VeriSign®

BUSINESS GUIDE

Everything You Need to Know About SSL Security

Authentication and Encryption—The Cornerstones of Online Security

Where it all comes together.™

CONTENTS

+ Executive Summary 3
+ Overview 4
+ Why Is Authenticated SSL Necessary? 4
+ How Authenticated SSL Certificates Work 6
+ Risk of Unauthenticated SSL Certificates 7
+ How You Can Tell If a Web Site Is Authentic 9
+ The VeriSign Authentication Process 11
+ Why VeriSign Authenticated Practices Are More Trustworthy 12
+ The Benefits to Your Business 12
+ Conclusion 14
+ For More Information 14

Executive Summary

In light of the risks associated with electronic commerce and online communication, it is imperative not only to use secure encryption technology when conducting online business but also to prove one's identity and develop trust relationships with customers and partners.

Building online trust relationships with partners and customers involves being authenticated by a trusted third party and receiving an authenticated Secure Sockets Layer (SSL) Certificate that is signed by that trusted third party. Encryption, the process of transforming information to make it unintelligible to all but the intended recipient(s), forms the basis of data integrity and privacy necessary for online business. Without authentication, however, encryption technology does not sufficiently protect online users. Authentication must be used in conjunction with encryption to provide:

- Confirmation that the organisation named in the certificate has the right to use the domain name included in the certificate
- Confirmation that the organisation named in the certificate is a legal entity
- Confirmation that the individual who requested the SSL Certificate on behalf of the organisation was authorised to do so

Some Certificate Authorities (CAs) believe that encryption alone is enough to ensure a secure Web site and to build trust between you and your customers. But in fact, there is a distinction between authenticated ("high assurance") certificates, which provide trust and security, and unauthenticated ("low-assurance") certificates that threaten consumer confidence and online security. In addition to using encryption technology, it is vital that your Web site is authenticated, which will improve Web visitors' trust in your Web site and in your business.

When you establish your secure Web site with VeriSign, you can take advantage of a wealth of options to further enhance your e-commerce operation. With the VeriSign Secured™ Seal, included with every SSL Certificate, you can display the number-one trust brand on the Internet to give your customers the confidence to communicate and transact business with your site. This seal allows your visitors to check your SSL Certificate's information and status in real time, thus increasing their trust in your online business and increasing your sales and revenues.

VeriSign® SSL Certificate Services offer you the power to secure and e-commerce-enable your site, giving your customer the most trustworthy Web experience possible. Increased trust in the safety of online transactions has numerous benefits, of which increased revenue and profitability are the most important. There are real challenges—and significant opportunities—for online businesses to deliver the same level of trust and personalisation over the Internet as is offered by brick-and-mortar storefronts.

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.

Overview

Until recently, most SSL Certificates could be categorised as medium- to high-assurance certificates, providing three security services: confidentiality, authentication, and integrity. Digital certificates uniquely identify individuals and Web sites on the Internet and enable secure, confidential communications. Unfortunately, some providers of SSL Certificates have elected to provide unauthenticated or low-assurance SSL Certificates in order to lower costs and accelerate order fulfillment. This conflicts with generally accepted industry practices, erodes customer confidence, and serves as a source of confusion for Web site visitors.

"Low-assurance" SSL Certificates provide confidentiality and integrity but lack authentication. In the past, the lock icon in the user's browser was perceived to be a reliable sign of authentication. Today, users are forced to examine the SSL Certificate itself to distinguish between a high-assurance, authenticated certificate and a low-assurance, unauthenticated certificate.

If, for example, a user intends to securely communicate with a Web site bearing an SSL Certificate with the organisation name "ABC Inc.," the user is compelled to check whether the certificate is authenticated by a third party. The SSL Certificate intends to convey assurance that the visited Web site (e.g., *www.abc-incorporated.com*) is definitely an "ABC Inc." Web site and that it is not another entity pretending to be ABC Inc., trying to trick Web site visitors into doing business with them. Only through rigorous authentication can a company prove to its customers and partners that its Web site is authentic and has the right to use the domain name presented on the certificate.

Why Is Authenticated SSL Necessary?

