

Perfect Forward Secrecy (PFS)

Es un principio que garantiza la confidencialidad de las comunicaciones, incluso si las claves privadas utilizadas para cifrar los datos se ven comprometidas.

Se generan claves de sesión únicas y temporales para cada conexión, en lugar de utilizar una única clave a largo plazo. Estas claves de sesión se generan mediante algoritmos de intercambio de claves efimeras, como Diffie-Hellman, que permite que los participantes acuerden una clave sin necesidad de compartirlo directamente.

PKI (Public Key Infrastructure)

Confidencialidad y privacidad

Facilita el intercambio seguro de información cifrada, donde solo el destinatario autorizado puede descifrar los datos utilizando su clave privada.

Certificación y autenticación

Emite certificados digitales que garantizan la identidad y autenticidad de los participantes en una comunicación, permitiendo verificar la integridad de los datos y establecer conexiones seguras.

Firma digital

Permite generar firmas digitales, que son mecanismos criptográficos para asegurar la integridad y autenticidad de documentos digitales, garantizando que no han sido modificados y provienen de la fuente esperada.



Gestión de claves

Administra y controla la generación, almacenamiento y distribución de claves criptográficas utilizadas en sistemas de cifrado asimétrico.

PKI (Public Key Infrastructure)