



BEGINNERS GUIDE

BEGINNERS GUIDE TO DIGITAL SSL CERTIFICATES

THE BEST DECISION
WHEN CONSIDERING YOUR
ONLINE SECURITY OPTIONS.





BEGINNERS GUIDE TO DIGITAL SSL CERTIFICATES

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 Web site. It is important to understand the potential risks and then to 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 de-mystify the technology involved and give you the information you require 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.

For further information or assistance, please feel free to contact us at +61 3 9674 5500.

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 Web site, which it will display to visitors on your Web site when they click on the lock or trust mark (*VeriSign Secured® Seal*). With Extended Validation (*EV*) Certificates the vetting criteria are most stringent; making it the most trusted SSL Certificate available today.
2. **Encryption:** The SSL Certificate also enables encryption, which means that the information exchanged via the Web site cannot be intercepted or read by anyone other than the person for whom it is intended.

In the same way that a physical identity document or passport may only be issued by the relevant country’s government officials, an SSL Certificate is most reliable when issued by a known Certificate Authority (*CA*). The CA has to follow very strict rules and policies about who may or may not receive a SSL Certificate. This means that when you have a valid SSL Certificate from a trusted CA, it implies a higher degree of trust.

A QUICK LOOK AT ONLINE IDENTITY AND AUTHENTICATION

Identity and Authentication services are the Internet’s way of saying, *“I need to deliver a package.*

May I have your signature please?”



HOW DOES SSL ENCRYPTION WORK?

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

Each SSL session consists of two keys:

1. The public key is used to encrypt (jumble up) the information
2. The private key is used to decrypt (un-jumble) the information and restore it to its original format.

The process: Every SSL Certificate is issued for a specific server and Web site domain (*Web site address*) for a verified entity. When a person enters into their Internet browser or navigates to the Web site address of a Web site with a SSL Certificate, an SSL handshake (*greeting*) occurs between the browser and server. This requests information from the server which is then made visible to the person in their Internet browser. You will notice changes in your browser (*please see How do I know that a site has a valid SSL Certificate?*) 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 Certificate and issuing Certificate Authority. 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 Web site without SSL security displays *HTTP://* before the Web site address in the browser address bar. This 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*).



WHAT IS SSL?

SSL stands for “Secure Socket Layer” and is a technology that establishes a secure session link between the visitor’s Web browser and your Web site so that all communications transmitted through this link are encrypted and 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.



2. You will also see a Padlock 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 Web site. VeriSign customers use the VeriSign Secured® Seal. When you click on the VeriSign Secured® Seal or the padlock on the page, it will display the relevant 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 VeriSign Secured® Seal*), the Web site visitor sees the authenticated organisation name. In high-security browsers, the authenticated organisation name is prominently displayed and the address bar turns green when an Extended Validation 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 Web site 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 CERTIFICATE

There are a number of different SSL Certificates on the market today. In this guide, we will introduce you to the latest and more popular options available.

1. 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 Certification Authority. Since the owner generates their own certificate, it does not hold the same weight as a fully authenticated and verified SSL Certificate issued by a Certificate Authority.
2. A **Domain Validation Certificate** is considered as an entry-level SSL Certificate and can be issued very quickly. The reason for this is that the only verification check done is to ensure that the applicant owns the domain (*Web site address*) for which they want the Certificate. No additional checks are done to ensure that the owner of the domain is a valid business entity.
3. 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 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.
4. 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. Without an SGC certificate on the Web server, Web 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 Web site with an SGC-enabled SSL Certificate. SSL Certificates with SGC enable 128- or 256-bit encryption to over 99.9% of Web site visitors. For more information about SGC please visit:
5. A domain name is often used with a number of different host suffixes. For this reason, we introduced the **Wildcard Certificate** that allows you to provide full SSL security to any host of your domain for example: *host.yourdomain.com (host varies but the domain name stays constant)*.
6. Similar to the **Wildcard Certificate** but a little more versatile, the **SAN (Subject Alternative Name) SSL Certificate** allows for more than one domain to be added to one Certificate.
7. **Code signing Certificates** are specifically designed to ensure that the software you have downloaded was not tampered with while en route. There are many cyber criminals 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.
8. **Extended Validation (EV) SSL Certificates** offer the highest industry standard for authentication at present and offer the best level of customer confidence available. An EV Certificate turns the address bar of the latest versions of Internet browsers green (*See "How do I know that a site has a valid SSL Certificate?" Point 4 above*). It also displays the name of the Certificate holder and Certificate Authority (CA) in the address bar. Research shows that 97% of online shoppers feel confident sharing their private and banking details with a Web site that displays the green address bar. (*Tec-Ed 2007*)

All VeriSign® brand SSL Certificates are fully authenticated.

TECH TALK MADE SIMPLE

Encryption: this is where information is jumbled up so that it cannot be used by anyone other than the person for whom it is intended.

Decryption: to un-jumble 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 key, the stronger the encryption.

Browser: the program that you use to access the Internet. Most popular are Microsoft Internet Explorer (*IE*); Mozilla Firefox, Apple Safari, Flock, Google Chrome, and many others.

CONCLUSION

SSL Certification is no longer merely a technical component on a network, it is a technology that could have a significant impact on the level of consumer confidence when they visit your Web site. The effective implementation of SSL Certificates and correct placement of the trust mark have proven time and again that your business could experience an increase in sales as a direct result.

Visit www.Verisign.com.au/ssl/ for more information.

SSL CERTIFICATION

Would you feel safe locking your home or business with these keys?



Remember: You get what you pay for.



In the same way that locking your door does not prevent burglars from entering through the window, SSL Certification only forms a part of your network security. In order to help ensure maximum protection, it is imperative that your entire network infrastructure is secure.