**How SSL Works**

When an Internet user visits a secure web site, an SSL certificate provides identification information about the web server and establishes an encrypted connection. This process happens in a fraction of a second.

**What Happens Between The Web Browser And Server**

1. A browser attempts to connect to a web site secured with **SSL**. The browser requests that the web server identify itself.
2. The server sends the browser a copy of its **SSL certificate**.
3. The browser checks whether it trusts the SSL certificate. If so, it sends a message to the server.
4. The server sends back a digitally signed acknowledgement to start an SSL encrypted session.
5. Encrypted data is shared between the browser and the server.

**SSL Fundamentals**

There are 3 essential elements at work in the process described above: a protocol for communications (SSL), credentials for establishing identity (the SSL certificate), and a third party that vouches for the credentials (the certificate authority).

* Computers use protocols to allow different systems to work together. Web servers and web browsers rely on the **Secure Sockets Layer (SSL) protocol** to enable encrypted communications. The browser’s request that the server identify itself is a function of the SSL protocol.
* **Credentials** for establishing identity are common to our everyday lives: a driver’s license, a passport, a company badge. An SSL certificate is a type of digital certificate that serves as a credential in the online world. Each SSL certificate uniquely identifies a specific domain (such as thawte.com) and a web server.
* Our trust of a credential depends on our confidence in the organization that issued it. **Certificate authorities** have a variety of methods to verify information provided by individuals or organizations. Established certificate authorities, such as Thawte, are well known and trusted by browser vendors. Browsers extend that trust to digital certificates that are verified by the certificate authority.

**Lifecycle Of An SSL Certificate**

If you need to secure your web site, it is quick and easy to request an SSL certificate and install it.

1. Generate a [Certificate Signing Request](https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=AR1108&ampactp=LIST) (CSR) for the web server you plan to secure. If you do not manage your own web server, contact your web host or Internet service provider to request a CSR.
2. Select an [SSL Certificate](https://www.thawte.com/ssl/index.html) and click buy.
3. Pick up your certificate in to your [Thawte® Certificate Center Account](https://ssl-certificate-center-enterprise.thawte.com/vcce/enterprise/console_login?application_locale=THAWTE_US).
4. Follow [installation instructions](https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=SO1498&actp=LIST) for your Web server.
5. Download the [Thawte® Trusted Site Seal](https://www.thawte.com/ssl/secured-seal/index.html) to display on pages within your secured domain.

At the end of the SSL certificate’s validity period (1-5 years, depending on the certificate type and your selection), you have the option to renew your SSL certificate. You may need to provide additional information for authentication or [generate a new CSR](https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=SO157).

**Why choose Thawte?**

Thawte is trusted by millions of people worldwide. When we issue an SSL certificate, we know that our name will appear next to yours as the trusted third party who verified it. We take that trust seriously and lead the industry with rigorous authentication methods and a global infrastructure to support real-time certificate look-ups.