A QUICK GUIDE TO SSL CERTIFICATES

MAKING THE BEST CHOICE WHEN CONSIDERING YOUR WEBSITE SECURITY OPTIONS

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.

What Is an SSL Certificate?

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

1. **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 Norton™ Secured Seal). The vetting criteria used by Certificate Authorities to determine if an SSL certificate should be issued is most stringent with an Extended Validation (EV) SSL certificate; making it the most trusted SSL certificate available.

2. **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.

In the same way that an identity document or passport may only be issued by the country's government officials, an 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 SSL certificate. When you have a valid SSL certificate from a trusted CA, there is a higher degree of trust by your customers, clients or partners.

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. SSL is also used for transmitting secure email, secure files, and other forms of information.

Would you send your private information or banking details to someone on the back of a postcard? SSL creates a safe and private channel for you to communicate.

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. Unless you have the right key, you will not be able to "open" the information. Each 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.

The Process: Every 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 an SSL certificate, an 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 SSL certificate, the domain secured, the type of 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 SSL Certificate?

1 A standard website without SSL security displays "http:// " before the website address in the browser address bar. This moniker stands for "Hypertext Transfer Protocol," and is the conventional way to transmit information over the Internet.
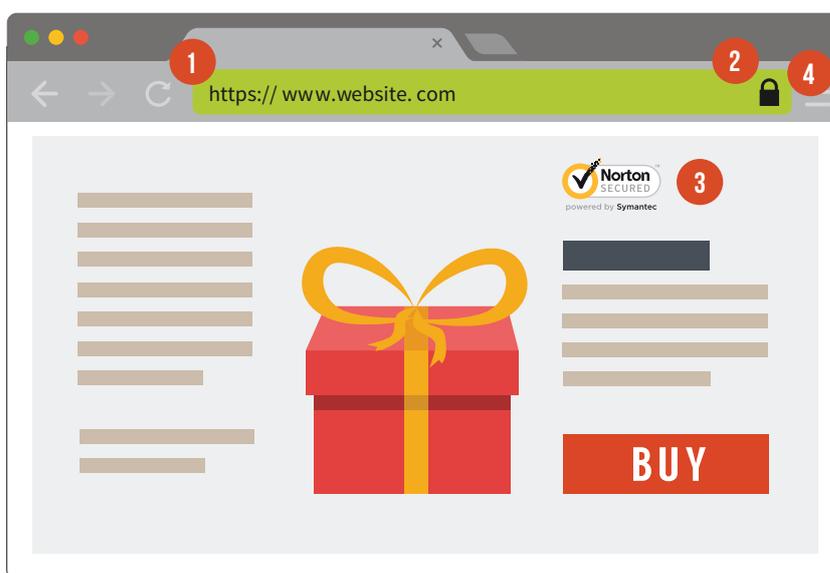
However, a website that is secured with a SSL certificate will display "https:// " before the address. This stands for "Secure HTTP."

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. Symantec™ customers use the Norton Secured Seal trust mark on their websites. When you click on the Norton Secured Seal 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 SSL trust marks such as the Norton Secured Seal, the website visitor sees the authenticated organization name. In high-security browsers, the authenticated organzation name is prominently displayed and the address bar turns green when an Extended Validation (EV) 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 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.

Here are some examples:

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.

Self-signed certificate

The first type of 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 SSL certificate issued by a CA.

A Domain Validated certificate is considered an entry level SSL certificate

A Domain Validated certificate is considered an entry-level 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 SSL certificate is the first step to true online security

A fully authenticated 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 organization 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.

Even though an SSL certificate is capable of supporting 128-bit or 256-bit encryption, certain older browsers and operating systems still cannot connect at this level of security. SSL certificates with a technology called Server-Gated Cryptography (SGC) enable 128- or 256-bit encryption to over 99.9 percent of website visitors. Without an SGC certificate on the Web server, browsers and operating systems that do not support 128-bit strong encryption will receive only 40- or 56-bit encryption. Users with certain older browsers and operating systems will temporarily step-up to 128-bit SSL encryption if they visit a website with an SGC-enabled SSL certificate.

- 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 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) SSL certificate allows for more than one domain to be added to a single SSL certificate.

- Code signing certificates are specifically designed to ensure that the software you have downloaded was not tampered with while en route. There are many cybercriminals who tamper with software available on the Internet. They may attach a virus or other malicious software to an innocent package as it is being downloaded. These certificates make sure that this doesn't happen.

- Extended Validation (EV) 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 SSL certificate, the address bar turns green (in high-security 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 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-scramble" 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 Internet Explorer (IE); Mozilla Firefox, Apple Safari,
RockMelt, 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 SSL certificates and correct placement and use of trust marks are proven tools in the establishment of customer trust.

For more information, visit us at **www.markmonitor.com**

About MarkMonitor

MarkMonitor, the leading enterprise brand protection solution and a Clarivate Analytics flagship brand, provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of advanced technology, comprehensive protection and extensive industry relationships to address their brand infringement risks and preserve their marketing investments, revenues and customer trust. For more information, visit **www.markmonitor.com**.

About Clarivate Analytics

Clarivate Analytics accelerates the pace of innovation by providing trusted insights and analytics to customers around the world, enabling them to discover, protect and commercialize new ideas faster. We own and operate a collection of leading subscription-based services focused on scientific and academic research, patent analytics and regulatory standards, pharmaceutical and biotech intelligence, trademark protection, domain brand protection and intellectual property management. Clarivate Analytics is now an independent company with over 4,000 employees, operating in more than 100 countries and owns well-known brands that include *Web of Science, Cortellis, Derwent, CompuMark, MarkMonitor* and *Techstreet*, among others. For more information, visit **www.clarivate.com**.

More than half the Fortune 100 trust MarkMonitor to protect their brands online.
See what we can do for you.

MarkMonitor Inc.
Europe   +44 (0) 207 433 4000
U.S.   (800) 745-9229
www.markmonitor.com

MarkMonitor
Protecting brands in the digital world

Clarivate
Analytics