VeriSign®

BUSINESS GUIDE

How to Set Up a Secure E-Commerce Site the Right Way

SSL Certificates and Online Payment Services

Where it all comes together.™

CONTENTS

CONTENTS

Introduction

E-commerce has become an increasingly important and effective means to sell products and services. While there are many resources available that discuss the customer facing aspects of e-commerce (e.g., Web site design, use of graphics, page layout, product presentation, promotion, etc.), this paper focuses on the back-end, behind the scenes, technology infrastructure-related requirements, necessary for online merchants to:

- allow customers to safely and securely place orders online
- ensure that merchants reliably process orders and receive payment
- communicate to customers that the entire process is safe and secure

In addition, this paper will describe the services that VeriSign offers to satisfy these requirements:

- VeriSign® SSL Certificates
- VeriSign® Payment Services
- VeriSign® Commerce Site Services
- VeriSign Secured™ Seal

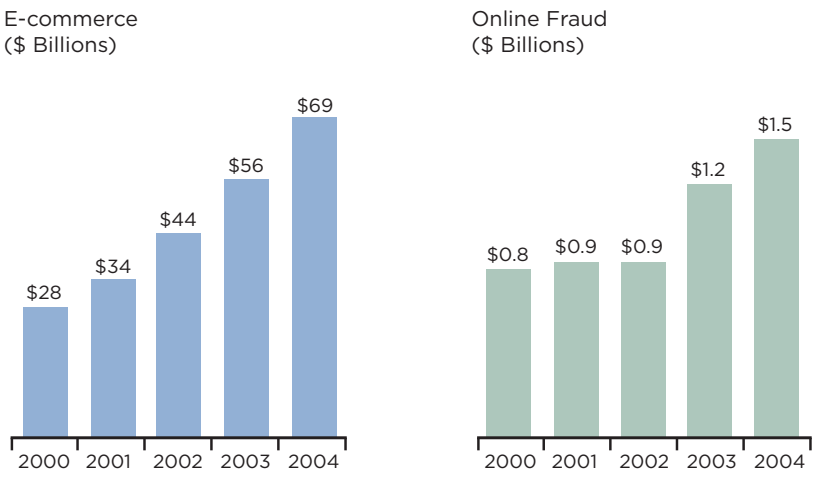
To maintain topical continuity, the paper is organized to discuss a specific requirement, followed directly by a description of VeriSign's products and services that address that requirement.

E-Commerce Overview

Gaining the trust of online customers is vital for the success of e-commerce. Based on recent online business statistics, some companies have earned that trust by showing strong overall growth in e-commerce. The U.S. Department of Commerce reports retail e-commerce sales have grown from $27.8 billion in 2000 to $69.1 billion in 2004, representing growth of 25 percent per year. At the same time, there remains significant opportunity for continued growth. E-commerce sales in 2004 will be just 1.9 percent of total retail sales, growing from 0.9 percent in 2000.[1] Most consumers have access to the Web, so the relatively small size of e-commerce compared to traditional, offline spending does not owe itself to lack of opportunity. In fact, in 2004, 75 percent (204 million) of people in the United States, above age two, and in households with a fixed phone line have Internet access,[2] and more than 50 percent of them (111 million) buy online.[3] The reality is that many people deliberately limit the transactions they do online because they don't fully trust the e-commerce process. These people simply fear for the security of personal and financial information transmitted over the Web. The number one factor (cited by 70 percent of people) discouraging U.S. consumers from using a credit card online was concern about security.[4]

[1] "Quarterly Retail E "Quarterly Retail E-Commerce Sales," U.S. Department of Commerce, November 19, 2004
[2] Nielsen/NetRatings Enumeration Study, February 2004
[3] Jupiter Research, cited in ePaynews, Feburary 19, 2004
[4] Payment One, April 2003

E-commerce is increasing rapidly. . . and so is online fraud



Source: U.S. Department of Commerce 2004, Celent Communications 2003

Fear of online fraud is well founded. Gartner reports that nearly two million Americans were scammed over the Internet during a recent 12 month period. The direct loss to banks and consumers was $2.4 billion, according to an April 2004 survey. Gartner estimates that 57 million Internet users in the United States have received email related to phishing scams that impersonate popular Web sites; about 1.8 million people have consequently divulged personal information. Three-fourths of phishing attacks have occurred in the previous six months.[5]

Fortunately, companies can prevent most online fraud with stringent screening and prevention measures. Fraud rates at sites with sales of greater than $25 million, which typically invest more on screening and prevention measures, are half that of fraud at smaller sites.[6] Companies using these measures hold average fraud losses to just over one percent of sales, according to research by Jupiter Media Metrix.

VeriSign can help your company establish or improve customer trust by securing your Web site for business. VeriSign offers one of the strongest security solutions in the industry by securing information exchange between Web servers and clients, from server to server, and even among other networking devices such as server load balancers or SSL accelerators. VeriSign solutions can provide complete cross-network security by protecting servers facing both the Internet and private intranets. VeriSign Internet payment processing services simplify online payment processing by providing reliable, secure, and affordable payment connectivity among merchants, customers, and financial networks. VeriSign payment processing services allow merchants to securely and easily authorize, process, and manage multiple payment types, without investing in or maintaining significant technological resources.

[5] "Phishing Attack Victims Likely Targets for Identity Theft," Gartner, May 4, 2004
[6] "Online Fraud Costs $2.6 Billion This Year," MSNBC Interactive, November 11, 2004

Goals for Implementing Secure E-Commerce

To take advantage of the opportunities of e-commerce and avoid the risks of communicating and transacting business online, every business must address customer concerns and requirements as well as their own needs.

