



WHITE PAPER

Security and Trust: The Backbone of Doing Business over the Internet





CONTENTS

+ Introduction	3
+ Encryption Technology and SSL Certificates	4
Levels of Encryption and SGC	5
Levels of Authentication and Trust	5
+ Extended Validation (EV) is the New Standard for Trust	7
+ VeriSign SSL Certificates, for the Strongest Security and Trust	9
+ Conclusion	10



Security and Trust: The Backbone of Doing Business over the Internet

+ Introduction

Gaining the trust of online customers is vital for the success of any company that transfers sensitive data over the Web. When shopping online, consumers are concerned about identity theft and are therefore wary of providing untrusted sources with their personal information, especially their credit card details. Other types of online businesses require different but equally sensitive information. People are reluctant to provide their national insurance numbers, passwords, or other confidential personal information, or sometimes even just name, address, and phone number. Perhaps the information will be intercepted in transit, they fear, or perhaps the destination itself is manned by imposters with ill intent.

The result is an abandoned transaction. In fact, TNS Research reported in 2006 that 54% of online shoppers have abandoned a purchase because of security concerns.¹ Others may overcome their fears enough to make small purchases but limit the size of their transactions for fear the money they spend will be pocketed and nothing delivered in return.

Such consumer fears are very well founded. Industry body APACs reported in October 2008 that Internet shoppers are more at risk than ever of falling victim to fraudsters, and that online fraud had risen by 185 per cent in the first six months of 2008 because of an increase in phishing attacks and scams. The number of phishing incidents - has quadrupled in the last two years, from 5,087 in the first half of 2006, to 20,682 now.²

Online businesses have much to gain by taking steps to overcome customer fears. Concern about Internet fraud is a very big deterrent to sales. YouGov research reported in January 2008 that 78% of the British population worries about becoming a victim of identity theft and that 51% of UK online consumers feel businesses (banks, credit card companies, and web site owners) don't do enough to safeguard information online.³ Since fears of scams limit not only the number of transactions conducted but also their size, the potential business that can be reaped by building trust is huge indeed.

Consumers too have much to gain from hurdling the trust barrier. The convenience of online shopping cannot be beaten nor can the prices. Often a consumer shopping for a particular item finds it not only on a trusted Web site but also on another site that charges less or offers other advantages. Wouldn't consumers be better off if there were a way to quickly gain trust in the off-brand site? But fear of identity theft stops many from taking advantage of these benefits—in fact, according to Forrester Research in December, 2006, 24% do not purchase online at all.

Fortunately technology is in place today that helps online businesses protect sensitive customer data, authenticate themselves, and build consumer trust—technology that also helps customers differentiate trustworthy Web sites from clones produced by scam artists intent on wrongdoing.

¹ TNS Research, August 2006

² Source: http://www.timesonline.co.uk/tol/money/consumer_affairs/article4860081.ece

³ YouGov January 2008

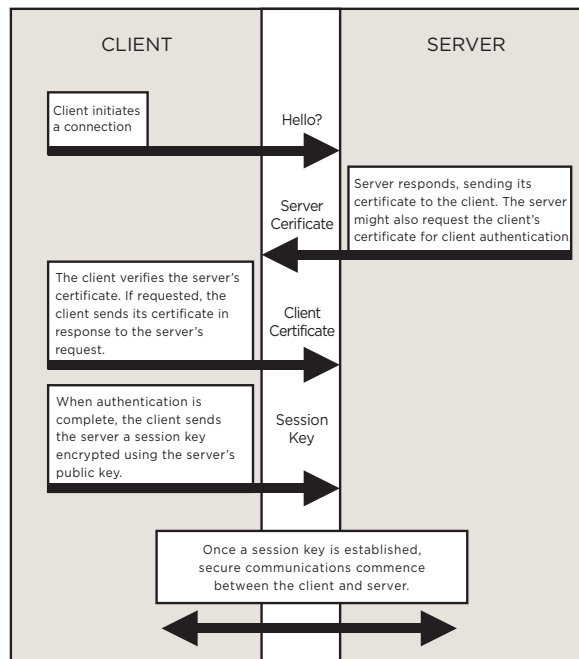
This paper explores the current state of this technology and the contributions VeriSign is making to help organisations to protect critical data and instill trust for their customers. It begins with encryption and Secure Sockets Layer (SSL), the technology that addresses the most obvious and oldest problem in online business—the susceptibility of data in transit to interception by cybercriminals. But with the rising sophistication of Internet crooks, encryption is no longer enough. Therefore this paper proceeds to present the issues of authentication and trust building that have recently grown critical and the Extended Validation (EV) SSL technology that addresses these issues. Finally, it presents VeriSign® solutions that deliver the utmost in all these security technologies.

