



Securing Your Web Site

For Business

A step-by-step guide
for secure online commerce



Table of

Contents

Introduction	1
Increase your competitive edge with a secure Web site	3
Secure your Web site with a VeriSign Server ID	7
Enhance sales, convenience, and security with other VeriSign solutions	14
Step-by-step instructions	17
Conclusion	23
Appendix: How digital certificates work	24

Introduction

Businesses that accept transactions via the Web can gain a competitive edge by reaching a worldwide audience, at very low cost. But the Web poses a unique set of security issues, which businesses must address at the outset to minimize risk. Customers will submit information via the Web only if they are confident that their personal information, such as credit card numbers, financial data, or medical history, is secure.

VeriSign, Inc., the leading provider of trust services for electronic commerce and communication, offers a low-cost, proven solution for securely conducting business over the Web. By installing a VeriSign Server ID (available as part of VeriSign's Secure Site solutions) on your server, you can securely collect sensitive information online, and increase business by giving your customers confidence that their transactions are safe.

Immediately after installing your VeriSign Server ID, you can establish secure communications with any customer using a browser from Netscape or Microsoft. This proven technology is in use now—by the top 40 e-commerce sites, all of the Fortune 500 companies with a Web presence, and thousands of other leading sites.

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

This guide explains key issues related to Web security, describes the technologies VeriSign uses to address the issues, and provides step-by-step instructions for obtaining and installing a VeriSign Server ID. We invite you after reading this Guide to obtain your free trial Secure Server ID at <http://www.verisign.com/server/trial/index.html> or purchase one of VeriSign's Secure Site solutions which include either a full one-year Secure Server ID or a Global Server ID, at <http://www.verisign.com/server>

Acquiring airtight security for your Web site is as easy as installing a VeriSign Server ID. The simple installation process turns on the SSL encryption capabilities already built into your Web server software. Immediately after installing your Server ID, you can communicate securely with the tens of millions of potential customers who use Netscape and Microsoft browsers.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

Increase your competitive edge with a secure Web site

A secure Web site can provide your business with powerful competitive advantages, including online sales and streamlined application processes for products such as insurance, mortgages, or credit cards. Credit card sales can be especially lucrative: according to independent analysts, cash transactions on the Internet will reach \$9 billion by 2000, and \$30 billion in 2005. No merchant can afford to ignore a market this large.

To succeed in this market, however, you must become fully aware of Internet security threats, take advantage of the technology that overcomes them, and win your customers' confidence. This section describes the benefits of e-commerce, and the specific risks you must address to realize the benefits.

"According to independent analysts, cash transactions on the Internet will reach \$9 billion by 2000, and \$30 billion in 2005. No merchant can afford to ignore a market this large."

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

Extend your reach to more customers

By offering your product on the Web, your business can gain unique benefits:

- **Worldwide presence**—The Web represents a new source of customers. Anyone with an Internet connection is a potential customer: More than 50 million people around the world are already using the Internet for business transactions. Your Web storefront is open all the time, and requires no investments in brick and mortar.
- **Market share**— In a 1998 Yankelovich Partners study (http://www.cpawebtrust.com/developer/dvlp_content.html), eighty-five percent of Web users surveyed reported that a lack of security made them uncomfortable sending credit card numbers over the Internet. The merchants who can win the confidence of these customers will gain their loyalty—and an enormous opportunity for expanding market share.
- **Cost-effective delivery channel**—Many products and services, such as software or information, can be distributed directly to customers via the Web. This saves time for your customers, which increases your competitive appeal. It also increases your profitability by eliminating the shipping and overhead costs associated with order fulfillment.
- **Streamlined enrollment**—Paper-based enrollment workflows are fraught with delays. Applications for insurance, a mortgage, or a credit card, for example, can be held up in the mail and your mailroom. Once received, the application must be entered into your computer system, a labor-intensive process that can introduce errors. By accepting applications via a secure Web site, you can

“Eighty-five percent of Web users surveyed reported that a lack of security made them uncomfortable sending credit card numbers over the Internet. The merchants who can win the confidence of these customers will gain their loyalty—and an enormous opportunity for expanding market share.”

