SSL Certificates: How It Works

This article helps you understand the SSL conception and explains how SSL certificates work.

For a glossary of abbreviations and terms, see “Glossary” at the end of this document.

Overview

SSL stands for “Secure Socket Layer.” The SSL-based technology establishes a secure session link between a web browser and a website so that all communications transmitted through this link are secure. SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely.  To ensure visitors their connection is secure, browsers provide visual cues, such as a lock icon or a green bar.

***NOTE****:*

*Additionally, SSL helps you transmit secure email, secure files, and other forms of information*.

About SSL Certificates

SSL certificates creates a safe and private channel for you to communicate.

An SSL certificate is a digital computer file (or small piece of code) that has two specific functions:

* **Authentication and verification**: the SSL certificate has detailed information on the identity of a business or website. To display this information in a popup window, the site visitors should click the browser’s padlock symbol:


***NOTE****:
Additionally, this window lets the site visitors configure the site settings and permissions, such as a permission to use the visitor’s location, the device camera, pop-ups, etc*.
* **Data encryption:** SSL certificates have a *key* pair: a public and a private key. These keys work together to establish an encrypted connection, which means that the sensitive information exchanged via the website cannot be read by anyone other than the intended recipient.

Each SSL certificate has a digital signature of a trusted Certificate Authority (CA). The browsers only trust certificates that come from an organization on their pre-installed list of trusted CAs, known as the Trusted Root CA store.

An SSL certificate is most reliable when issued by a trusted CA.

How SSL Encryption Works

When a browser attempts to access an SSL-secured website, the browser and the web server establish an SSL connection using a process called an “SSL Handshake” (see diagram below). This process happens instantaneously and is invisible for users.

The following diagram illustrates the SSL Handshake process:



|  |  |
| --- | --- |
| **1** | **Browser** connects to a web server (website) secured with SSL.  |
| **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. If the browser trusts the certificate, it creates, encrypts, and sends back a special 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. |

Glossary

|  |  |
| --- | --- |
| **Browser:** | A software tool that you use to access the Internet sites. Examples include Mozilla Firefox, Microsoft Internet Explorer (IE), Apple Safari, and others. |
| **CA:** | Certificate Authority. |
| **CSR:** | Certificate Signing Request |
| **Digital signature:** | A digital code (generated and authenticated by public key encryption) attached to an electronically transmitted document to verify its contents and the sender's identity. |
| **Encryption:** | “Scrambling” information.  |
| **Decryption:** | “Un-scrambling” information and put it back in its original format. |
| **Key:** | A mathematical algorithm for encrypting or decrypting your information. |
| **SSL:** | Secure Sockets Layer. |
|  |  |
|  |  |
|  |  |