+ Encryption Technology and SSL Certificates

Customers know that any information they submit to an unsecured Web site is seriously at risk. To survive in the market, therefore, e-businesses need to incorporate SSL Certificates and the encryption technology they employ.

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 that are serious about e-commerce is to implement a trust infrastructure based on encryption technology.

Secure Sockets Layer (SSL), the standard for Web security, is the technology used to encrypt and protect information transmitted over the Web with the ubiquitous HTTP protocol. SSL protects data in motion which can be intercepted and tampered with if sent unencrypted. Support for SSL is built into all major operating systems, Web browsers, Internet applications, and server hardware.



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 an SSL Certificate is a Certificate Authority (CA). VeriSign is by far the world’s leading CA with more than one million Web servers secured worldwide.⁴

The diagram on the left 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.

⁴ Includes VeriSign subsidiaries, affiliates, and resellers.



Levels of Encryption and SGC

Encryption comes in various strengths, determined by the number of bits used in the encryption algorithm. The current standard is 128 bits, which is considered for all intents and purposes unhackable at current computing speeds. Older versions of some operating systems and browsers, in certain combinations, including many Windows 2000 systems, do not support more than 40- or 56-bit encryption. These levels are easily crackable today, rendering users of those operating systems and browser combinations vulnerable.

A technology called Server-Gated Cryptography (SGC), available with certain VeriSign SSL Certificates, overcomes this problem for 99.9% of Web site visitors. (Certain older browser versions are not capable of 128-bit encryption with any SSL certificate.) Web sites equipped with SGC “step up” to 128-bit encryption for communications with systems that normally can perform only 40- or 56-bit encryption. Therefore businesses who employ SGC SSL Certificates can guarantee the highest level of encryption available to all of their customers. VeriSign Secure Site Pro and Secure Site Pro with EV support SGC 128-bit encryption. All VeriSign SSL Certificates support up to 256-bit encryption on all connections where both the client and the server are capable of encrypting at this level.

Levels of Authentication and Trust

One of the key purposes of SSL Certificates is to help assure consumers that they are actually doing business with the Web site they believe they are accessing. Therefore CAs perform validation checks before issuing them. There are three commonly recognised categories of SSL authentication: domain authentication, organisation authentication, and EV, and the differences in the level of security provided and trust engendered are vitally important. Even within a level, specific authentication processes vary from CA to CA—a key reason for choosing a widely known, respected and trusted CA. No other CA is as trusted or well known as VeriSign.

Domain Authentication

Domain authenticated certificates are the lowest form of authentication available. CAs conduct a process to verify that an entity requesting a domain authenticated certificate either owns the domain requested or has the right to use that domain name. They may also verify that the email address for the contact requesting the certificate is either listed in the WHOIS directory or meets the CA’s predetermined email alias requirements. VeriSign does not offer domain authenticated SSL Certificates.

Organisation Authentication

Organisation authentication is the validation process that VeriSign and other CAs employ for ordinary (non EV) SSL Certificates. CAs begin by verifying the organisation’s existence through a government-issued business credential, normally by searching government and private databases. If necessary they may request such items as articles of incorporation, business licenses, and fictitious names statements. Before issuing an SSL Certificate, CAs verify a company’s identity and confirm it as a legal entity, confirm that it has the right to use the domain name included in the certificate, and verify that the individual who requested the SSL Certificate on behalf of the company was authorised to do so.



