What is SSL? | SSL definition

Secure Sockets Layer (SSL) is a security protocol that provides privacy, authentication, and integrity to Internet communications. SSL eventually evolved into Transport Layer Security (TLS).

Share

What is SSL? What is an SSL Certificate? What is TLS? Why Use HTTPS? What is HTTPS? SSL Glossary of Terms

SSL
Learning Objectives

After reading this article you will be able to:

- Define SSL
- Understand the difference between SSL and TLS
- Understand SSL certificates

Related Content

What is an SSL Certificate?

SSL Handshake

Keyless SSL

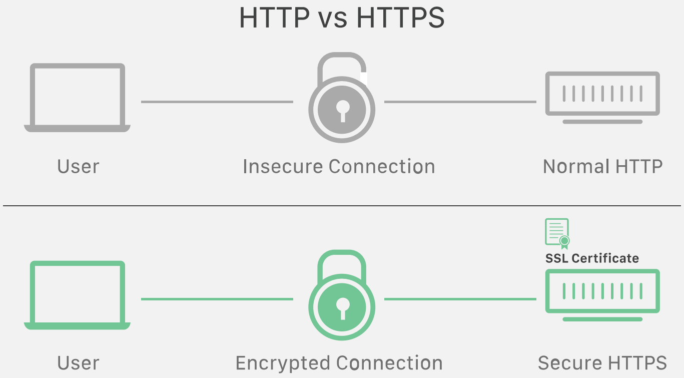
Public Key Encryption

Why Use HTTPS?

What is SSL?

SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.

A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP."



How does SSL/TLS work?

- In order to provide a high degree of privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
- SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
- SSL also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.

There have been several iterations of SSL, each more secure than the last. In 1999 SSL was updated to become TLS.

Why is SSL/TLS important?

Originally, data on the Web was transmitted in plaintext that anyone could read if they intercepted the message. For example, if a consumer visited a shopping website, placed an order, and entered their credit card number on the website, that credit card number would travel across the Internet unconcealed.

SSL was created to correct this problem and protect user privacy. By encrypting any data that goes between a user and a web server, SSL ensures that anyone who intercepts the data can only see a scrambled mess of characters. The consumer's credit card number is now safe, only visible to the shopping website where they entered it.

SSL also stops certain kinds of cyber attacks: It authenticates web servers, which is important because attackers will often try to set up fake websites to trick users and steal data. It also prevents attackers from tampering with data in transit, like a tamper-proof seal on a medicine container.

Are SSL and TLS the same thing?

SSL is the direct predecessor of another protocol called TLS (Transport Layer Security). In 1999 the Internet Engineering Task Force (IETF) proposed an update to SSL. Since this update was being developed by the IETF and Netscape was no longer involved, the name was changed to TLS. The differences between the final version of SSL (3.0) and the first version of TLS are not drastic; the name change was applied to signify the change in ownership.

Since they are so closely related, the two terms are often used interchangeably and confused. Some people still use SSL to refer to TLS, others use the term "SSL/TLS encryption" because SSL still has so much name recognition.

Is SSL still up to date?

SSL has not been updated since SSL 3.0 in 1996 and is now considered to be deprecated. There are several known vulnerabilities in the SSL protocol, and security experts recommend discontinuing its use. In fact, most modern web browsers no longer support SSL at all.

TLS is the up-to-date encryption protocol that is still being implemented online, even though many people still refer to it as "SSL encryption." This can be a source of confusion for someone shopping for security solutions. The truth is that any vendor offering "SSL" these days is almost certainly providing TLS protection, which has been an industry standard for over 20 years. But since many folks are still searching for "SSL protection," the term is still featured prominently on many product pages.

What is an SSL certificate?

SSL can only be implemented by websites that have an SSL certificate (technically a "TLS certificate"). An

SSL certificate is like an ID card or a badge that proves someone is who they say they are. SSL certificates are stored and displayed on the Web by a website's or application's server.

One of the most important pieces of information in an SSL certificate is the website's public key. The public key makes encryption possible. A user's device views the public key and uses it to establish secure encryption keys with the web server. Meanwhile the web server also has a private key that is kept secret; the private key decrypts data encrypted with the public key.

Certificate authorities (CA) are responsible for issuing SSL certificates.

What are the types of SSL certificates?

There are several different types of SSL certificates. One certificate can apply to a single website or several websites, depending on the type:

- Single-domain: A single-domain SSL certificate applies to only one domain (a "domain" is the name of a website, like www.cloudflare.com).
- Wildcard: Like a single-domain certificate, a wildcard SSL certificate applies to only one domain. However, it also includes that domain's subdomains. For example, a wildcard certificate could cover www.cloudflare.com, blog.cloudflare.com, and developers.cloudflare.com, while a single-domain certificate could only cover the first.
- Multi-domain: As the name indicates, multi-domain SSL certificates can apply to multiple unrelated domains.

SSL certificates also come with different validation levels. A validation level is like a background check, and the level changes depending on the thoroughness of the check.

- Domain Validation: This is the least-stringent level of validation, and the cheapest. All a business has to do is prove they control the domain.
- Organization Validation: This is a more hands-on process: The CA directly contacts the person or business requesting the certificate. These certificates are more trustworthy for users.
- Extended Validation: This requires a full background check of an organization before the SSL certificate can be issued.

How can a business obtain an SSL certificate?

Cloudflare offers free SSL certificates for any business. A website protected by Cloudflare can activate SSL with a few clicks. Websites may need to set up an SSL certificate on their origin server as well: this article has further instructions.

More about SSL/TLS

For more on how SSL/TLS encryption works, see What is TLS? Use the Cloudflare Diagnostic Center to check if a website is properly implementing SSL/TLS encryption.

About SSL

What is SSL?

What is TLS?

How SSL Works

Contact Sales:

+1 (888) 99 FLARE

About HTTPS

What is HTTPS?

Why Use HTTPS?

HTTP Security Gaps

Connection Not Private

About Encryption

What is Encryption?

Public Key Encryption

Asymmetric Encryption

Lava Lamp Encryption

Cryptographic Key

What is a Session Key?

SSL Glossary

What is Mixed Content?

SSL Handshake

What is an SSL Certificate?

SSL Certificate Types

Why Use TLS 1.3?

What is SNI?

What is Encrypted SNI?

What is Domain Spoofing?

Learning Center Navigation

Learning Center Home

DDoS Learning Center

CDN Learning Center

DNS Learning Center

Performance Learning Center

Security Learning Center

Serverless Learning Center

Bots Learning Center

Cloud Learning Center

Access Management Learning Center

Network Layer Learning Center

Privacy Learning Center

Video Streaming Learning Center