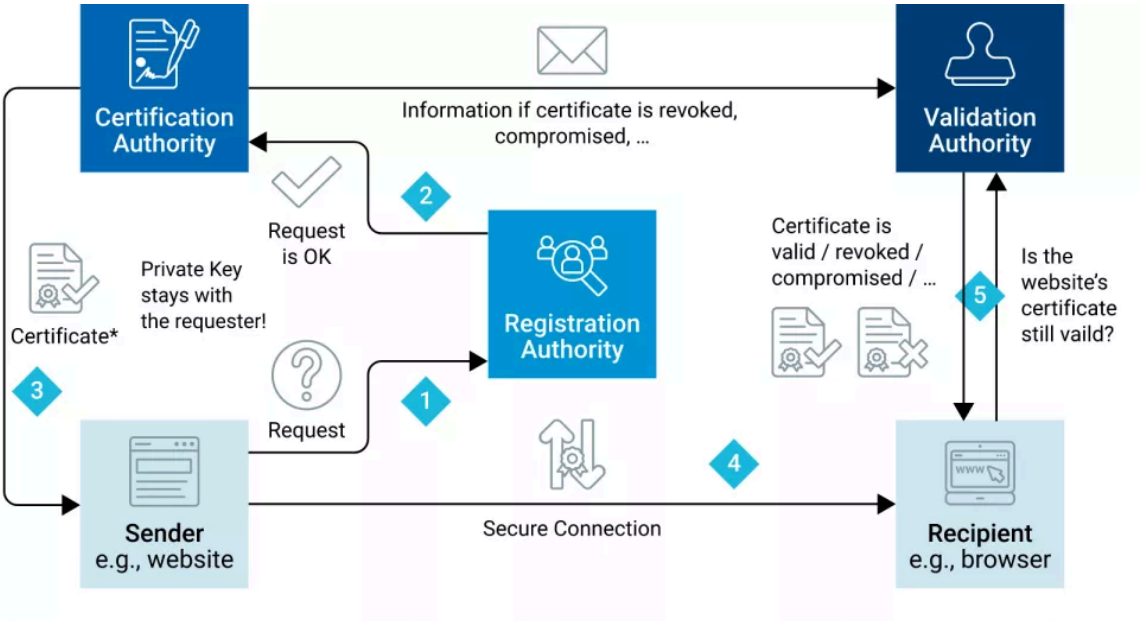
SAD - U2.5. Infraestructura de Clave Pública

Descargar estos apuntes

Índice

1. Infraestructura de Clave Pública (PKI)



* The step of registering and requesting a certificate usually happens once each 1-2 years if it is a certificate used for HTTPS

La PKI (Public Key Infraestructure) hace referencia a herramientas utilizadas para crear y gestionar la seguridad basada en cifrado asimétrico o de clave pública.

Este tipo de cifrado se utiliza para asegurar las comunicaciones en Internet, y lo usamos todo el tiempo en nuestros navegadores, en los servidores web, en la infraestructura de correo electrónico, etc, por lo que entender su funcionamiento es parte fundamental para garantizar la seguridad en nuestras infraestructuras.

> **El cifrado asimétrico en el mundo real**
>
> Ya sabemos cómo funciona el cifrado y descifrado utilizando criptografía asimétrica en OpenSSL.
>
> Ahora bien, ¿cómo se usa esto en el mundo real?

Básicamente, las entidades que necesitan garantizar autenticidad, como los servidores web por ejemplo, tienen su par de claves, pública y privada, y encapsulan su clave pública dentro de un certificado digital x509.

Este certificado añade metadatos como la validez del mismo, firmas digitales, **autoridad certificante**, etc.

Y aquí surge un término importante en la PKI: la **CA** o Autoridad Certificante (Certificate Authority), y una nueva variable en las ecuaciones criptográficas: la **confianza**.

1.1. ¿Cómo funciona una PKI?

La PKI se basa en el uso de certificados digitales, que son documentos digitales que contienen la clave pública de un usuario o entidad, y que han sido firmados digitalmente por una entidad de confianza, llamada Autoridad Certificante (CA).