Extended Validation (EV) Authentication

EV, which is described in the next section, has the highest level of authentication available with an SSL Certificate. EV authentication adds structure and controls to the organisation authentication process. It begins with an in-depth validation of an entity's authenticity starting with a signed acknowledgement of agreement from the corporate contact. A company registration document may also be required if the CA is unable to confirm the organisation's details through a government database. A legal opinion letter may also be requested to confirm the following details about the organisation:

- Physical address of place of operation
- Telephone number
- Confirmation of exclusive right to use the domain
- Additional confirmation of the organisation's existence (if less than 3 years old), and
- Verification of the corporate contact's employment.

The process represents little burden for legitimate organisations but is a substantial obstacle for a fraudster.

Trust Marks

To earn trust and maximise online business, you need to not only protect your customers' online transmissions but make it clear to them that you are doing so. Therefore CAs provide you with seals bearing their trust mark that you may be post on various pages of your Web site. The VeriSign Secured® Seal depicted below is the world's most used and most recognised security seal. Clicking on this seal brings up a display showing the name of the certificate owner, the validity period, and information about the level of protection provided and the owner validation process VeriSign conducted before issuing the certificate. 78% of people transacting online in the UK look for security cues such as the VeriSign Secured Seal to know that they are on a secure site. And 78% of UK consumers that have been internet fraud victims or know someone who has been a victim, now look for security mark before using a website.⁵



⁵ YouGov January 2008

+ Extended Validation (EV) Is the New Standard for Trust

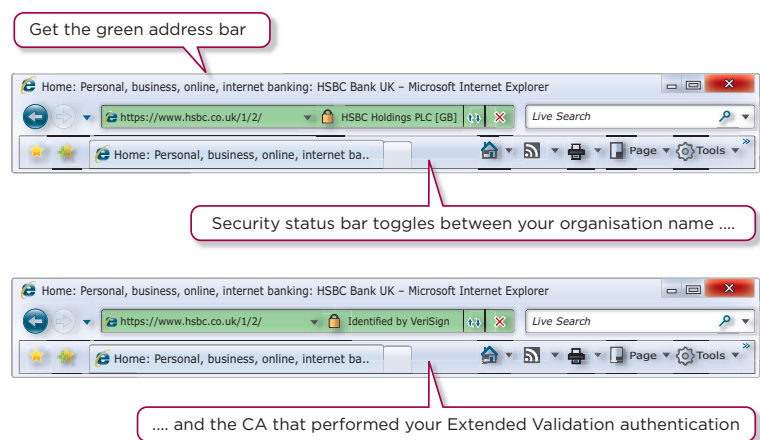
In the past indicators of a SSL session such as “https” in the URL or the gold lock icon were sufficient to quell most consumer fears by providing assurance that sensitive data transmission is protected by sufficient levels of encryption. But even the strongest encryption is no longer enough today because of a very different problem. Internet thieves have become adept at posing as genuine e-businesses. They purchase SSL Certificates—which unfortunately are all too readily available from CAs that perform flimsy background checks—and use them to trick customers into sending them sensitive information. That is why encryption is no longer enough—it does no good if the recipient of the encrypted transmission is a falsified business and proceeds to use it for identity theft or some other form of malfeasance. How are people to know if a Web site they are not familiar with is indeed legitimate? And even if a site appears to be that of a known and trusted online business, how are people to know that it is not a clone from a clever imposter with malicious intent? 90% of users are unable to distinguish phishing sites from legitimate ones.⁶

To earn trust, you need an easy, reliable way to show customers that not only are their transactions secure, but that you are a legitimate business and you are who you say you are. To meet this need, security vendors and Internet browsers have combined forces to establish the Extended Validation (EV) standard, the first fundamental change in the world’s secure e-commerce backbone in more than ten years. VeriSign adheres to this standard in its Extended Validation SSL Certificates.

