



BUSINESS GUIDE

What Every E-Business Should Know about
SSL Security and Consumer Trust



Where it all comes together.™



CONTENTS

+ Introduction	3
The Security of Your Web Site Is the Backbone of Trust for E-Business	3
Secure Sockets Layer (SSL) Is the World Standard for Web Security	3
VeriSign Solutions for the Strongest Security	4
+ Encryption Technology and SSL Certificates	4
+ Making E-Commerce Secure with VeriSign SSL	5
+ VeriSign Is the Commercial Standard for SSL Security	5
Authenticating Your Web Site with VeriSign SSL Ensures Trust	5
+ VeriSign SSL Solutions	6
VeriSign Secure Site Pro Guarantees the Strongest Available SSL Encryption to Every Site Visitor	6
VeriSign Secure Site SSL Certificates for Protecting Sensitive Data on Intranets and Public Web Sites	7
Simplify Management of Multiple SSL Certificates	7
+ Conclusion	8
Try a VeriSign SSL Certificate for Free	8
For More Information	8



VeriSign offers a cost-effective, proven solution for securely doing business over the Web. This proven technology is in use now by top e-commerce sites, Fortune 500 companies, and hundreds of thousands of other leading Web sites.

Introduction

+ The Security of Your Web Site Is the Backbone of Trust for E-Business

Gaining the trust of online customers is vital for the success of e-commerce. Based on recent online business statistics, some companies have earned that trust by showing strong overall growth in e-commerce. According to the latest research from the Interactive Media in Retail Group (IMRG) an estimated £4bn was spent over the net in November and December 2004 an increase of 64 percent over the same period in 2003. But there is huge room for expansion. E-commerce sales during that period were just 6.8 percent of total retail.¹ Most consumers have access to the Web, so the relatively small size of e-commerce compared to traditional, off-line spending does not owe itself to lack of opportunity. In fact, many people deliberately limit the transactions they do online because they don't fully trust the e-commerce process. These people simply fear for the security of personal and financial information transmitted over the Web.

Fear of online fraud is well founded. Gartner reports nearly two million Americans were victims of fraud over the Internet during a recent 12-month period. The direct loss to banks and consumers was \$2.4 billion, according to an April 2004 survey.² Gartner estimates that 57 million Internet users in the United States have received email related to phishing scams that impersonate popular Web sites; about 1.8 million people consequently divulged personal information. Three-fourths of phishing attacks have occurred in the previous six months.³ Fortunately, companies can prevent most online fraud with stringent screening and prevention measures. Companies using these measures hold average fraud losses to just over one percent of sales, according to research by Jupiter Media Metrix.

VeriSign can help your company establish or improve customer trust by securing your Web site for business. VeriSign offers the strongest security in the industry by securing information exchange between Web servers and clients, from server to server, and even among other networking devices such as server load balancers or SSL accelerators. VeriSign solutions can provide complete crossnetwork security by protecting servers facing both the Internet and private intranets.

+ Secure Sockets Layer (SSL) Is the World Standard for Web Security

SSL⁴ technology is used to encrypt and protect information transmitted over the Web with the ubiquitous HTTP protocol. SSL provides your Web site's users with the assurance of access to a valid, "non-spoofed" site, and it prevents data interception or tampering with sensitive information. Support for SSL is built into all major operating systems, Web applications, and server hardware — meaning that your business can use SSL for its powerful encryption capabilities and the increased consumer confidence that comes from VeriSign's mark of security. VeriSign® SSL Certificates are just the thing to protect sensitive data transmitted between your servers, consumers, and business partners.

¹See www.census.gov/mrts/www/current.html.

²Information Week, 6/15/04, www.informationweek.com/story/showArticle.jhtml?articleID=21800505.

³The Wall Street Journal, 6/15/04, <http://online.wsj.com/article/0,SB108724856255936731,00.html>.

⁴The Internet Engineering Task Force has renamed SSL to Transport Layer Security (TLS), and is working on wider adoption of the TLS protocol. SSL, however, remains the popular nomenclature.



Consumers Cite VeriSign as the #1 Brand for Web Site Security.

The VeriSign Secured™ Seal included with every Secure Site Service allows your company to display the number one trust brand on the Internet. This seal is recognized by 83 percent of U.S. online shoppers, according to a July 2004 study by TNS.

More than four in five of these shoppers prefer the VeriSign Secured Seal, according to the study. Significantly, 93 percent of shoppers say it's important for sites to display a trust mark and 64 percent of consumers who have terminated a transaction online would have gone through with it if a recognized trust mark had been present.