- **Security and privacy**—Concern about security is the number one factor deterring people from using a credit card online. In addition to having concerns about online credit card fraud, consumers believe that online purchasing poses a significant risk to becoming a victim of identity theft.[7] E-commerce Web sites must address consumers' concerns about security, safety, and privacy.
- **Reliability and up time**—Consumers have come to expect nearly perfect up time and reliability performance from e-commerce sites. A single instance of a site not working properly can significantly reduce the likelihood of customers completing a purchase or returning to purchase at a later time.
- **Confidence and trust**—93 percent of shoppers say it's important for sites to display a trust mark, and 64 percent of consumers who have terminated a transaction online would have gone through with it if a recognized trust mark had been present.[8] Displaying a well-recognized, third-party trust mark or security seal is a requirement to inspire consumer confidence and trust.
- **Payment processing integrity**—Merchants depend upon the integrity and reliability of the back-end payment processing system to ensure that there are no problems between the time a merchant receives an order and the time the payment is credited at the merchant's bank.
- **Quick and easy implementation**—To facilitate quick and easy implementation of e-commerce security solutions, companies with e-commerce Web sites need a vendor that offers comprehensive solutions, has a track record of success, has well developed and tested processes and procedures, and offers industry-leading service and support.

The Solution: How to Build a Secure E-Commerce Site

The solution for meeting the goals above includes three essential components:

- **SSL Certificates—**Digital certificates for Web servers, to provide security, authentication, privacy, and data integrity through encryption.
- **Payment processing gateways—**A secure online payment system, to allow e-commerce Web sites to securely, reliably, and automatically accept, process, and manage payments online.
- **Trust mark—**A trust mark (also called a security seal), from a trusted third-party, placed on a Web site, allows merchants to communicate to customers that information exchange and transaction processing are secure.

Together, these components form the foundation for developing a secure e-commerce Web site.

[7] "MasterCard Targets Phishing, ID Theft," Keith Regan, Ecommerce Times, June 23, 2004
[8] The TNS Study, conducted June-July 2004 was sponsored by VeriSign and was comprised of online shoppers, at least 18 years old. U.S. respondents were recruited from the TNS NFO Panel and all international participants were recruited from GMI country-specific panels.

SSL Certificates

SSL Certificates form the basis of a secure e-commerce site by allowing Web sites to offer safe, secure, and private information exchange to their customers.

+ SSL Defined

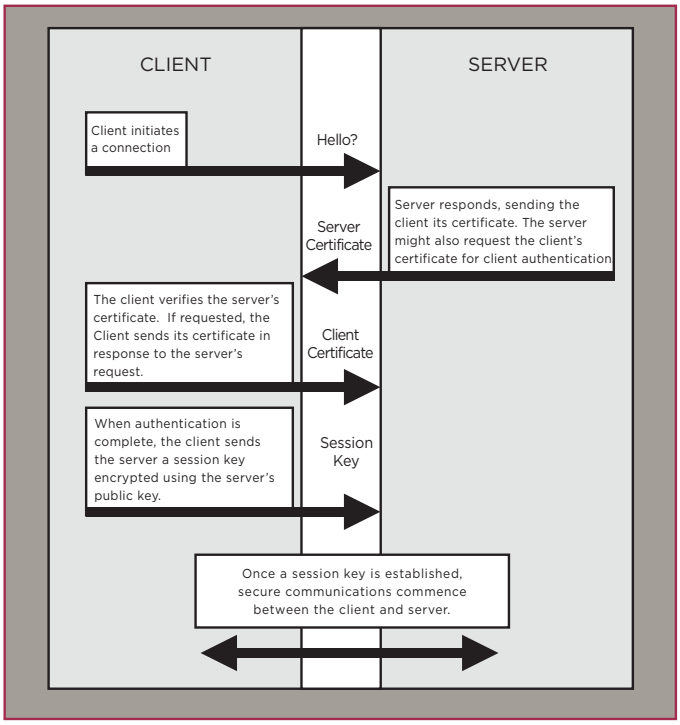
Secure Sockets Layer (SSL) is the worldwide standard for Web security. SSL technology is used to encrypt and protect information transmitted over the Web with the ubiquitous HTTP protocol. SSL provides your Web site's users with the assurance of access to a valid, "non-spoofed" site, and it prevents data interception or tampering with sensitive information. Support for SSL is built into all major operating systems, Web applications, and server hardware—meaning that your business can use SSL's powerful encryption capabilities to increase consumer confidence. SSL Certificates fulfill two necessary functions to establish e-commerce trust: encryption and authentication.

+ Encryption Technology and SSL Certificates

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

An SSL Certificate is an electronic file that uniquely identifies individuals and Web sites and enables encrypted communications. SSL Certificates serve as a kind of digital passport or credential. Typically, the "signer" of a SSL Certificate is an SSL provider (also known as a Certificate Authority), such as VeriSign.

Figure 2



The previous diagram illustrates the process that guarantees protected communications between a Web server and a client. All exchanges of SSL Certificates occur within seconds and require no action by the consumer.

+ Authenticating Your Web Site with an SSL Certificate

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

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

Different SSL providers employ varying levels of thoroughness in their authenticating processes, with customers preferring Web sites secured by SSL providers that abide by the strictest standards.

Choosing an SSL provider with well established and rigorous authentication and verification procedures can help your company comply with the security provisions of various security regulations, inspire trust and confidence in customers and business partners by verifying your identity, and reduce risk of fraud.

