## What is SSL?

[SSL](https://www.cloudflare.com/learning/ssl/what-is-ssl/) stands for Secure Sockets Layer, and it refers to a protocol for encrypting and securing communications that take place on the Internet. Although SSL was replaced by an updated protocol called [TLS (Transport Layer Security)](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/) some time ago, "SSL" is still a commonly used term for this technology.

The main use case for SSL/TLS is securing communications between a client and a server, but it can also secure email, VoIP, and other communications over unsecured networks.

## How does SSL/TLS work?

These are the essential principles to grasp for understanding how SSL/TLS works:

* Secure communication begins with a [TLS handshake](https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/), in which the two communicating parties open a secure connection and exchange the public key
* During the TLS handshake, the two parties generate session keys, and the session keys encrypt and decrypt all communications after the TLS handshake
* Different session keys are used to encrypt communications in each new session
* TLS ensures that the party on the server side, or the website the user is interacting with, is actually who they claim to be
* TLS also ensures that data has not been altered, since a message authentication code (MAC) is included with transmissions

With TLS, both [HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) data that users send to a website (by clicking, filling out forms, etc.) and the HTTP data that websites send to users is encrypted. Encrypted data has to be decrypted by the recipient using a key.

#### The TLS handshake

TLS communication sessions begin with a TLS handshake. A TLS handshake uses something called asymmetric encryption, meaning that two different keys are used on the two ends of the conversation. This is possible because of a technique called public key cryptography.

In public key cryptography, two keys are used: a public key, which the server makes available publicly, and a private key, which is kept secret and only used on the server side. Data encrypted with the public key can only be decrypted with the private key, and vice versa.

During the TLS handshake, the client and server use the public and private keys to exchange randomly generated data, and this random data is used to create new keys for encryption, called the session keys.

#### Symmetric encryption with session keys

Unlike asymmetric encryption, in symmetric encryption the two parties in a conversation use the same key. After the TLS handshake, both sides use the same session keys for encryption. Once session keys are in use, the public and private keys are not used anymore. Session keys are temporary keys that are not used again once the session is terminated. A new, random set of session keys will be created for the next session.

## Authenticating the origin server

TLS communications from the server include a message authentication code, or MAC, which is a digital signature confirming that the communication originated from the actual website. This authenticates the server, preventing [man-in-the-middle attacks](https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/) and domain spoofing. It also ensures that the data has not been altered in transit.

## What is an SSL certificate?

An SSL certificate is a file installed on a website's [origin server](https://www.cloudflare.com/learning/cdn/glossary/origin-server/). It's simply a data file containing the public key and the identity of the website owner, along with other information. Without an SSL certificate, a website's traffic can't be encrypted with TLS.

Technically, any website owner can create their own SSL certificate, and such certificates are called self-signed certificates. However, browsers do not consider self-signed certificates to be as trustworthy as SSL certificates issued by a certificate authority.

## How does a website get an SSL certificate?

Website owners need to obtain an SSL certificate from a certificate authority, and then install it on their web server (often a web host can handle this process). A certificate authority is an outside party who can confirm that the website owner is who they say they are. They keep a copy of the certificates they issue.

## Is it possible to get a free SSL certificate?

Many certificate authorities charge for SSL certificates. To help make the Internet more secure, Cloudflare offers [free SSL certificates](https://www.cloudflare.com/ssl/). Cloudflare was the first Internet security and performance company to do so. Cloudflare also has worked to optimize SSL/TLS performance so that websites moving from HTTP to HTTPS don't have their [performance](https://www.cloudflare.com/learning/performance/why-site-speed-matters/) impacted. [Learn more about Cloudflare and SSL](https://www.cloudflare.com/ssl/).

## What is the difference between HTTP and HTTPS?

The S in "HTTPS" stands for "secure." HTTPS is just HTTP with SSL/TLS. A website with an HTTPS address has a legitimate SSL certificate issued by a certificate authority, and traffic to and from that website is authenticated and encrypted with the SSL/TLS protocol.