Pongamos un ejemplo, como los vistos en el caso de las claves privadas y públicas vistas en el apartado anterior:

- **Alice** quiere enviar un mensaje a **Bob** de forma segura.
- **Bob** genera un par de claves, una privada y otra pública.
- **Bob** envía su clave pública a **Alice**. --> `Equivale a un certificado digital`.
- **Alice** cifra el mensaje con la clave pública de **Bob**.
- **Alice** envía el mensaje cifrado a **Bob**.
- **Bob** descifra el mensaje con su clave privada.

En este caso, **Bob** ha generado su par de claves, y ha enviado su clave pública a **Alice**. **Alice** ha utilizado esta clave para cifrar el mensaje, y **Bob** ha utilizado su clave privada para descifrarlo.

Ataque MITM

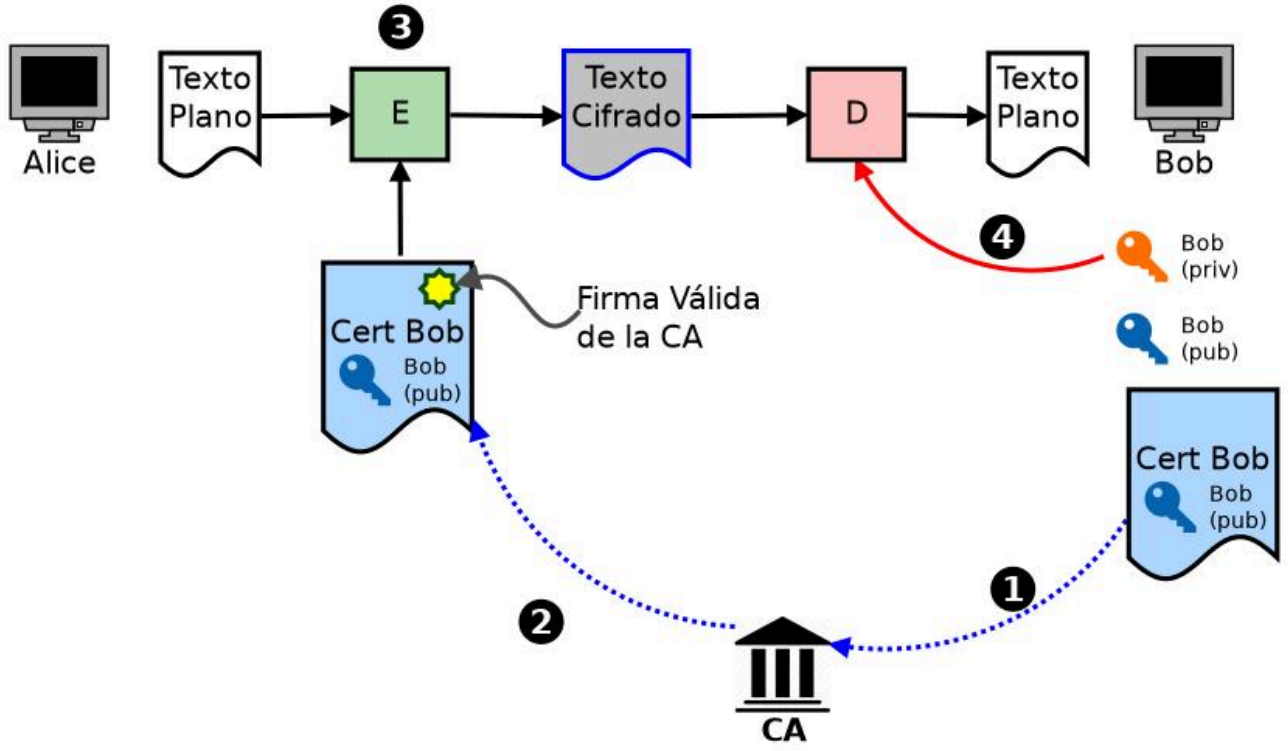
Ahora, imaginemos que un atacante, intercepta el mensaje en el que Bob le envía su clave pública a Alice.
Nada le impide al atacante crear su propio par de claves.
Con ese par de claves puede suplantar la identidad de Bob. Le envía su clave publica a Alice.
A partir de ese momento puede establecer una comunicación con Alice haciéndose pasar por Bob.
Como tiene la clave pública de Bob, el atacante puede cifrar los mensajes con esa clave y hacérselos llegar a Bob.De esta forma puede descifrar tanto los mensajes de Alice a Bob como los de Bob a Alice.

