



Understanding Secure Socket Layer (SSL) Certification

What is an SSL Certificate?

An SSL certificate is a digital certificate that authenticates the identity of a web site to visiting browsers, and encrypts information for the server via Secure Sockets Layer (SSL) technology. A certificate serves as an electronic “passport” that establishes an online entity’s credentials for their website and stored data. When there is an attempt to send confidential information to a web server, the user’s browser will access the server’s digital certificate to establish a secure connection.

Installing an SSL certificate on a web site secures online information with up to 256-bit encryption. The SSL certificate builds an impenetrable fortress around sensitive client information, which is kept securely encrypted and safe from prying eyes. Rigorous authentication methodology also guarantees that SSL certificates are issued only to entities whose existence and domains can be verified.

Ensuring Data Safety & Security

An SSL certificate insures that data stored on the internet is both safe and secure. Once an internet user enters a secure area (by entering an e-mail address or other personal data for example), the site’s SSL certificate enables the browser and web server to build a secure, encrypted connection. If a user attempts to submit information to an unsecured web site, the browser’s built-in security mechanism triggers a warning that the site is not secured and sensitive data may be at risk.

The industry standard encryption is 128-bit (used by all banking infrastructures to safeguard sensitive data) and high-grade 256-bit SSL encryption for secured online transactions. The actual encryption strength on a secure connection using a digital certificate is determined by the level of encryption supported by the user’s browser and the server that the web site resides on. Encryption strength is measured in key length — number of bits in the key. To decipher an SSL communication, a decoding key must be generated. For example, 40-bit encryption involves 240 possible values. 128- and 256-bit keys involve 2128 and 2256 possible combinations, respectively, rendering the encrypted data de facto impervious to intrusion. Even with a brute-force attack, decoding a 128- or 256-bit encryption is computationally unfeasible.

Rigorous & Stringent Authentication Methodology

Before SSL certification is issued, the applicant’s company or personal information undergoes a rigorous authentication

procedure that verifies the domain control. SSL certificates are only issued to entities whose domain control, business credentials, and contact information have been verified. Issuance of an SSL certificate guarantees that the entity which owns the certificate is who it claims to be and has a legal right to use the domain from which it operates.

SSL Establishes a Secure Connection

An SSL-encrypted connection is established via the SSL “handshake” process. In essence, the visitor’s browser requests a secure session from the web server when accessing an SSL secured web site. The server responds by sending the visitor’s browser its server certificate. The browser verifies that the server’s certificate is valid and being used by the web site for which it has been issued, and has been issued by a Certificate Authority that the browser trusts. If the certificate is validated, the browser generates a one-time “session” key and encrypts it with the server’s public key. The visitor’s browser sends the encrypted session key to the server so that both server and browser have a copy. The server decrypts the session key using its private key. The SSL “handshake” process is completed, and a secure SSL connection is established.

SSL Prevents Phishing & Pharming

SSL certification assists in thwarting phishing and pharming schemes that pose constant threats to sensitive online information that is under siege by cyber criminals.

Phishing schemes are attempts to steal and exploit sensitive personal information by tricking victims into accessing fraudulent sites that pose as legitimate entities, such as online banks and other businesses. SSL technology and its fraud-prevention measures detect schemes and deny certificate requests for suspicious domains. Pharming revolves around the concept of hijacking an Internet Service Provider’s (ISP) domain name server (DNS) entries. When a “pharmer” succeeds in such DNS “poisoning”, every computer using that ISP for Internet access is directed to the wrong site when the user types in a specific web address (URL). SSL technology also helps prevent pharming attacks because “pharmers” are unable to obtain an SSL certificate since they do not control the domain for which the certificate is requested. Internet users that attempt to access a site that is posing as the owner of the web site (and SSL Certificate) will be instantly alerted to a problem with the supposedly secure connection.

