Securing Your Web Site

For Business

A step-by-step guide

for secure online commerce

VeriSign™

The Sign of Trust on the Net℠

Table of Contents

Introduction

Businesses that accept transactions via the Web can gain competitive edge by reaching a worldwide audience, at very low cost. Like any other distribution channel, 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 number, financial data, or medical history, is secure.

VeriSign, Inc., the industry leader in security services for electronic commerce and communication, offers a low-cost, proven solution for securely conducting business over the Web. By installing a VeriSign Secure Server ID 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 Secure 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 95 of the Fortune 100 companies and 65,000 other leading e-commerce sites.

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 Secure Server ID. After you read this paper, we invite you to obtain your free trial Secure Server ID or a full one-year Secure Server ID from http://www.verisign.com/server.

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

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.

> *"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 win 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 of the guide describes the benefits of e-commerce, and the specific risk areas you must address to realize the benefits.

Extend your reach to more customers

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

- Worldwide presence – A major attraction of the Web is that it 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 recent 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 these customers' confidence will gain their loyalty—and an enormous opportunity for expanding market share.

  "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 these customers' confidence 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 from 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, mortgage, or credit card, for example, are 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 speed application processing, reduce processing costs, and improve customer service.

> *"By accepting applications via a secure Web site, you can 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—or tailoring 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

Ensure the security of your electronic transactions

In person-to-person transactions, security is based on physical cues. Consumers don't worry about using their credit card in places like department stores because they can see and touch the merchandise, they can make judgments about the store and they feel comfortable that their credit card number is not being used by a third party. In the absence of physical cues on the Internet, 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 altered en route, either maliciously or accidentally. User names, credit card numbers, and dollar amounts are all vulnerable to such alteration.

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

Secure your Web Site
with A VeriSign Server ID

The good news: a proven, low-cost solution to secure online transactions is available today. VeriSign Secure Server IDs have earned the trust of businesses worldwide, including 95 of the Fortune 100 companies and all of the Relevant Knowledge, Inc. Top 20 Commerce Sites. In total, VeriSign has issued over 65,000 Secure Server IDs. This section describes how the VeriSign Secure Server ID works to make online transactions secure.

> *"VeriSign Secure Server IDs have earned the trust of businesses worldwide, including 95 of the Fortune 100 companies and all of the Relevant Knowledge, Inc. Top 20 Commerce Sites."*

Present your credentials via a VeriSign Secure 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 65,000 Secure 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 the applicant's credentials—such as Dun & Bradstreet number or Articles of Incorporation—and takes several other steps to ensure the organization is what it claims to be, and is not claiming a false identity. Then VeriSign issues the organization a Server ID, which is an electronic credential that your business can present to prove its identity or right to access information (see sidebar).

A Server ID from VeriSign provides the ultimate in credibility for your online business. VeriSign is known for its rigorous authentication practices. In fact, VeriSign is the only CA in the world to have passed an extensive SAS 70 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.) 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.

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 secret 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 Secure 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 Secure Server ID uses a matched pair of keys that uniquely complement each another. When a message is encrypted by one key, only the other key can decrypt it.

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 Secure 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 Secure 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 Secure 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.

Secure your online transactions
without hardware investment

VeriSign Secure Server IDs work in conjunction with Secure Sockets Layer (SSL) technology, which is the 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. SSL becomes functional only after you install a digital certificate, such as your VeriSign Secure Server ID.

After you install your ID, your server is able to establish SSL. SSL establishes a secure communications channel between your server and your customer's browser. You can communicate securely with any customer using Netscape Navigator, Microsoft Internet Explorer, or most popular e-mail programs. Once activated by your Secure Server ID, SSL immediately begins providing you with the following components of secure online commerce:

- Authentication—By checking your VeriSign Secure 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.

