VeriSign®

Strong Security on Multiple Server Environments

Where it all comes together.™

CONTENTS

Where it all comes together.™

+ 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 unauthorised interference.

For information exchange between servers and client browsers and server-to-server, load balancing devices and SSL accelerators, SSL Certificates from VeriSign, Inc. have become recognised as the bottom line in security. Working with the Secure Sockets Layer (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 Managed PKI for SSL. If you need to secure five or more servers, enrolments 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 IDs to servers and load balancing devices within your organisation. You can customise 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 ID 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 organisation.

+ Security Solutions - The Digital ID System

Given the security risks involved in conducting business on-line, what does it take to make your Internet transactions and company communications safe? Industry leaders agree that the answer is the VeriSign Digital ID or SSL Certificate. VeriSign has issued over 485,000 Digital IDs. Companies using VeriSign's Digital IDs include 90 of the Fortune 100 companies and all of the Relevant Knowledge Inc. Top 20 Commerce Sites.

SSL stands for Secure Sockets Layer. A socket in this context refers to the connection established between a client and a server.

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 million 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 (IEFT), 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 as 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 network layer and the application level layer (where other protocols such as HTTP or IMAP operate).
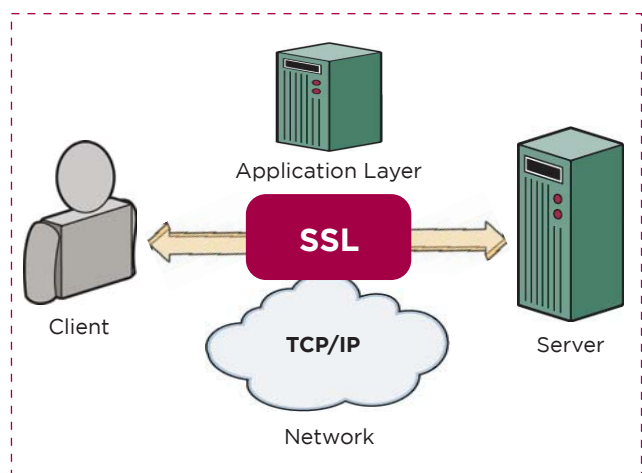
Network - TCP/IP facilitates the delivery of network packets between network points. TCP/IP is a peer to peer protocol (e.g. a client connects to a server). The life of such a connection is determined by the duration of the particular exchange.

Application Layer - The application layer refers to a common protocol that applications utilise 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.

How Is a Digital ID?
A Digital ID, also known as a digital certificate or SSL certificate, is the electronic equivalent to a passport or business license. It is a credential issued by a trusted authority that individuals or organisations can present electronically to prove their identity or their right to access information.

When a Certification Authority (CA) such as VeriSign issues Digital IDs, 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 Digital IDs Work?
The solution to problems of identification, authentication and privacy in computer-based systems lies in the field of cryptography. Due to 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 on-line 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.

Digital ID 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, a Digital ID 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 a Digital ID. Customers, partners or employees who want to communicate privately with your server can use the public key in your Digital ID 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 Digital ID tells customers and correspondents that your public key in fact belongs to you. Your Digital ID contains your name and identifying information, your public key and VeriSign's own digital signature as certification.

How Do SSL Certificates Work?
VeriSign SSL Certificates allow any server to implement the Secure Sockets Layer (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 a SSL Certificate, your website 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 unauthorised 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.
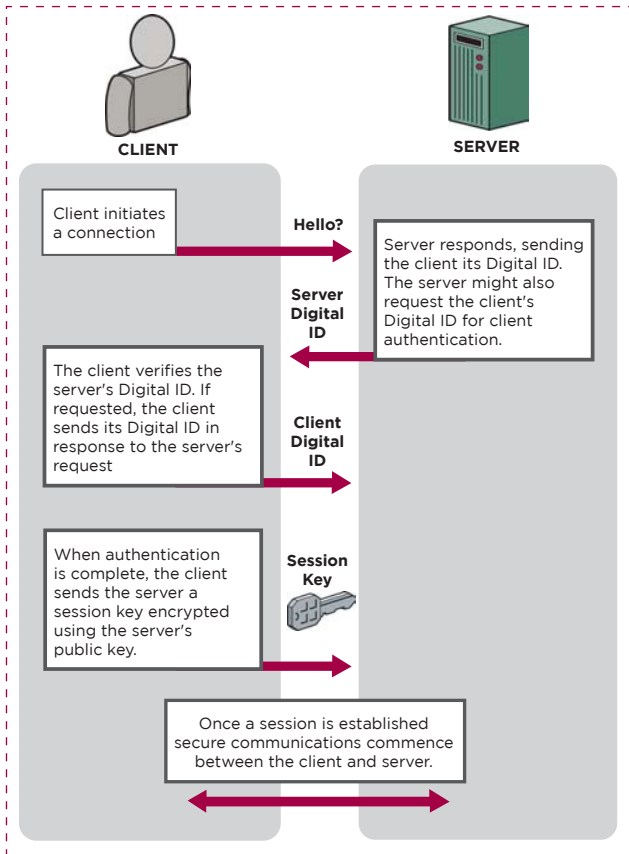
All of this technology translates to online communications that are safe for you and your customers. End users know exactly who they are dealing with and feel comfortable that the information they send is not falling into unknown hands. You know that your server is receiving accurate transmissions that 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 show a warning by default, 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 similar to 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's 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 Organisation
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 organisation. Following are several factors you should consider.