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

“By accepting applications via a secure Web site, you can speed application processing, reduce processing costs, and improve customer service.”

speed application processing, reduce processing costs, and improve customer service.

- **Better marketing through better customer knowledge—** Establishing a storefront on the Web positions you for one-to-one marketing—the ability to customize your products and services to individual customers rather than large market segments. The Web facilitates one-to-one marketing by enabling you to capture information about demographics, personal buying habits, and preferences. By analyzing this information, you can target your merchandise and promotions for maximum impact, tailor your Web page to appeal to the specific consumer who is visiting, and conduct effective, tightly focused marketing campaigns.

When you secure your Web site, you can increase business by reassuring the 85 percent of Web users with concerns about Internet security. You can also improve competitiveness by securely delivering electronic products at no cost, streamlining enrollment, and learning valuable information about your customers.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

Ensure the security of your electronic transactions

In person-to-person transactions, security is based on physical cues. Consumers have come to accept the risks of using credit cards in places like department stores because they can see and touch the merchandise and make judgments about the store. On the Internet, without those physical cues, it is much more difficult to assess the safety of a business. Also, serious security threats have emerged. By becoming aware of the risks of Internet-based transactions, businesses can acquire technology solutions that overcome those risks:

- **Spoofing**—The low cost of Web site creation and ease of copying existing pages makes it all too easy to create illegitimate sites that appear to be published by established organizations. In fact, con artists have illegally obtained credit card numbers by setting up professional-looking storefronts that mimic legitimate businesses.
- **Unauthorized disclosure**—When transaction information is transmitted “in the clear,” hackers can intercept the transmissions to obtain your customers’ sensitive information.
- **Unauthorized action**—A competitor or disgruntled customer can alter your Web site so that it refuses service to potential clients or malfunctions.
- **Data alteration**—The content of a transaction can be intercepted and altered en route, either maliciously or accidentally. User names, credit card numbers, and dollar amounts sent “in the clear” are all vulnerable to such alteration.

Securing your Web site for business protects both your company and your customers. A VeriSign Server ID makes it safer to conduct business on the Web than in the physical world.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

Secure your Web site

with a VeriSign Server ID

A proven, low-cost solution to secure online transactions is available today. VeriSign Server IDs have earned the trust of businesses worldwide, including virtually all of the Fortune 500 companies on the Web and all of the top 40 e-commerce sites. To date, VeriSign has issued over 180,000 Server IDs. This section describes how VeriSign Server IDs work to make online transactions secure.

Present your credentials via a VeriSign Server ID

A Server ID, also known as a digital certificate, is the electronic equivalent of a business license. Server IDs are issued by a trusted third party, called a Certification Authority (CA). VeriSign is the world's leading CA, having issued more than 180,000 Server IDs. The CA that issues a Server ID is vouching for your right to use your company name and Web address, just as the office of the Secretary of State does when it issues Articles of Incorporation. CAs can also issue digital certificates to individuals.

Before issuing a Server ID, VeriSign reviews your credentials—such as your organization's Dun & Bradstreet number or Articles of Incorporation—and completes a thorough background checking process to ensure that your organization is what it claims to be, and

“VeriSign Server IDs have earned the trust of businesses worldwide, including virtually all of the Fortune 500 companies on the Web and all of the top 40 e-commerce sites.”

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

is not claiming a false identity. Then VeriSign issues your organization a Server ID, which is an electronic credential that your business can present to prove its identity or right to access information (see “How Digital Certificates Work” below).