"By checking your 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."
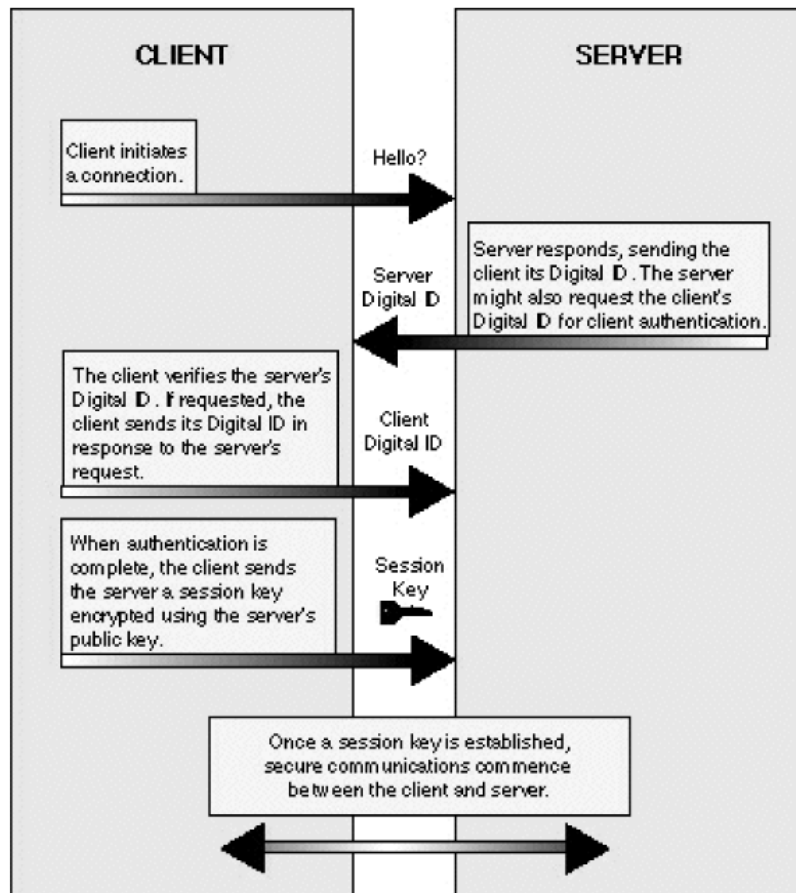
- Message privacy–SSL encrypts all traffic between your Web server and customers, using a unique session key. To securely transmit the session key to the consumer, your server encrypts it with your public key. Each session key is used only once, during a single session with a single customer. These layers of privacy

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

protection ensure that information cannot be viewed if it is inter-cepted by unauthorized parties.

- 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, 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 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.
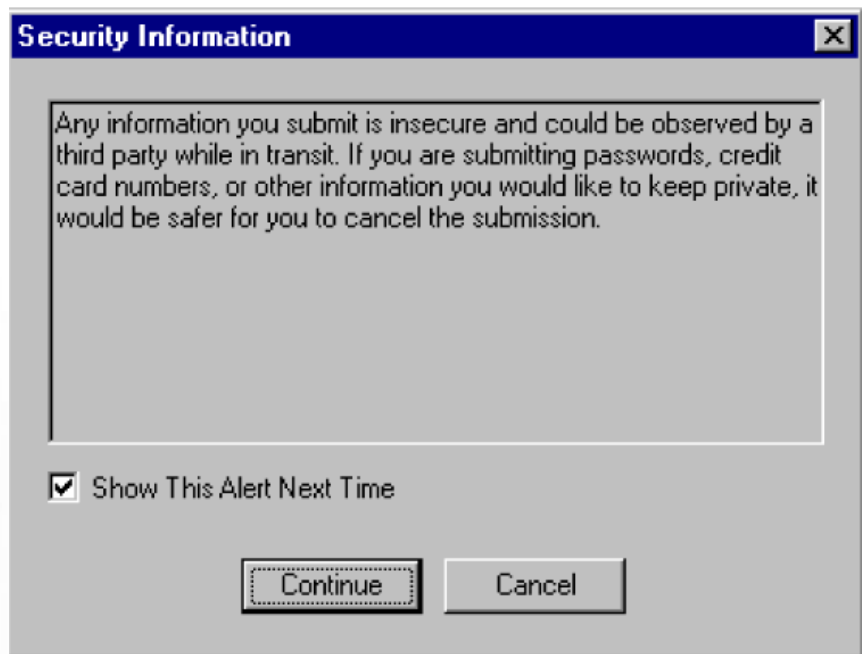
CLIENT

SERVER

Client initiates a connection.

Hello?