The Size of Your Network
If your company will be hosting 10 or more servers within the next year, you are a good candidate for Managed PKI for SSL. You can begin with 10 SSL Certificates and the administrator's kit. This should meet your current needs as well as additional needs for the next 12 months. You will save money through a bulk discount, while increasing efficiency significantly by eliminating the need to enrol and pay separately for each SSL Certificate.

An Administrator may select to license a certificate with up to twenty (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 VeriSign's service centre. 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 organisation 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 disorganisation, 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 overlaps or lapses in the security of your electronic communications.

The Needs of Your End Users

Would your end users benefit from a Web and e-mail interface that is designed for their specific use? With Managed PKI for SSL, VeriSign provides a hosted environment for the applicable enrolment pages, certain features of which can be customised. With one-by-one management, each person hosting a secure server interacts with the VeriSign system for enrolment, 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's enrolment and support screens. You can provide instructions specific to your server software, your organisational 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 Digital ID 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 organisation. 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 organisation oversees a local control centre 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 organisation 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 Centre 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 Centre is up and running, you are ready to start issuing SSL Certificates.

Instant Enrolment for SSL Certificates

The local Control Centre 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 organisation. The enrolment process goes as follows:

1. A user within your network generates a Certificate Signing Request (CSR) on the server being secured.

2. The user submits the CSR, along with the necessary enrolment forms, to the VeriSign Digital ID Centre.

3. VeriSign instantly and automatically sends a pending request to the Managed PKI for SSL Control Centre at your organisation.

4. The Managed PKI for SSL Administrator within your organisation validates the user's enrolment request.

5. VeriSign generates a SSL Certificate and sends it to the user's e-mail address.

6. 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 recognised 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 cheaper and more efficient and enhances coordination within your organisation. Managed PKI for SSL provides the options of customised 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 0800 032 2101 or visit VeriSign on the Web at http://www.verisign.co.uk/products-services/security-services/ssl/sslcertificates/index.html.

Other VeriSign Solutions

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

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

+ Appendix A - Supported Servers

VeriSign has made an exceptional effort to support almost all the available servers that our customers may utilise. Below we provide a complete list of the supported servers for the customer's edification. We strive to add servers 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 SERVERS

- Advanced Businesslink
- Ingrian Networks
- Quarterdeck/StarNine
- AliBaba (WarpGroup)
- Intel
- Red Hat
- AOL/Navisoft
- Internet Factory
- r3
- Apache Freeware with SSLeay
- iPlanet
- Radnet
- Aventail
- Iserver
- Roxen
- BEA WebLogic
- JavaSoft
- s2
- Backweb
- Lotus
- SilverStream Software

- Beyond Software
- Luckman
- Silver Stream
- Brokat
- Marimba
- Sirius Software
- C2Net Apache SSL-US
- Microsoft
- Sonic WALL
- Cacheflow
- Microsoft FrontPage 98
- Sterling Software
- Compaq
- Microsoft Visual InterDev 6.0
- Stronghold (C2Net)
- Compuserve/Spry
- Mirapoint
- Sun Microsystems
- Connect - OneServer
- Mitem
- Tandem

- Consensus
- Nanoteq
- Tektonic
- Control Data Systems
- NetCentric
- Tempest Software
- Covalent
- Netscape
- Tenon (WebTen)
- Dascom
- Netscreen
- Transarc
- F5
- Netscape Merchant
- Thawte Consulting
- Frontier Technologies
- Nokia
- Unify
- FTP Software
- Novell
- Unisys

MANAGED PKI FOR SSL - SUPPORTED SERVERS (CONTINUED)

- GLACI
- OpenConnect Systems
- Unwired Planet
- Gradient
- Open Market
- Velocity Software
- Hummingbird
- Oracle

- Volera
- IBM
- O'Reilly & Associates
- Wall Data
- I/NET
- Preview Software
- WebMethods
- Information Builders

- Process Software
- WebSTAR
- Information Hyperlink
- Purveyor
- Zeus
- V1 Server

MANAGED PKI FOR SSL - PREMIUM EDITION[1]

- AOL
- Intel
- Silver Stream
- Apache
- iPlanet
- Sonic WALL
- Aventail
- Lotus
- O'Reilly WebSite 2.5 (or higher)
- BEA WebLogic
- Microsoft

- C2Net Stronghold
- Microsoft FrontPage 98
- Red Hat
- Cacheflow
- Microsoft Visual InterDev 6.0
- Tandem
- Compaq
- Mirapoint
- Velocity Software
- Covalent
- Nanoteq

- WebMethods
- F5
- Netscape
- Zeus
- Hummingbird
- Netscreen
- IBM HTTP
- Nokia
- Ingrian Networks

1 Previously referred to as Global Server Certificate 128-bit