A Server ID from VeriSign provides the ultimate in credibility for your online business. VeriSign’s rigorous authentication practices set the industry standard. VeriSign documents its carefully crafted and time-proven practices and procedures in a Certificate Practices Statement. And VeriSign annually undergoes an extensive SAS 70 Type II audit by KPMG. (The Statement of Auditing Standard 70, SAS 70, was established by the American Institute of Certified Public Accountants to certify trusted practices.) Employees responsible for dealing with certificates undergo complete background checks and thorough training. VeriSign has achieved its unsurpassed reputation as a trusted third party by paying as careful attention to physical security as electronic security. For example, the company’s 22,000-square-foot plant where keys are issued has five tiers of security, the last three requiring fingerprint identification.

VeriSign’s rigorous authentication practices, leading-edge cryptographic techniques, and ultra-secure facilities are designed to maximize your confidence in our services. These practices, technology, and infrastructure are the foundation for Server IDs to secure transactions working in conjunction with your Web server.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

Secure your online transactions without hardware investment

VeriSign Server IDs work in conjunction with Secure Sockets Layer (SSL) technology, which is the industry-standard protocol for secure, Web-based communications. Your Web server is ready now to work with VeriSign Secure Server IDs if it's from Apache Freeware, C2Net, IBM, Lotus, Netscape, Microsoft, OpenMarket, or dozens of other vendors.

After you install your VeriSign Server ID, your server automatically activates SSL, creating a secure communications channel between your server and your customer's browser. Your site can communicate securely with any customer who uses Netscape Navigator, Microsoft Internet Explorer, or most popular e-mail programs. Once activated by your Server ID, SSL immediately begins providing you with the following components of secure online transactions:

- **Authentication**—By checking your VeriSign Server ID, your customers can verify that the Web site belongs to you, and not an impostor. This bolsters their confidence in submitting confidential information.
- **Message privacy**—SSL encrypts all information exchanged between your Web server and customers, such as credit card numbers and other personal data, using a unique session key. To securely transmit the session key to the consumer, your server encrypts it with your public key. Each session key is used only once, during a single session (which may include one or more transactions) with a single customer. These layers of privacy protection ensure that information cannot be viewed if it is intercepted by unauthorized parties.

“By checking your VeriSign Server ID, your customers can verify that the Web site belongs to you, and not an impostor. This bolsters their confidence in submitting confidential information.”

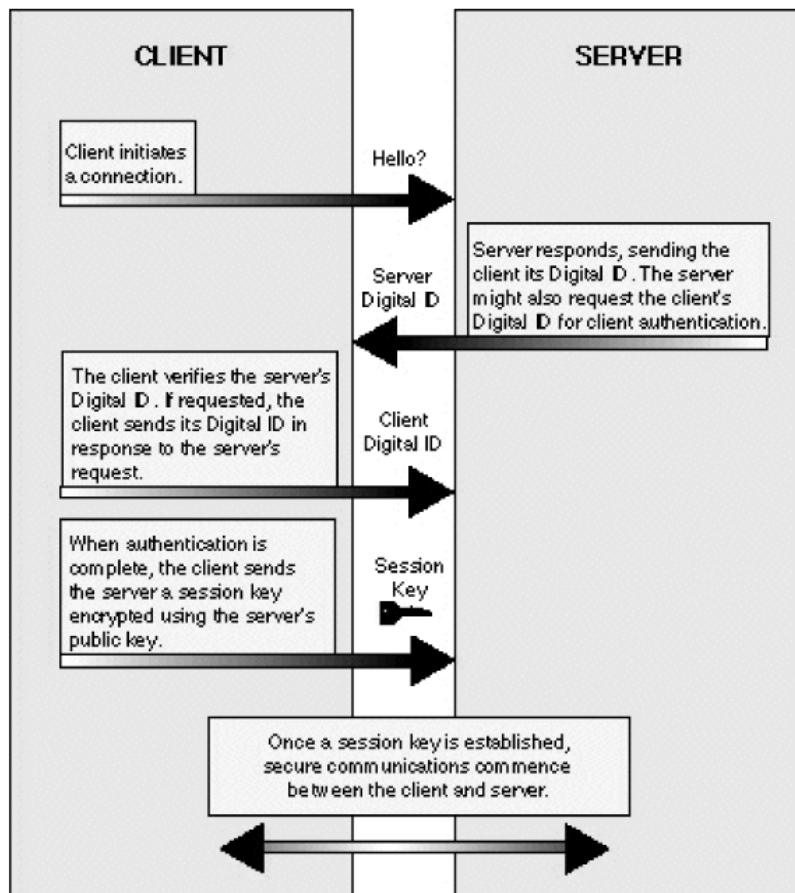
With a VeriSign Server ID, you become part of the VeriSign Trust NetworkSM, tapping into millions of browsers already enabled with VeriSign's digital certificate technology. As your credibility grows, so does your potential market share.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