+ SGC: How to Offer the Strongest SSL Encryption

At this point, you probably understand the importance of SSL Certificates and the critical role that they play in developing a comprehensive Web security platform, but it is also important to understand that not all SSL Certificates offer the same level of security. There is an important protocol within SSL, called Server Gated Cryptography, or SGC, which has the potential to significantly alter the level of protection offered to any given Web site's visitors. Using an SGC-enabled SSL Certificate increases the encryption level available to many site visitors and ensures that the most possible site visitors will connect at 128-bit encryption, the strongest encryption currently available.

+ Two Levels of SSL Encryption

There are two basic levels of SSL encryption, which we will refer to as the low-level and the high-level of encryption. Low-level SSL encryption occurs at either 40 or 56 bits. High-level SSL encryption is encrypted at a full 128 bits, which represents that strongest SSL encryption currently available for Web servers. Whether a given SSL session occurs at the low or high level of encryption depends on both the configuration of the client system and the type of SSL Certificate in place on the Web server. Many clients' systems are unable to take advantage of full 128-bit SSL encryption, unless an SGC-enabled certificate is in place.

There is a dramatic difference between these two levels of encryption. 128-bit encryption offers 2^{88} times as many possible combinations as 40-bit encryption, meaning that 128-bit encryption is approximately 300 septillion (300,000,000,000,000,000,000,000,000) times stronger than 40-bit encryption. That's over a trillion times a trillion stronger. The most common approach to breaking encryption is "brute force" computation, which involves

inputting every possible variable into a prompt until the correct one is found. In 1997, 40-bit encryption was broken in about four hours by a college student using this method, and currently it can be broken by a hacker with the right skills and a high-end home system in a matter of minutes. If the same hacker were to attack a 128-bit SSL session, it would take more than a trillion years to break that session.

+ Factors Determining the Level of SSL Encryption

Whether or not a specific client will step up to 128-bit encryption depends upon both the browser version that a client system is running and the operating system that is installed on the client. Either of these factors can cause a client system to fail to step up. It's important to note that these configuration issues exist entirely on the computer that is visiting the Web site, which means that the server's hardware, software, and operating system have no influence over a visitor's ability to step up to 128-bit encryption.

There are three categories of browser. The first category, which represents well under 0.1 percent of browsers in use today, includes those that are simply incapable of connecting at 128 bits. These browsers are so extremely old that they were released before the capability was available, and no SSL Certificate in existence can connect to them with 128-bit encryption. These browsers include Internet Explorer versions prior to 3.02 and Netscape® prior to 4.02. Clients running these extremely old browsers are the only visitors' machines that will ever connect to an SGC-enabled SSL Certificate at less than 128-bit encryption.

The second category of browser is still old but not as old as the first. These browsers include Internet Explorer versions after 3.02 but before 5.5 and Netscape versions after 4.02 and up through 4.72. They offer 128-bit encryption when connecting with SSL Certificates that are SGC-enabled but fail to use 128-bit encryption when connecting with SSL Certificates that are not. These browsers are present on well under half the systems in use today but still have a significant presence in the market.

The third category includes the newest browsers, Internet Explorer starting with version 5.5 and Netscape versions after 4.72. These browsers are capable of providing 128-bit encrypted sessions for both types of SSL Certificates, as long as the operating system allows it.

Which certificates offer 128-bit SSL to all possible systems

	Old browsers	Many Windows 2000 systems	Other Systems
Secure Site (no SGC support)	No	No	128-bit
Secure Site Pro (SGC support)	128-bit	128-bit	128-bit
SSL from other leading providers (no SGC support)	No	No	128-bit

Even among those who are well informed on the subject of Web security, many people don't realize that the client machine's operating system can also cause an SSL session not to step up to 128-bit encryption. In particular, many Windows 2000® systems will fail to step up to 128 bits unless the SSL Certificate supports SGC. It's especially important to understand that this security weakness occurs regardless of the version of Internet Explorer running on the client system. Even those computers running the very most recent version of Internet Explorer still fail to connect at 128 bits.

Any copy of Windows 2000 shipped prior to approximately March 2001 that was not subsequently upgraded with one of several Windows upgrade packs will suffer this limitation. The exact number of affected systems is unknown, but with over 156 million Windows 2000 systems in use—representing almost 40 percent of all personal computers encompassing all operating systems[9]—this number is certainly very large.

VeriSign SSL Certificates

VeriSign is the world's leading SSL provider, having issued almost 500,000 SSL Certificates. Web users are accustomed to seeing commercial e-commerce sites display the VeriSign Secured Seal—prominently featured to assure online users that a Web business is authentic and that its site is capable of securing confidential information with SSL encryption. In fact, in a 2004 study of the 12 most prominent trust marks on the Web, the VeriSign Secured Seal ranked highest by a wide margin in perceived safety of visitors' information, perceived trustworthiness, purchase likelihood, and overall preference. Subjects also ranked the VeriSign Secured Seal as the most recognized of the tested trust marks.[10]

+ Secure Site Pro SSL

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

VeriSign[11] is the only leading SSL provider to offer SGC-enabled certificates. That means among leading SSL providers, only VeriSign can offer the strongest available SSL encryption to every site visitor, regardless of the browser version or operating system that the visitor is using. SGC enables SSL Certificates such as Secure Site Pro to "step-up" to 128-bit SSL encryption when communicating with many client systems that otherwise could only connect at 40- or 56-bit encryption. Over 99.9 percent of desktop computers on the Internet connect to SGC-enabled certificates with 128-bit encryption. VeriSign is the only leading SSL provider that can guarantee that every one of the over 156 million Windows 2000 users is connecting with the unbroken protection of 128-bit SSL.