Notions of identity and authentication are fundamental concepts in every marketplace. People and institutions need to get to know one another and establish trust before conducting business. In traditional commerce, people rely on physical credentials—such as a business license or letter of credit—to prove their identities and assure the other party of their ability to consummate a trade.

In the age of e-business, authenticated SSL Certificates provide crucial online identity and security to help establish trust between parties involved in online transactions over digital networks. Regardless of whether commerce takes place in the digital world or in the physical world, the parties involved must be able to answer these questions:

- Who are you? (Requirement of identity.)
- To what community do you belong? Are you a trusted member? (Trust by association.)
- How can you prove your identity? (Validation of identity.)

Customers must be assured that the Web site with which they are communicating is genuine and that the information they send via Web browsers stays private and confidential.

+ Encryption

The Web presents a unique set of trust issues, which businesses must address at the outset to minimise risk. Customers submit information and purchase goods or services via the Web only when they are confident that their personal information, such as credit card numbers and financial data, is secure. The solution for businesses that are serious about e-commerce is to implement a complete e-commerce trust infrastructure based on encryption technology. Encryption, the process of transforming information to make it unintelligible to all but the intended recipient, forms the basis of data integrity and privacy necessary for e-commerce.

+ Authentication

Some CAs believe that encryption is enough to ensure a secure Web site and to build trust between you and your customers. But in fact, encryption is not enough; it is imperative that your Web site is also authenticated, which will improve Web visitors' trust in you and your Web site. Authentication means that a trusted authority can prove that you are who you say you are. To prove that your business is authentic, your Web site needs to be secured by best-of-breed encryption technology and authentication practices.

+ Digital Certificates

A digital certificate is an electronic file that uniquely identifies individuals and Web sites on the Internet and enables secure, confidential communications. Digital certificates serve as a kind of digital passport or credential.

Typically, the "signer" of a digital certificate is a CA (Certificate Authority), such as VeriSign. Some digital certificates are authenticated by trusted authorities, but unfortunately some CAs provide unauthenticated SSL Certificates. This practice exposes online users to the risks of false online storefronts operating on the Internet. As the leading provider of trust services, VeriSign provides authenticated SSL Certificates that secure the trust relationship between you and your clients.

Authenticated SSL Certificates enable a Web site visitor to:

- Securely communicate with the Web site, such that information provided by the Web site visitor cannot be intercepted in transit (e.g., confidentiality) or altered without detection (e.g., integrity)
- Verify that the site the user is actually visiting is the company's Web site and not an impostor's site (e.g., authentication)

VeriSign assures trust by coupling its authentication service with state-of-the-art encryption technology in its digital certificate solutions. Your online business will only be issued an authenticated VeriSign SSL Certificate after:

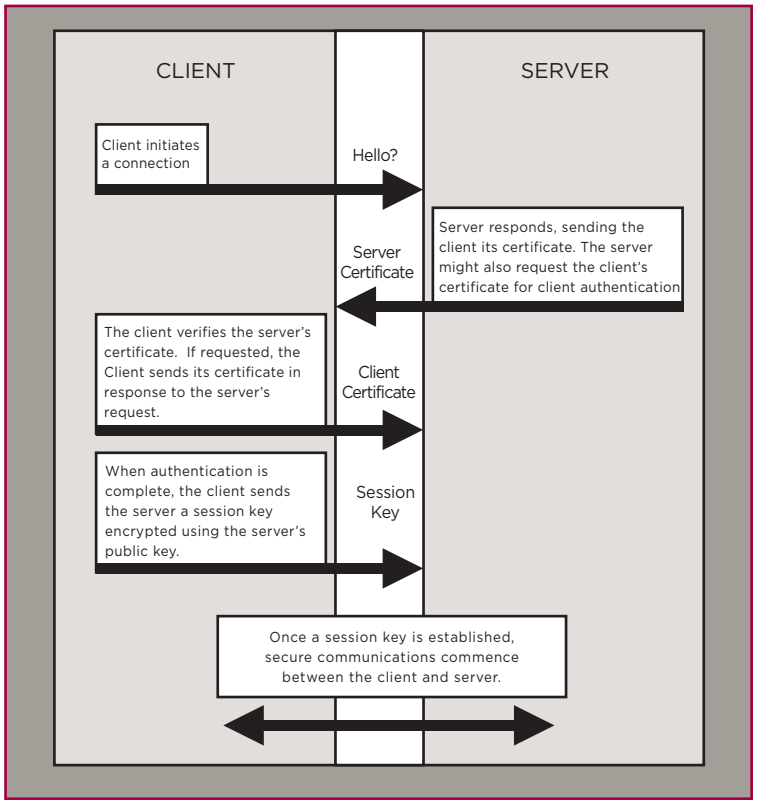
- Verifying your identity and confirming that your organisation is a legal entity
- Confirming that that you have the right to use the domain name included in the certificate
- Verifying that the individual who requested the SSL Certificate on behalf of the organisation was authorised to do so

