



---

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

# Contents

Introduction	3
Encryption Technology and SSL Certificates	4
Levels of Authentication and Trust Trust Marks	4
Extended Validation (EV) is the New Standard for Trust	6
GeoTrust SSL Certificates, for the Strongest Security and Trust	8
Conclusion	9
About GeoTrust	9
Learn More	9

## Introduction

Gaining the trust of online customers is vital for the success of any company that requires sensitive data to be provided over the Web. In e-commerce, consumers are concerned about identity theft and are therefore justifiably leery of providing untrusted sources with their personal information, especially their credit card numbers to pay for transactions. Other types of online businesses require different but equally sensitive information. People are reluctant to provide their Social Security numbers, passwords, health and other confidential personal information, or sometimes even just their 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 for many wary consumers is an abandoned transaction. In fact, TNS Research reported in 2006 that 70% of online shoppers have abandoned a purchase because of security concerns. 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. In 2007, an estimated \$3.6 billion in online revenues was lost to online fraud—up more than 16% from 2006.<sup>1</sup> The total number of unique phishing reports submitted to the Anti-Phishing Working Group (APWG) in January 2008 was 29,284, an increase of nearly 9% from the previous month.<sup>2</sup>

Online businesses have much to gain by taking steps to overcome customer fears. Concern about Internet fraud is a very big deterrent to sales. TNS Research reported in August 2006 that 87% of online shoppers are concerned about credit card fraud, and that 83% are concerned about sharing personal information. 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 beat, 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 (felt by 85% of shoppers, according to a TNS Study, August 2006) clearly inhibits 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 malfeasance.

This paper explores the current state of this technology and the contributions VeriSign and GeoTrust® are making to help organizations 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 more recently grown critical, as well as the Extended Validation (EV) SSL technology that addresses these issues. Finally, it presents GeoTrust solutions that deliver the utmost in all these security technologies.

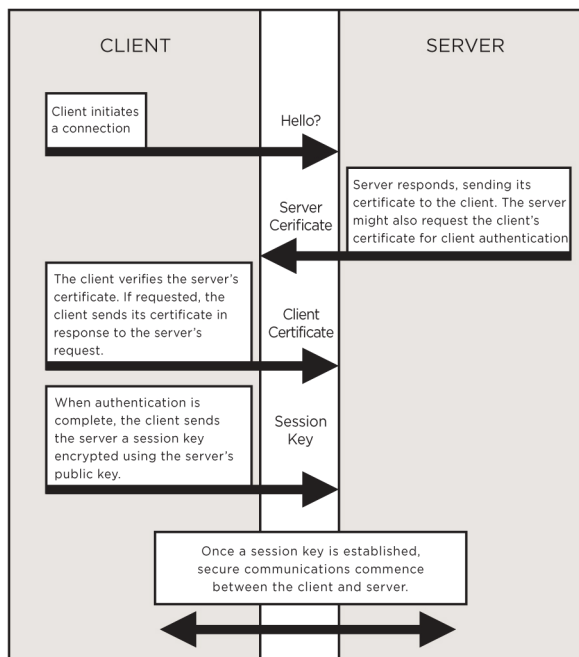
## Encryption Technology and SSL Certificates

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 world 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 that 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). GeoTrust is a leading CA, with more than one million Web servers secured worldwide.<sup>3</sup>

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.

## 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 recognized categories of SSL authentication: domain authentication, organization 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 GeoTrust.

### *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. GeoTrust offers domain authenticated SSL Certificates.

### *Organization Authentication*

Organization authentication is the validation process that GeoTrust and other CAs employ for ordinary (non EV) SSL Certificates. CAs begin by verifying the organization'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 authorized to do so.

### *Extended Validation 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 organization's 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 organization's details through a government database. A legal opinion letter may also be requested to confirm the following details about the organization:

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

### **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. This seal is recognized by 79 percent of U.S. online shoppers, according to an August 2006 study by TNS. Significantly, 86 percent of shoppers say it is important for sites to display a trust mark. 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.*

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

### Trust Marks

To earn trust and maximize online business, you need to not only protect your customers' online transmissions, but also make it clear to them that you are doing so. Therefore, CAs provide you with seals bearing their trust mark that you may post on various pages of your Web site. Clicking on the GeoTrust® True Site Seal depicted below 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 GeoTrust conducted before issuing the certificate.



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

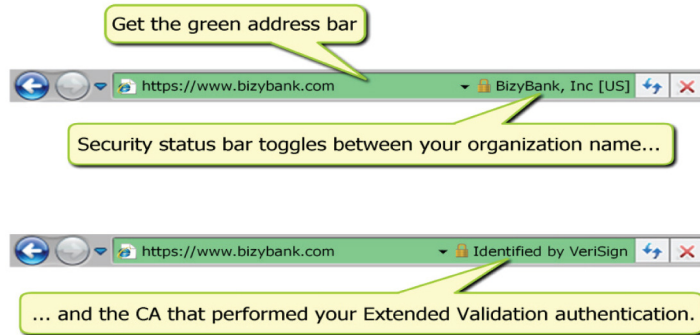
In the past, indicators of an SSL session such as “https” in the URL or the gold lock icon were sufficient to quell most consumer fears by providing assurance that sensitive data transmission was protected by sufficient levels of encryption. But even the strongest encryption is no longer enough today 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.<sup>4</sup>

To earn trust, you need an easy, reliable way to show customers that not only are their transactions secure, but also 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. GeoTrust 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 (beginning with Internet Explorer 7), Firefox (beginning with Firefox 3), and Opera (beginning with Opera 9.5) possess this capability. These and others with EV capability now comprise over 62% of the browsers in use.<sup>5</sup>

Besides turning green, the browser also displays the name of the organization 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 (e.g., GeoTrust) as well as the organization, and toggles between the two names as shown below.