+ Secure Site SSL

VeriSign® Secure Site SSL Certificates are a cost effective solution for less security sensitive intranets, extranets, and Web sites. They enable 128-bit encryption for users with newer operating systems and browsers. VeriSign Secure Site enables 40-bit SSL encryption when communicating with a large number of older systems currently in use, including many Windows 2000 systems (regardless of whether these systems are using the most recent version of Internet Explorer or not), and some older browser versions as well. Secure Site SSL Certificates run on virtually all server software platforms. Secure Site and other non-SGC enabled certificates represent an option for environments in which having the best possible security is not as important a factor as cost.

[9] "PC Market by Operating System: Worldwide, 2004-2007," Gartner-Dataquest, January 14, 2004
[10] TNS Study, June-July 2004
[11] SSL Certificates may be obtained from VeriSign's affiliates, resellers, or subsidiaries in addition to directly from VeriSign, Inc.

Online Payment Services

Once you have built a Web site and implemented SSL Certificates to authenticate your company to customers and encrypt communications and transactions, you must address another crucial component to secure your e-commerce Web site. Online payment services enable customers to easily pay for products and services online and facilitate processing and managing those payments in conjunction with a network of financial institutions.

+ Online Payment Processing Basics

Purchasing online may seem to be quick and easy, but most consumers give little thought to this seemingly instantaneous process. For e-commerce to work correctly, merchants connect to a network of banks (both acquiring and issuing banks), processors, and other financial institutions so that payment information provided by the customer can be routed securely and reliably. The solution is a payment processing service that connects your online store to these institutions and processors. Because payment information is highly sensitive, trust and confidence are essential elements of any payment transaction. Therefore the payment processing service should be provided by a company with in-depth experience in payment processing and security.

+ The Payment Processing Network

Here's a breakout of the participants and elements involved in processing payments:

- **Acquiring Bank**—In the online payment processing world, an Acquiring Bank provides Internet Merchant Accounts. A merchant must open an Internet Merchant Account with an Acquiring Bank to enable online credit card authorization and payment processing. Examples of Acquiring Banks include Merchant eSolutions and most major banks.
- **Authorizations**—The process by which a customer's credit card is verified as active and the credit availability sufficient to make a transaction is confirmed. In the online payment processing world, an authorization also verifies that the billing information the customer has provided matches up with the information on record with the relevent credit card company.
- **Credit Card Associations**—A financial institution that provides credit card services that are branded and distributed by Customer Issuing Banks. Examples include Visa and MasterCard.
- **Customer**—The holder of the payment instrument—such as credit card, debit card, or electronic check
- **Customer Issuing Bank**—A financial institution that provides a customer with a credit card or other payment instrument. Examples include Citibank, Suntrust, etc. During a purchase, the Customer Issuing Bank verifies that the payment information submitted to the merchant is valid and that the customer has the funds or credit limit to make the proposed purchase.
- **Internet Merchant Account**—A special account with an Acquiring Bank that allows the merchant to accept credit cards over the Internet. The merchant typically pays a processing fee for each transaction processed, also known as the discount rate. A merchant applies for an Internet Merchant Account in a process similar to applying for a commercial loan. The fees charged by the Acquiring Bank will vary.

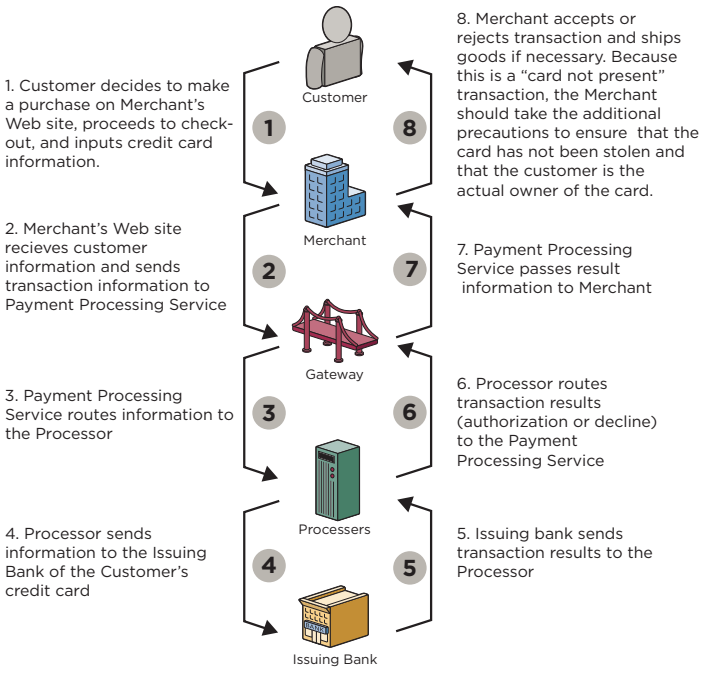
- **Merchant**—Someone who owns a company that sells products or services.
- **Payment Processing Service**—A service that provides connectivity among merchants, customers, and financial networks to process authorizations and payments. The service is usually operated by a third-party provider such as VeriSign.
- **Processor**—A large data center that processes credit card transactions and settles funds to merchants. The processor is connected to a merchant's site on behalf of an Acquiring Bank via a Payment Processing Service.
- **Settlement**—The process by which transactions with authorization codes are sent to the processor for payment to the merchant. Settlement is a sort of electronic bookkeeping procedure that causes all funds from captured transactions to be routed to the merchant's Acquiring Bank for deposit.