- **Message integrity**—When a message is sent, the sending and receiving computers each generate a code based on the message content. If even a single character in the message content is altered en route, the receiving computer will generate a different code, and then alert the recipient that the message is not legitimate. With message integrity, both parties involved in the transaction know that what they're seeing is exactly what the other party sent.

The diagram below illustrates the process that guarantees protected communications between a Web server and a client. All exchanges of Server IDs occur within seconds, and require no action by the consumer.

VeriSign offers you two varieties of SSL Server IDs as part of its Secure Site services. Each variety enables different levels of SSL encryption



When you secure your Web site with a Server ID, your customers are assured that your site is legitimate. Information sent either way remains private, even if intercepted. And both parties know that messages are received exactly as sent.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

power that vary according to the browser version used by visitors to sites secured by the Server ID.

Standard Secure Server IDs (included with VeriSign's Secure Site and Secure Site Plus services) enable 40-bit SSL sessions when communicating with export-version Netscape and Microsoft Internet Explorer Web browsers. Export-version browsers are used by over 50 percent of Internet users. 40-bit SSL is strong enough for most intranets and lower-volume Web sites. But when communicating with domestic-version Web browsers, standard Secure Site IDs enable super-strong 128-bit SSL encryption, the world's most powerful. 128-bit SSL encryption has never been broken: according to RSA Labs, it would take a trillion-trillion years to crack using today's technology.

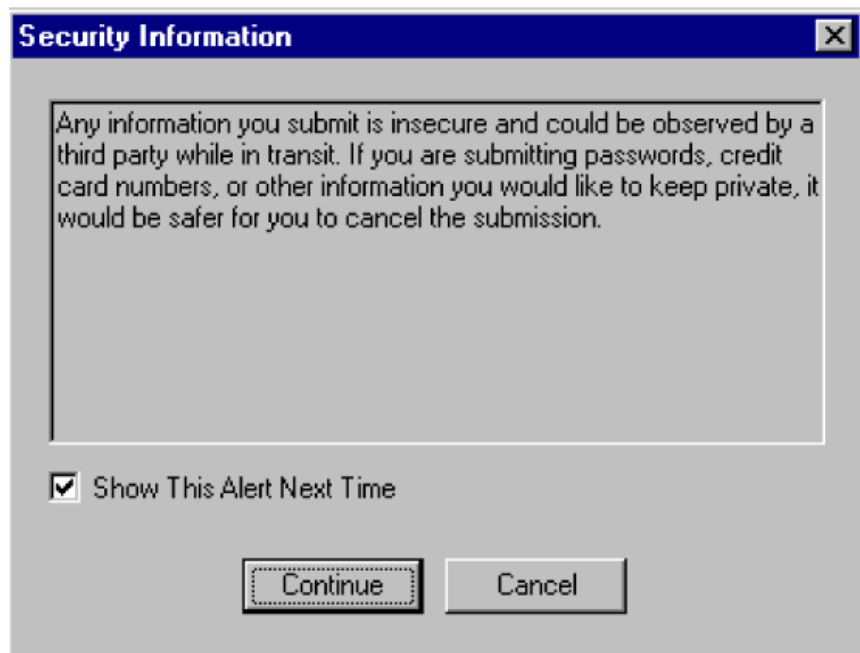
Global Server IDs (included with VeriSign's Global Site and Global Site Plus services) automatically ensure a minimum level of 128-bit SSL encryption when communicating with both domestic and export versions of Netscape Communicator and Internet Explorer. The encryption power of Global Server IDs make them ideal for sites that exchange sensitive, personal information, such as credit card numbers, with customers. VeriSign is one of the only providers authorized by the U.S. Department of Commerce to sell 128-bit SSL IDs in the U.S., and may sell them only to specified categories of organizations, including online merchants, healthcare organizations, insurance companies, and banks and financial institutions.

