# All About SSL/TLS

Learn how SSL/TLS certificates work—and the benefits of better website security

Symantec Website Security™

Today's online consumers are more security-savvy than ever, and they won't stay on a site they don't trust. That's why a high-assurance certificate from a reliable internet security provider is critical to your success as an online business—and that's where Secure Socket Layer (SSL/TLS) certificates come in. According to the Symantec 2016 Internet Security Threat Report, SSL/TLS remains at the heart of online privacy, authentication and encryption.[1]

SSL/TLS certificates help websites create a secure line of communication across the internet so that every bit and byte of data is protected by a process that visitors can trust.

## Expanding Security Measures

It's not just online consumers that are getting smarter—browsers are getting smarter too. Some browsers are beginning to flag sites that don't have the right level of security. For example, Google Chrome will display a message next to the web address that labels unencrypted sites as "Not Secure." Regardless of these changes, with the right security measures in place, you can boost your business' reputation and search engine ranking—and help keep browsers from mislabeling your site as unsafe.

This guide provides an introduction to SSL/TLS security and how it works. We will also discuss how SSL/TLS can help you ensure compliance and provide your customers with a consistent site experience that will help them trust your business.

## What Is SSL/TLS and What Are SSL/TLS Certificates?

SSL/TLS was developed in 1995 and quickly became the preferred method for securing data transmitted across the internet. It is now built into every major web server and browser so that websites can be positively identified by a third party as secure.

You can think of digital certificates as a kind of electronic ID card, not unlike a driver's license. Before establishing a secure communication channel to transfer the website's data across the web, SSL/TLS certificates validate the server to the client, thereby proving that the website is who it claims to be.

Certificates are issued by independent, trusted third-party companies, like Symantec, known as Certificate Authorities (CA).

SSL/TLS remains at the heart of online privacy, authentication and encryption.[1]

## SSL/TLS Features

People tend to associate SSL/TLS solely with encryption. But an SSL/TLS certificate actually provides four distinct features, all of which are critical to giving customers and users the security they demand: encryption, integrity, authentication and non-repudiation.

**Encryption**

Encryption utilizes mathematical algorithms to transform data so that it can only be read by the intended parties. In the case of SSL/TLS, the private and public keys provided as part of the server's digital certificate play an important role in securing data sent to and from the web browser.

**Integrity**

By encrypting data so that only the intended parties can read it, SSL/TLS certificates also ensure the integrity of that data. In other words, if nobody else can successfully read the data, the data cannot be modified in transit. Modifying the encrypted data would render it useless, and the intended parties would then know that someone had tried to tamper with the data.

**Authentication**

One of the primary roles of the CA in issuing a digital certificate is to validate the identity of the organization, or person, requesting the certificate. SSL/TLS certificates are tied to an internet domain name, and by verifying ownership of that name, a CA ensures that users know with whom they are dealing at a basic level. For example, when you connect to an SSL/TLS-enabled website, such as Amazon.com, the certificate identifies its owner as Amazon, Inc., and you can be sure that you are dealing with Amazon.

**Non-Repudiation**

Encryption, integrity and authentication combine to establish non-repudiation, which means that neither party in a secured transaction can legitimately state that their communications came from someone other than themselves. This feature removes the option for one party to repudiate, or "take back," information that they have communicated online.

Some CAs, like Symantec, also offer additional protection beyond SSL/TLS certificates that include things like vulnerability and malware assessments that will identify viruses, or "holes," in your website's security structure.

## SSL/TLS Applications

SSL/TLS can be used in many ways and for different purposes, including:

**Browser-to-server communications**

Most commonly, SSL/TLS is used to secure communications between a web server and a web browser, often when sensitive information is being transmitted. This information may relate to an online purchase, a patient's medical data or banking details. SSL/TLS helps ensure that the user of the web browser knows to whom their information is being sent and that only the intended recipient can access the information.

**Server-to-server communications**

SSL/TLS can also be used to secure communications between two servers, such as two businesses that transact with one another. In this scenario, both servers usually have a certificate, mutually authenticating them to each other as well as securing the communications between them.

