



WHITE PAPER

The Latest Advancements in SSL Technology





CONTENTS

+ Introduction	3
+ SSL Overview	3
+ Server Gated Cryptography: Enabling the Strongest Level of Encryption	4
+ Extended Validation SSL (EV SSL): The Gold Standard for Authentication	5
+ Browser Support for EV SSL	6
+ Third Party Trust Marks: Inspiring Consumer Confidence	6
+ Summary	7



The Latest Advancements in SSL Technology

+ Introduction

Secure Sockets Layer (SSL) Is the World Standard for Web Security. SSL technology confronts the potential problems of unauthorized viewing of confidential information, data manipulation, data hijacking, phishing and other insidious Web site scams, by encrypting sensitive data so that only authorized recipients can read it. In addition to preventing tampering with sensitive information, SSL helps provide your Web site's users with the assurance of having accessed a valid Web site. Support for SSL is built into all major operating systems, Web applications, and server hardware—meaning that SSL's powerful encryption technology helps provide your business with a system-wide, liability limiting security blanket for fortifying consumer confidence, boosting the percentage of completed transactions, and enriching the "bottom line." Due to recent advances in SSL technology, there is a variety of different kinds of SSL. In this paper, we will discuss some of these advances, to help you decide which would be best for your organization.

+ SSL Overview

SSL became the standard over a decade ago to ensure the privacy of online communications. A special data file called an SSL Certificate is created for a specific server in a specific domain for a specific entity. Similar to a passport or driver's license, SSL Certificates are issued by trusted authorities, such as VeriSign. Every entity that receives an SSL Certificate must pass some form of authentication that verifies they are who they say they are. With the explosion of phishing and other fraudulent Web activity aimed at stealing people's personal information, identity authentication is more important now than ever before. The level of identity authentication verified by an SSL Certificate differs from one SSL Certificate to another, and from one Certification Authority (CA) to another.

With SSL, a private and public key system encrypts the connection between two parties, such as a consumer and a Web site bearing an SSL Certificate. When the consumer's browser points to a Web site secured with SSL, a secure handshake between the two systems authenticates both parties. Each session uses a unique session key for encryption (the longer the key, the stronger the encryption). Once this connection is established the two parties can begin a secure session guaranteeing the privacy and integrity of their communications. This security is particularly important when people are sharing sensitive, confidential information over the Internet, an extranet, or even within an intranet. In the case of e-commerce, a secure SSL connection is critical to doing business, as most Internet users are afraid to share information with a Web site that doesn't offer SSL protection.

A small purchase here, a smaller purchase there, and a reluctance to change age-old buying habits or reveal personally identifying information characterizes an enormous segment of the world's viable online consumer population. The question remains: Will potential customers feel secure enough in their Internet dealings with your Web site to take a meaningful plunge into the world of transacting online?

+ Server Gated Cryptography: Enabling the Strongest Level of Encryption

If your reputation in the online community depends upon the stringent safeguarding of information processed through your Web site, then your Internet security solution should include the strongest encryption available to each Web site visitor. Encryption, as mentioned above, is the process whereby data is transformed into a code that will be indecipherable to an unauthorized viewer. The stronger the encryption, the more difficult it is for someone to eavesdrop on your online communications. This is especially important if you accept any kind of online payments, connect to a bank or brokerage account, transmit health records, must meet a governmental or other regulatory organization's privacy and security standards, or process any kind of potentially sensitive information.

Industry experts recommend a minimum of 128-bit encryption be used for all secure online sessions. Some web server-client browser configurations enable sessions with up to 256-bit encryption protection, the strongest level of encryption commercially available today. The strength of encryption enabled for any session depends on what your customer's browser and operating system supports, as well as what your host server systems will support. If your consumer's browser or operating system doesn't support higher levels of encryption, the session will default down to the highest level that they can support.

For years the U.S. imposed export restrictions prohibiting browser manufacturers from distributing products that supported higher levels of encryption. Although these export restrictions have been somewhat lifted, there are many consumers, especially outside the U.S., who are still using older browsers (such as those before Microsoft® Internet Explorer 5.5) and operating systems (such as Windows 2000), which may default to risky, lower encryption levels. The Yankee Group estimates that tens of millions of Internet users connect to the Web using substandard encryption levels.