+ How Payment Processing Works

Payment processing in the online world is similar to payment processing in the offline or "brick-and-mortar" world, with a few exceptions. In the online world, the store and the transaction are virtual. This means that the card is "not present" at the transaction and that the transaction information is submitted and processed via the merchant store network. Because of this, merchants are held liable for fraudulent transactions by the credit card associations. Merchants must take additional steps to guard against online fraud, including verification that the card information is being submitted by the actual owner of the card and protection of their store and network infrastructure from hacking attempts.

Payment processing can be divided into two major phases or steps: authorization and settlement. Authorization verifies that the card is active and that the customer has sufficient credit available to make the purchase. Settlement involves transferring money from the customer's account to the merchant's account. Online payment processing may also allow you to set up automatically recurring billing payments if your payment processing service provider offers this feature.

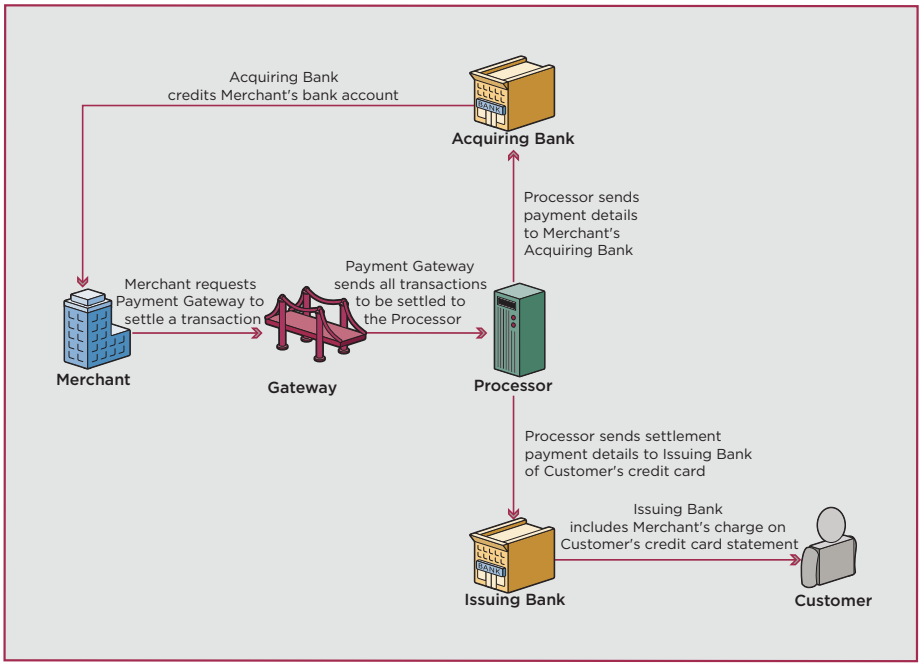
Payment processing—authorization



+ Payment Processing—Settlement

The settlement process transfers authorized funds for a transaction from the customer's bank account to the merchant's bank account. The process is basically the same whether the transaction is conducted online or offline.

Figure 5



+ What to Look for in a Payment Processing Solution

Finding a reliable, secure, and flexible payment processing solution for your business is critical, so it's important to take the time to investigate and assess the options available to you. A payment processing solution should provide you:

- **Fast, reliable and flexible transaction processing**—Reliably and cost-effectively accept and process a variety of payment types, including credit cards, debit cards, and electronic checks. Not only does this ability reduce lost sales, but it also enhances the quality of your site by allowing your customers the freedom and flexibility to pay you quickly and conveniently.
- **Real-time authorization**—Provide real-time credit card authorization results allowing you to accept or reject orders immediately and reduce risk of fraudulent transactions.
- **Payment tracking and management**—Easily track and manage payments from multiple payment types or processors so you can spend more time on your business, not on managing transactions. It should also act as a virtual terminal to allow for processing offline transactions. That gives you the flexibility to process orders received by telephone, by fax, over email, or in person. Lastly it should store transaction records letting you easily search for transactions and create reports.

- **Seamless, scalable growth**—Scale rapidly and seamlessly to accommodate increased transaction volumes so your systems grow as your business grows.
- **Fast and easy integration**—Provide flexible, easy integration with the Merchant's Web site. The sooner you can start accepting payments, the sooner you can start generating revenue from your site. The service should also be able to work with all leading Internet Merchant Accounts, allowing you to switch your banking relationship without having to worry about installing new software or performing new integrations.
- **World-class security**—Offer standard processing level anti-fraud features such as card security code (CSC), and address verification service (AVS) as well as other comprehensive online fraud protection feature options that protect your online business from fraud. These options should be integrated seamlessly into the payment processing solution. Most importantly, these options should be cost-effective and simple to understand, so that you don't waste valuable time and money while protecting your online business against fraud.
- **Established and trusted solution**—Be provided by a well-established and trustworthy company. That ensures that your payment service provider will continue to provide reliable payment services as well as new features.

