

A Quick Guide to SSL/TLS Certificates

Making the best choice when considering your website security options

Whether you are an individual or a company, you should approach online security in the same way that you would approach physical security for your home or business. Not only does it make you feel safer but it also protects people who visit your home, place of business, or website. It is important to understand the potential risks and then make sure you are fully protected against them. In the fast-paced world of technology, it is not always easy to stay abreast of the latest advancements. For this reason it is wise to partner with a reputable Internet security company.

What is an SSL Certificate?

SSL stands for “**Secure Socket Layer**.” It’s a technology that establishes a secure connection between a visitor’s web browser and your website so that **all communication transmitted between them is encrypted** and, therefore, secure. SSL is also used for transmitting secure email, secure files, and other forms of information. You wouldn’t send your private information or banking details to someone on the back of a postcard, right? Well, that’s essentially what you’re doing when you communicate online without SSL.



Authentication and Verification: The SSL certificate has information about the authenticity of certain details regarding the identity of a person, business or website, which it will display to visitors on your website when they click on the browser’s **padlock symbol or trust mark** (e.g., the DigiCert Smart Seal). The vetting criteria used by Certificate Authorities to determine if an SSL certificate should be issued is most stringent with Extended Validation.



Data Encryption: The SSL certificate also enables encryption, which means that the sensitive information exchanged via the website **cannot be intercepted and read** by anyone other than the intended recipient. Specifically, all information is cryptographically hashed, to a third-party it would appear as a jumbled mess of different inputs. Only someone with a corresponding key can decrypt the information and make sense of it.

How Does SSL Encryption Work?

In the same way that you lock and unlock doors using a key, encryption makes use of **keys to lock and unlock your information**. Each SSL session consists of two keys:



The public key is used to **encrypt** (scramble) the information before transmission.



The private key is used to **decrypt** (un-scramble) the information so that it can be read.

The Process

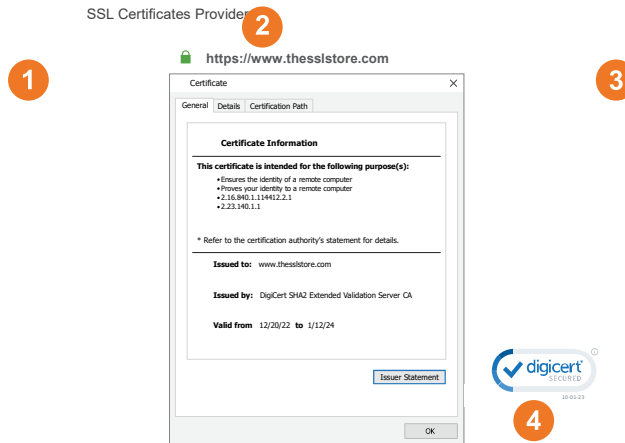
When a user arrives on a website equipped with SSL, the two begin the **SSL handshake**. During this process, the user’s browser checks the validity of the certificate before negotiating a secure connection. Once this is complete, **session keys** are exchanged and an encrypted connection begins. This all takes place behind the scenes, the only evidence is the **padlock indicator** in the address bar.

How Do I Know That a Site Has a Valid SSL Certificate?

Having SSL is great, but let's be honest, it's also important that your customers can easily see that you've made an investment in **protecting their information**. Here's how you can tell whether a website has SSL:

For **Extended Validation** Certificates, the organization's name will appear in the certificate details.

Depending on the browser, a **padlock** icon will either be placed in the address bar or at the bottom.



A **Trust Seal** may also be displayed on some pages, clicking the seal will display verified certificate details.

Where Would I Use an SSL Certificate?

The short answer to this question is that you would use an SSL certificate anywhere that you wish to **transmit information securely**.



Securing **communication** between your website and your customer's Internet browser



Securing **internal communications** on your corporate intranet



Securing email communications sent to and from **your network** (or private email address)



Securing **information between servers** (both internal and external)



Securing information sent and received **via mobile devices**

Different Types of SSL Certificates

There are a **number of different** SSL certificates on the market today.

Single Domain Certificates

Single Domain Certificates are SSL certificates that, as the name might imply, cover a **single domain**. These are available at all validation levels: DV, OV and EV.

Multi-Domain Certificates

A Multi-Domain SSL certificate is capable of covering multiple websites on a single certificate. Multi-Domain certificates are sometimes called **SAN certificates**. They are available at all three validation levels.

Wildcard

For websites with sub-domains there is a specialized SSL certificate called a wildcard. Wildcards cover a single domain and **all accompanying sub-domains**. They are only available at the DV and OV levels.



Tech Talk Made Simple

- ✓ **Encryption:** Information is “scrambled” so that it **cannot be used** by anyone other than the person for whom it is intended.
- ✓ **Decryption:** Information is “un-scrambled” and put back in its original form.
- ✓ **Key:** A mathematical formula, or algorithm, that is used to encrypt or decrypt your information.
- ✓ **Browser:** A software program that you use to access the Internet.

In Conclusion

Trust makes all the difference in the world of online business. Investment in technology to protect customers and earn their trust is a critical success factor for any company that does business online or hosts an e-commerce website. The effective implementation of SSL certificates and correct placement and **use of trust marks are proven tools** in the establishment of customer trust.

Need to get more details?

Visit us at <https://thqcyberdivision.github.io> or thqcyberdivision@gmail.com