The ultimate result of a VeriSign Server ID on your site: safe online transactions that protect customers and your business. Customers gain confidence that they are sending their personal information to a legitimate business and not an impostor. In turn, you know that your company is receiving accurate information that the customer cannot later refute.

Get a **FREE Trial Secure Server ID**. Go to
<http://www.verisign.com/server/trial/index.html>

Make online commerce easy for your customers

Installing VeriSign Server IDs not only makes e-commerce safer for your customers; it actually makes it easier to submit information, such as a credit card number over the Internet. The Netscape Navigator and the Microsoft Internet Explorer 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 Server ID), the browsers will, by default, show a warning, which can make the purchase process seem threatening.



In contrast, if a user submits credit card or other information to a site with a valid Server ID and an SSL connection, the warning does not appear. The secure connection is seamless, making the online shopping experience more pleasant. In addition, when you install a VeriSign Server ID, the 100 million prospective customers with Microsoft and Netscape browsers are reassured that they are shopping on a secure site. Visitors can be sure that transactions with your site are secured

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

by looking for the following cues:

- The URL in the browser window displays “https” at the beginning, instead of http.
- In Netscape Communicator, the padlock in the lower left corner of the Navigator window will be closed instead of open. Netscape users can also follow these steps to see what level of encryption is protecting their transactions with your site:
 - Go to the Web site you want to check.
 - Click the Security button in the Navigator’s toolbar. The Security Info dialog box indicates whether the Web site uses encryption.
 - If it does, click the Open Page Info button to display more information about the site’s security features, including the type of encryption used.
- In Internet Explorer, a padlock icon appears in the bar at the bottom of the IE window. IE users can find out a Web site’s encryption level by following these steps:
 - Go to the Web site you want to check.
 - Right-click on the Web site’s page and select Properties.
 - Click the Certificates button.
 - In the Fields box, select “Encryption type.” The Details box shows you the level of encryption (40-bit or 128-bit).



Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

Enhance sales, convenience, and security with VeriSign Solutions

When you have established your secure Web site, you can take advantage of a wealth of options from VeriSign to further enhance your e-commerce operation.

Attract more customers with VeriSign's Secure Site Seal



With the Secure Site Seal, included with every Secure Site service, you can display the number-one trust brand on the Internet (Cheskin/Studio Archetype Study) to give your customers the confidence to communicate and transact business with your site. The Seal allows your visitors to check your Server ID's information and status in real time, and provides additional protection against the misuse of revoked and expired certificates.

A Secure Site Seal icon also appears next to your organization's listing in Network Solutions' comprehensive Web site directory at <http://www.dotcomdirectory.com>, alerting every directory user that your site is set apart from the crowd by VeriSign's superior security features.

Simplify management of multiple Server IDs

Is your site hosted on 10 or more servers? With one simple purchase, VeriSign's OnSite managed service lets you issue all the Server IDs you need—either standard or universal 128-bit SSL certificates—in bundles

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

of 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 OnSite the most cost-effective way to secure big sites. OnSite is simple to set up and configure: start issuing server certificates quickly via our intuitive Web-based process. Renewing IDs or buying additional IDs is just as easy. To find out more about OnSite for Multiple Server IDs, go to <http://www.verisign.com/server/prd/m/index.html> .

Learn more about your customers through client authentication

A Secure Server ID tells your customers exactly who you are. Suppose you want to learn who your customers are, or to restrict access to your content to certain consumers. You can set up your Web site to authenticate visitors' identities with VeriSign Server IDs for Individual Users. Compared to asking customers to supply a user name and password, Server ID registration is more convenient for customers and more informative for your business. Visit <http://www.verisign.com/clientauth/> for more information and a demonstration of client authentication.

