



BUSINESS GUIDE



VeriSign® Managed PKI for SSL  
Strong Security for Multiple  
Server Environments



Where it all comes together.™



**CONTENTS**

+ Introduction	3
+ Security Solutions— The Digital-Certificate System	3
A Brief Review of SSL	4
SSL—The Protocol	4
What is a an SSL Certificate?	4
How Do SSL Certificates Work?	5
What Do End Users See?	6
+ The Needs of Your Organization	9
The Size of Your Network	9
Change within Your Network	9
Cross-Departmental Coordination	9
The Needs of Your End Users	9
+ The Managed PKI for SSL System	10
The Managed PKI For SSL Administrator	10
Instant Enrollment For SSL Certificates	10
+ For More Information	11
Other VeriSign Solutions	11
+ Appendix A—Supported Servers	12
Managed PKI For SSL—Supported Servers	12
Managed PKI For SSL—Premium Edition	13



## Introduction

---

In today's businesses, electronic communication is a central part of the everyday flow of information, and privacy is a top priority. Whether your company conducts sales over the Internet or hosts a company-specific network, you want to know that your communications are safe from unauthorized interference.

For information exchange between servers and client browsers and server-to-server, load balancing devices and Secure Sockets Layer (SSL) accelerators, SSL Certificates from VeriSign have become recognized as the bottom line in security. Working with the SSL protocol for encryption, SSL Certificates protect businesses against site spoofing, data corruption, and repudiation of agreements. They assure customers that it is safe to submit personal information, and provide colleagues with the trust they need to share sensitive business information.

For companies with multiple servers and load balancing devices in their network, VeriSign now offers the option of locally managing your SSL Certificates with VeriSign® Managed PKI for SSL. If you need to secure five or more servers, enrollments and cancellations can become cumbersome when managed one by one. With Managed PKI for SSL, you save money by purchasing your SSL Certificates in bulk, then save time by issuing your own certificates to servers and load balancing devices within your organization. You can customize your end-user support to meet your company-specific needs, and integrate your server and client security systems. With Managed PKI for SSL, VeriSign provides the technical tools and back-end support you need, while an administrator at your site manages your secure network from day to day. In other words, you get VeriSign-strength security within your own control.

This paper provides you with a basic introduction to digital-encryption technology and SSL Certificates from VeriSign. It then describes the reasons that you would want to consider Managed PKI for SSL as an alternative to one-by-one purchasing. Finally, it will present the features you can expect if you decide Managed PKI for SSL is right for your organization.

## Security Solutions— The Digital-Certificate System

---

Given the security risks involved in conducting business online, what does it take to make your Internet transactions and company communications safe? Industry leaders agree that the answer is the VeriSign SSL Certificate. VeriSign has issued over 450,000 SSL Certificates. Companies using VeriSign SSL Certificates include 90 of the Fortune 100 companies and all of the Relevant Knowledge, Inc., Top 20 Commerce Sites.

### + A Brief Review of SSL

Netscape Communications originally developed SSL in 1994 at the same time that the original Web browser, Netscape® Navigator® was launched. SSL was thereafter included in every version of the Netscape browser and thus gained distribution in millions of computers worldwide. Microsoft used SSL V2.0 as the model for the development of the PCT (Private Communications Technology) protocol that was embedded in the Internet Explorer browser. In 1996, SSL V3.0 was introduced including some features that had originally appeared in PCT as well as features related to user validation and data confidentiality. Netscape turned over SSL V3.0 to the Internet Engineering Task Force (IETF), the large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF has “officially” renamed SSL to TLS (Transport Layer Security) and is working on several RFCs seeking wider adoption of the TLS protocol and approach.

### + SSL—The Protocol

SSL is implemented as an intermediate network layer, operating between the TCP/IP (Transmission Control Protocol/Internet Protocol) network layer and the application level layer, where other protocols such as HTTP (Hypertext Transfer Protocol) or IMAP (Internet Message Access Protocol) operate. A “socket” in the context of “Secure Sockets Layers” refers to the connection established between a client and a server.

**Network**—TCP/IP facilitates the delivery of network packets between network points. TCP/IP is a peer to peer protocol (e.g., a client connects to a server). The life of such a connection is determined by the duration of the particular exchange.

**Application Layer**—The application layer refers to a common protocol that applications utilize to communicate over an established TCP/IP connection. In the case of browsers and servers, the HTTP protocol is used. Application layer communications are initiated when a client establishes a TCP/IP connection with a server.