Most commonly, SSL/TLS is used to secure communications between a web server and a web browser.

**Compliance with legislative and industry requirements**

Many legal and industry requirements call for levels of authentication and privacy that SSL/TLS certificates provide. The Payment Card Industry Data Security Standard (PCI DSS), for example, requires the use of authentication and encryption technologies during any online payment transaction.

**Securing exchange services**

You can use SSL/TLS certificates to secure email servers like Microsoft Exchange or Lync Server. It is necessary to secure every communication with these servers to protect sensitive data.

## The SSL/TLS User Experience

When users visit a website that has been secured with an SSL/TLS certificate, their web browser provides visual cues to let them know that SSL/TLS is working. One prominent cue is the address displayed in the browser's address field, which will start with "https://" for an SSL/TLS-secured connection, and "http://" for non-secured connections.

Most browsers also display some kind of lock icon (see Figure 1), although the location and appearance will vary from browser to browser.

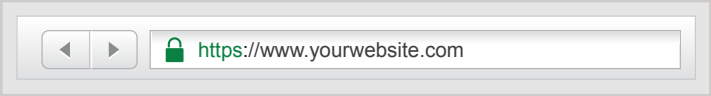


Figure 1: What visitors might see if they access an encrypted website.

Browsers may also allow the user to click the lock icon to view more information about the certificate.

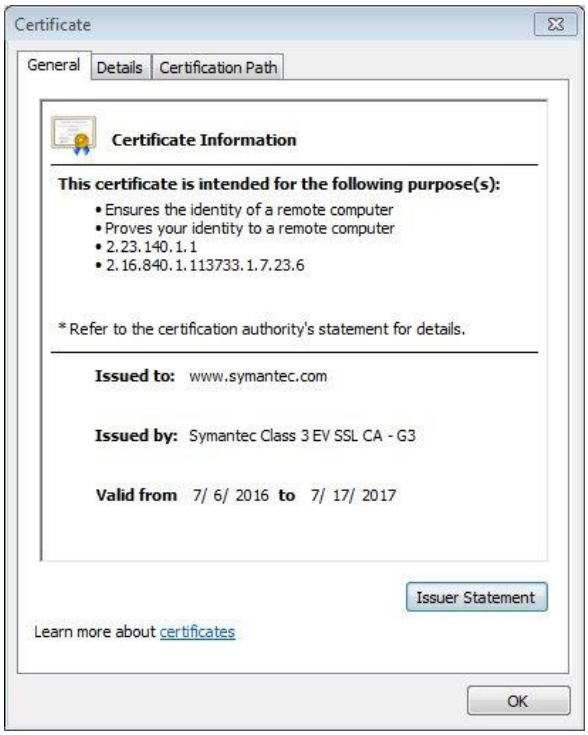


Figure 2: Details about a certificate, including the owner and issuer.

**Several key pieces of information are provided:**

- **The name of the domain** to which the certificate was issued. The certificate is only valid when used with this domain; a browser will reject a request if it is presented along with a different domain name.
- **The owner of the certificate**, allowing users to see the name of the entity with which they are dealing.
- **The date on which certificate validity begins and ends**. Like most other forms of identification, digital certificates expire and must be renewed, allowing the CA to reverify the identity of the certificate owner.

## Strong Certificate Validation

There are three available types of SSL/TLS certificates available, each with varying levels of validation: Domain Validation (DV), Organization Validation (OV), and more recently, Extended Validation (EV).

DV certificates are issued very quickly, but no company information is checked or displayed on the certificate. With OV the final vetted company information, which may include the company's address or name of a specific company contact, is displayed for visitors more visibly. These two options work well for situations where trust and credibility of a site are less important, either because the site is not consumer-facing, or the site doesn't involve passwords, payments or other sensitive data.

So, as a way to help websites and consumers differentiate between the three and ensure a secure overall internet infrastructure for sites that transfer sensitive information, the CA/Browser Forum, an independent industry group, produced guidelines for an EV certificate.