Deploy strong security for worldwide commerce

Until recently, strong 128-bit encryption was not exportable. The United States Department of Commerce has approved VeriSign to issue certificates for 128-bit encrypted communications, the highest level of encryption ever allowed across United States borders. With a VeriSign Global Server ID, available from VeriSign as part of its Global Site and Global Site Plus Services, your international customers can now enjoy unparalleled security when visiting your Web site. Available to U.S. corporations and banks, financial institutions, insurance companies, health care organizations and online merchants worldwide, the VeriSign Global Server ID is a septillion times more secure than any other product. For more information about VeriSign's Global Server 128-bit ID, see <http://www.verisign.com/prd/g/index.html>

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

Try a VeriSign Secure Server ID for free

As part of a special offer from VeriSign, you can secure your Web site for a free two-week trial. To apply immediately for your free trial Secure Server ID, please visit <http://www.verisign.com/server/trial/index.html> now. You can complete the entire enrollment process online in about 15 minutes and immediately begin using your trial Secure Server ID.

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

Step-by-step instructions

You can purchase a one-year full-service Secure Server ID as part of VeriSign's Secure Site Service from VeriSign by visiting <http://www.verisign.com/server>. The application process takes about 15 minutes. In one to three days, after VeriSign has verified your credentials, you will receive your Secure Server ID via e-mail. Simply install the Secure Server ID on your server, and then immediately begin conducting transactions online—with the confidence that you and your customers are protected.

The U.S. Department of Commerce requires your company to qualify before buying the 128-bit SSL encryption power of Global Server IDs, included with Global Site and Global Site Plus services. All companies within the United States are eligible for Global Server IDs. There are restrictions on certain international companies, which must fall into one of a series of specified categories:

- Banks and Financial Institutions
- Insurance Companies
- Health and Medical Organizations
- Online Merchants
- U.S. Subsidiaries

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

For detailed information about the eligibility requirements, see <http://digitalid.verisign.com/server/global/globalDetails.htm>

Before you begin

Before beginning VeriSign's online enrollment, check to make sure you are ready to proceed:

- **Install server software**—Nearly all brands support VeriSign Secure Server IDs. VeriSign Global Server IDs are supported by Microsoft IIS 3.0+, Netscape Enterprise 3.0+, Lotus Domino 4.6.2, Nanoteq Netseq server, IBM, Compaq/Tandem iTP Web server, and C2Net Stronghold Server. Check with your vendor to be sure yours will.
- **Register your domain name**—If you haven't already, register your URL at <http://www.networksolutions.com> or a local equivalent.
- **Confirm firewall configuration**—Secure Server ID enrollment requires that you can make both HTTP and HTTPS connections to VeriSign's Web site.
- **Prepare payment**—If you are applying for a free 14-day trial Secure Server ID, no payment is necessary. If you are purchasing a one-year, full-service Server ID, you can pay with a purchase order, check, wire transfer, or an American Express, Visa, Mastercard, or Discover card.
- **Review legal agreement**—In the process of enrolling, you will need to sign the VeriSign Secure Server Subscriber Agreement. To review it in advance, see <http://www.verisign.com/repository/SUBAGR.html>
- **Gather proof of right documents**—Before issuing your Secure Server ID, VeriSign must confirm that your company is

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

legitimate and is registered with the proper government authorities. If you have a Dun & Bradstreet DUNS number, simply supply your number. International DUNS numbers must be in the Dun & Bradstreet database for at least two months before VeriSign can verify the information. If you do not have a DUNS number, either go to <http://www.dnb.com> and apply for one, or submit a hard copy of at least one of the following filed documents for your company: articles of incorporation, partnership papers, business license, or fictitious business license. All documents must be in English.

