguro, como el fichero seguro o PKCS#12, etc).

Las comunicaciones con seguridad PKI no requieren del intercambio de ningún tipo de clave secreta para su establecimiento, por lo que se consideran muy seguras si se siguen las políticas de seguridad pertinentes.

Ejemplos de Uso

Los sistemas de PKI, de distintos tipos y proveedores, tienen muchos usos, incluyendo la asociación de una llave pública con una identidad para:

Cifrado y/o autenticación de mensajes de correo electrónico (ej., utilizando OpenPGP o S/MIME).

Cifrado y/o autenticación de documentos (ej., la firma XML * o Cifrado XML * si los documentos son codificados como XML).

Autenticación de usuarios o aplicaciones (ej., logon por tarjeta inteligente, autenticación de cliente por SSL).

Bootstrapping de protocolos seguros de comunicación, como Internet key exchange (IKE) y SSL.

Seguridad de los certificados

La seguridad en la infraestructura PKI depende en parte de cómo se guarden las claves privadas. Existen dispositivos especiales denominados tokens de seguridad para facilitar la seguridad de la clave privada, así como evitar que ésta pueda ser exportada. Estos dispositivos pueden incorporar medidas biométricas, como la verificación de huella dactilar, que permiten aumentar la confiabilidad, dentro de las limitaciones tecnológicas, en que sólo la persona dueña del certificado pueda utilizarlo.

Diez riesgos sobre las PKI

Bruce Schneier y Carl Ellison publican un ensayo de ocho páginas sobre los riesgos de la "Infraestructura de Clave Pública", tal y como se define en la actualidad. El documento fue publicado originalmente en el primer número del año 2.000 de la revista "Computer Security Journal".

El documento, disponible en formatos ASCII y HTML, analiza en profundidad diez riesgos de las estructuras PKI actuales. Las PKI constituyen, entre otras cosas, las bases actuales de las entidades de certificación, por ejemplo.

1. ¿En quien debo confiar?
   Hoy en día existen multitud de entidades de certificación pero, ¿quien te garantiza que los datos que certifican son correctos (por ejemplo, un email o un nombre)?. ¿Quien las ha situado en el contexto comercial en el que se encuentran?.

2. ¿Quién tiene acceso a mi clave?
   La criptografía de clave pública o asimétrica supone la existencia de dos claves: una pública y disponible de forma universal, y otra privada y bajo el control exclusivo del

usuario.

Pero, hoy en día, la clave secreta o privada no está segura. Los sistemas operativos y los navegadores adolecen de multitud de problemas de seguridad, además de existir virus y troyanos. Por tanto, no se puede garantizar que un documento firmado con una clave secreta constituya una firma confiable.

3. ¿Cómo de seguro es el ordenador verificador?
   Como ocurre con el caso anterior, el ordenador que realiza la verificación del certificado puede haber sido manipulado. Puede, por ejemplo, haberse instalado una entidad de certificación espúrea en el navegador, algo absolutamente trivial.

4. ¿Qué "Jesús Cea" es el correcto?
   Habitualmente los certificados se expiden a un nombre determinado, sin tener en cuenta que pueden existir diferentes personas con dicho nombre. En caso de disponer de información adicional, como su dirección de correo electrónico, tenemos que saber también si ésta es correcta o no, amén de vincular al usuario con datos que pueden quedar anticuados en un plazo breve.

5. ¿La entidad de certificación es realmente una autoridad?
   Por lo general, una entidad de certificación tradicional emite un certificado cubriendo datos sobre los que no tiene control. Por ejemplo, un certificado fusionando el nombre y la dirección de correo electrónico de un usuario no tiene en cuenta si el usuario se llama real y legalmente así, ni considera la posibilidad de que el email cambie o el ISP dé de baja la cuenta y la reasigne a otro usuario (o que todo el ISP desaparezca, por ejemplo).

6. ¿El diseño de seguridad considera al usuario?
   Son muy pocos los usuarios, por ejemplo, que verifican los certificados del servidor remoto cuando establecen una conexión SSL con su navegador.

7. ¿Autoridades de certificación o autoridades de certificación con autoridades de registro?

8. ¿Cómo identifica la autoridad de certificación al usuario?
   Antes de emitir un certificado, la autoridad de certificación debe tener la certeza de que los datos que certifica son correctos.

9. ¿Los certificados son seguros?
   El uso de certificados no garantiza la seguridad. Una cadena es tan fuerte como su eslabón más débil.

10. ¿Por qué existen entidades de certificación?
    La conclusión más clara que se puede extraer de la lectura de este ensayo, elaborado por dos expertos de gran prestigio, es doble: los certificados deben ser expedidos por organismos oficiales con control sobre la información que están certificando (por ejemplo, el ministerio de hacienda y el Número de Identificación Fiscal) y, por otra parte, es necesario almacenar los certificados personales en medios seguros tales

como tarjetas Chip. En este contexto, iniciativas oficiales tales como el proyecto CERES español, por ejemplo, pueden ser la respuesta.

Autor: Fabian Martinez Portantier

Fuentes:

- www.wikipedia.org