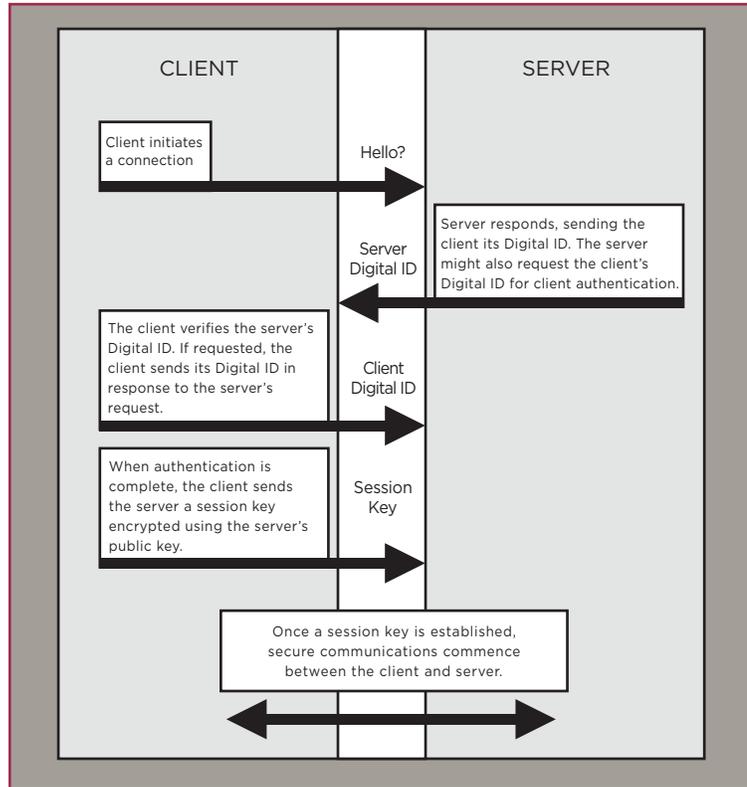
The VeriSign Secured Seal also allows your visitors to check your SSL Certificate's information and status in real time — increasing customers' trust in your e-business.

+ VeriSign Solutions for the Strongest Security

VeriSign® Secure Site Services offer your company the power to secure its Web site for safe information transfer, especially for e-commerce and other financial transactions. VeriSign is the leading global provider of SSL Certificates and the only leading provider who can guarantee that every Web site visitor will receive the strongest SSL encryption available — regardless of operating system or browser version. With VeriSign, customers and business partners using your site will get the trustworthy Web experience they demand. Information on obtaining a free trial of a VeriSign SSL Certificate is available at the end of this guide.

Encryption Technology and SSL Certificates

Encryption is the process of transforming information to make it unintelligible to all but the intended recipient. Encryption is the basis of data integrity and privacy necessary for e-commerce. Customers and business partners will submit sensitive information and transactions to your site via the Web only when they are confident that their sensitive information is secure. The solution for businesses who are serious about e-commerce is to implement a trust infrastructure based on encryption technology.



An SSL Certificate is an electronic file that uniquely identifies individuals and Web sites and enables encrypted communications. SSL Certificates serve as a kind of digital passport or credential. Typically, the “signer” of a SSL Certificate is a “Certificate Authority,” such as VeriSign. The previous diagram illustrates the process that guarantees protected communications between a Web server and a client. All exchanges of SSL Certificates occur within seconds and require no action by the consumer.

Making E-Commerce Secure with VeriSign SSL

Installing VeriSign SSL Certificates makes e-commerce transactions with your Web site safer and submitting sensitive information over the Internet easier. Browsers have built-in security mechanisms to prevent users from unwittingly submitting their personal information over insecure channels. If a user tries to submit information to an unsecured site (a site without a SSL Certificate), the browser will by default show a warning, which can lead the user to question the trustworthiness of this e-commerce site.

VeriSign Is the Commercial Standard for SSL Security

VeriSign is the world’s leading Certificate Authority, having issued more than 400,000 SSL Certificates. Web users are accustomed to seeing commercial e-commerce sites display the VeriSign Secured™ Seal – prominently featured to assure online users that their Web business is authentic and that this site is capable of securing their confidential information with SSL encryption. In fact, in a 2004 study of the 12 most prominent trust marks on the Web, the VeriSign Secured Seal ranked highest by a wide margin in perceived safety of visitors’ information, perceived trustworthiness, purchase likelihood, and overall preference. Subjects also ranked the VeriSign Secured Seal as the most recognised of the tested marks.