To encourage the Internet as a whole to move to the more secure HTTPS, many web browsers have started to mark HTTP websites as "not secure" or "unsafe." Thus, not only is HTTPS essential for keeping users safe and user data secure, it has also become essential for building trust with users. [Test a website for SSL/HTTPS issues](https://www.cloudflare.com/diagnostic-center/).

**What Is SSL? How Do SSL Certificates Work?**

Ever wondered about the difference between HTTP and HTTPS?

[**[](https://dzone.com/users/3344321/comodosslstore.html)**](https://dzone.com/users/3344321/comodosslstore.html)**by**

[**Sanjay Barot**](https://dzone.com/users/3344321/comodosslstore.html)

**·**

**Nov. 19, 18 ·**[**Security Zone**](https://dzone.com/application-web-network-security)**· Presentation**

**Like** [**(20)**](https://dzone.com/articles/what-is-ssl-how-do-ssl-certificates-work)

**Comment (3)**

**Save**

[**Tweet**](https://dzone.com/articles/what-is-ssl-how-do-ssl-certificates-work)

**35.87k Views**

Join the DZone community and get the full member experience.

[**JOIN FOR FREE**](https://dzone.com/articles/what-is-ssl-how-do-ssl-certificates-work)

"What is an SSL Certificate?" This is one of the most-asked questions on the Internet. Technically, SSL/TLS can be defined as a ‘cryptographic protocol’ that provides secure communication between a web browser and a server.

SSL stands for the Secure Socket Layer. It is also known as TLS, short for ‘Transfer Layer Security.’ SSL certificates are widely used in websites, mobile apps, emails, fax, messaging, etc. Generally, an SSL certificate is deployed on a website — its most common usage. While browsing on the Internet, you may have noticed that some sites say HTTPS while some say HTTP. You may have wondered what’s the difference between the two. Well, an SSL certificate is the difference.

The ‘S’ in HTTPS stands for security. An SSL certificate secures the communication between your PC/smartphone and the web server of an HTTPS-enabled website.

**Why SSL?**

When you access a website, communication takes place between the web browser of your PC or mobile device and the web server of the website. Information is then transferred from both sides. An SSL certificate protects the information transferred between both. This is compelling from a security and privacy point of view. Every day, we all send confidential information across the Internet in abundance. This includes delicate information such as email IDs, user IDs, passwords, credit/debit card details, bank account details, etc. If such confidential data is transmitted over an unprotected protocol, there is a significant risk of such private information coming in the hands of cyber criminals. Such interception of data being transmitted is called a Man-in-the-middle (MITM) attack.

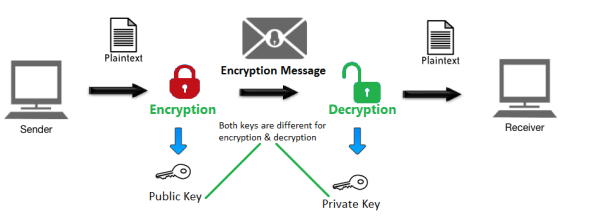
As far as organizations are concerned, the importance of data security should be taken even more seriously. In any organization, a colossal amount of secret data is transferred, whether it is inside the organization or outside. If even a single document is leaked, it can cause a considerable amount of damage to the organization. This is where SSL certificates enter the picture.

**What Does an SSL Certificate Do?**

We all have sent/received something in an envelope, right? You must have used (or at least seen!) an envelope seal to keep the documents safe. Simply put, that is what an SSL certificate does. An SSL certificate safeguards any information being transferred between a client and a server. This is done via **Encryption**.

**What Is Encryption?**

As stated above, SSL certificates facilitate Encryption. Let’s talk about how that works. If you send any data on an HTTPS-enabled website, that piece of information is converted into an unreadable string of characters. For example, if your password is 1234, then it might be converted into something like ^%jrt5/\*u. This makes it virtually impossible for any hacker to interpret the information, even if they manage to intercept the data somehow.



This [Encryption technique](https://comodosslstore.com/blog/what-is-encryption-and-why-do-you-need-it.html) has been used for centuries. It is believed that Julius Caesar was the first person to use it. It is referred to as Caesar’s Cipher. Compared to Caesar’s Cipher, today’s encryption methods are much more complex. Specific algorithms are applied to change the bundle of data into an undecipherable format. Forget about humans — these algorithms are so complex in nature that even supercomputers can’t crack them. Seriously, it would take a supercomputer over 100 years to crack the 256-bit encryption.

