

SSL CERTIFICATES EXPLAINED





It's now a standard that every website adds an SSL certificate to protect customer information and secure transactions online.

This means that when you visit a website with an SSL Certificate, the information sent between your computer and the server is encrypted, so it can't be read by anyone else on the network. The encryption protects any sensitive information such as credit card numbers, passwords, emails, etc.

A website with an SSL certificate is notable as there is a padlock icon next to the URL on a browser's address bar. It's right to assume that a website with this padlock icon is protected with an SSL certificate.

How Do SSL Certificates Work?

An SSL certificate is the internet's way of ensuring that criminals cannot hijack, read, or modify information between your browser and servers.

Without an SSL Certificate, data could be intercepted by anyone on a local network between your web visitors and your server. The encryption protects any sensitive information such as credit card numbers, passwords, emails, etc.

Here is a step-by-step process on how SSL certificates work.

1. A server or browser attempts to connect to a website that is secured with SSL certificates.
2. The server or browser requests for "identification" from the webserver.
3. The web server sends a copy of its SSL certificate to the browser or server.
4. The server or browser checks the SSL certificate to see if the certificate is trustworthy. If the certificate is trustworthy, it signals approval to the webserver.
5. The web server then sends an acknowledgment that is signed digitally, and an SSL encrypted session begins.
6. Encrypted data can now be shared between the browser, server, and web server.

While it seems like a lengthy communication process between your website, server, and browser, the process takes only a few milliseconds to complete.

Before a website is secured by an SSL certificate, the first part of the URL shows as HTTP (which stands for HyperText Transfer Protocol.) After securing the site with an SSL certificate, the first part of the URL shows as HTTPS to mean HyperText Transfer Protocol Secure.

To access details about the SSL certificates on a website, click the padlock symbol next to the URL of a website in the browser bar.



Typical details you should expect to find within SSL certificates are;

1. The domain name to which the certificate was issued
2. The person, device, or organization that the certificate was given to
3. The specific Certificate Authority that issued it
4. The expiry date of the certificate
5. The public key

Why Do You Need an SSL Certificate?

The primary role of SSL certificates is to protect a user's data, prevent attackers from creating a fake copy of the website, and verify ownership of the website.

It's important that a website keeps users' data safe it requires that users enter personal information such as their credit card information or view confidential information.

SSL certificates assure users that the connection is secure and private and that the website they are using is authentic and safe to share private information.

Types of private information that SSL certificates secure include;

- 
1. Medical records
 2. Proprietary information
 3. Legal contracts and documents
 4. Personally identifiable information such as names, addresses, dates of birth, and cellphone numbers
 5. Login credentials
 6. Financial information such as transaction and bank account details

Types of SSL Certificates

There are six main types of SSL certificates that offer different levels of validation. These include;

1. Domain Validated Certificates (DV SSL)
2. Organization Validated certificates (OV SSL)
3. Extended Validated SSL Certificates (EV SSL)
4. Wildcard SSL Certificates (WC SSL)
5. Unified Communications Certificates (UCC)
6. Multi-domain SSL certificates (MDC)

Domain Validated Certificates

Domain validated certificates are a type of SSL certificate that verifies the domain name only (e.g., example.com) without validating the organization behind it. This type of certificate is the cheapest and quickest to set up but offers low levels of encryption and validation because the organization that is requesting the certificate has not been verified.

Organization Validated Certificates

Organization validated certificates are used when the organization requesting the certificate has gone through a substantive verification process. This type of SSL certificate offers more validation than domain validated certs and they display the owner's information in the SSL certificate (e.g., example.com, Inc.)

Extended Validated SSL Certificates

The extended validated SSL certificate offers the highest levels of validation, but it requires a substantial amount of validation and is expensive to obtain. This type of certificate is generally reserved for companies that need to present high levels of trust and security, such as banks.

Wildcard SSL Certificates

A wildcard certificate is used when a company secures a domain and unlimited subdomains in a single certificate. This certificate works well if you have many sub-domains that you need to secure.

Unified Communications Certificates

A unified communications certificate was developed initially to secure Live Communications and Microsoft Exchange servers. Also considered as Multi-Domain SSL Certificates, UCCs allow for a single certificate to secure multiple domains. These certificates are validated organizationally and can act as EV SSLs to provide the highest level of assurance through the green address bar.

How To Acquire an SSL Certificate

SSL certificates can be obtained either directly from a Certificate Authority or through a third party.

The cost of an SSL certificate varies depending on the level of security you need and could be anywhere between free to hundreds of dollars.

Certificate Authorities will often issue certificates for a one-time fee, which is ideal if you have an expiration date for your certificate in the near future.

Third-parties will often charge a fee on top of their one-time charges as well as monthly fees.

It is important to know the differences when deciding where you want to purchase your certificate.

Steps to obtaining an SSL certificate are as follows;

1. Set up your server and ensure that you have updated your WHOIS records and match the information you are submitting to the Certificate Authority
2. Generate a Certificate Signing Request on your server. Most web hosting companies can help you do this.
3. Submit your CSR to the Certificate Authority to validate your company and website details
4. Install the certificate issued once the approval process ends