¿Cómo funciona SSL/TLS?

¿Qué es el protocolo de enlace de SSL/TLS?

Los protocolos SSL/TLS se utilizan para cifrar información entre dos puntos. Dichos puntos suelen ser el servidor y el cliente, pero en ocasiones es necesario cifrar entre dos servidores o entre dos clientes. Este artículo se centrará solo en la negociación entre el servidor y el sistema cliente.

El cifrado protege los datos durante la transmisión

Negociación entre el servidor y el sistema cliente

Para que tenga lugar la negociación de SSL/TLS, el administrador del sistema debe preparar al menos dos archivos: la clave privada y el certificado Cuando se solicita a una autoridad de certificación, se debe crear un archivo adicional. Este archivo se denomina solicitud de firma de certificado, que se genera de la clave privada.

*Las****autoridad de certificación****, o****certificadoras****, o las siglas****CA****(Certification Authority), señalan a una entidad de confianza, responsable de emitir y revocar los*[*certificados*](https://es.wikipedia.org/wiki/Certificado_digital)*,*

*Utilizando en ellos la*[*firma electrónica*](https://es.wikipedia.org/wiki/Firma_electr%C3%B3nica)*, para lo cual se emplea la*[*criptografía*](https://es.wikipedia.org/wiki/Criptograf%C3%ADa)*de*[*clave pública*](https://es.wikipedia.org/wiki/Clave_p%C3%BAblica)*.*

*Jurídicamente, se trata de un caso particular de*[*Prestador de Servicios de Certificación*](https://es.wikipedia.org/wiki/Prestador_de_Servicios_de_Certificaci%C3%B3n)*. Una autoridad de certificación expide los certificados digitales, que ya contienen las identificaciones numéricas y las contraseñas que se necesitan, poniendo a disposición el procedimiento de verificación para validar el certificado proporcionado.*

Es posible que se deban instalar en el servidor unos certificados adicionales denominados certificados de autoridad de certificación intermedia y certificados raíz de autoridad de certificación. Eso depende también del software de servidor. En general, no hace falta instalar en los navegadores o las aplicaciones cliente los archivos de certificado de autoridad de certificación intermedia y de certificado raíz de autoridad de certificación (CA).

Protocolo de enlace de SSL estándar

A continuación, se muestra un protocolo de enlace de SSL estándar cuando se utiliza un algoritmo de intercambio de claves RSA:

**1. Hola cliente**

Información que el servidor necesita para comunicarse con el cliente mediante SSL. Incluye el número de versión de SSL, la configuración de cifrado y datos específicos de la sesión.

**2. Hola servidor**

Información que el servidor necesita para comunicarse con el cliente mediante SSL. Incluye el número de versión de SSL, la configuración de cifrado y datos específicos de la sesión.

**3. Autenticación y número secreto principal preliminar**

El cliente autentica el certificado de servidor, por ejemplo, nombre común / fecha / emisor. El cliente (según el cifrado) crea el número secreto principal preliminar de la sesión, cifra con la clave pública del servidor y envía el número secreto principal preliminar cifrado al servidor.

**4. Descifrado y número secreto principal**

El servidor utiliza su clave privada para descifrar el número secreto principal preliminar. El servidor y el cliente efectúan pasos para generar el número secreto principal con el cifrado acordado.

**5. Cifrado con clave de sesión**

El cliente y el servidor intercambian mensajes para informar de que se cifrarán futuros mensajes.

Identidad de cliente o de usuario

Si hablamos de PKI o certificados de cliente, a muchas personas le vienen a la cabeza imágenes de empresas protegiendo y completando las transacciones online de sus clientes.

Sin embargo, dichos certificados se encuentran en muchos aspectos de nuestra vida cotidiana:

**Ejemplos:**

* Cuando iniciamos sesión en una VPN o cuando utilizamos una tarjeta bancaria en un cajero.
* Una tarjeta para acceder a un edificio.
* Una tarjeta inteligente SUBE para el transporte público.

“Estos *certificados digitales se encuentran en las gasolineras, los robots de cadenas de montaje de automóviles o, incluso, en los pasaportes.*

*Los gobiernos emiten documentos de identidad que tienen diferentes usos, por ejemplo, para pagar impuestos locales, facturas de electricidad y permisos de conducir.*

*Y la razón es fácil de entender: los certificados de cliente son muy importantes para la protección en Internet de las personas.*

*Como su nombre indica, se utilizan para identificar a un cliente o a un usuario autenticando el cliente en el servidor y estableciendo con exactitud su identidad.”*

**Los certificados de cliente y de servidor SSL desempeñan una función muy similar, pero los segundos se utilizan para identificar al cliente o al individuo, y los primeros autentican al propietario del sitio web.**

En general, los certificados de servidor se emiten para nombres de host, que pueden ser un nombre de equipo (por ejemplo, “XYZ-SERVER-01”) o un nombre de dominio (por ejemplo, “www.digicert.com”).

Un navegador web se pone en contacto con el servidor y valida la autenticidad del certificado de servidor SSL.

Eso indica al usuario que no hay curiosos observando su interacción con el sitio web y que el sitio web es exactamente lo que afirma ser.

¿Cómo se efectúa?

En la práctica**, un operador de sitios web obtiene un certificado pidiendo una solicitud de firma de certificado a un proveedor de certificados**.

Dicho **certificado es un documento electrónico** que contiene toda la información esencial: nombre del sitio web, dirección de correo electrónico de contacto e información de la empresa.

**Antes de emitir un certificado**, el proveedor solicitará la dirección de correo electrónico de contacto del sitio web a un registrador de dominios públicos y comprobará que la dirección publicada coincide con la dirección de correo electrónico indicada en la solicitud de certificado, con lo cual se asegurará de que el ciclo de seguridad se haya cerrado.

**El proveedor de certificados firma la solicitud**, lo cual genera un certificado público que se facilita a cualquier navegador web que se conecte con el sitio web, pero lo importante es que demuestra al navegador web que el proveedor ha emitido un certificado para la persona que considera que es el propietario del sitio web.

Asimismo, puede configurar un sitio web para que cualquier usuario que desee conectarse proporcione un certificado de cliente, un nombre de usuario y una contraseña que sean válidos.