Server Gated Cryptography (SGC) helps fix this problem for 99.9% of users. An SGC-enabled SSL Certificate automatically steps-up the encryption level for the vast majority of legacy browser and operating systems to the industry recommended 128-bit level of protection. This step-up improves the security of online communications significantly. With a normal desktop PC, a hacker can break 40-bit and 56-bit encryption in hours, whereas it would take that same hacker more than a trillion years to break a 128-bit encrypted session.¹

SGC is an SSL extension originally created for financial institutions exempted from the U.S. encryption export restrictions. With SGC, encryption levels are controlled by the server and not dependent on the client system. Now that these original export restrictions have been lifted, SGC-enabled SSL Certificates can be issued to all types of Web sites, not just authorized financial institutions.

VeriSign offers market-leading SGC-enabled SSL Certificates so virtually every visitor to your Web site will be protected by the industry recommended minimum of 128-bit encryption.

¹ 2005, Yankee Group, Building Blocks of Transparent Web Security: Servers-Gated Cryptography

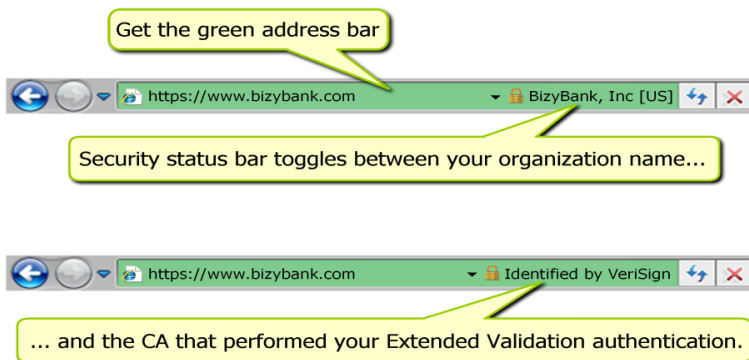
+ Extended Validation SSL (EV SSL): The Gold Standard for Authentication

While more and more people are comfortable searching the Internet, there remains a significant disconnect between the numbers of surfers and those psychologically disposed to transact business online. As a Gartner 2006 survey revealed, security concerns led almost half of online customers to alter the way they use the Internet, at a cost of almost \$2 billion to the online business community.² Clearly, too many potential e-commerce clients remain distrustful or fearful of revealing personal or financial information to an unseen and personally unknown entity. They need assurance and are increasingly demanding it before they proceed through a personal revelation or financial transaction.

These and similar observations led a group of CAs, browser providers, and WebTrust auditors to establish the CA/Browser Forum for developing a new SSL standard — one that the online consumer world could easily comprehend and embrace. This consortium, which includes representatives from both Microsoft and VeriSign as well as others, created Extended Validation (EV) SSL. This new standard aims to combat the growth of Internet threats such as phishing attacks. EV SSL requires a rigorous process of Web site authentication and is considered the “gold standard” in the e-commerce industry for authenticating the legitimate identity of a Web site. In order to issue EV SSL Certificates, a CA must pass a rigorous WebTrust audit. VeriSign remains at the forefront in the development and implementation of this new standard.

An EV SSL Certificate offers the online business and consumer a highly endorsed and widely recognized level of protection from increasingly sophisticated Internet spoofing scams. EV SSL contains a number of user interface enhancements aimed at making the identification of an authenticated site immediately more noticeable to the end user.

New high-security browsers display EV SSL Certificates differently than traditional SSL certificates. Rather than the subtle padlock symbol displayed by traditional SSL Certificates, EV SSL Certificates trigger the browser address bar in high-security browsers to change to an eye-catching green color. This change is immediately evident to an end user and delivers a confidence building effect. Overstock.com noticed that after implementing an EV SSL Certificate from VeriSign, their Microsoft® IE7-using visitors on average completed transactions 8.6% more often than those using legacy non-EV-enabled browsers. And, after deploying VeriSign EV SSL, DebtHelp.com realized an 11% increase in completed transactions by visitors to their Web site.



