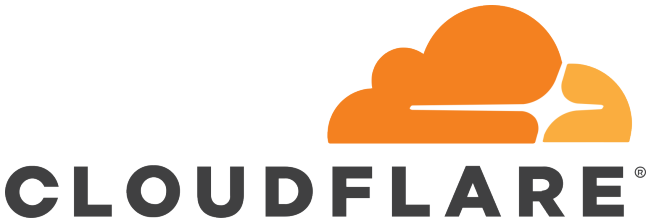
How SSL Certificates Work: A Breakdown



What is SSL?

SSL stands for Secure Sockets Layer, a protocol for encrypting, securing, and authenticating communications on the Internet. Although SSL has been replaced by TLS (Transport Layer Security), the term "SSL" is still widely used to describe this technology.

Primary Use Cases

- Securing communications between a client and a server (e.g., web browsers and websites)
- Securing email, VoIP, and other communications over unsecured networks

How does SSL/TLS work?

SSL/TLS operates based on several key principles:

- A secure connection begins with a TLS handshake, where the client and server exchange public keys and establish a secure session.
- Session keys are generated during the handshake and used to encrypt/decrypt all communications within the session.
- Each session uses unique session keys.
- TLS authenticates the server's identity to ensure it is legitimate.

- Data integrity is ensured using a message authentication code (MAC).

The TLS Handshake

The TLS handshake is the process by which two parties establish a secure connection. This involves:

- **Asymmetric encryption:** Public and private keys are used for secure communication during the handshake.
- **Session keys:** Generated during the handshake and used for symmetric encryption for the remainder of the session.

Symmetric Encryption

After the handshake, both parties use the same session key for encryption. These keys are temporary and unique to each session, ensuring high levels of security.

Authenticating the Origin Server

TLS communications include a digital signature (MAC) that authenticates the server and prevents data alteration during transmission.

What is an SSL Certificate?

An SSL certificate is a data file installed on a website's server. It contains:

- The public key
- The identity of the website owner
- Other identifying information

SSL certificates are essential for enabling encrypted communications using TLS.

Self-Signed Certificates

Website owners can create self-signed certificates, but these are not as trusted as certificates issued by a certificate authority (CA).

Obtaining an SSL Certificate

SSL certificates are issued by certificate authorities (CAs) after verifying the website owner’s identity. The CA maintains a copy of the certificates they issue.

Free SSL Certificates

Many CAs charge for SSL certificates, but some, like Cloudflare, offer them for free to encourage secure Internet practices.

HTTP vs. HTTPS

HTTPS is HTTP with SSL/TLS encryption. A website using HTTPS:

- Has a valid SSL certificate issued by a CA
- Encrypts all traffic to and from the website
- Ensures data authenticity and integrity

Modern browsers mark HTTP websites as "not secure," making HTTPS essential for trust and security.

For further details on SSL/TLS, visit the official Traefik documentation.

Revision #2
Created 7 October 2024 16:18:17 by aeoneros
Updated 12 January 2025 13:21:13 by aeoneros