+ Authenticating Your Web Site with VeriSign SSL Ensures Trust

Encryption alone is not enough to ensure a secure Web site and to build trust between your business and its customers and business partners. It is imperative that your company’s identity be verified to improve Web visitors’ trust in you and your Web site. VeriSign assures trust by coupling rigorous business authentication practices with state-of-the-art encryption technology in its SSL Certificate solutions. VeriSign will only issue an SSL Certificate to your online business after it has performed the following authentication procedures:

- Verify your company’s identity and confirm it as a legal entity
- Confirm that your company has the right to use the domain name included in the certificate
- Verify that the individual who requested the SSL Certificate on behalf of the company was authorised to do so

What every online shopper should know about Windows 2000 and 128-bit SSL encryption.

Many savvy online shoppers understand that 128-bit encryption is the strongest offered for SSL today. They know that many export version⁶ browsers will fail to step up to 128-bit encryption except when an SGC-capable SSL Certificate is available on the server. But most people don't understand that a significant number of Windows 2000 systems will fail to step up to 128-bit encryption unless the SSL Certificate supports SGC and that this limitation occurs regardless of the version of Internet Explorer running on the client system. Even the most current version of Internet Explorer still fails to step up in the absence of SGC when it is run on one of these Windows 2000 systems.

Which systems are they? Any copy of Windows 2000 shipped prior to approximately March 2001 that was not subsequently upgraded with one of several Windows upgrade packs will suffer this limitation. The exact number of affected systems is unknown, but with over 156 million Windows 2000 systems in use — almost 40 percent of all personal computers encompassing all operating systems — this number is certainly very large. Among leading providers of SSL Certificates, only VeriSign⁵ offers a solution that guarantees 128-bit SSL encryption for every one of these 156 million Windows 2000 systems.

⁵SSL Certificates may be obtained from VeriSign's affiliates, resellers, or subsidiaries in addition to directly from VeriSign, Inc.

⁶For many years, the U.S. government restricted U.S. vendors from exporting "strong" cryptography. As a result, many Internet users around the world downloaded or purchased computers with export version browsers, capable of supporting only 40- or 56-bit SSL encryption. To allow vendors to adhere to the export restrictions while still addressing the need for secure communications outside the United States, Microsoft developed "Server Gated Cryptography" ("SGC") and Netscape developed "step-up" technology. SGC allows users with an export version browser temporarily to step-up to 128-bit SSL encryption if they visit a Website with an SGC-compatible SSL certificate, such as VeriSign's Secure Site Pro certificate. Without an SGC certificate on the Web server, Web browsers and PCs that do not inherently support 128-bit strong encryption will receive only 40- or 56-bit encryption.

VeriSign's rigorous authentication practices are designed to set the industry standard. VeriSign documents its carefully crafted and time-proven practices and procedures in a published Certificate Practices Statement and annually undergoes an extensive Statement of Auditing Standard 70 (SAS 70) Type II audit by KPMG. (SAS 70 was established by the American Institute of Certified Public Accountants to certify trusted practices.) The authentication and verification procedures established by VeriSign can help your company comply with the security provisions of various security regulations, inspire trust and confidence in customers and business partners by verifying your identity, and reduce the risk of fraud. Procedures used by VeriSign are the result of years of operating trusted infrastructure for the Internet and authenticating more than half a million commercial businesses.

VeriSign SSL Solutions

+ VeriSign[®] Secure Site Pro Guarantees the Strongest Available SSL Encryption to Every Site Visitor

VeriSign[®] Secure Site Pro is the best SSL solution to protect confidential transmissions to and from your Web site from being read or modified by anyone other than the communicating parties. Secure Site Pro takes advantage of Server Gated Cryptography (SGC) technology to provide powerful 128-bit SSL encryption to the most possible site visitors. No other SSL Certificate offers stronger encryption to any site visitor than Secure Site Pro.

In fact, among leading SSL providers, VeriSign is the only one to offer SGC-enabled certificates. That means only VeriSign can offer the strongest available SSL encryption to every site visitor, regardless of the browser and operating system that the visitor is using. SGC enables SSL Certificates such as Secure Site Pro to "step-up" to 128-bit SSL encryption when communicating with many client systems that otherwise could only connect at 40- or 56-bit encryption. Systems that require SGC to provide 128-bit encryption are those using older browsers in a certain range of versions and many Windows[®] 2000 systems — even those using the very latest version of Internet Explorer (see sidebar).