**SSL Layer**—SSL is used to authenticate endpoints and secure the contents of the application level communication. The SSL transaction initiation (handshake) establishes the identity of the peers as well as an encryption method and key in a secure manner. The application level communication can then commence. All incoming traffic is decrypted by the SSL layer and passed on to the application; similarly outgoing traffic is encrypted by the SSL layer before transmission.

It is important to note that while typically HTTP applications operate on server port 80, SSL secured HTTP (HTTPS) applications operate on port 443.

### + What Is a an SSL Certificate?

An SSL Certificate is the electronic equivalent to a passport or business license. It is a credential, issued by a trusted authority, that individuals or organizations can present electronically to prove their identity or their right to access information.

When a Certification Authority (CA) such as VeriSign issues SSL Certificates, it verifies that the owner is not claiming a false identity. Just as when a government issues a passport it is officially vouching for the identity of the holder, when a CA gives your business a digital certificate it is putting its name behind your right to use your company name and Web address.

### + How Do SSL Certificates Work?

The solution to problems of identification, authentication, and privacy in computer-based systems lies in the field of cryptography. Because of the non-physical nature of electronic communication, traditional methods of physically marking transactions with a seal or signature are useless. Rather, some mark must be coded into the information itself in order to identify the source and provide privacy against eavesdroppers.

One widely used tool for privacy protection is what cryptographers call a “secret key.” Log-on passwords and cash card PINs are examples of secret keys. Consumers share these secret keys only with the parties they want to communicate with, such as an online subscription service or a bank. Private information is then encrypted with this password, and it can only be decrypted by one of the parties holding that same password.

Despite its widespread use, this secret-key system has some serious limitations. As network communications proliferate, it becomes very cumbersome for users to create and remember different passwords for each situation. Moreover, the sharing of a secret key involves inherent risks. In the process of transmitting a password, it can fall into the wrong hands. Or one of the sharing parties might use it maliciously and then deny all action.

SSL-Certificate technology addresses these issues because it does not rely on the sharing of secret keys. Rather than using the same key to both encrypt and decrypt data, an SSL Certificate uses a matched pair of keys, which are unique complements to one another. In other words, what is done by one key can only be undone by the other key in the pair.

In this type of key-pair system, your “private key” gets installed on your server and can only be accessed by you. Your “public key” gets widely distributed as part of an SSL Certificate. Customers, partners or employees who want to communicate privately with your server can use the public key in your SSL Certificate to encrypt information, and you are then the only one who can decrypt that information. Since the public key alone does not provide access to communications, you do not need to worry about who gets hold of this key.

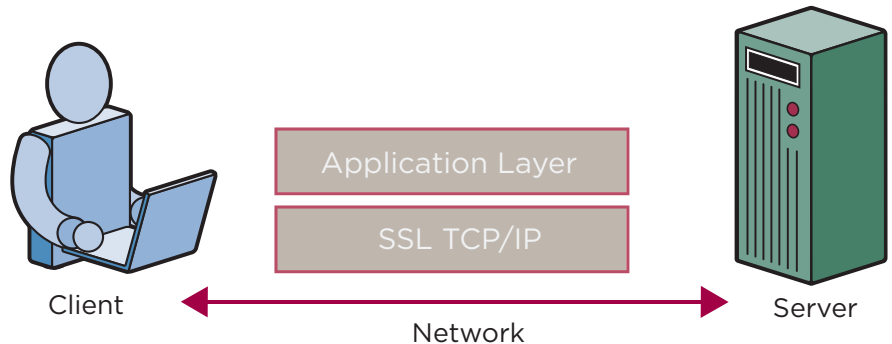
Your SSL Certificate tells customers and correspondents that your public key in fact belongs to you. Your SSL Certificate contains your name and identifying information, your public key, and VeriSign’s own digital signature as certification.

VeriSign SSL Certificates allow any server to implement the SSL protocol, which is the standard technology for secure Web-based communications. SSL capability is built into server hardware, but it requires a digital certificate in order to be functional. With the latest SSL and an SSL Certificate, your Web site will support the following functions:

- **Mutual Authentication**—The identity of both the server and the customer can be verified so that all parties know exactly who is on the other end of the transaction.
- **Message Privacy**—All traffic between the server and the customer is encrypted using a unique “session key.” Each session key is only used with one customer during one connection, and that key is itself encrypted with the server’s public key. These layers of privacy protection guarantee that information cannot be intercepted or viewed by unauthorized parties.
- **Message Integrity**—The contents of all communications between the server and the customer are protected from being altered en route. All those involved in the transaction know that what they’re seeing is exactly what was sent out from the other side.