When customers visit a Web page secured with an EV SSL Certificate, provided they are using an EV-equipped browser version, the address bar turns green. Current and future versions of Microsoft Internet Explorer (starting with Internet Explorer 7), Firefox (starting with Firefox 3), and Opera (starting with Opera 9.5) possess this capability. These and others with EV capability now comprise over 66% of the browsers in use.⁷

Besides turning green, the browser also displays the name of the organisation listed in the certificate (for example, your company). Implementation details vary somewhat from browser to browser. IE7 for example displays the name of the certificate’s security vendor (for example, VeriSign) as well as the organisation’s, and toggles between the two names as shown below.

Figure 2: Green Address Bar and Extended Validation



⁶ Rachna Dhamija, Harvard University; J.D. Tygar, UC Berkeley; and Marti Hearst, UC Berkeley

⁷ <http://marketshare.hitslink.com/> September 2008



VeriSign Secure Site Pro with EV SSL Certificates enable the strongest SSL encryption available to each site visitor and provide highest trust. By using VeriSign Secure Site Pro with EV SSL Certificates, you can guarantee that your Web site customers and business partners get the most secure experience available to them—regardless of the operating system or browser version that they use. With VeriSign Secure Site Pro with EV, your company can achieve the trust you need to drive growth in your e-business.

The browser and the security vendor control the display to deter phishers and counterfeiters from hijacking your brand and your customers. Fraudsters are becoming adept at mimicking almost everything about a Web site, but without the legitimate company's EV SSL Certificate there is no way they can display its name on the address bar because the information shown there is outside of their control. And they cannot obtain the legitimate company's EV SSL Certificates because of the stringent authentication process.

Why is EV so comforting to consumers?

- Online customers can look at the visual display of the certificate owner's name on the address bar to make sure the site is indeed authored by the intended source and not an imposter
- CAs conduct additional levels of validation of organisations' legitimacy and authenticity before issuing them EV certificates as described above to keep fraudsters from posing as legitimate Internet businesses
- The CAs themselves must satisfy more rigorous criteria in order to be eligible to issue EV SSL Certificates. They must pass regular third-party WebTrust audits confirming that they meet the requirements set out in the standards of the CA/Browser Forum, a consortium of CAs and browser suppliers. This essentially eliminates chances of a feeble background check that sets an imposter loose with EV. With EV customers do not have to question whether the organisation was properly vetted or not.
- The colour change to green appears to have a soothing psychological effect on consumers. Even customers who are not familiar with the "real" reasons why EV protects them better are more inclined to convert to sales and buy more per sale if they see a green bar.

Evidence that EV works is overwhelming. In January 2007, Tec-Ed researched usage and attitudes of 384 online shoppers and found that:

- 100% of participants notice whether a site shows the green EV bar
- 93% of participants prefer to shop on sites that show the green bar
- 97% are likely to share their credit card information on sites with the green EV bar, as opposed to only 63% with non-EV sites
- 77% of participants report that they would hesitate to shop at a site that previously showed the green EV bar and no longer does so.

In the same study Tec-Ed found that 88% trust the name VeriSign on a site, as opposed to only 22% for the next most trusted SSL provider.

Studies like these dispel any doubt about the value and importance of EV and the VeriSign name on recognition, trust, and preferences. But does that translate into more sales? Here too the answer is yes, and the evidence is overwhelming. Many VeriSign EV SSL Certificate owners are measuring the difference the green bar makes in conversions and the data is in: As of August 2008, 14 customers have measured significant uplifts with more reports coming in all the time. Overstock.com, for example, found an 8.6% drop in shopping cart abandonment among shoppers who saw the green bar. Other customers experienced even more substantial improvements. See www.Verisign.com.au/case-studies/ for all the details.

CONSUMERS CITE VERISIGN AS THE #1 BRAND FOR WEB SITE SECURITY.