- **Select an option for obtaining payment**—Collecting credit card payments—in person or via the phone or Web—always involves two steps. First, obtain the credit card number from the customer. Second, secure payment from an acquiring processor on behalf of the credit card issuing bank. When your business uses a Server ID to obtain billing information from your customers, you have two options for collecting payments from the acquiring processor: traditional phone-in, or online processing.

Obtain your Server ID

To complete your Server ID enrollment, please visit <http://www.verisign.com/server>. There you will be instructed to complete the following steps.

1. Generate Certificate Signing Request

Follow the instructions in your server software manual, or online at <http://digitalid.verisign.com/server/enrollStep3.htm>, to create a Certificate Signing Request (CSR) and a key pair. After the server software creates the two files, make backup copies of them on a floppy disk, and store the disk in a secure location. This is important: If your private key is lost, VeriSign will not be able to recover it for you.

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

2. Submit the Certificate Signing Request (CSR) to VeriSign

Open the CSR file in a text editor, such as WordPad, NotePad, or Textpad. Do not use a word processing application such as Microsoft Word or Adobe FrameMaker.

Select the text in the CSR, beginning with and including:

—BEGIN NEW CERTIFICATE REQUEST—

and ending with

—END NEW CERTIFICATE REQUEST—

Copy and paste the CSR into the VeriSign online enrollment form for the trial or the one-year subscription. Click the Submit button.

3. Complete application

Fill out the online application form with information about your company and contacts.

The technical contact must be authorized to run and maintain your secure Web server and must be employed by your organization. If you access the Web through an Internet Service Provider (ISP), the ISP may complete the CSR for you and serve as the technical contact, and you can then enroll. If your ISP does not offer VeriSign IDs, refer it to www.verisign.com/isp/index.html for information about VeriSign's Secure Site ISP Program.

The organizational contact must be authorized to make binding agreements, such as the Secure Server Service Agreement, and must be employed by your organization. It is best to select a different person from the technical contact.

The billing contact will receive invoices. This can be the same person as the technical or organizational contact.

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

4. Authentication takes 1-3 days

Within a few hours of receiving your application, VeriSign will send a confirming e-mail to your technical and organizational contacts. The e-mail will include a URL where you can check the status of your application, as well as a Personal Identification Number (PIN) you will need to view the status.

If the information you submitted is complete, your technical contact and organizational contact will receive your Server ID by e-mail in 1–3 working days.

5. Install your Server ID

When you receive your Server ID, make a backup copy of it and store it on a labeled floppy disk, noting the date you received it. Store the floppy disk in a secure place. To install your Server ID, follow the instructions in your server software documentation for digital certificates.

6. Enable SSL on your server

Consult your server software manual to enable SSL. The process should take approximately five minutes.

7. Post the Secure Site Seal on all your secure pages

You should receive a file of the Seal, complete with instructions on how to install it, via e-mail shortly after completing the enrollment process. You can also find downloadable Seal files and instructions at <http://www.verisign.com/server/prg/seal/install.html>

NOTE: SSL imposes some performance overhead. Therefore, most server software applications allow you to apply SSL selectively to Web pages that require encryption, such as payment pages. There is no benefit from applying SSL to product information pages, for example.

Get a FREE Trial Secure Server ID. Go to
<http://www.verisign.com/server/trial/index.html>

Options for obtaining payment

Congratulations! You can now offer secure transactions to your online customers.

- Traditional phone-in. If your business already collects credit card payments from person-to-person or telephone sales, you are probably using this method currently. Simply read each customer's card number from your Internet order form and transmit it to the processor using a point-of-sale (POS) terminal.

If your business is not yet set up to collect credit card payments, contact a merchant services company, such as First Data Corporation Web Info. Merchant service companies generally charge a nominal set-up fee, also called an underwriting fee, and then charge a percentage of each transaction.

- Online processing. Most leading credit card processors offer their merchants the option to collect payments online. The payment-enabling software needed for these transactions depends on the system that the credit card service provider uses. Options include CyberCash, DigiCash, and IC Verify.