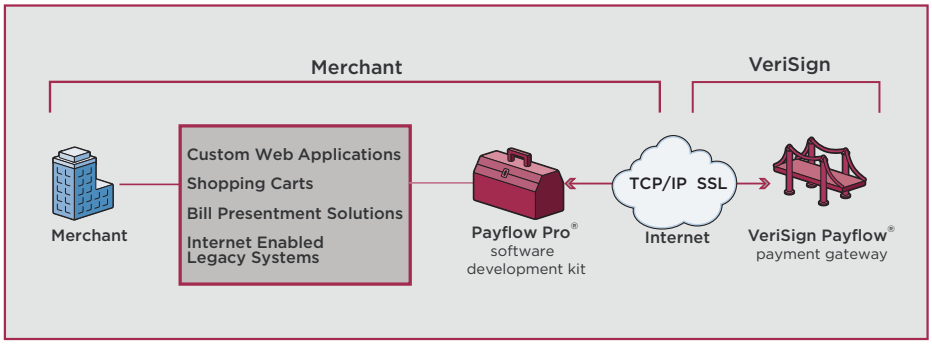
VeriSign Payment Processing Services—Easy, Secure, and Reliable

The VeriSign Payment Services, now the industry standard for online payment processing solutions, was developed to meet the demanding and diverse needs of online merchants. It is an Internet payment processing service that simplifies online payment processing by providing reliable, secure and affordable payment connectivity among merchants, customers, and financial networks. VeriSign Payment Services allow merchants to securely and easily authorize, process, and manage multiple payment types—without investing in or maintaining significant technological resources. Developed to fit a variety of merchant needs, VeriSign Payment Services offer important value-add options, like our Fraud Protection Service, Payflow® Recurring Billing Service, and customer service packages that include professional integration support. The VeriSign suite of services was also designed to scale quickly and seamlessly as your business grows. Most importantly, VeriSign offers a payment processing service with immediate connectivity to all major processors and integration with most shopping carts.

+ Payflow Pro®

Scalable and fully customizable, the VeriSign® Payflow Pro® service is recommended for merchants who require peak site performance and direct control over payment functionality on their site. The Payflow Pro service allows merchants to process payments through their Web sites with a software download that includes a software developer kit for simple API integration. The Payflow Pro service features credit card, debit card, and check processing as well as purchase card levels II and III. The Payflow Pro service is integrated with most major shopping carts.

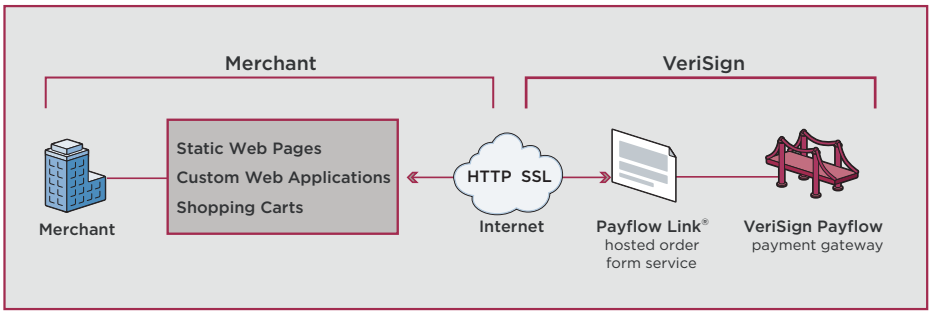
The Payflow Pro service gives merchants more control via a direct TCP/IP conection



+ Payflow Link®

The Payflow Link® service is designed for merchants who require a simple, low-cost solution to selling on the Web. The Payflow Link service is a hosted order-form service that allows a customer to securely input credit card information. To use the Payflow Link service, merchants need only add a small piece of HTML code that will link a customer from their Web site to the order forms hosted by VeriSign. The Payflow Link service offers merchants a simple package for payment processing, including credit card, debit card, and check processing functionality as well as offline order processing. The Payflow Link service works with most major shopping-cart software.

The Payflow Link service allows merchants to process online payments using a simple Web Link



VeriSign® Payment Services Features

Both the Payflow Pro and the Payflow Link services include the following important features:

- **Fast and easy integration**—The Payflow Pro service is already fully integrated with most major e-commerce solutions and shopping carts. The Payflow Link service works with most of the leading shopping carts available today. VeriSign Payment Services offer immediate connection to all major payment processors.
- **Real-time authorization and transaction verification**—VeriSign Payment Services allow merchants to get authorization results for purchases in a matter of seconds, so merchants can accept or reject orders immediately. Merchants also get immediate confirmation that a transaction has occurred.
- **Convenient payment tracking and management**—VeriSign's secure VeriSign® Manager, standard with the Payflow Pro service and Payflow Link service, allows merchants to easily search for transactions and create transaction reports. VeriSign Manager also allows merchants to submit offline transactions such as those submitted via telephone, by fax, or in person and return/credit transactions.
- **Seamless, scalable growth**—VeriSign's product line allows your business to grow easily and seamlessly as your transaction volume grows.
- **Fast, reliable transaction processing**—High-bandwidth, fault-tolerant network connections ensure maximum uptime and processing speed.
- **World-class security**—From the market leader in Internet security. Both Payflow services use SSL encryption to secure transaction information. The Payflow Pro client encrypts information between the merchant's site and the Payflow payment processing platform. The Payflow Link service uses secure, VeriSign-hosted order forms for the collection and transmission of transaction information. Both Payflow services come with standard, processing-level, anti-fraud features such as AVS and CSC. Payflow services also integrate seamlessly with VeriSign® Fraud Protection Services, offering you cost effective options that help protect your online business as it grows.
- **Maximum flexibility**—Merchants can switch banking relationships or add new payment types without having to install new software.
- **Expert technical support**—VeriSign offers various customer support options via its state-of-the-art Customer Care center, including 24/7 phone support.
- **Optional Recurring Billing Services**—An upgrade feature available with VeriSign Payflow Pro and Payflow Link services allows you to charge your customers on a recurring basis, automatically. The VeriSign® Recurring Billing Service integrates seamlessly with the Payflow Pro and Payflow Link services.
- **Trusted solutions from a trusted provider**—The Payflow service is provided by VeriSign, the leading provider of digital trust services that enable businesses and consumers to engage in commerce and communications with confidence. VeriSign has helped millions of businesses and individuals build, promote, and enable their Web sites for e-commerce.