The VeriSign Secured Seal included with all VeriSign SSL Certificates allows your company to display the number one sign of trust on the Internet. Significantly, 78% of online shoppers in the UK look for security cues such as the VeriSign Secured Seal before transacting. 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 SSL Certificates, for the Strongest Security and Trust

VeriSign is the leading global provider of SSL Certificates. VeriSign is also by far the foremost provider of EV SSL Certificates with a market share of over 75%, including the biggest names in e-commerce and banking.⁸ The world's 40 largest banks and over 95% of Fortune 500 companies choose SSL Certificates sold by VeriSign,⁹ and over 90,000 domains in 145 countries display the VeriSign Secured Seal, the most recognised trust mark on the Internet. 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 their site is capable of securing their confidential information with SSL encryption.

To accommodate the variety of needs, VeriSign offers four primary types of SSL solutions.

VeriSign Secure Site

This most basic VeriSign solution includes:

- Organisational authentication
- 40-bit minimum up to 256-bit encryption
- The right to display the VeriSign Secured Seal
- US\$100,000 warranty
- Installation Checker

VeriSign Secure Site Pro

VeriSign® Secure Site Pro enables the strongest encryption available to each site visitor. This solution contains everything in VeriSign Secure Site plus SGC encryption for a minimum of 128-bit encryption for 99.9% of Internet users. Includes a US\$250,000 warranty.

VeriSign Secure Site with EV

This solution contains everything in VeriSign Secure Site plus Extended Validation. Extended Validation SSL gives Web site visitors an easy and reliable way to establish trust online. Only SSL Certificates with Extended Validation (EV) will trigger high security Web browsers to display a green address bar with the name of the organisation that owns the SSL Certificate and the name of the Certificate Authority that issued it.

VeriSign Secure Site Pro with EV

VeriSign Secure Site Pro with EV is the best SSL solution available for keeping confidential transmissions to and from your Web site from being read or modified by anyone other than the communicating parties, and for engendering customer trust. This solution contains all the technologies in the other solutions including both SGC encryption and EV SSL Certificates as well as a US\$250,000 warranty.

For the very best in encryption and trust, VeriSign recommends Secure Site Pro with EV SSL Certificate. This solution triggers the EV green bar in high security browsers and enable all site visitors to connect at the highest encryption level available to them.

⁸ Netcraft, August 2008

⁹ Includes VeriSign subsidiaries, affiliates, and resellers.



VeriSign can help your company establish or improve customer trust by securing your Web site for business. VeriSign SSL Certificates secure 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 cross-network security by protecting servers facing both the Internet and private intranets.

+ Conclusion

With the increase in Internet fraud, security of personal data transmissions has never been as important as it is today, and tomorrow will only get worse. The prevalence—and consequences—of identity theft are all too well known and documented. Your potential online customers have become more savvy, more skeptical, and frankly more scared. They expect you to protect them, and right now 51% of them believe you're not doing it well enough.¹⁰

Trust makes all the difference. Your investment in technologies to protect your customers and earn their trust is a trivial portion of your cost of doing business, and the return you make through extra sales can be astronomical.

When the stakes are so large and the costs so small, why not make the obvious choice? Go with the name that is by far the best known and most trusted, because name recognition and trust are THE things that matter in an SSL supplier. VeriSign has earned that name recognition and trust by doing security right, and customers know it. So don't stop short—go all the way with VeriSign Secure Site Pro with EV SSL Certificates so that you can tell ALL your customers that their sensitive information will be transmitted without compromise, and that the destination is indeed what they intended it to be.

+ Learn More

VeriSign offers a range of additional e-commerce site services described on www.VeriSign.com.au to suit every online business's needs. To speak with a VeriSign security expert about your company's Web site security needs, please call +61 3 9674 5500. VeriSign can also be reached by email at sales@VeriSign.com.au

+ 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 VeriSign Secure Site SSL Certificate, please visit www.VeriSign.com.au/trial now. You can complete the entire enrolment process online in about 15 minutes and immediately begin using your trial VeriSign SSL Certificate.

+ About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit www.VeriSign.com.au for more information.

¹⁰ YouGov January 2008