Beginner's Guide to TLS/SSL Certificates

Making the best choice when considering your online security options

digicert®

Table of contents

Introduction

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.

This guide will demystify the technology involved and give you the information you need to make the best decision when considering your online security options. For a glossary of terms, please see "Tech talk made simple" at the end of this document.

What is a TLS/SSL Certificate?

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are the most widely used security protocol today and are primarily used to serve two specific functions:

1. **Authentication and verification:** The TLS/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® Secured Seal or Norton Seal powered by DigiCert). All that information was validated by the Certificate Authority (CA) which issued the SSL certificate. There are various strengths of validation available, which we'll cover later.
2. **Data encryption:** The TLS/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.

In the same way that an identity document or passport may only be issued by the country's government officials, an TLS/SSL certificate is most reliable when issued by a trusted Certificate Authority (CA). The CA has to follow very strict rules and policies about who may or may not receive an TLS/SSL certificate. When you have a valid TLS/SSL certificate from a trusted CA, there is a higher degree of trust by your customers, clients or partners.

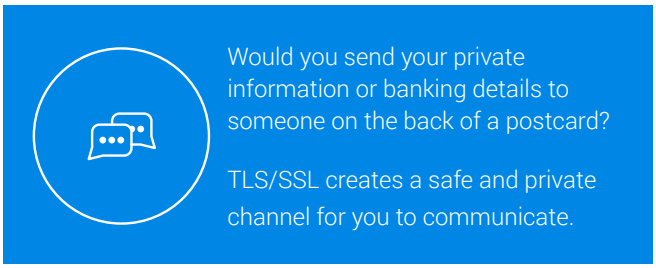
How does TLS/SSL encryption work?

In the same way that you lock and unlock doors using a key, encryption makes use of keys to lock and unlock your information. Unless you have the right key, you will not be able to "unlock" the information.

Each TLS/SSL session consists of two keys:

- The public key is used to encrypt (scramble) the information.
- The private key is used to decrypt (un-scramble) the information and restore it to its original format so that it can be read.

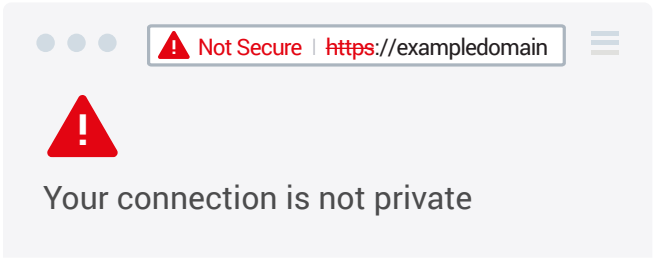
TLS/SSL stands for "Secure Socket Layer." It is a technology that establishes a secure session link between the visitor's web browser and your website so that all communications transmitted through this link are encrypted and are, therefore, secure.



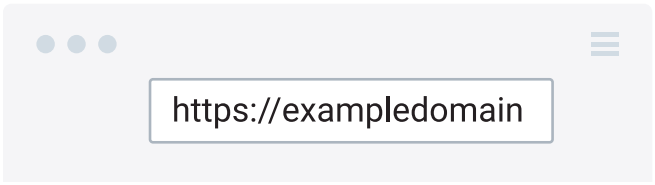
The Process: Every TLS/SSL certificate that is issued for a CA-verified entity is issued for a specific server and website domain (website address). When a person uses their browser to navigate to the address of a website with a TLS/SSL certificate, a TLS/SSL handshake (greeting) occurs between the browser and server. Information is requested from the server–which is then made visible to the person in their browser window. You will notice changes to indicate that a secure session has been initiated – for example, a trust mark will appear. If you click on the trust mark, you will see additional information such as the validity period of the TLS/SSL certificate, the domain secured, the type of TLS/SSL certificate, and the issuing CA. All of this means that a secure link is established for that session, with a unique session key, and secure communications can begin.

How do I know that a site has a valid TLS/SSL Certificate?

1. A standard website without TLS/SSL security displays "http:// " before the website address in the browser address bar. This moniker stands for "Hypertext Transfer Protocol," and is a non-secured way to transmit information over the Internet. Most browsers today will show a warning to those visiting a webpage that does not have a TLS/SSL certificate installed correctly which can lead visitors to abandon the site.



However, a website that is secured with a TLS/SSL certificate will display "https:// " before the address. This stands for "Secure HTTP."



2. You will also see a padlock symbol on the top or bottom of the Internet browser (depending on which browser you are using).

3. Often, you will also notice a trust mark displayed on the website itself. DigiCert™ customers use the DigiCert® Secured Seal or Norton Seal powered by DigiCert trust mark on their websites. When you click on the DigiCert or any Powered by DigiCert trust mark, or the padlock symbol on the page, it will display details of the certificate with all the company information as verified and authenticated by the CA.

