BEGINNERS GUIDE

BEGINNERS GUIDE TO SSL CERTIFICATES:

MAKING THE BEST CHOICE WHEN CONSIDERING YOUR ONLINE SECURITY OPTIONS

VeriSign®

BEGINNERS GUIDE TO 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 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 our sales department at 1-866-893-6565 Option 3, or 1-650-426-5112 or email: isales@verisign.com.

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 browser's padlock symbol or trust mark (e.g., the VeriSign seal). The vetting criteria used 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 web site cannot be intercepted and read by anyone other than the intended recipient.

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 trusted Certificate Authority (CA). The CA has to follow very strict rules and policies about who may or may not receive an SSL Certificate. So, when you have a valid SSL Certificate from a trusted CA, there is 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.

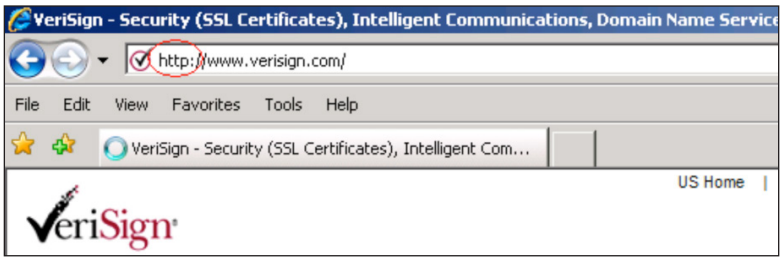
Each SSL session consists of two keys:

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 so that it can be read.

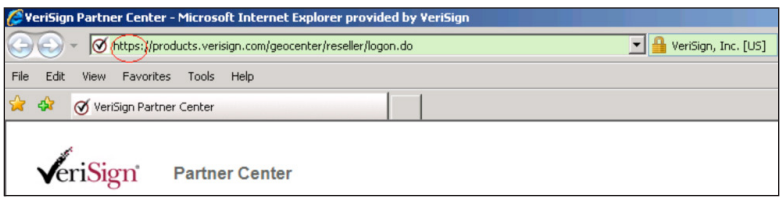
The Process: Every SSL Certificate is issued for a specific server and web site domain *(web site address)* for a CA-verified entity. When a person uses their browser to navigate to the address of a web site with an SSL Certificate, an SSL handshake *(greeting)* occurs between the browser and server. Information is requested from the server—which is then made visible to the person in their browser. You will notice changes in your browser (for more details, please see "How Do I Know That a Site Has a Valid SSL Certificate?" below). 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. 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 moniker stands for "Hypertext Transfer Protocol," and is the conventional way to transmit information over the Internet.



However, a web site that is secured with a SSL Certificate will display "*https://*" before the address. This stands for "Secure HTTP."



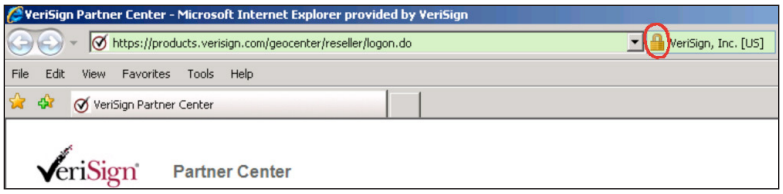
WHAT IS SSL?

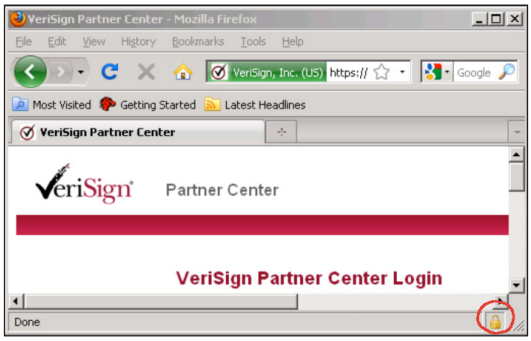
SSL stands for "Secure Socket Layer." It is a technology that establishes a secure session link between the visitor's web browser and your web site so that all communications transmitted through this link are encrypted and are, therefore, secure. SSL is also used for transmitting secure email, secure files, and other forms of information.

