Actividad 17. Infraestructura de clave pública PKI

1. Elabora un documento explicando el funcionamiento de una infraestructura de clave pública (PKI)

1. Elabora un documento explicando el funcionamiento de una infraestructura de clave pública (PKI)

La **infraestructura de Clave Pública** (*PKI*, *Public Key Infrastructure*) es un conjunto de hardware, software, políticas y procedimientos necesarios para gestionar de manera segura las claves criptográficas y certificados digitales. Dichos elementos son fundamentales para la seguridad en sistemas de comunicación, autenticación y cifrado en los entornos digitales.

El **objetivo** de las **PKI** es proporcionar de forma segura y fiable la gestión de las identidades, autenticación de entidades y protección de los datos a través de los mecanismos criptográficos basados en el sistema de claves asimétricas.

Los conceptos fundamentales:

1. **Criptografía Asimétrica**: Se basan en el sistema de criptografía de clave pública. Cada entidad tiene 2 claves asociadas:
    a. ***Clave pública***: Se comparte públicamente y se usa para cifrar datos o verificar firmas digitales.
    b. ***Clave privada***: Se mantiene secreta y se utiliza para descifrar información o firmar digitalmente documentos.
2. **Certificados Digitales**: Son archivos electrónicos que vinculan una clave pública con la identidad de su propietario. Estos certificados son emitidos y firmados por una Autoridad de Certificación (CA).

Los componentes de una PKI:

1. **Autoridad de Certificación (CA)**: Entidad confiable que emite y gestiona los certificados digitales. Verifica la identidad del solicitante antes de emitir un comunicado. Dicho certificado incluye la clave pública del solicitante, la información de identidad y la firma digital de la CA, que confirma la autenticidad del certificado.
2. **Autoridad de Registro (RA)**: Intermediario que verifica la identidad de las personas o entidades que solicitan un certificado digital antes de que la CA lo emita. La RA no emite certificados, pero valida las solicitudes para garantizar que la CA emite certificados a usuarios autenticados.
3. **Certificados Digitales**: Contienen la clave pública del usuario y datos sobre su identidad (nombre, dirección de correo electrónico, etc.), así como la firma de la CA que garantiza su validez. Estos certificados son fundamentales para realizar la autenticación y la encriptación de datos.
4. **Repositorio de los Certificados**: Base de datos donde se almacenan los certificados emitidos, así como las listas de certificados revocados (CRL, Certificate Revocation List). Los usuarios y aplicaciones pueden acceder a este repositorio para verificar el estado de los certificados.
5. **Autoridad de Validación (VA)**: Ofrece servicios de verificación de certificados. Utiliza la información del repositorio de certificados y las listas de revocación para verificar si un certificado es válido o ha sido revocado.

El funcionamiento de la PKI:

1. **Generación de Claves**: El primer paso en una PKI es la generación de un par de claves (clave privada y clave pública), que pueden ser creadas por el usuario o por la CA.
2. **Solicitud de Certificado**: El usuario solicita un certificado a la CA enviando su clave pública y otros datos de identificación, generalmente a través de una RA, que verifica su identidad.
3. **Emisión del Certificado**: Una vez que la CA valida la identidad del solicitante, emite un certificado firmado digitalmente. Esta firma asegura que la clave pública en el certificado pertenece al usuario que lo solicitó.
4. **Distribución de Certificados**: El certificado digital es compartido con otras entidades que necesitan verificar la identidad del usuario.
5. **Autenticación y Cifrado**: Con el certificado, el usuario puede autenticarse en servicios seguros y establecer comunicaciones

cifradas. La clave pública se utiliza para cifrar datos que solo el poseedor de la clave privada puede descifrar.

6. **Revocación de Certificados**: Si un certificado deja de ser confiable, la CA puede revocar. Las listas de certificados revocados (CRL) se publican para que otras entidades no acepten certificados comprometidos.

Usos comunes de la PKI:

- **Cifrado de Comunicaciones**: La PKI se utiliza en protocolos como SSL/TLS para establecer conexiones seguras entre navegadores y servidores web.
- **Firmas Digitales**: Permite a las personas firmar electrónicamente documentos o transacciones, garantizando la autenticidad e integridad de los datos.
- **Autenticación**: Las PKI permiten la autenticación fuerte de los usuarios en redes o sistemas, evitando el uso de contraseñas débiles.
- **Correo Electrónico Seguro**: Proporciona cifrado y firma digital para correos electrónicos, asegurando que sólo el destinatario previsto pueda leer el mensaje y que el mensaje no ha sido alterado.

Beneficios de la PKI:

- **Confidencialidad**: El cifrado de los datos asegura que sólo los destinatarios autorizados puedan acceder a la información.
- **Integridad**: Las firmas digitales garantizan que los datos no han sido alterados durante su transmisión.
- **Autenticación**: La PKI proporciona una forma robusta de autenticar usuarios y dispositivos, utilizando certificados digitales en lugar de contraseñas.
- **No Repudio**: La firma digital proporciona evidencia de la participación de una entidad en una transacción, evitando que se niegue posteriormente su intervención.

Desafíos de la PKI:

- **Gestión de Claves**: El manejo de claves privadas y su protección es un desafío crítico, ya que su compromiso puede afectar gravemente la seguridad de la infraestructura.

- **Escalabilidad**: Implementar y gestionar una PKI a gran escala puede ser complicado debido a la necesidad de administrar grandes cantidades de certificados.
- **Confianza en la CA**: Las CA deben ser entidades completamente confiables, ya que un fallo en su seguridad podría comprometer toda la infraestructura.