Is 128-bit SSL encryption really that much stronger than 40-bit encryption? Yes in fact, it is. 128-bit encryption offers 2⁸⁸ times as many possible combinations as 40-bit encryption, which is equal to approximately 300 septillion (300,000,000,000,000,000,000,000) times stronger. That's over a trillion times a trillion times stronger. The most common form of encryption breaking is "brute force" computation, the inputting of every possible variable into a prompt until the right one comes up. A hacker could theoretically crack a standard 40-bit encrypted session in less than a day, but doing so would require expertise and an elaborate setup with a dozen or so computers; for small low-risk businesses, 40-bit encryption remains safe. For larger organisations, or those particularly concerned with security, 128-bit encryption, the preferred security level of government and financial institutions, offers protection that is virtually unbreakable. If a hacker could crack a standard 40-bit SSL session in a day, it would take well beyond a trillion years to accomplish the same thing against a 128-bit SSL session.

VeriSign's recommendation for strongest SSL security is to use one Secure Site Pro SSL Certificate per domain name, per server.

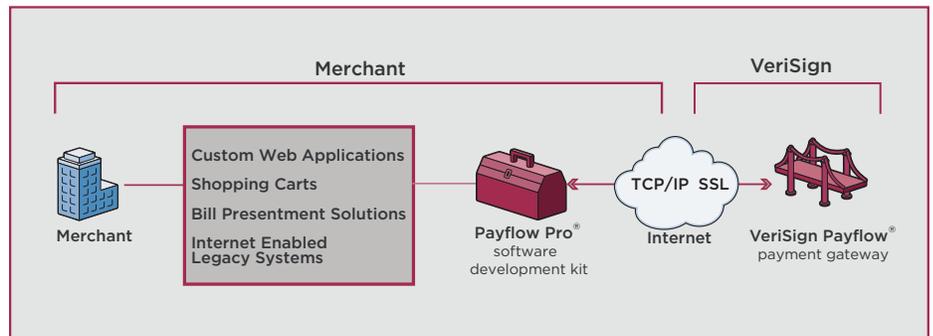
+ VeriSign Secure Site SSL Certificates for Protecting Sensitive Data on Intranets and Public Web Sites

VeriSign Secure Site SSL Certificates are ideal for security-sensitive extranets and Web sites. They enable 128-bit SSL encryption for users with newer operating systems and browsers. VeriSign Secure Site enables 40-bit SSL encryption when communicating with a large number of older systems currently in use, including many Windows 2000 systems (regardless of whether these systems are using the most recent version of Internet Explorer or not), and some older browser versions as well. Secure Site SSL Certificates run on virtually all server software platforms.

+ Simplify Management of Multiple SSL Certificates

Is your Web site hosted on five or more servers? With one simple purchase, VeriSign® Managed Public Key Infrastructure (PKI) for SSL and Managed PKI for SSL Premium Edition services let you issue all the SSL Certificates you need in bundles of 5, 10, 25, 50, 100, or more. A convenient one-step purchasing process lets you take advantage of a single purchase order, and volume discounts make Managed PKI for SSL the most cost-effective way to secure Web sites with large numbers of Web servers or other trust devices. Managed PKI for SSL is simple to set up and configure. Start issuing server certificates quickly via our intuitive Web-based portal. Renewing certificates or buying additional certificates on demand is just as easy. To find out more about VeriSign Managed PKI for SSL, please go to <http://www.verisign.co.uk/products-services/security-services/ssl/ssl-certificates/index.html>.

VeriSign Solutions Grow with Your E-Commerce Business



Conclusion

VeriSign Secure Site Pro SSL Certificates provide the industry's strongest SSL encryption and security. Properly implemented VeriSign Secure Site Pro SSL Certificates guarantee that your Web site customers and business partners get the most secure experience available — regardless of the operating system or browser version that each visitor uses. With VeriSign Secure Site Pro, your company can achieve the trust you need to drive growth in your e-commerce business.

+ Try a VeriSign SSL Certificate for Free

You can secure your Web site for a free two-week trial. To apply for your free trial Secure Site SSL Certificate, please visit www.verisign.co.uk now. You can complete the entire enrollment process online in about 15 minutes and immediately begin using your trial VeriSign SSL Certificate.

+ For More Information

To speak with a VeriSign security expert about your company's Web site security needs, please call 0800 032 2101. VeriSign can also be reached by email at sales@verisign.co.uk.

Visit us at www.verisign.co.uk for more information.