The diagram below illustrates the process that guarantees protected communications between a server and a client. All exchanges of digital certificates happen within a matter of seconds and appear seamless to the client.

Figure 1

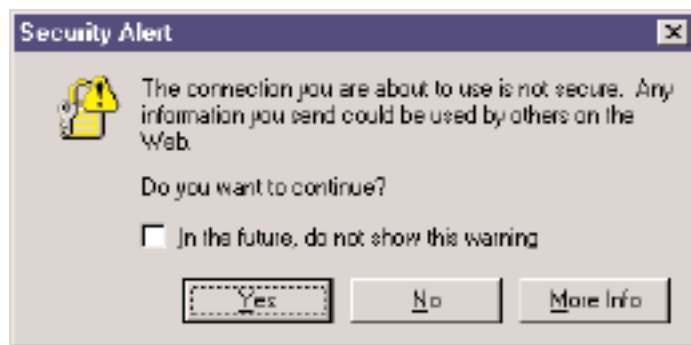


All of this technology translates to online communications that are safe for you and your customers. End users know exactly who they are dealing with and feel comfortable that the information they send is not falling into unknown hands. You know that your server is receiving accurate transmissions that have not been tampered with or viewed en route.

**+ What Do End Users See?**

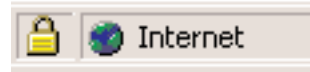
Both the Netscape Navigator and the Microsoft® Internet Explorer browsers have built-in security mechanisms to prevent users from unwittingly submitting sensitive information over insecure channels.

If a user tries to submit information to an unsecured site, the browsers will, by default, show a warning such as the following:



By contrast, if a user attempts to submit information to a site with a valid SSL Certificate and an SSL connection, no such warning is sent. Furthermore, both the Microsoft and Netscape browsers provide users with a positive visual clue that they are at a secure site.

In Netscape Navigator 3.0 and earlier, the key icon in the lower left hand corner of the browser, which is normally broken, is made whole. In Netscape Navigator 4.0 and later, as well as in Microsoft Internet Explorer, the normally open padlock icon becomes shut, as shown below:

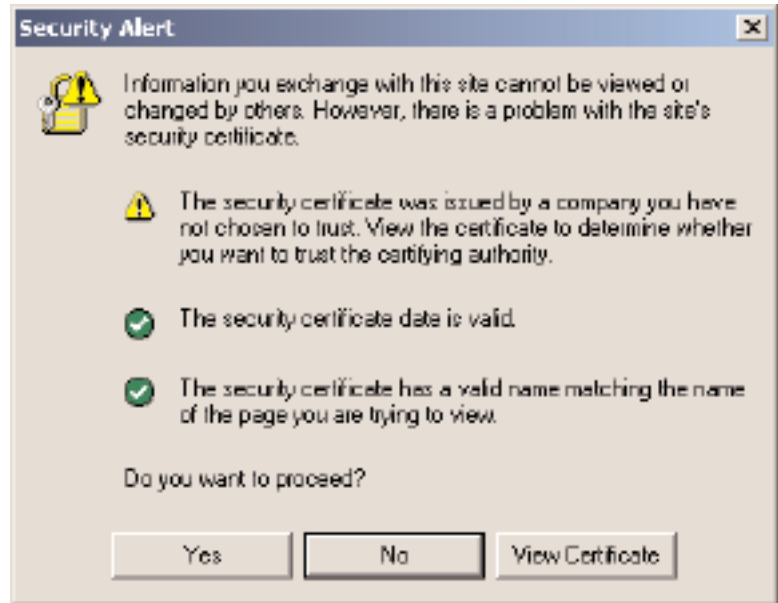


For more information, users may visually inspect the site's SSL Certificate by double clicking on the security icon. They will then see a display like the following:

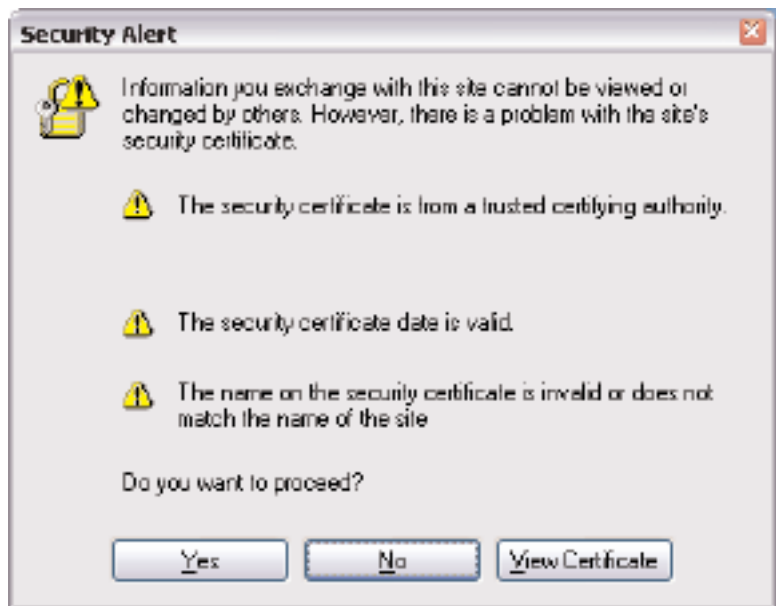


This SSL Certificate display establishes that the site (webtrust.resource-marketing.com) really does belong to Resource Marketing, Inc. of Fort Thomas, Kentucky. It also establishes that VeriSign issued the SSL Certificate and is vouching for the site's validity.

These positive visual cues only occur if the site has a valid digital certificate, issued by a Certificate Authority that is trusted by the browser. Technically, this means the CA's public key must be listed in the browser's directory of trusted roots. VeriSign public keys are bundled with 98 percent of all of the browsers in use today. By contrast, if a site has a certificate issued by an untrusted authority, the browser will display a warning such as the following:



Similarly, if a site is falsifying its claim to a certificate (e.g. if *www.hacker.com* tries to use a certificate for *www.bookstore.com*), the user will also receive a warning, such as the following:



When you install a VeriSign SSL Certificate on your server and enable SSL, your customers and partners see clearly that they are operating in a secure environment.

## The Needs of Your Organization

Once you have decided to invest in the peace of mind that comes with VeriSign SSL Certificates, you will need to decide whether one-by-one purchasing or Managed PKI for SSL meets the needs of your organization. Following are several factors you should consider.

### + The Size of Your Network

If your company will be hosting five or more servers within the next year, you are a good candidate for Managed PKI for SSL. You can begin with five SSL Certificates and the administrator's kit. This should meet your current needs plus your renewals for later in the year. You will save money through a bulk discount, while increasing efficiency significantly by eliminating the need to enroll and pay separately for each SSL Certificate.

An administrator may select to associate a certificate with up to 20 servers. Furthermore, the administrator may specify the life of the certificate to be either one or two years.

### + Change within Your Network

If you want the ability to expand, reduce, or restructure your network with no hassle, Managed PKI for SSL is the answer. With one-by-one purchasing, each addition, renewal, or cancellation of a secure server must go through the VeriSign service center. Each SSL Certificate requires 3–5 business days to be issued and must be paid for with a separate credit card processing or purchase order. When you purchase in bulk through Managed PKI for SSL, your Managed PKI for SSL administrator can issue and cancel SSL Certificates instantly, giving you superior control of your operations, especially in critical times.

### + Cross-Departmental Coordination

If several groups within your organization are likely to work with secure servers, Managed PKI for SSL will simplify and enhance your information system management. When server hosts from each department apply separately for SSL Certificates from VeriSign, the result can be disorganization, compromising both the efficiency and integrity of your network's security. A department might "reinvent the wheel" that has already been invented within the company, or alternatively a group might assume that a given security issue is being handled elsewhere and thus fail to address it. With one administrator distributing SSL Certificates as the need arises, you reduce the possibility for overlap or lapse in the security of your electronic communications.

### + The Needs of Your End Users

Would your end users benefit from a Web and email interface that is designed for their specific use? With Managed PKI for SSL, VeriSign provides a hosted environment for the applicable enrollment pages certain features of which can be customized. With one-by-one management, each person hosting a secure server interacts with the VeriSign system for enrollment, renewal, and cancellation. This interface, while straightforward and user-friendly, is designed for general use with any server.

If you purchase your SSL Certificates through Managed PKI for SSL, your package includes VeriSign enrollment and support screens. You can provide instructions specific to your server software, your organizational structure, or other company specifics. You can design certain features of the look and feel to better accommodate the interface your users are comfortable with, and even integrate it with your personal SSL Certificate interface if you use Managed PKI for SSL to issue digital certificates to individuals.

When your users need technical support, they can immediately access the Managed PKI for SSL administrator within your organization. If the problem cannot be addressed locally, the Managed PKI for SSL administrator can always contact a member of the support team at VeriSign.

## The Managed PKI for SSL System

Managed PKI for SSL is designed to be easily installed and administered. The following features provide the backbone of your network security system.

