SSL Explained

What Is SSL (Secure Sockets Layer) and What Are SSL Certificates?

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).

SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.

More specifically, SSL is a security protocol. Protocols describe how algorithms should be used; in this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

SSL secures millions of peoples' data on the Internet every day, especially during online transactions or when transmitting confidential information. Internet users have come to associate their online security with the lock icon that comes with an SSL-secured website or green address bar that comes with an extended validation SSL-secured website. SSL-secured websites also begin with https rather than http.

Where do Certificates Come In?

All browsers have the capability to interact with secured web servers using the SSL protocol. However, the browser and the server need what is called an SSL Certificate to be able to establish a secure connection.

What is an SSL Certificate and How Does it Work?

SSL Certificates have a key pair: a public and a private key. These keys work together to establish an encrypted connection. The certificate also contains what is called the "subject," which is the identity of the certificate/website owner.

To get a certificate, you must create a Certificate Signing Request (CSR) on your server. This CSR creates the private key and a CSR data file that you send to the SSL Certificate issuer (called a Certificate Authority or CA). The CA uses the CSR data file to create a public key to match your private key without compromising the key itself. The CA never sees the private key.

Once you receive the SSL Certificate, you install it on your server. You also install a pair of intermediate certificates that establish the credibility of your SSL Certificate by tying it to your CA's root certificate. The instructions for installing and testing your certificate will be different depending on your server.

In the image below, you can see what is called the certificate chain. It connects your server certificate to your CA's (in this case DigiCert's) root certificate through a series of intermediate certificates.

The most important part of an SSL Certificate is that it is digitally signed by a trusted CA. Anyone can create a certificate, but browsers only trust certificates that come from an organization on their list of trusted CAs. Browsers come with a pre-installed list of trusted CAs, known as the Trusted Root CA store. In order to be added to the Trusted Root CA store and thus become a Certificate Authority, a company must comply with and be audited against security and authentication standards established by the browsers.

An SSL Certificate issued by a CA to an organization and its domain/website verifies that a trusted third party has authenticated that organization's identity. Since the browser trusts the CA, the browser now trusts that organization's identity too. The browser lets the user know that the website is secure, and the user can feel safe browsing the site and even entering their confidential information.

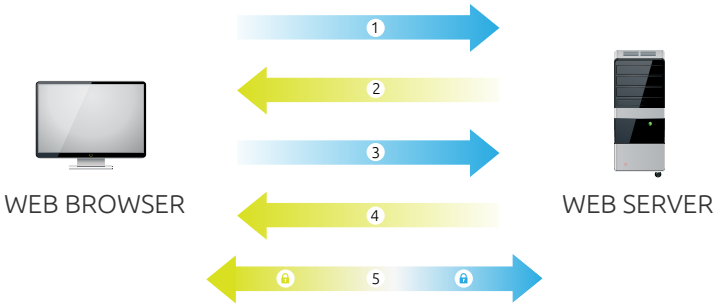
SSL Explained

How Does the SSL Certificate Create a Secure Connection?

When a browser attempts to access a website that is secured by SSL, the browser and the web server establish an SSL connection using a process called an "SSL Handshake" (see diagram below). Note that the SSL Handshake is invisible to the user and happens instantaneously.

Essentially, three keys are used to set up the SSL connection: the public, private, and session keys. Anything encrypted with the public key can only be decrypted with the private key, and vice versa.

Because encrypting and decrypting with private and public keys takes a lot of processing power, they are only used during the SSL Handshake to create a symmetric session key. After the secure connection is made, the session key is used to encrypt all transmitted data.



*1. **Browser** connects to a web server (website) secured with SSL (https). Browser requests that the server identify itself.*

*2. **Server** sends a copy of its SSL Certificate, including the server's public key.*

*3. **Browser** checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.*

*4. **Server** decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.*

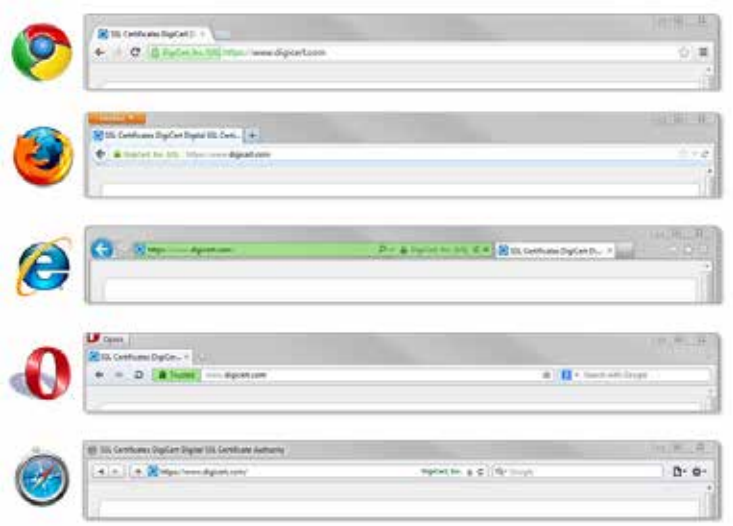
*5. **Server** and **Browser** now encrypt all transmitted data with the session key.*

To learn more about DigiCert's SSL Certificates call 1-855-800-3444 or visit www.digicert.com

Why Do I Need SSL?

One of the most important components of online business is creating a trusted environment where potential customers feel confident in making purchases. Browsers give visual cues, such as a lock icon or a green bar, to help visitors know when their connection is secured.

In the below image, you can see the green address bar that comes with extended validation (EV) SSL Certificates.



If your site collects credit card information you are required by the Payment Card Industry (PCI) to have an SSL Certificate. If your site has a login section or sends/receives other private information (street address, phone number, health records, etc.), you should use SSL Certificates to protect that data.

Your customers want to know that you value their security and are serious about protecting their information. More and more customers are becoming savvy online shoppers and reward the brands that they trust with increased business.

About DigiCert

For over a decade DigiCert has been providing SSL Certificates to the top eCommerce websites around the globe. Over 72,000 customers in 146 countries, including half of the Alexa Top Ten websites, rely on DigiCert to secure their sites. With unmatched issuance speed, 2048-bit encryption, award-winning customer support, and countless product innovations, it's no wonder that DigiCert is the fastest-growing high-assurance Certificate Authority in the world.

digicert®
Your Success is Built on Trust™