¿Qué es SSL/TLS?

SSL/TLS utiliza [certificados](https://www.ssl.com/faqs/what-is-an-x-509-certificate/) para establecer un enlace cifrado entre un servidor y un cliente. Esto permite que información confidencial, como los datos de tarjetas de crédito, se transmita de forma segura por internet.

El certificado contiene una clave pública que autentica la identidad del sitio web y permite la transferencia de datos cifrados mediante criptografía asimétrica o de clave pública. La clave privada correspondiente se mantiene en secreto en el servidor.

¿Cómo funciona SSL/TLS?

Los certificados SSL/TLS autentican identidades y permiten conexiones cifradas a través del [protocolo de enlace SSL/TLS](https://www.ssl.com/article/ssl-tls-handshake-overview/) :

1. El cliente solicita acceso a un recurso protegido, como una página de inicio de sesión.
2. El servidor responde enviando su certificado SSL, incluida la clave pública.
3. El cliente verifica que el certificado sea válido y confiable. Esto garantiza la autenticidad del servidor.
4. El cliente genera una clave de sesión simétrica y la cifra con la clave pública del servidor. Esto transmite la clave de sesión al servidor de forma segura.
5. El servidor descifra la clave de sesión con su clave privada.
6. Ambas partes utilizan la clave de sesión simétrica para cifrar y descifrar todos los datos transmitidos.

Este protocolo de enlace permite a ambas partes negociar un canal cifrado sin compartir información confidencial a través de canales inseguros. La sesión cifrada protege los datos en tránsito entre el cliente y el servidor.

Cifrado y claves SSL/TLS

Hay dos tipos de claves de cifrado utilizadas en SSL/TLS:

* **Claves asimétricas** : el par de claves pública y privada se utiliza para identificar el servidor e iniciar la sesión cifrada. La clave privada solo la conoce el servidor, mientras que la clave pública se comparte mediante un certificado.
* **Claves de sesión simétricas** : Se generan claves desechables para cada conexión y se utilizan para cifrar/descifrar los datos transmitidos. Las claves simétricas se intercambian de forma segura mediante cifrado asimétrico.

SSL/TLS admite múltiples cifrados simétricos y algoritmos de clave pública asimétricos. Por ejemplo, AES con claves de 128 bits es un cifrado simétrico común, mientras que RSA y ECC suelen utilizar algoritmos asimétricos.

Para una comparación detallada de los dos algoritmos de firma digital más utilizados, lea nuestro artículo [Comparación de ECDSA vs RSA](https://www.ssl.com/article/comparing-ecdsa-vs-rsa/) .

Proteja su sitio web y aumente la confianza de sus usuarios. No espere a que lleguen las amenazas. Explore hoy mismo nuestras completas opciones de certificados SSL/TLS y garantice su seguridad en línea.

[**Obtenga más información sobre los certificados SSL/TLS**](https://www.ssl.com/certificates/)

Navegación web segura con HTTPS

El uso más común de SSL/TLS es [HTTPS](https://www.ssl.com/faqs/what-is-https/) , que protege el tráfico web. Los sitios web con HTTPS utilizan SSL/TLS para autenticar y cifrar todo el tráfico entre el navegador y el servidor.

Para verificar que un sitio web tiene un certificado SSL válido, busque estos indicadores en su navegador:

* **Icono de candado** : Indica que la conexión es segura y está autenticada. Puede ir acompañado del nombre de la empresa.
* **https://** – La S después de http indica que se está utilizando cifrado.

Sin HTTPS, los datos se transmiten sin cifrar y son vulnerables a la interceptación y manipulación por parte de [intermediarios](https://www.ssl.com/faqs/what-is-a-man-in-the-middle-attack/) . HTTPS garantiza la autenticidad y la privacidad del sitio web.

Obtención de un certificado SSL/TLS

Para habilitar HTTPS en su sitio web, debe obtener un certificado SSL/TLS de una autoridad de certificación (CA) de confianza, como [SSL.com](https://www.ssl.com/) . El proceso general es el siguiente:

1. Genere una solicitud de firma de certificado (CSR) en su servidor. Esta contiene su clave pública y los datos del dominio.
2. Envíe la CSR a la CA para verificar su identidad y emitir un certificado confiable.
3. Instale el certificado emitido en su servidor web para implementar HTTPS.

Puede elegir niveles de certificado solo para validación de dominio o validación extendida para máxima credibilidad. Mantenga sus certificados actualizados y utilice el protocolo TLS 1.3 más reciente para una seguridad óptima.

Resumen

SSL/TLS y HTTPS proporcionan seguridad esencial para las comunicaciones por internet. Los certificados vinculan identidades validadas a pares de claves criptográficas, mientras que los protocolos de enlace SSL/TLS negocian sesiones cifradas entre un cliente y un servidor. Busque el candado y HTTPS en su navegador y obtenga un certificado SSL/TLS de una CA de confianza como SSL.com para proteger su sitio web. Comprender los fundamentos del cifrado de clave pública y la autenticación con certificados es fundamental para aprovechar SSL/TLS y garantizar la seguridad de las transacciones y comunicaciones en línea.

**¿Qué es IPSec?**

**IPSec (Internet Protocol Security)** es un conjunto de protocolos que protege las comunicaciones IP mediante autenticación y cifrado, muy usado en **VPNs (Virtual Private Networks)**.

**Modos de funcionamiento:**

* **Modo Transporte:** Cifra solo el contenido del paquete IP.
* **Modo Túnel:** Cifra todo el paquete IP original, añadiendo uno nuevo (muy común en VPNs).

**¿Cómo funciona?**

1. **Negociación de seguridad (IKE):**
   * Se establecen políticas de seguridad entre los puntos finales (gateway y cliente).
   * Se realiza un intercambio de claves seguro.
2. **Cifrado y autenticación del tráfico:**
   * Se utiliza cifrado simétrico (por ejemplo, AES).
   * Se autentican los datos usando HMAC o SHA.

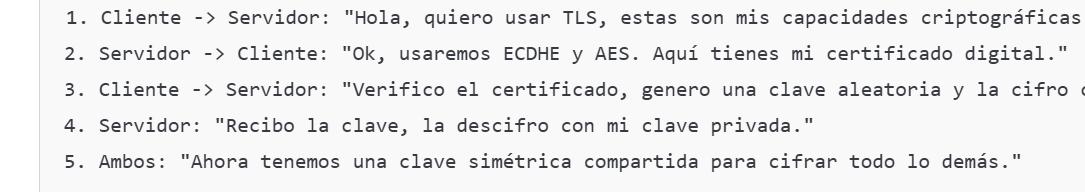
**Algoritmos utilizados:**

* **Cifrado:** AES, 3DES.
* **Autenticación:** SHA-1, SHA-256.
* **Intercambio de claves:** Diffie-Hellman.

**Ejemplo de aplicación:**

* VPNs corporativas que conectan oficinas remotas con la red interna de la empresa.
* VPNs personales para proteger la navegación en redes Wi-Fi públicas.

|  |  |  |
| --- | --- | --- |
| Característica | TLS/SSL | IPSec VPN |
| Capa del modelo OSI | Capa de Aplicación (HTTP, SMTP) | Capa de Red (IP) |
| Uso común | Navegación web, correo | Acceso remoto a redes, túneles VPN |
| Cifrado | Cifrado de datos de aplicación | Cifrado de todo el paquete IP |
| Ejemplo real | https://www.banco.com | Conexión VPN entre sucursales |

Ejemplo de Demostracion