### + The Managed PKI for SSL Administrator

When you use Managed PKI for SSL to manage your secure network, an administrator within your organization oversees a local control center to issue SSL Certificates. This Managed PKI for SSL administrator, using a standard PC with a browser, purchases Managed PKI for SSL from VeriSign and receives the Administrator's Kit. Before issuing the Administrator's Kit, VeriSign conducts the necessary background checks to ensure that your organization is legitimate and has the right to use the domain names being secured.

The Administrator's Kit includes all of the software necessary to establish the Managed PKI for SSL Control Center on the administrator's PC. It also includes an optional smart-card reader and a Managed PKI for SSL Administrator ID stored on a smart card.

Once the administrator's kit is installed and the Control Center is up and running, you are ready to start issuing SSL Certificates.

### + Instant Enrollment for SSL Certificates

The local Control Center allows users within your network to receive SSL Certificates without any manual intervention from VeriSign. Since VeriSign has already verified your company and domain names, the only approval necessary is from the Managed PKI for SSL Administrator at your organization. The enrollment process goes as follows:

- A user within your network generates a Certificate Signing Request (CSR) on the server being secured.
- The user submits the CSR, along with the necessary enrollment forms, to the VeriSign SSL Certificate Center.
- VeriSign instantly and automatically sends a pending request to the Managed PKI for SSL Control Center at your organization.
- The Managed PKI for SSL Administrator within your organization validates the user's enrollment request.
- VeriSign generates an SSL Certificate and sends it to the user's email address.
- The user downloads the SSL Certificate and installs it on the server.

All communications with VeriSign occur in protected SSL sessions and are thus safe for your company.

## For More Information

---

For the strongest, most reliable protection of your client-browser communications, VeriSign SSL Certificates are widely recognized as the industry standard. SSL Certificates allow your Internet site or corporate network to enable SSL encryption, which authenticates your server and guarantees against alteration and interception of data.

For SSL Certificate protection on multi-server networks, Managed PKI for SSL makes managing your SSL Certificates less expensive and more efficient, and enhances coordination within your organization. Managed PKI for SSL provides the options of customized end-user support, private label certification, and Managed PKI for SSL for issuing digital certificates to individuals integration, making it the security system that fits the unique needs of your company.

To learn more about Managed PKI for SSL, contact a VeriSign sales representative at 650-426-5115.

### + Other VeriSign Solutions

VeriSign Managed PKI allows an organization to issue digital certificates to individuals within its network. These SSL Certificates can replace password log-on to a company network and allow your Web site to control who accesses its content. Personal SSL Certificates also make it possible to send digitally signed and encrypted email, using the S/MIME (Secure Multipurpose Internet Mail Extension) protocol.

If your company already uses Managed PKI services to issue digital certificates to individuals within its network, or if you are interested in doing so, you can integrate this system with your Managed PKI for SSL Certificate management. The Managed PKI Administrator's Kit gives you the option of controlling all certificates from one Control Center.

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**

## Appendix A—Supported Servers

VeriSign has made an exceptional effort to support almost all the available servers that our customers may use. Below is a complete list of server vendors that Managed PKI for SSL supports. We strive to add server vendors to this list, so if you do not see a specific one that you may be interested in please contact VeriSign to obtain the latest support status.

### + Managed PKI for SSL—Supported Server Vendors

Microsoft	Netscape	Apache
iPlanet	Advanced Businesslink	AliBaba(WarpGroup)
AOL/Navisoft	Aventail	Backweb
BEA WebLogic	Beyond Software	Brokat
C2Net Apache SSL-US	Cacheflow	Compaq
Consensus	Control Data Systems	Covalent
Dascom	Domino	F5
Frontier Technologies	Gradient	Hummingbird
I/NET	IBM	Information Builders
Information Hyperlink	Ingrian Networks	Intel
Internet Factory	Iserver	JavaSoft
Lotus	Marimba	Microsoft FrontPage 98
Microsoft Visual InterDev 6.0	Mirapoint	Mitem
Nanoteq	NetCentric	Netscreen
Nokia	Novell	Open Market
OpenConnect Systems	Oracle	O'Reilly & Associates
Process Software	Purveyor	Quarterdeck/StarNine
r3	Radnet	Red Hat
Roxen	SilverStream Software	Sirius Software
Sonic WALL	Sterling Software	Stronghold (C2Net)
Sun Microsystems	Tandem	Tektonic
Tempest Software	Tenon (WebTen)	Thawte Consulting
Unify	Unisys	Unwired Planet
Velocity Software	Volera	Wall Data
WebMethods	WebSphere	WebSTAR
Zeus		