

HTTPS

Es la versión segura del Protocolo HTTP y se utiliza para proteger la transferencia de datos confidenciales a través de internet. Al utilizar HTTPS, se establece una conexión segura entre un cliente (navegador) y un servidor web mediante la utilización de un certificado digital SSL/TLS.

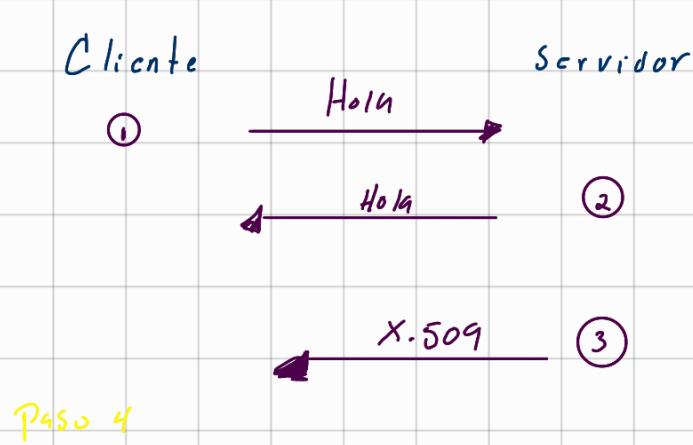
SSL

Desarrollado por Netscape en la década de 1990. SSL es un protocolo de seguridad que proporciona autenticación, confidencialidad e integridad.

TLS

TLS ofrece las mismas funciones que SSL, pero utilizando algoritmos de cifrado más fuertes y modernos, lo que lo hace más seguro y confiable. La mayoría de los navegadores y servidores web admiten TLS en lugar de SSL.

Como pasa todo esto?



Paso 1 y 2

El cliente y el servidor intercambian mensajes de "Hola" que incluyen información sobre las versiones de TLS y los algoritmos de cifrado que admiten.

Paso 3

El servidor presenta su certificado X.509 al cliente, este certificado contiene info como:

- Subject: El nombre del sitio web (nombre común o CN) al que pertenece el certificado
- Issuer: La CA que emitió el certificado
- Validity: Período de validez
- PK del servidor que se utilizará para cifrar
- Signature Algorithm: Algoritmo utilizado para firmar

1. El cliente verifica la validez del certificado presentado por el servidor, esto incluye:

- Comprobar que la fecha actual esté dentro del periodo de validez del certificado
- Verificar que el certificado fue emitido por una CA de confianza web
- Asegurar que el nombre de dominio sea igual al de el certificado
- Comprobar que la firma digital del certificado sea valida utilizando la clave Pública de CA

2. 4

- Signature : Firma del CA

Paso 5

-1. El servidor descifra la l/a sesión utilizando su clave Privada. Ahora,

tanto el cliente como el servidor tienen la misma clave de sesión, que se utilizará para cifrar y descifrar la comunicación entre ellos.

2. El cliente y el servidor comienzan a intercambiar mensajes cifrados utilizando la clave de sesión. Esto garantiza que la comunicación entre ellos sea segura y confidencial.