Server responds, sending the client its Digital D. The server might also request the client's Digital D for client authentication.

Server Digital D

The client verifies the server's Digital D. If requested, the client sends its Digital ID in response to the server's request.

Client Digital ID

When authentication is complete, the client sends the server a session key encrypted using the server's public key.

Session Key

Once a session key is established, secure communications commence between the client and server.

The ultimate result of a VeriSign Secure Server ID: 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 billing information, which the customer cannot later refute.

Make online commerce easy for your customers

Installing VeriSign Secure 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 Secure Server ID), the browsers will, by default, show a warning, which can make the purchase process seem threatening.

Security Information

Any information you submit is insecure and could be observed by a third party while in transit. If you are submitting passwords, credit card numbers, or other information you would like to keep private, it would be safer for you to cancel the submission.

☑ Show This Alert Next Time

[Continue]   [Cancel]

In contrast, if a user submits credit card or other information to a site with a valid Secure 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 Secure Server ID, the 100 million prospective customers with Microsoft and Netscape browsers are reassured that they are shopping on a secure site. In Netscape Navigator 3.0 and earlier, the key icon in the lower left corner of the browser, which is normally broken, is made whole. In Netscape Navigator 4.0 and later and in Microsoft Internet Explorer, the normally open padlock icon becomes shut, as shown below.

Enhance sales, convenience, or security
with other solutions from VeriSign

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 through VeriSign's free Authentic Site program

As a participant in the VeriSign Authentic Site program, which is free of charge, you can display the VeriSign Authentic Site seal on your Web site. When consumers click on this seal, they are provided with detailed information about online security, as well as instructions for verifying the authenticity of your digital certificate. Participation in this program also allows you to be listed in VeriSign's Authentic Site Index, which is a searchable index of certified sites targeted at security-conscious online consumers. The index helps new and current customers find you online, and the seal confirms that they have found your site. Visit http://www.verisign.com/authentic/ to register or receive more information.

Simplify management of multiple Secure Server IDs

If you host your secure Web site on ten or more servers, VeriSign offers a special program to simplify additions, renewals, and

cancellations of each server's Secure Server ID. Through the OnSite Server ID program, you apply just once for all servers in your domain. This service is available in bundles of 10, 25, 50, 100 or more. For more information about VeriSign OnSite Server ID program, visit http://www.verisign.com/serveronsite, where you'll find a guide to securing intranets and extranets.

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' identity, 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 international 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, your international customers can now enjoy unparalleled security when visiting your Web site. Available to banks worldwide and to U.S. corporations, the VeriSign Global Server ID is several trillion times more secure than any other product. For more information about VeriSign's global 128-bit ID, see http://www.verisign.com/globalserver.

Conclusion

With its worldwide reach, the Web promises to be a lucrative distribution channel with unprecedented potential. By setting up an online storefront, businesses can reach the 50 million people around the people 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 competitive edge.

VeriSign Secure Server IDs are a proven solution, working today on more than 65,000 Web sites worldwide, including 95 of the Fortune 100 companies. Join them today, and expand your market by securing your online business. For a free 14-day trial Secure Server ID, visit https://www.verisign.com/server.

Step-by-step instructions

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 now. You can complete the entire enrollment process online in about 15 minutes and immediately begin using your trial Secure Server ID.

You can also purchase a one-year full-service Secure Server ID from 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.

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. Check with your vendor to be sure yours will.

- Register your domain name – If you haven't already, register your URL at http://rs.internic.net 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 or check, 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/server/help/serverAgreement.html.

- Gather proof of right documents – Before issuing your Secure Server ID, VeriSign must confirm that your company is 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 documents for your company: articles of incorporation, partnership papers, business license, fictitious business license, or federal tax ID confirmation. 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, you obtain the credit card number from the customer. Second, you secure payment from an acquiring processor on behalf of the credit card issuing bank. When your business uses a Secure 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 (see sidebar).

Obtain your Secure Server ID

To complete your Secure 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://www.versign.com/library/server/csr, 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.

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 contact people.

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 needs to complete our ISP online enrollment for you.

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.

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 Secure Server ID by e-mail in 1–3 working days.

5. Install your Secure Server ID

When you receive your Secure 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 Secure 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.

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.

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

Options for obtaining payment

- 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/.