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 unicas y temporales para cada conexion, en lugar de utilizar una unica clave a largo Plazo. Estas claves de sesión se generan mediante algoritmos de intercambio de claves efimeras, como Diffie-Helman, que permite que los Participantes acuerden una clave sin necesidad de compartirla directamente

PKI (Public Key Infrastructure)