How Authenticated SSL Certificates Work

An authenticated SSL Certificate allows the receiver of a digital message to be confident of both the identity of the sender and the integrity of the message. Fundamental to the process of issuing high-assurance SSL Certificates to an organisation for use on its Web site are three basic authentication and verification steps:

- Confirmation that the organisation named in the certificate has the right to use the domain name included in the certificate
- Confirmation that the organisation named in the certificate is a legal entity
- Confirmation that the individual who requested the SSL Certificate on behalf of the organisation was authorised to do so

When Web visitors connect to Web sites, they reach one of two kinds of servers. If they reach servers that are secure, they will get messages indicating that fact. Similarly, if they reach servers that are not secure, there will be warnings to that effect. A truly secure Web server is one that has an authenticated SSL Certificate. The authenticated certificate tells users that an independent, trustworthy third party has verified that the server belongs to the company it claims to belong to. A valid authenticated certificate means that users can have confidence that they are sending confidential information to the place to which they think they are sending it.



A Webmaster generates a certificate request, which in turn creates two encrypted keys: one private, one public. The Webmaster sends the public one off to a CA, such as VeriSign. CAs should then make certain that they are issuing certificates to the "correct" company. CAs must ensure:

- That the company they are certifying is the registrant of the Internet domain name they have certified
- That it is registered as a company in one or more countries
- That its registered name is the same as that on the certificate the CA is signing
- That the person requesting the certificate is an employee of that company

Once the verification and background check has been done, the CA signs off on the public key. The public key comes back to the Webmaster, who loads it into the server. As soon as both the private and public keys, a matching pair, align perfectly, the SSL will start functioning. SSL ensures that the information sent by a server is identical to the information received by a Web visitor and that no change has taken place.

Risk of Unauthenticated SSL Certificates

Currently, browsers do not distinguish between high-assurance (e.g., authenticated) and low-assurance (e.g., unauthenticated) SSL Certificates. As long as the SSL Certificate was issued by a trusted CA and the domain name in the certificate matches the domain of the visited Web site, the user will generally trust the SSL Certificate automatically.

The "lock icon" built into the user's browser will appear exactly the same to the user regardless of whether a particular site is using an authenticated high-assurance SSL Certificate or an unauthenticated low-assurance SSL Certificate.

Until recently, this simple approach has worked well and has facilitated the expansion of online commerce. However, recent changes in the SSL Certificate marketplace pose a potential threat to consumer confidence and a security risk in the practice of online commerce. One major risk associated with unauthenticated SSL Certificates is "spoofing." The low cost of Web site design and the ease with which existing pages can be copied makes it all too easy to create illegitimate sites that appear to be secure and published by established organisations. In fact, con artists have illegally obtained credit card numbers by setting up professional-looking storefronts that mimic legitimate businesses, using a deceptively similar domain name, and presented misleading content in order to trick the victim into making an inappropriate security-relevant decision.

Why else is authentication so important? Because fraud on the Internet remains a huge barrier to consumer spending, and a consistent source of fraud results from customers doing business with entities they know little or nothing about.