Would you send your private information or banking details to someone on the back of a postcard?

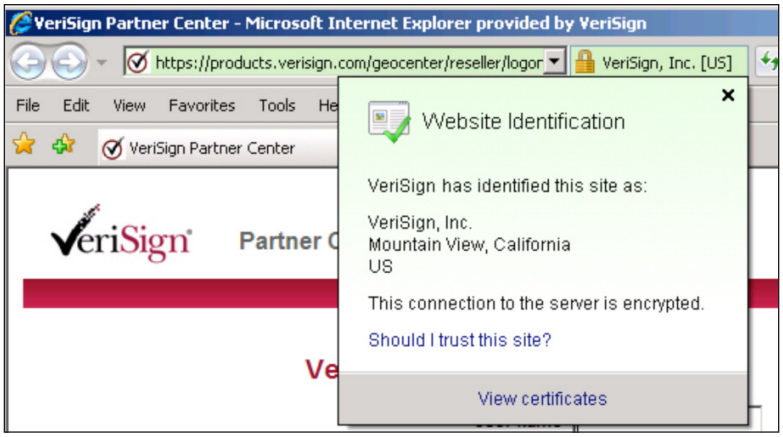
SSL creates a safe and private channel for you to communicate.

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

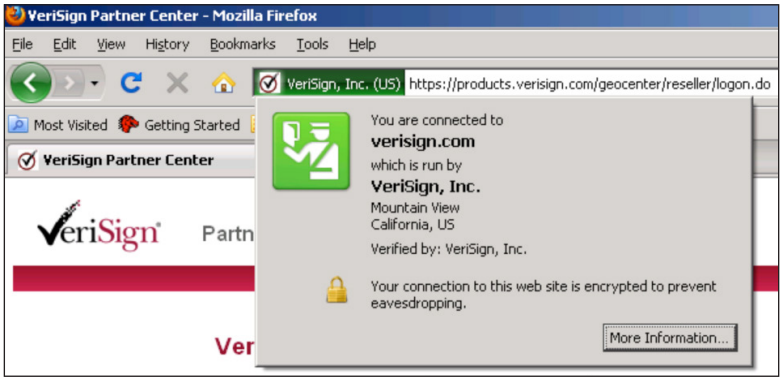




3. Often, you will also notice a trust mark displayed on the web site. VeriSign customers use the VeriSign® seal trust mark on their web sites. When you click on the VeriSign seal or the padlock symbol on the page, it will display details of the relevant certificate with all of the company information 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 seal), the web site visitor sees the authenticated organization name. In high-security browsers, the authenticated organization 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 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.

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 CA. Since the web site owner generates their own certificate, it does not hold the same weight as a fully authenticated and verified SSL Certificate issued by a CA.

2. 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 (web site 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.

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 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.

All VeriSign® brand SSL Certificates are fully authenticated.

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 of security. SSL Certificates with a technology called Server-Gated Cryptography (SGC) enable 128- or 256-bit encryption to over 99.9% of web site 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 web site with an SGC-enabled SSL Certificate. For more information about SGC please visit: www.verisign.com/sgc.

5. 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).

6. 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.

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 and provide the best level of customer trust available. When consumers visit a web site 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 web site 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 "jumbled up" so that it cannot be used by anyone other than the person for whom it is intended.

Decryption: "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 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, Flock, 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 e-commerce web site. The effective implementation of SSL Certificates and correct placement and use of trust marks are proven tools in the establishment of consumer trust.

VeriSign is the world's leading provider of SSL Certificates, and over 90,000 domains in 160 countries display the VeriSign seal, the most recognized trust mark on the Internet. To ensure that current and future customers are fully aware of security investments being taken by e-commerce businesses, it is critical to go with a security vendor whose brand name is the best known and the most trusted. VeriSign has earned its industry-leading brand name recognition, and related customer trust, by delivering the state-of-the-art in online security and trust solutions.

Visit us at www.VeriSign.com/ssl/index.html
for more information.