2. 2006, Gartner, Trends in Consumer Society

In addition to the noticeable green color, a security status bar prominently displays the name of the owner of that Web site and the CA who has issued that EV SSL certificate. This field reveals both names in turn when a visitor first arrives on the Web site.

Like its traditional SSL predecessors, an EV SSL Certificate facilitates secure encrypted communication between a Web site and a consumer's browser. It also authenticates the genuine nature of the Web site so each visitor knows they have indeed reached the site they intended to visit and not a counterfeit site.

You gain the benefit of this gold standard for authentication as well as the powerful protection of SGC encryption with VeriSign SSL Certificates. VeriSign offers a certificate with both of these SSL advancements.

+ Browser Support for EV SSL

Microsoft, the first browser manufacturer to support this new standard, integrated the EV SSL interface enhancement with Microsoft IE7. Although relatively new to the market, IE7 has already garnered 31% of the browser market.³ Additionally, Firefox 2.0 users can download an extension that enables them to see the green address bar when they encounter a VeriSign EV SSL Certificate. Within a month of this extension's release over 55,000 Firefox users had downloaded it. As of June 2007, no other CA offers this benefit.

+ Third Party Trust Marks: Inspiring Consumer Confidence

Virtually all shoppers acknowledge their concerns about identity theft, credit card fraud and other Internet scams. They have a reason to be concerned. During the one-year period ending July 2006, the monetary loss from identity theft scams totaled \$56.6 billion with an average cost per episode of \$6,383.⁴

The good news is that consumer awareness of solutions to security issues is destined to increase as both the Internet security industry and certain governmental agencies get the word out. To be sure, online consumers are already becoming increasingly savvy about Internet security. Many now expect to see a familiar third party trust mark identifying an online retailer's Web site as a secure and viable shopping avenue. Inclusion of an established third party trust mark on one's Web site is now essential for guiding shoppers from the "surfing" stage through the completion of a transaction.

Research has shown that the majority of online shoppers recognize the VeriSign Secured™ Seal and indicate they would make an online purchase because of that seal's presence.⁵ If you purchase a VeriSign SSL Certificate for your Web site you are entitled to display the exclusive VeriSign Secured Seal. Displaying the seal should increase your customer's confidence in your Web site and increase the number of completed transactions you experience. Also, visitors can click on the seal to verify your site. One week after posting a VeriSign Secured Seal on their Web site, Opodo, a leading pan-European travel service saw a 10% jump in completed sales.⁶

³ May 2007, www.marketshare.com

⁴ 2006, Javelin Strategy/Better Business Bureau, Identify Fraud Survey Report

⁵ 2006, Tech-Ed study

⁶ Warren Jonas, Head of Services Management, Opodo



Once you secure your Web site with a VeriSign SSL Certificate, all you need to do to benefit from the VeriSign Secured Seal trust mark is download and install it.

+ Summary

Credibility means a lot in the world of Internet security. With instant recognition by 88% of Web users⁷, VeriSign is by far the most recognizable Secure Sockets Layer (SSL) security brand in the world today. VeriSign gained its leadership position by helping the Internet security industry develop standards, update protocols, and apply the latest technologies for the Web community. Savvy online consumers trust the VeriSign name and feel confident about doing business with Web sites secured by a VeriSign SSL Certificate. Naturally, this reputation wasn't created overnight. It was built upon a platform of trust that has been cultivated for years and enhanced by the company's long-time involvement and support of the development of the Internet security infrastructure.

Organizations that rely on Internet transactions have learned that a reliable and secure Internet is necessary for company profitability. The more secure the online consumer feels, the more successful the online company will be in recruiting and retaining a worthy client base. The creation of a successful online business requires the development and cultivation of a trustworthy relationship with each potential client. VeriSign's products enhance the building of such relationships. If you want to ensure that potentially sensitive information is kept confidential and secure, and especially if you want your potential customers to trust that your company will value, respect and safeguard their private information, a VeriSign SSL Certificate is right for you.

Displaying VeriSign's name emphasizes your Web site's genuineness, credibility and trustworthiness to your customers. Your customers can then feel secure about completing the transaction that led them to your site in the first place.

Visit us at www.VeriSign.com for more information.

⁷ 2006, Tec-Ed study

©2007 VeriSign, the VeriSign logo, the checkmark circle, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.