**What is SSL?**

SSL (Secure Sockets Layer) is a standard security protocol for establishing encrypted links between a web server and a browser in an online communication.

The usage of SSL technology ensures that all data transmitted between the web server and browser remains encrypted.

An **SSL certificate** is necessary to create SSL connection. You would need to give all details about the identity of your website and your company as and when you choose to activate SSL on your web server. Following this, two cryptographic keys are created - a Private Key and a Public Key.

**Show your website is secure with Comodo SSL!** [**Learn More**](https://www.instantssl.com/ssl-certificate.html?track=9019) [**GET NOW**](https://www.instantssl.com/compare-ssl-certificates.html?track=9020)

The next step is the submission of the CSR (Certificate Signing Request), which is a data file that contains your details as well as your Public Key. The CA (Certification Authority) would then validate your details. Following successful authentication of all details, you will be issued SSL certificate. The newly-issued SSL would be matched to your Private Key. From this point onwards, an encrypted link is established by your web server between your website and the customer's web browser.

On the apparent level, the presence of an **SSL protocol** and an encrypted session is indicated by the presence of the lock icon in the address bar. A click on the lock icon displays to a user/customer details about your SSL. It's to be remembered that SSL Certificates are issued to either companies or legally accountable individuals only after proper authentication.

An **SSL Certificate** comprises of your domain name, the name of your company and other things like your address, your city, your state and your country. It would also show the expiration date of the SSL plus details of the issuing CA. Whenever a browser initiates a connection with a SSL secured website , it will first retrieve the site's SSL Certificate to check if it's still valid. It's also verified that the CA is one that the browser trusts, and also that the certificate is being used by the website for which it has been issued. If any of these checks fail, a warning will be displayed to the user, indicating that the website is not secured by a valid SSL certificate.

**What is SSL/TLS Certificate?**

SSL or **TLS (Transport Layer Security)** certificates are data files that bind a cryptographic key to the details of an organization. When SSL/TLS certificate is installed on a web server, it enables a secure connection between the web server and the browser that connects to it. The website's URL is prefixed with "https" instead of "http" and a padlock is shown on the address bar. If the website uses an extended validation (EV) certificate, then the browser may also show a green address bar.

**What is SSL used for?**

The *SSL protocol* is used by millions of online business to protect their customers, ensuring their online transactions remain confidential. A web page should use **encryption** when it expects users to submit confidential data, including personal information, passwords, or credit card details. All web browsers have the ability to interact with secured sites so long as the site's certificate is issued by a trusted CA.

**Why do I need SSL certificate?**

The internet has spawned new global business opportunities for enterprises conducting online commerce. However, that growth has also attracted fraudsters and cyber criminals who are ready to exploit any opportunity to steal consumer bank account numbers and card details. Any moderately skilled hacker can easily intercept and read the traffic unless the connection between a client (e.g. internet browser) and a web server is encrypted.

**How Does SSL Work?**

The following graphic explains how SSL Certificate works on a website. The process of how an 'SSL handshake' takes place is explained below:

* An end-user asks their browser to make a secure connection to a website (e.g.https://www.example.com)
* The browser obtains the IP address of the site from a DNS server then requests a secure connection to the website.
* To initiate this secure connection, the browser requests that the server identifies itself by sending a copy of its SSL certificate to the browser.
* The browser checks the certificate to ensure:
  + That it is signed by a trusted CA
  + That it is valid - that it has not expired or been revoked
  + That it confirms to required security standards on key lengths and other items.
  + That the domain listed on the certificate matches the domain that was requested by the user.
* When the browser confirms that the website can be trusted, it creates a symmetric session key which it encrypts with the public key in the website's certificate. The session key is then sent to the web server.
* The web server uses its private key to decrypt the symmetric session key.
* The server sends back an acknowledgement that is encrypted with the session key.
* From now on, all data transmitted between the server and the browser is encrypted and secure.

**How do I implement SSL on my website?**

Implementing SSL for a website is quite easy! A typical installation of SSL certificate involves the following steps:

**Step 1. Acquire SSL certificate**

To implement SSL/TLS security on your website, you need to get and install a certificate from a trusted CA. A trusted CA will have its root certificates embedded in all major root store programs, meaning the certificate you purchase will be trusted by the internet browsers and mobile devices used by your website visitors.