Here are some facts regarding fraud on the Internet:

- In 2004, the Internet Crime Complaint Center received 207,449 complaints regarding online fraud, a 66.6 percent increase over the previous year.
- According to the Gartner Group, fraud on the Internet is taking its toll on e-tailers. Gartner surveyed more than 160 companies and found that 12 times more fraud exists in Internet transactions than in traditional retail. Moreover, Web merchants bear the liability and costs in cases of fraud, while credit card companies generally absorb the fraud costs for traditional retailers, as long as the retailer follows procedures and saves the signature on the receipt.
- Research from Jupiter Media Metrix showed that fears of online fraud are more common than fraud itself.

"Online shopping gets a bad rap in the press, but most of the stories reported are anecdotal tales of companies that haven't put successful defensive measures in place," says Harry Wolhanlder, VP of Market Research at ActivMedia. "Web businesses running proper screening of customer information are suffering very little, with average fraud losses held to just over one percent. Fraud control is clearly possible online, although many companies do not implement stringent screening and prevention measures."

The following section describes some of the risks of insufficient subscriber authentication by describing two possible scenarios in which secure online business will be at risk.

+ Scenario 1: No Authentication of Organization by the CA

Bad Bob registers *www.abcbankonline.com*, spoofs ABC Global Bank's site, lures unsuspecting

	Option 1	Option 2	Option 3	Option 4
Organisation (O) =	ABC Global Bank	abcbankonline.com	abcbankonline.com	
Common Name (CN) =	abcbankonline.com	abcbankonline.com	abcbankonline.com	abcbankonline.com
Disclaimer	Organization not authenticated	Organization not authenticated		

customers to his spoofed site, and obtains an unauthenticated SSL Certificate. This certificate includes one of the following in the subject-distinguished name (see graphic above).

When a customer visits Bad Bob's "spoofed site" site, the customer has no easy way to know the site is not legitimate. If the customer sees the "lock" icon, he or she may get a false sense of security. He will likely think that he is connected to ABC Global Bank's Web site but really is connecting to Bad Bob's fraudulent site. Seeing the lock icon on an information submission page will make the user more likely to enter his user ID and password. Bad Bob could be intending to capture the user ID and password and then divert the user to the legitimate site.

If the customer looks at the SSL Certificate and sees an "organisation not authenticated" disclaimer or sees that ABC Global Bank was not named in the certificate, Bad Bob will be thwarted. But this assumes that the user will take several additional steps before entering his or her user ID and password or even personal or sensitive information.

Suppose ABC Global Bank registers a domain, *www.abcbank.com*, and implements a legitimate online banking Web site using an SSL Certificate. This certificate includes the following in the subject-distinguished name:

Organisation (O) =	ABC Global Bank
Common Name (CN) =	abcbank.com

Requiring authentication of the organisation guards against the possibility that a malicious individual or entity can obtain a certificate containing another organisation's name. Including an authenticated organisation name in the SSL Certificate provides assurance to users that the organisation that implemented the certificate on its Web site is a legitimate organisation.

+ Scenario 2: No Check of Organization Existence by the CA

Bad Bob registers a domain to Internet Bank Corp. (which does not exist) using a stolen credit card as the method of payment. Bad Bob creates a Web site and obtains an unauthenticated SSL Certificate that gives the appearance of legitimacy to his Web site. A customer will see the browser's "lock icon" and think that his information is secure. If Bob offers higher-than-average interest rates on deposits or attractive financing, he may be able to entice users to provide personal information.

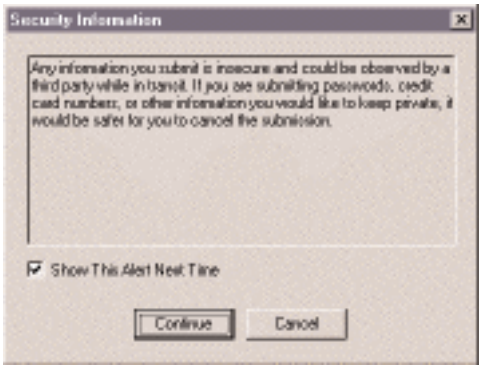
Requiring verification of the organisation's existence guards against the possibility of an individual pretending to be a legitimate organisation.