4. By clicking the closed padlock in the browser window, or certain TLS/SSL trust marks such as the DigiCert® Secure Trust Seal or the Norton Secured Seal, the website visitor sees the authenticated organization name. In more secure browsers, the authenticated organization name is prominently displayed and the address bar or text may turn green when an Extended Validation (EV) TLS/SSL certificate is detected. If the information does not match, or the certificate has expired, the browser displays an error message or warning.

Where would I use a TLS/SSL Certificate?

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

Here are some examples:

- Securing communication between your website and your customer's Internet browser.
- Securing internal communications on your corporate intranet.
- Securing information between servers (*both internal and external*).
- Securing information sent and received via mobile devices.

Different types of TLS/SSL Certificates

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

- The first type of TLS/SSL certificate is a self-signed certificate. As the name implies, this is a certificate that is generated for internal purposes and is not issued by a CA. Since the website owner generates their own certificate, it does not hold the same weight as a fully authenticated and verified TLS/SSL certificate issued by a CA.
- A Domain Validated certificate is considered an entry-level TLS/SSL certificate and can be issued quickly. The only verification check performed is to ensure that the applicant owns the domain (website address) where they plan to use the certificate. No additional checks are done to ensure that the owner of the domain is a valid business entity.
- A fully authenticated TLS/SSL certificate is the first step to true online security and confidence building. Taking slightly longer to issue, these certificates are only granted once the organisation passes a number of validation procedures and checks to confirm the existence of the business, the ownership of the domain, and the user's authority to apply for the certificate.

All DigiCert TLS/SSL Certificates are fully authenticated.

- A domain name is often used with a number of different host suffixes. For this reason, you may employ a Wildcard certificate that allows you to provide full TLS/SSL security to any host of your domain – for example, host.your_domain.com (where "host" varies but the domain name stays constant).
- Similar to a Wildcard certificate, but a little more versatile, the SAN (Subject Alternative Name) TLS/SSL certificate allows for more than one domain to be added to a single TLS/SSL certificate.
- Extended Validation (EV) TLS/SSL certificates offer the highest industry standard for authentication and provide the best level of customer trust available. When consumers visit a website secured with an EV TLS/SSL certificate, the address bar turns green (in some browsers) and a special field appears with the name of the legitimate website owner along with the name of the security provider that issued the EV TLS/SSL certificate. It also displays the name of the certificate holder and issuing CA in the address bar. This visual reassurance has helped increase consumer confidence in e-commerce.

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: "Un-scrambling" information and put it back in its original format.

Key: A mathematical formula, or algorithm, that is used to encrypt or decrypt your information. In the same way that a lock with many different combinations is more difficult to open, the longer the length of the encryption key (measured in number of bits), the stronger the encryption.

Browser: A software program that you use to access the Internet. Examples include: Microsoft Edge; Mozilla Firefox, Apple Safari, and Google Chrome.

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 TLS/SSL certificates and correct placement and use of trust marks are proven tools in the establishment of customer trust.

DigiCert is now the leading provider of TLS/SSL certificates globally, helping to assure customers that they are safe from search to browse to buy and sign in*. DigiCert secures more than one million web servers worldwide, more than any other CA.* DigiCert also secures over two-thirds of websites using Extended Validation TLS/SSL – including the biggest names in e-commerce and banking.* When you choose DigiCert, you can rest assured that your website and your reputation are protected by the CA with a proven track record and the most recognized trust mark on the Internet.

For more information, visit us at https://resources.digicert.com/ssl-tls.

*Includes DigiCert subsidiaries, affiliates, and resellers.

For more information, email our security experts
at contactus@digicert.com

Americas

Lehi, USA
2801 North Thanksgiving Way, Lehi, Utah 84043, USA

Mountain View, USA
485 Clyde Ave., Mountain View, California 94043, USA

Asia Pacific, Japan

Bangalore, India
RMZ Eco World, 10th Floor, 8BCampus,
Marathalli Outer Ring Road, Bangalore - 560103, India

Melbourne, Australia
437 St Kilda Road, Melbourne, 3004, Australia

Tokyo, Japan
Ginza Six 8F, 6-10-1 Ginza Chuo-Ku, Tokyo,
104-0061, Japan

Europe, Middle East, Africa

Amsterdam, Netherlands
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein,
Netherlands

Cape Town, South Africa
Gateway Building, Century Blvd & Century Way 1,
Century City, 7441,Cape Town, South Africa

Dublin Ireland
Block 21 Beckett Way, Park West Business Park,
Dublin 12, D12 C9YE, Ireland

Gallen, Switzerland
Poststrasse 17, St Gallen, Switzerland, 9000

London, England
7th Floor, Exchange Tower,
2 Harbour Exchange Square, London E14 9GE

Mechelen, Belgium
Schaliënhoevedreef 20T, 2800 Mechelen, Belgium

Munich, Germany
Ismaninger Strasse 52, 81675 Munich, Germany

digicert®