**How Do SSL Certificates Work?**

[SSL certificates work](https://comodosslstore.com/blog/how-do-ssl-certificates-works.html) based on public key infrastructure (PKI) or public key cryptography. This method involves two distinct cryptographic keys — Private Key and Public Key. The public key is used for encryption purposes and the private key is for decryption.

As the name implies, the Public Key is shared with everyone who receives the certificate upon visiting a website. You are using the public key without even knowing it. These keys are stored in the digital certificate. You can see the public key of a website by viewing the SSL certificate details in your browser.

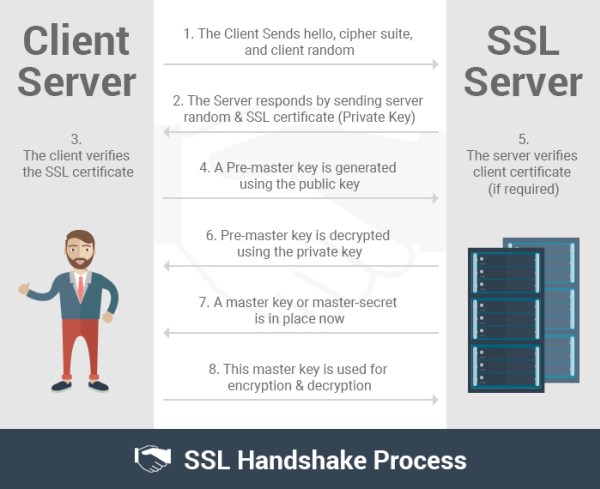


Both the keys are different but related to each other. This means that the information encrypted using a particular public key can only be decrypted using the private key attached to it. A secure connection is established if the client can verify that the public key matches the private key. This is called ‘Asymmetric Encryption.'

**The SSL Handshake**

The process of establishing a secure connection is referred to as an ‘SSL handshake.’ It’s not like the old-fashioned handshake that we all do every day. Instead, it’s a modern-day version of a handshake (just like the “cool” millennials do). This handshake involves three steps (no dabbing involved!)— hello, server verification, and transfer of keys.

* **Hello**: As we (well, most of us!) all do upon meeting someone, the client and the server say *Hello*to each other. The client sends a ClientHello message to the server. This “Hello” contains some SSL certificate information. In response to this ClientHello message, the server responds to it by ServerHello message. Likewise, it also consists of similar information as the ClientHello  message.
* **Server Verification**: Now, a secure connection is in place between the client and the server (a good amount of comfort between the two). Now, this is the stage where the client verifies the identity of the server. How exactly? Through an SSL certificate. An SSL certificate contains information of the owner/organization, its location public key, validity dates, etc. The client makes sure that a valid certificate authority (CA) has validated the certificate.
* **Transfer of Keys**: Once the client verifies and authenticates the server, it’s time for both the parties to share their keys. After the verification of the server is done, the client uses the public key to generate a pre-master key. Then, this pre-master key is sent to the server. The server decrypts this pre-master key using its private key. This way a new key is computed by the client and the server. This is an example of **Asymmetric Encryption**. This master key is used to encrypt and decrypt the information transferred between the client and the server. This is called **Symmetric Encryption**. Thus, both the techniques of Encryption are deployed to ensure a secure connection.



**What Details Does an SSL Certificate Include?**

An SSL certificate includes the details of the party to whom the certificate has been issued. It includes the following information:

* Domain Name
* Certificate Validity Period
* Certificate Authority (CA) Details
* Public Key
* Public Key Algorithm
* Certificate Signature Algorithm
* SSL/TLS Version
* Thumbprint
* Thumbprint Algorithm

The aforementioned information is included no matter which type of SSL certificate has been installed on the website. However, some additional information is also provided in the advanced level SSL certificates. For instance, organization validation (OV) and extended validation (EV) SSL certificates include details of the organization such as:

* Name of the organization
* Website owner
* Address
* City
* State
* Country