How You Can Tell If a Web Site Is Authentic

Before submitting information or purchasing goods from an online merchant, you need to know that the company you are doing business with is who it claims to be. While Web sites can buy server certificates from many different CAs, Internet browsers are configured to trust only those server certificates that come from a few highly reputable companies. When you visit an online business that is secured by VeriSign, for example, you can be certain that the site is authentic.

While many consumers and merchants do not fully understand the detailed practices behind VeriSign authentication services, they do know to look for the VeriSign Secured Seal as evidence that a business is real and that its site is a safe place to shop. Every authenticated Web business gets the seal along with their certificate solution to increase customers' confidence in their site.

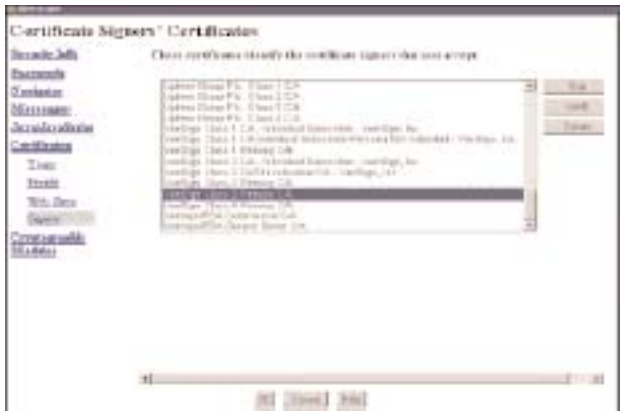
The Microsoft® Internet Explorer and Firefox browsers have built-in security mechanisms to prevent users from unwittingly submitting their personal information over insecure channels. If a user tries to submit information to an unsecured site (a site without an authenticated SSL Certificate), the browsers will by default show a warning, which can make the purchase process seem threatening.



VeriSign certificates prove your identity when processing electronic transactions much in the way a drivers' license or a passport does in face-to-face interactions. With a VeriSign SSL Certificate, you can assure customers that the electronic information they receive from you is authentic.

Above is an example of a particular SSL Certificate, viewed in Netscape Communicator v4.0.

Begin by clicking the "Security" toolbar icon



Choose Certificate Signers and view the list of certificates.

The VeriSign Authentication Process

VeriSign has established authentication and verification procedures to help merchants grow their online businesses, inspiring trust and confidence in consumers by verifying online merchants' identities and reducing the risk of fraud. These procedures are the result of years of operating trusted infrastructure for the Internet and authenticating over half a million businesses. To appreciate the power and trustworthiness of this process and the benefits it can have on your growing online business, an outline of the VeriSign authentication process is presented below:

+ Step 1

Individuals and businesses initiate authentication by providing information to VeriSign as part of the fast, convenient online process for purchasing digital certificate solutions.

+ Step 2

VeriSign then verifies that:

- The organisation and organisational contact personnel are not listed on any of the three U.S. government denied entity lists: Denied Persons List, Denied Entities List, U.S. Treasury Department List
- The organisation has government-issued credentials such as articles of incorporation or a business license that allow it to conduct business
- The organisation owns the domain name for which the certificate is issued OR has obtained legal right to use that domain name from the owner of the domain
- The organisation's corporate contact personnel can be verified via a third-party number as an employee of the organisation that is ordering the certificate

+ Step 3

VeriSign issues the certificate in compliance with VeriSign Operations Policies, which dictate:

- Separation of Duties: two different VeriSign employees must complete authentication of the organisation applying for the certificate and verification of the corporate contact's employment
- All VeriSign employees that process digital certificates must pass extensive criminal and financial background checks
- "Department-of-Defense-grade security" with biometrics are required for all facilities where digital certificates are processed
- All customer data is strictly confidential and data centers containing customer information are housed in highly secure locations with biometrics

+ Step 4

Once a VeriSign SSL Certificate has been issued and the authenticated Web business installs it on its Web server, visitors to the site can instantly access the authentication data. This data assures Web site visitors that the site is what it appears to be and belongs to a real business simply by clicking on the lock icon or on the VeriSign Secured Seal, which is provided to every Web site equipped with an SSL Certificate.

Why VeriSign Authentication Practices Are More Trustworthy

The VeriSign authentication process is efficient and secure: we offer the fastest possible turnaround time on certificate requests *without* compromising the reliability of our process.