THE VALUE OF A TRUST MARK

Online Shoppers Are Concerned about Security

- 69 percent of Americans consider online credit card fraud a major concern.
- 85 percent of Americans are concerned about being the victim of identity theft.
- 37 percent of Americans believe that online purchasing poses the greatest threat for becoming a victim of identity theft.

... and with Good Reason

- Nearly 10 million Americans have experienced inappropriate use of their personal information to open new accounts without authorization, to misuse existing credit card accounts, and to abuse other personal financial resources.
- Since November 2003, the Anti-Phishing Work Group has seen reports of phishing scams increase by about 4,000 percent.

Security Concerns Limit Spending

- 64 percent of online shoppers have abandoned a shopping cart or failed to complete an online purchase because they didn't get a sense of trust when it came time to provide payment information.
- 56 percent of Americans report they are protecting themselves from identity theft specifically by limiting their online purchases to reputable websites.

+ Internet Merchant Account

VeriSign has also created a fast and easy way to apply online for an Internet Merchant Account through a partnership with one of the industry's premier Merchant Account providers, Merchant e-Solutions. The Merchant e-Solutions application is provided as an option within the VeriSign Payment Services registration process. As a VeriSign customer, the application fee is waived and the application qualifies for an instant decision.

VeriSign Commerce Site

VeriSign Commerce Site Pro and Commerce Site Payment Services combine SSL Certificates with the VeriSign Payflow Pro payment gateway to form a complete, integrated solution that's ideal for e-commerce sites and online stores.

- Commerce Site Pro includes Payflow Pro and a 128-bit SGC-enabled SSL Certificate—the world's strongest SSL encryption and the standard for online merchants, plus value-added services, including VeriSign's guaranteed two-day delivery
- Commerce Site includes Payflow Pro and an SSL Certificate—ideal for less security sensitive intranets, extranets, and Web sites, plus other value-added services.

Trust Marks

With the recent surge in phishing, identity theft, and other online scams, a trust mark (also called a security seal) is an indispensable tool in your effort to improve your customers' perception of safety when they do business online. 85 percent of Americans are concerned that they may become victims of identity theft,[12] with 37 percent believing that online purchasing poses the greatest risk.[13] 56 percent of Americans report they are protecting themselves from identity theft specifically by limiting their purchasing to reputable Web sites.[14]

Displaying a trust mark on your SSL-secured Web site reassures visitors and can lead to increased visitor-to-sales conversions, lower shopping cart abandonment, and a larger average purchase price.

The process is relatively quick and easy, involving the copying and pasting of a small line of code to your home page and any other page of your Web site where you want to display the trust mark. When visitors click on this trust mark, they instantly link to a pop-up window containing information about your SSL Certificate, assuring them that transactions with your site are encrypted by SSL and allowing them to verify your site's authenticity.

The criteria that you use to select an SSL provider and its associated trust mark should include the following:

- Level of recognition and preference among consumers
- Rigorous and thorough process for verifying a Web site's identity

[12] "Steely-Eyed About Identity Theft," eMarketer, May 4, 2004
[13] "MasterCard Targets Phishing, ID Theft," Keith Regan, Ecommerce Times, June 23, 2004
[14] "Steely-Eyed About Identity Theft," eMarketer, May 4, 2004

Third-Party Trust Marks Alleviate Security Concerns

- 52 percent of online shoppers say that trust marks stand for "security."
- 93 percent of U.S. online shoppers say it is important for an e-commerce site to include a trust mark.
- 64 percent of consumers who have terminated an online transaction due to a lack of security feel they would have gone through with the original purchase if the site had included a recognized trust mark.

VeriSign Secured Seal

Be sure to post the VeriSign Secured Seal on your home page or other pages where confidential information exchange takes place. The VeriSign Secured Seal lets your site visitors know that you have chosen leading services to help protect them.

THE VALUE OF THE VeriSign SECURED SEAL

The VeriSign Secured Seal Increases the Likelihood to Buy

- 83 percent of U.S online shoppers are familiar with the VeriSign Secured Seal, more than any other mark
- And among them, more than four in five say it is their preferred seal
- The VeriSign Secured Seal rates best worldwide among endoresement programs in terms of consumer trust (60 percent), with customers indicating they believe the seal represents security, protection, verification, and reputation.
- The majority of shoppers (53 percent) prefer to use sites that display the VeriSign Secured Seal.

- Experience and number of SSL Certificates issued
- Time-proven practices and procedures
- Ability to offer the strongest encryption to your site visitors
- Annual audits by a third party
- Investment in marketing programs to promote consumer awareness

VeriSign's Trust Mark: The VeriSign Secured™ Seal

VeriSign Secure Site and Commerce Site Services include the VeriSign Secured Seal.

The VeriSign Secured Seal is designed for display on Web sites as a symbol of security and trust, encouraging consumers to confidently provide credit card numbers and other sensitive information. When you purchase Secure Site, Commerce Site, or VeriSign Payment Services, you can post the seal on your home page, security/privacy page, transaction pages, etc. When visitors click on the seal, they instantly link to a dynamic pop-up screen of information about the SSL Certificate, assuring them that transactions with your site are encrypted by SSL, allowing them to verify your site's identity and check the certificate's status in real time. If you are using VeriSign Payment Services, the pop-up screen will also let your customers know that their payment transactions are being processed securely through VeriSign's secure payment infrastructure.