Aquí es donde la PKI aporta su granito de arena para lograr la comunicación segura, y dificulta a los atacantes realizar este tipo de ataque.

> El problema con el caso anterior es que, si bien Alice puede verificar la firma recibida utilizando la clave incluida en el certificado digital recibido, no es capaz de verificar la autenticidad de dicho certificado.

2. La solución: Las CA's

La **CA es una tercera entidad dentro de la PKI**, que también dispone de su clave privada y su clave pública encapsulada en un certificado digital x.509.



Una **CA** es una entidad en la que ambos, Alice y Bob, **confían**. Tanto Alice como Bob tienen el certificado de la CA, firmado por la propia CA para verificar su autenticidad.

> La CA es la entidad encargada de emitir y revocar certificados digitales (pares de claves privadas y públicas).

Verificación de claves

Supongamos que Alice quiere enviar a Bob un mensaje encriptado usando la clave pública de Bob.
Ahora Bob tiene un certificado firmado por una CA.
Alice, cuando recibe un certificado puede verificar que dicho certificado es efectivamente de Bob, y no de un intermediario como intentando suplantar su identidad.

2.1. Otras entidades en la PKI

Existen otras entidades involucradas en la PKI, pero no se las suele nombrar demasiado porque muchas veces su funcionalidad está incorporada en la propia CA, o en las implementaciones de software de los emisores y receptores dentro de una comunicación segura.

Entre ellas se encuentra la **Autoridad de Registro**, o `RA (Registration Authority)`, que verifica que las claves públicas incluidas en los certificados a firmar por la CA pertenezcan efectivamente a la entidad que solicita la firma. Por ejemplo, si Alice quiere firmar su certificado con una CA confiable, la RA debe verificar que la clave pública incluida en el certificado de Alice pertenezca efectivamente a Alice.

Por otro lado, existe la **Autoridad de Validación**, o `VA (Validation Authority)`, encargada de comprobar la validez de los certificados digitales, tanto la validez de su firma digital, como las fechas de expiración.

Finalmente, la **Autoridad de Sellado de Tiempo**, o `TSA (Time Stamp Authority)`, encargada de firmar documentos con el fin de constatar que dichos documentos existían en un determinado instante de tiempo.

3. Seguridad en la PKI

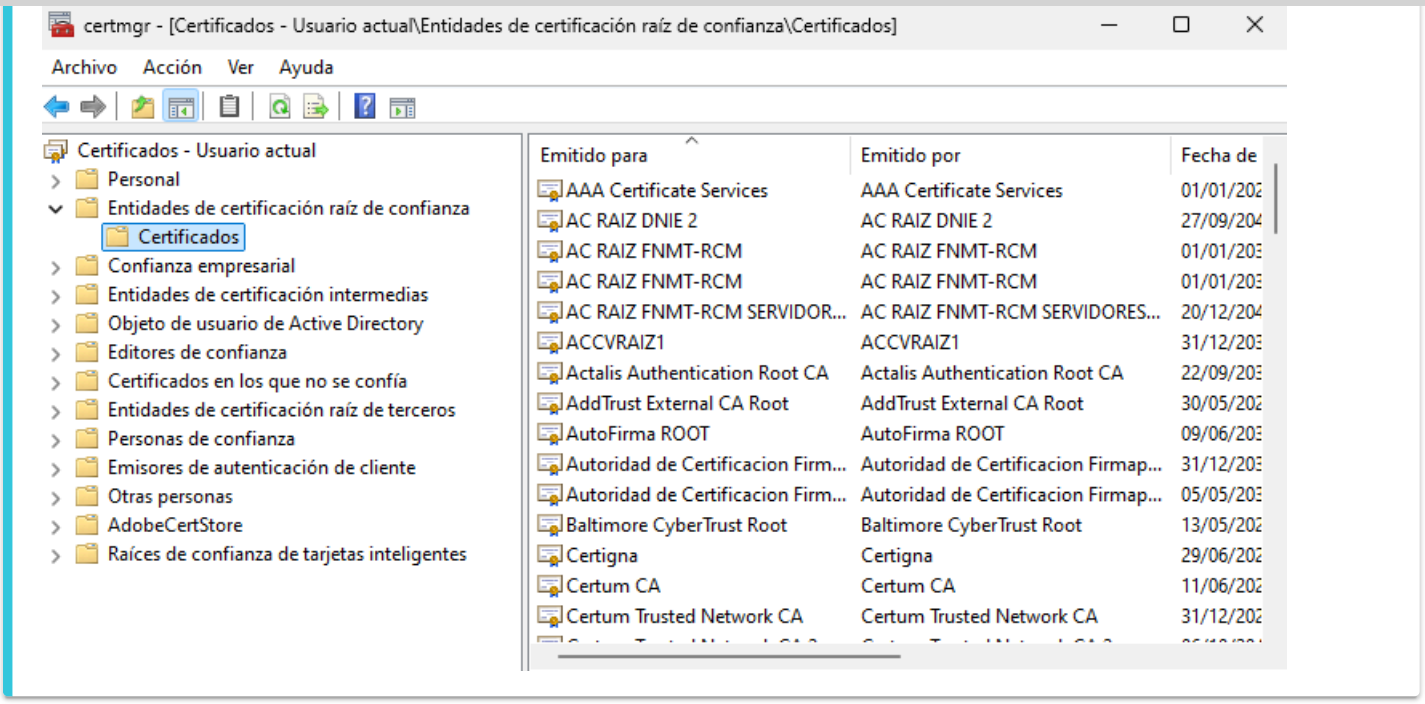
La seguridad en la PKI se basa en la confianza que se tiene en las CA's. Si una CA es comprometida, toda la PKI se ve comprometida.