An EV certificate is an SSL/TLS certificate that requires the issuing CA to take rigorous steps to validate the certificate requestor's identity. CAs must also pass an independent audit of their validation procedures in order to continue offering EV certificates, meaning EV certificates tend to only be available from top-tier, highly trusted CAs, such as Symantec. Symantec is the #1 most recognized trust mark on the web and protects 81 percent of all global e-commerce revenue.[2]

These enhanced visual cues from EV certificates make it easier for users to positively confirm the identity of the website they are communicating with. Users who see the "Not Secure" label next to your web address may stop in the middle of the sign-up process, abandon their shopping cart or simply stop reading and close the tab.

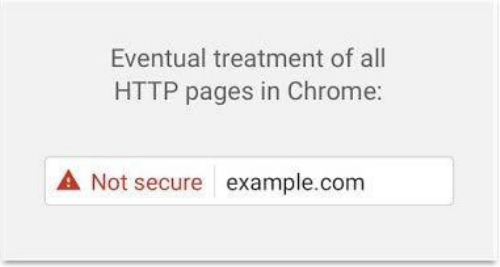


Figure 3: Many web browsers will begin showing "Not Secure" warnings on many websites that are unencrypted.

## Why Choose Symantec

Symantec offers a number of SSL/TLS certificate products, each one designed for specific business scenarios. Symantec certificates can help you grow your online business with:

- **Customer recognition**. The Norton Secured Seal that accompanies Symantec's SSL/TLS certificates is the #1 most recognized trust mark on the web today.[3]

- **Trusted reputation**. Ninety percent of the Fortune 500 and 96 of the world's 100 largest financial institutions depend on Symantec to safeguard their websites. That's why Symantec secures 81 percent of the world's e-commerce revenue.[3]

96% of the world's 100 largest financial institutions depend on Symantec.[3]

- **Unmatched customer support for both SMB and Enterprises**. Symantec was recently awarded the 2016 North America Frost & Sullivan Award for Customer Value Leadership.[4]

By making use of SSL/TLS certificates on your organization's web servers, you can securely collect sensitive information online and give your customers and users the confidence they need to trust your website. Consult a Symantec sales representative for information about our certificate products.

## To learn more, contact our sales advisors:

- **Via phone**
  U.S. toll-free: 1-866-893-6565

- **Visit our website at**
  www.symantec.com/ssl

[1] Symantec 2016 Internet Security Threat Report https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[2] International Online Consumer Research by Ipsos: U.S., Germany, U.K., France, Australia and Singapore, October 2015. comScore Analysis with top e-commerce organizations. comScore Analysis of Global Internet Traffic.
[3] Internal customer analysis against Forbes Global 2000 list published in 2015; Internet Retailer Top 500 Guide 2015 Edition; Internet Retailer Europe Top 500 2015 Edition; Internet Retailer Latin America Top 500 Guide 2015 Edition; comScore Analysis 2016; Thomson Reuters Top 100 Global Innovators Award, 2015; comScore Analysis with top ecommerce organizations; comScore Analysis of Global Internet Traffic.
[4] http://ww2.frost.com/news/press-releases/frost-sullivan-applauds-breadth-symantecs-security-solutions-well-collaborations-customers-and-peers-provide-customized-tools

## For global offices and contact numbers, please visit our website.

**For product information in the U.S., call:**
1-866-893-6565 or 1-520-477-3111

**Symantec World Headquarters**
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

**For product information in Asia Pacific, call:**
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

**Symantec Website Security Solutions Pty Ltd**
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

**For product information in the Americas (Non-U.S.), call:**
Mexico: 554 738 0448
Brazil: 800 038 0598

**For product information in the U.K., call:**
0800 032 2101 or +44 (0) 208 6000 740

**Symantec (UK) Limited**
350 Brook Drive
Green Park, Reading
Berkshire, RG2 6UH UK
www.symantec.co.uk/ssl

**For product information in Europe, call:**
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298

**Follow Us:**


Symantec Website Security™