Secure Site and Commerce Site solutions also include up to $250,000 of NetSure® protection, an extended warranty program that protects e-business against economic loss resulting from theft, corruption, impersonation, or loss of use of a certificate.

VeriSign E-Commerce Solutions: Summary

VeriSign offers a complete range of products and services to help your business implement an end-to-end security solution for e-commerce. VeriSign® SSL Certificates are available with or without SGC support as part of Secure Site services. VeriSign Payment Services enable businesses to easily accept, manage, and process payments electronically. VeriSign Commerce Site Services combine SSL Certificates, payment services, and other value-added features to form a complete, secure e-commerce solution. The VeriSign Secured Seal inspires upfront trust and confidence among customers prior to and during the purchase process. And for large enterprises operating multiple servers, VeriSign® Managed PKI for SSL simplifies the process of issuing and managing large numbers of SSL Certificates.

+ VeriSign Product and Service Overview

SSL Certificates

- **Secure Site Pro** includes a 128-bit SGC-enabled SSL Certificate to ensure the strongest available encryption to every visitor and value-added services
- **Secure Site** includes an SSL Certificate, plus additional value-added services
- **Managed PKI for SSL** for companies securing five or more servers (see VeriSign's Web site or call for details)

Payment processing services

- **Payflow Pro** is recommended for merchants who require peak site performance and direct control over payment functionality on their site. Includes a software development kit for simple API integration.
- **Payflow Link** is designed for merchants who require a simple, low-cost solution to selling on the Web. Merchants need only add a small piece of HTML code that will link a customer from their Web sites to the order forms hosted by VeriSign.

Commerce site services (SSL Certificates + Payflow Pro)

- **Commerce Site Pro** includes the Payflow Pro service and a 128-bit SGC-enabled SSL Certificate— the world's strongest SSL encryption and the standard for online merchants
- **Commerce Site** includes the Payflow Pro service and an SSL Certificate—ideal for less security sensitive intranets, extranets, and Web sites

How to Enroll for Commerce Site and Secure Site Solutions

Phone: Toll free 1-866-893-6565 or 650-426-5112
Email: internetsales@verisign.com
Web: *www.verisign.com/products-services/security-services/ssl/index.html*

The VeriSign Advantage

VeriSign SSL Certificates and e-commerce payment services have earned the trust of businesses worldwide, including 93 percent of Fortune 500 companies and 94 percent of the top 50 e-commerce sites. To date, VeriSign, the world's leading SSL provider, has issued almost 500,000 SSL Certificates. VeriSign is the only leading vendor to offer 128-bit SGC-enabled SSL, the strongest encryption available to secure both the connection between the customer and the merchant and between the merchant and the network of financial institutions. That's part of the reason consumers rate the VeriSign Secured Seal, the most recognized and trusted security seal in the world.

VeriSign is committed to helping merchants achieve their goals with respect to secure e-commerce:

- **Security and privacy**—VeriSign offers the strongest encryption available to address consumers' concerns about security, safety, and privacy.

VeriSign Is the Solution of Choice for the Thought Leaders in Online Security

- 93 percent of the Fortune 500 use VeriSign.
- Almost 500,000 Web sites have VeriSign SSL Certificates.
- VeriSign serves over 135,000 merchants with payment processing services.
- 94 percent of the top 50 e-commerce sites use VeriSign SSL.
- VeriSign processes over 37 percent of all North American e-commerce.
- VeriSign is the only leading SSL provider to offer 128-bit SGC-enabled SSL, with the strongest encryption available.
- The top 10 U.S. nanks secure their Web sites with VeriSign SSL.
- 83 percent of shoppers are familiar with the VeriSign Secured Seal, more than any other mark, and more than four out of five of those say it is their preferred seal.
- The VeriSign Secured Seal rates best overall worldwide among endorsed programs in terms of consumer trust.
- VeriSign has offered SSL Certificates and Payment Processing Solutions longer than any other company.

- **Reliability and up time**—VeriSign provides solutions that ensure the highest levels of up time and reliable performance for e-commerce sites.
- **Confidence and trust**—VeriSign offers the most recognized and trusted third-party trust mark to inspire consumer confidence and trust.
- **Payment processing integrity**—VeriSign provides world-class security and highly reliable payment processing services from the consumer to the merchant and from the merchant to the network of financial institutions.
- **Quick and easy implementation**—VeriSign offers comprehensive solutions, enjoys a track record of success, has well-developed and tested processes and procedures, and offers industry-leading service and support.

For More Information

General Questions about VeriSign Offerings
Phone: Toll free 1-866-893-6565 or 650-426-5112
Email: internetsales@verisign.com
Web: *www.verisign.com*

Free Trial SSL Certificate
Phone: Toll free 1-866-893-6565 or 650-426-5112
Email: internetsales@verisign.com
Web: *www.verisign.com/prod/srv/trial/intro.html*

Commerce Site or Secure Site Services
Phone: Toll free 1-866-893-6565 or 650-426-5112
Email: internetsales@verisign.com
Web: *www.verisign.com/products-services/security-services/ssl/index.html*

Payment Services
Phone: Toll free 1-888-847-2747 or 650-426-3898 (select option 1)
Email: paymentsales@verisign.com
Web: *www.verisign.com/products/payment.html*

Visit us at www.VeriSign.com for more information.

00020998 06-15-2005