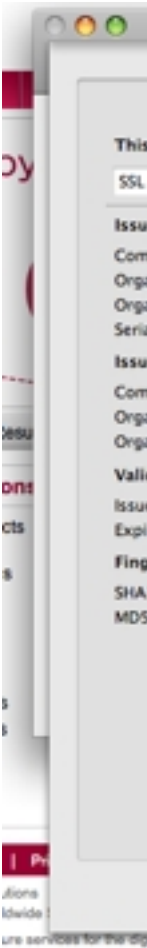


What SSL Certificates Do:

Secure Sockets Layer (SSL) technology protect websites and make it easy for visitors to trust



websites in three essential ways:

1. An SSL Certificate enables encryption of sensitive information during online transactions.
2. Each SSL Certificate contains unique, authenticated information about the certificate owner.
3. A Certificate Authority verifies the identity of the certificate owner when it is issued.

Who needs an SSL Certificate?

If you fit into any of the following categories, then an SSL Certificate is a must:

1. Operate an online store or accept online orders and credit cards
2. Offer a login or sign in on your site
3. Process sensitive data such as address, birth date, license, or ID numbers
4. Require compliance with privacy and security requirements
5. Value privacy and expect others to trust you.

How SSL Encryption Works

Imagine sending mail through the postal system in a clear envelope. Anyone with access to it can see the data. If it looks valuable, they might take it or change it. An SSL Certificate establishes a private communication channel between the browser and web server enabling encryption of the data during transmission. Encryption scrambles the data, essentially creating an envelope for message privacy.

Each SSL Certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a Web browser points to a secured domain, a Secure Sockets Layer handshake authenticates the server (the website) and the client (the web browser). An encryption method is established with a unique session key and secure transmission can begin. True 128-bit SSL Certificates enable every site visitor to experience the strongest SSL encryption available to them.

How Authentication Works

Imagine receiving an envelope with no return address and a form asking for your bank account number. In the case of organization- or Extended-validation certificates, every SSL Certificate is created for a particular server in a specific domain for a verified business entity. The validation process for EV certificates is quite extensive and provides fuller information about the website owner than a standard certificate. When the SSL handshake occurs, the browser requires authentication information from the server. By clicking the closed padlock in the browser window or certain SSL trust marks (such as the VeriSign Secured Seal or GeoTrust True Site Seal), the website visitor sees the authenticated organization name. In high-security browsers (IE7/8,

Firefox 3.0+, Safari 3.2+, Chrome and Opera 9.2+), the authenticated organization name is prominently displayed and the address bar turns green when an Extended Validation SSL Certificate is detected. If the information does not match or the certificate has expired, the browser displays an error message or warning.

A Matter of Trust

At the end of the day, SSL Certificates are all about trust. If you want to develop and instill a sense of trust with website visitors, an SSL Certificate is the way to do it. An SSL-protected site gives users the confidence to share personal information without having to worry about whether that data is safe as it travels around the Internet. And, the SSL Certificate provides further peace of mind to web users by offering verification that those in control of the web server are who the web surfer thinks they are.