You should also decide which type of certificate suits you best.

* **Single domain certificates** allow you to secure one fully qualified domain name (FQDN).
* **Wildcard certificates** secure a single domain and unlimited subdomains of that domain. For example, a wildcard certificate for '\*.domain.com' could also be used to secure 'payments.domain.com', 'login.domain.com', 'anything-else.domain.com'
* **Multi-domain certificates** allow website owners to secure multiple, distinct domains on a one certificate. For example, a single MDC can be used to secure domain-1.com, domain-2.com, domain-3.co.uk, domain-4.net and so on.
* **Extended Validation certificates** provide the highest levels of security, trust and customer conversion for online businesses. Because of this, EV certificates contain a unique differentiator designed to clearly communicate the trustworthiness of the website to its visitors. Whenever somebody visits a website that uses an EV SSL, the address bar will turn green in major browsers such as Internet Explorer, Firefox and Chrome.

**Step 2. Activate and install your SSL certificate**

When SSL certificate is purchased from a web host, its activation is taken care of by the web host. The administrator of the website can also activate the SSL through Web Host Manager (WHM) or cPanel. In the WHM dashboard select the **SSL/TLS** option and choose "Generate SSL Certificate and Signing Request". Next, generate your Private Key and fill out the form for Certificate Signing Request (CSR). Ensure that you enter your domain name in the box asking for "Host to make cert for". You will need to send this CSR to your CA in order to purchase a certificate. See <https://support.comodo.com/index.php?/Knowledgebase/List/Index/19/csr-generation/> for help to generate a CSR using various webserver types.

Comodo offers detailed guides for installing certificates on various webservers too. See [SSL Certificate Installation on Different Web Servers](https://www.instantssl.com/ssl-certificate-support/cert_installation/ssl-certificate-index.html) for a full list. The guides provides installation instructions for different software types such as Apache, Apache on Cobalt, BEA, C2Net Stronghold, Ensim, F5, Hsphere, IBM, Microsoft, Netscape / Sun, Novell, Plesk, SSL Accelerator, Website Pro, and Zeus.

**Step 3. Update Website from HTTP to HTTPS**

Your website is now capable of HTTPS! You must now configure you website so that visitors who access this site get automatically directed to the "HTTPS" version. Search engine providers like Google are now offering SEO benefits to SSL pages, so the effort to serve all pages on your site over HTTPS is well worth it.

**Who issues SSL Certificates?**

A certificate authority or certification authority (CA) issues [SSL certificates](https://www.instantssl.com/ssl-certificate.html). On receiving an application, the CA verifies two factors: It confirms the legal identity of the enterprise/company seeking the certificate and whether the applicant controls the domain mentioned in the certificate. The issued SSL certificates are chained to a 'trusted root' certificate owned by the CA. Most popular internet browsers such as Firefox, Chrome, Internet Explorer, Microsoft Edge, and others have these root certificates embedded in their 'certificate store'. Only if a website certificate chains to a root in its certificate store will the browser allow a trusted and secure https connection. If a website certificate does not chain to a root then the browser will display a warning that the connection is not trusted.

**What details are included in a SSL certificate**

SSL Certificates will contain details of whom the certificate has been issued to. This includes the domain name or common name, serial number; the details of the issuer; the period of validity - issue date and expiry date; SHA Fingerprints; subject public key algorithm, subject's public key; certificate signature algorithm, certificate signature value. Other important details such as the type of certificate, SSL/TLS version, Perfect Forward Secrecy status, and cipher suite details are included. Organization validated and extended validation certificates also contain verified identity information about the owner of the website, including organization name, address, city, state and country.

**How can I tell when a site uses SSL?**

A web page using SSL will display

* "https://" instead of "http://" before the website's address in the browser's address bar
* A padlock icon in the address bar of the browser before the address.
* With an Extended Validation Certificate, the address bar also shows the registered name of the company that owns the website, the name of the issuing CA and, an additional green security indicator.