The SET (Secure Electronic Transactions) protocol allows you to collect online payments from credit card companies with the same level of security provided by SSL. With SET, the credit card company or other financial institution issues you a digital certificate that allows you to receive direct payments electronically. Your SET merchant's digital certificate tells your customers that you are approved to accept credit cards, in the same way your POS terminal and credit card decals assure customers during in-person payment transactions. For more information on using SET, visit <http://www.verisign.com/set/>.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

Conclusion

With its worldwide reach, the Web is a lucrative distribution channel with unprecedented potential. By setting up an online storefront, businesses can reach the millions of people around the world already using the Internet for transactions. And by ensuring the security of online payments, businesses can minimize risk and reach a far larger market: the 85 percent of Internet users who still hesitate to shop online because of security concerns.

A VeriSign Secure Server ID enables you to immediately begin conducting online business securely, with authentication, message privacy, and message integrity. As a result, you can minimize risk, win customer confidence, and, ultimately, gain a competitive edge.

VeriSign Server IDs are a proven solution, working today on more than 180,000 Web sites worldwide, including all of the Fortune 500 companies with a Web presence. Join them today, and expand your market by securing your online business. For a free 14-day trial Secure Server ID, visit <http://www.verisign.com/server/trial/index.html>

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

Appendix: How digital certificates work

In physical transactions, the challenges of identification, authentication, and privacy are solved with physical marks, such as seals or signatures. In electronic transactions, the equivalent of a seal must be coded into the information itself. By checking that the electronic “seal” is present and has not been broken, the recipient can confirm the identity of the message sender and ensure that the message content was not altered in transit. To create an electronic equivalent of physical security, VeriSign uses advanced cryptography.

Throughout history, most private messages were kept secret with single key cryptography. Single key cryptography is the way that most secret messages have been sent over the centuries. In single key cryptography, there is a unique code (or key) for both encrypting and decrypting messages. Single key cryptography works as follows:

Suppose Bob has one secret key. If Alice wants to send Bob a secret message:

1. Bob sends Alice a copy of his secret key
2. Alice encrypts a message with Bob’s secret key
3. Bob decrypts the message with his secret key

Unfortunately, this method has several problems. First, Bob must find a secure method of getting his secret key to Alice. If the secret key is intercepted, all of Bob’s communications are compromised. Second, Bob needs to trust Alice. If Alice is a double agent, she may give Bob’s secret key to his enemies. Or, she may read Bob’s other private messages or even imitate Bob. Finally, if you have an organization with people who need to exchange secret messages, you will either need to have thousands (if not millions) of secret keys, or you will need to rely on a smaller number of keys, which opens the door to compromise.

VeriSign Server ID technology employs the more advanced public-key cryptography, which does not involve the sharing of secret keys. Rather than using the same key to both encrypt and decrypt data, a Server ID uses a matched pair of keys that uniquely complement each other. When a message is encrypted by one key, only the other key can decrypt it.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>

Appendix: continued

When a key pair is generated for your business, your “private key” is installed on your server; nobody else has access to it. Your matching “public key,” in contrast, is freely distributed as part of your Server ID. You can share it with anyone, and even publish it in directories. Customers or correspondents who want to communicate with you privately can use the public key in your Server ID to encrypt information before sending it to you. Only you can decrypt the information, because only you have your private key.

Your VeriSign Server ID contains your name and identifying information, your public key, and VeriSign’s own digital signature as certification. It tells customers and correspondents that your public key belongs to you.

For a detailed explanation of Public Key Infrastructure and cryptography, go to https://www.verisign.com/cgibin/clearsales_cgi/leadgen.htm?form_id=0152&toc=w028502570152000&email= on the Web.

Get a FREE Trial Secure Server ID. Go to <http://www.verisign.com/server/trial/index.html>



The Sign of Trust on the NetSM

1350 Charleston Road • Mountain View, CA 94043
phone 650.961.7500 • fax 650.961.7300
www.verisign.com

© 1999, VeriSign, Inc. All rights reserved. 11/99