En primer lugar, y como aspecto más importante, al igual que en criptografía asimétrica, la seguridad en la infraestructura PKI depende principalmente de la **protección que demos a las claves privadas**.

En segundo lugar, cabe mencionar los aspectos de seguridad de una de las herramientas que utilizan PKI y que usamos todo el tiempo: nuestros navegadores web (como parte del Sistema Operativo de un dispositivo).

1. Cuando ingresamos a un sitio seguro, vemos en la URL que el protocolo es HTTPS (HTTP over SSL/TLS). Eso significa que el navegador pudo establecer un canal seguro contra el servidor del sitio.
2. Para lograr esto, el servidor del sitio le envió al navegador su **certificado digital firmado por una CA reconocida en la que el navegador confía**. Esto significa que el navegador tiene una lista de CAs en las que confía almacenadas en sus configuraciones, y asociadas a sus certificados digitales.
   - Cuando un sitio le envía al navegador un certificado digital firmado por una CA, **el navegador utiliza la clave pública de esa CA para verificar la firma**.
     - Si el navegador posee dicha clave pública (certificado digital de la CA), podrá verificar la veracidad del sitio web.
     - En caso contrario, el navegador nos advertirá que el certificado no pudo verificarse, y que el sitio no es confiable.
       Seguramente también nos permita añadir el certificado a los sitios confiables, cosa que no debemos realizar nunca, salvo que sepamos lo que hacemos.

> **Gestor de certificados en Windows**
>
> En Windows, podemos acceder al gestor de certificados digitales desde el panel de control, en la sección de seguridad.
>
> La forma más rápida de acceder a esta configuración es ejecutando la consola de administración de certificados, `certmgr.msc`.
>
> También se puede acceder a esta configuración desde los navegadores. Por ejemplo, en **Chrome** la tenemos en `Configuración > Privacidad y Seguridad > Seguridad > Gestionar certificados`


certmgr - [Certificados - Usuario actual\Entidades de certificación raíz de confianza\Certificados]
Archivo Acción Ver Ayuda
Certificados - Usuario actual
Personal
Entidades de certificación raíz de confianza
Certificados
Confianza empresarial
Entidades de certificación intermedias
Objeto de usuario de Active Directory
Editores de confianza
Certificados en los que no se confía
Entidades de certificación raíz de terceros
Personas de confianza
Emisores de autenticación de cliente
Otras personas
AdobeCertStore
Raíces de confianza de tarjetas inteligentes
Emitido para
Emitido por
Fecha de
AAA Certificate Services
AC RAIZ DNIE 2
AC RAIZ FNMT-RCM
AC RAIZ FNMT-RCM
AC RAIZ FNMT-RCM SERVIDOR...
ACCVRAIZ1
Actalis Authentication Root CA
AddTrust External CA Root
AutoFirma ROOT
Autoridad de Certificacion Firm...
Autoridad de Certificacion Firm...
Baltimore CyberTrust Root
Certigna
Certum CA
Certum Trusted Network CA