Figure 2: Green Address Bar and Extended Validation



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 organizations' 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 the chances of a feeble background check that sets an imposter loose with EV. With EV customers do not have to question whether an organization was properly vetted or not.
- The color 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 are more inclined to convert to sales and buy more per sale if they see a green bar.

*True BusinessID with Extended Validation (EV) SSL Certificates enables the strongest SSL encryption available to each site visitor and provides the high levels of trust. With VeriSign Secure Site Pro with True BusinessID with Extended Validation (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 True BusinessID with Extended Validation (EV), your company can achieve the trust you need to drive growth in your e-business.*

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 and GeoTrust 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, including one who was amazed to see an 87% increase in registration rates. See <http://www.verisign.com/ssl/ssl-information-center/ssl-case-studies/index.html> for all the details.

## GeoTrust SSL Certificates, for Strong Security and Trust

Give your customers the confidence to make their purchases online with GeoTrust True BusinessID with EV. Users trust GeoTrust because of the company's encryption technology and rigorous business authentication practices. When you protect your site with True BusinessID with Extended Validation (EV) SSL and display the GeoTrust True Site Seal, your customers know that their transactions are secure.

Web users are accustomed to seeing commercial e-commerce sites display the GeoTrust® True Site 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, GeoTrust offers three primary types of SSL solutions:

### GeoTrust True BusinessID with EV

GeoTrust®: Maximize security and online sales potential using GeoTrust True BusinessID with EV enabling up to 256-bit encryption on web browsers and mobile phones. With Extended Validation, visitors using high-security browsers see the address bar turn green when they visit your site. Extended Validation SSL Certificates provide a convenient and visible sign that you have a highly authenticated, trustworthy site and that your customers' information is secure.

## True BusinessID

Assure customers that your site is trustworthy and secure with a GeoTrust® True BusinessID SSL Certificate, enabling up to 256-bit encryption on web browsers and mobile phones. A dynamic GeoTrust identity verification seal gives your customers and business partners the confidence to do business with you online at the desktop or on the go.

## QuickSSL Premium

Secure online transactions and applications in minutes with a GeoTrust® QuickSSL® Premium SSL Certificate, enabling up to 256-bit encryption on web browsers and mobile phones. GeoTrust QuickSSL Premium SSL Certificates show your customers and business partners that their information is secure during transmission from the desktop or on the go.

## Conclusion

With the skyrocketing rise 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 84% of them believe you're not doing it well enough.<sup>6</sup>

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—up to 48,000% for one VeriSign customer whose case study and many others you can read on VeriSign's Web site.

When the stakes are so gigantic and the costs so minuscule, 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 and GeoTrust have earned that name recognition and trust by doing security right, and customers know it. And don't stop short—go all the way with GeoTrust True BusinessID 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.

## About GeoTrust

GeoTrust is a leader in identity verification, credentialing and validation solutions. Its products include Web security services for secure e-commerce transactions and digital signing for documents and computer code. With more than 300,000+ companies worldwide using its technology for online security, GeoTrust has a reputation as a world class digital certificate provider.

## About Dotster

Dotster is a leading full-service provider of essential resources for businesses to get online and grow online. It has helped more than one million businesses and individuals establish their web presence, build their websites, and drive revenue. Dotster offers its customers a complete set of services including the ability to get online with a domain name and email address; build a major web presence with web hosting and customer website design; secure a website with industry leading SSL certificates; and reduce IT costs with VPS hosting.

Dotster, Inc.

(360) 449-5900  
P.O. Box 821066  
Vancouver, WA 98682

Visit us at [Dotster.com](http://Dotster.com)

<sup>1</sup> Cybersource, "9th Annual Online Fraud Report," 2008

<sup>2</sup> APWG, "Phishing Activity Trends," January 2008

<sup>3</sup> Includes VeriSign subsidiaries, affiliates, and resellers

<sup>4</sup> Rachna Dhamija, Harvard University; J.D. Tygar, UC Berkeley; and Marti Hearst, UC Berkeley

<sup>5</sup> Net Applications, MarketShare Report, August 2008

<sup>6</sup> Forrester Research, December 2005

© 2009 GeoTrust, Inc. All rights reserved. GeoTrust, the GeoTrust logo, the GeoTrust design, and other trademarks, service marks, and designs are registered or unregistered trademarks of GeoTrust, Inc. and its subsidiaries in the United States and in foreign countries.

Dotster, the Dotster logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Dotster, Inc. and its subsidiaries in the United States and in foreign countries.

Windows is a trademark of Microsoft Corporation.