Before issuing an SSL Certificate, VeriSign reviews your credentials and completes a thorough background checking process to ensure that your organisation is what it claims to be and is not claiming a false identity. Then VeriSign issues your organisation an authenticated SSL Certificate, which is an electronic credential that your business can present to prove its identity or right to access information.

The Benefits to Your Business

After you install your VeriSign certificate, your server automatically activates SSL technology, creating an authenticated, secure communication channel between your server and your customer's browser. Your site can communicate securely with any customer who uses Netscape Navigator, Microsoft Internet Explorer, and most popular email programs. Once activated by your server certificate, SSL immediately begins providing you with the following benefits of secure online transactions:

+ Attracting Customers

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. With the VeriSign Secured Seal, included with every SSL Certificate, you can display the number-one trust brand on the Internet to give your customers the confidence to communicate and transact business with your site. This seal allows your visitors to check your SSL Certificate's information and status in real-time and provides additional protection against the misuse of revoked and expired certificates.

VeriSign secures more Web servers than any other company in the world—more than 800,000. This diverse universe of customers includes over 93% of the Fortune 500, 47 of the world's 50 biggest e-commerce sites and the world's 40 largest banks.

The number of VeriSign-secured sites is so large, and faith in the VeriSign Secured Seal is so great, that more than 65,000 Web sites currently display the VeriSign Secured Seal, which is viewed over 100 million times a day. The seal provides evidence to customers that the Web site they are visiting has been authenticated as a real business and is secured with SSL encryption technology.

What is the ultimate result of a VeriSign server certificate on your site? Ensuring safe online transactions that protect both 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 refute later.

VeriSign Secure Site Services offer you the power to secure and e-commerce-enable your site, giving your customer the most trustworthy Web experience possible. Increased trust in the safety of online transactions has numerous benefits, of which increased revenue and profitability are the most important.

+ Authentication

By checking your VeriSign certificate, your customers can verify that the Web site belongs to you and not an impostor. This fact establishes their confidence to submit 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 transmit the session key to the consumer securely, 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 unauthorised parties intercept it.

+ 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 each seeing is exactly what the other party sent.

Conclusion

Some CAs believe that encryption without authentication is enough to ensure a secure Web site and to build trust between you and your customers. But encryption alone is not sufficient.

Unauthenticated SSL Certificates provide confidentiality and integrity but lack the third-party authentication necessary to:

- Verify that the user is actually visiting the company's Web site and not an impostor's site
- Allow the receiver of a digital message to be confident of both the identity of the sender and the integrity of the message
- Ensure safe online transactions that protect both customers and your business

For these reasons, it is critical that your Web site is authenticated, which will improve Web visitors' trust in you and your Web site. Furthermore, if certificates can be issued to unauthorised parties, the trustworthiness of legitimate certificates is diminished. Requiring verification of the certificate applicant's authority to request a certificate (e.g., employment with the organisation named in the certificate), guards against the threat of issuing a certificate to a malicious individual who is not associated with the organisation.

An authenticated SSL Certificate from VeriSign provides the ultimate in credibility for your online business. Our rigorous authentication practices set the industry standard to provide assurance that:

- Subscribers are properly identified and authenticated
- Subscriber certificate requests are accurate, authorised, and complete

And, by displaying the VeriSign Secured Seal, you can give your customers the confidence to communicate and transact business with your site. The VeriSign Secured Seal allows your visitors to check your SSL Certificate's information and status in real time and provides additional protection against the misuse of revoked and expired certificates.

VeriSign's rigorous authentication practices, as well as our leading-edge cryptographic techniques and ultra-secure facilities, are designed to maximise you and your customers' confidence in our services. These practices, technology, and infrastructure are the foundation for server certificates to secure transactions, working in conjunction with your Web server.

For More Information

To speak with a VeriSign security expert, please call +61 3 9674 5555,
or, contact a VeriSign representative via email at sales@verisign.com.au

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

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo VeriSign Secured, the VeriSign Secured logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Microsoft is a trademark of Microsoft Corporation. Netscape and Navigator are trademarks of Netscape.

00017655 05-24-2005