VeriSign®
The Value of Trust℠

Licensing VeriSign Certificates: Securing Multiple Web Server and Domain Configurations

CONTENTS

INTRODUCTION

To fully leverage the potential of the Internet as an efficient, far-reaching medium for electronic communications, business, and commerce, enterprises and service providers need a commonly accepted framework for securing online applications that can build a consistent expectation of trust for the user or consumer. Today, most enterprises rely on Secure Sockets Layer (SSL) certificates for that framework. SSL-based digital certificates enable users to authenticate Web sites, digitally sign documents, and encrypt sensitive data.

To reliably provide these functions, SSL certificates must be used in technically sound configurations that adhere to basic principles of trust. As enterprises and service providers enhance their Web sites and extranets with new technology to reach larger audiences, server configurations have become increasingly complex. Enterprises and service providers must not only support SSL digital certificates for authentication and encryption capabilities, but also accommodate multiple domains and sub-domains, load balancing, and SSL acceleration requirements.

As the leading supplier of trust services for the Internet, VeriSign has successfully issued SSL digital certificates to secure hundreds of thousands of Web sites using a wide range of network configurations. VeriSign's best practices and licensing requirements protect the use of its products and services to ensure a common, high-level standard of security across all types of configurations. This document explains the licensing and proper use of VeriSign® SSL certificates for securing multiple Web servers and/or multiple domains and sub-domains in the following network configurations:

- Redundant server backups
- Multiple servers supporting multiple site names
- Multiple servers supporting a single site name
- Networks using SSL acceleration
- Virtual and shared hosting configurations

VERISIGN LICENSING

To provide a reliable, scalable infrastructure that enables secure communications, transactions, and document exchange across the Internet, many enterprises rely on VeriSign SSL certificates to secure multiple domains and Web servers.

Proper licensing and use of VeriSign Server IDs ensure that certificates reliably provide their intended function uniformly across all types of deployments, allow subscribers to legitimately use VeriSign products, and entitle them to the NetSure® Protection Plan (see "NetSure® Protection Plan" sidebar).

VeriSign has published its licensing requirements in the following legal documents, which are all located on the company's Web site. Refer to these documents for the most up-to-date and authoritative licensing language:

• Certification Practice Statement (CPS): www.verisign.com/repository/cps. The CPS is the basis of practices and procedures for which VeriSign is responsible as a Certificate Authority.

• End User Subscriber Agreement: www.verisign.com/repository/ssid_agree.html. This agreement must be agreed to in order to use a VeriSign Server ID.

• VeriSign ISP Program Agreement: www.verisign.com/repository/isp/agree_isp.html. This agreement contains specific information for resellers of VeriSign Server IDs.

• Secure Site Seal Agreement: https://www.verisign.com/repository/sslicense_agree.html. Plan with each Server ID.

This agreement governs the use of the Secure Site Seal and other VeriSign branding tools on customer Web sites.

NetSure® Protection Plan
VeriSign offers its customers the NetSure Protection Plan with each Server ID. NetSure is an extended warranty program that protects VeriSign Server ID customers against economic loss resulting from the theft, corruption, impersonation, or loss of use of a VeriSign Server ID. NetSure is backed by Lloyd's of London, one of the world's largest A-rated insurance companies. VeriSign Server IDs each come with up to $250,000 of NetSure protection.

SERVER IDs USE RESTRICTIONS

One key requirement of the license is that subscribers retain control of the private key and take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use. Failure to do so can weaken or even jeopardize any certificate-based security measure, as possession of the private key allows a user to decrypt data and authenticate servers or users on behalf of the key's owner.

Server IDs are designed for use only by the organization authenticated within the certificate. The following are other important requirements:

• To use one Server ID on behalf of any other organization, subscribers must authenticate the end user to the consumer, by using the Shared Hosting Security Service (www.verisign.com/isp/shss/index.html).

• To use their Server ID to perform private or public key operations in connection with any domain name and/or organization name other than the name submitted during enrollment, subscribers must use the Shared Hosting Security Service.

• To use their Server ID on more than one server at a time, subscribers must have purchased the specific licensing option that permits the use of a Server ID on multiple servers. (Server IDs are designed for use on one server at a time.)

If not executed according to VeriSign licensing agreements, certificate sharing can interfere with site authentication, diminish customer trust, and disqualify subscribers from NetSure protection.

If an organization would like to use a certificate in multiple instances or for another organization, in some cases, certificate sharing without the appropriate VeriSign license may also expose an enterprise to charges of software piracy. When offering shared certificates, ISPs sometimes charge end-user merchants or other subscribers for use of the VeriSign Server ID and the SSL capabilities enabled by its deployment. This practice allows the ISP to profit from VeriSign's service (the Server ID) without paying VeriSign's required fee, and is considered software piracy. VeriSign strictly prohibits this and similar practices and will pursue violators to the full extent of the law.

Note: Although certain key requirements of VeriSign licensing are discussed here, this document should not be considered a substitute for carefully reading the entire contents of license agreements. VeriSign considers any misuse of its licensing requirements a breach of contract and will revoke the certificates of violators or pursue other appropriate legal measures. In addition, failure to comply with these agreements automatically disqualifies subscribers from coverage under the NetSure Protection Plan, which leaves the customer liable for damages in the event of any compromised situation.

BEST PRACTICES FOR ENSURING TRUST WITH DIGITAL CERTIFICATES

A number of practices related to digital certificates and licensing play an important role in ensuring the security of Web sites. These practices—site and enterprise authentication, private key protection, and prudent certificate use—often become more complex when deploying multi-server configurations, and if they are not followed, security may be compromised.

VeriSign Seal Branding Requirements
Besides protecting private keys and sharing certificates according to VeriSign requirements, subscribers must ensure the proper use of the VeriSign Secure Site Seal. This seal provides third-party verification of a site's identity when the customer clicks on it, and it is an important component of customer trust in Web transactions. To ensure reliable authentication, enterprises must install and display VeriSign's Secure Site Seal (if used) in accordance with the Secure Site Seal Licensing Agreement (www.verisign.com/repository/sslicense_agree.html).

Site Authentication (URL-to-Certificate Name Matching)

Client applications, such as Web browsers, must be able to verify that the site the user is visiting is the site that has been certified. In practice, this means that the URL of the site matches the common name of the certificate that the site presents to the client application (usually, the site's fully qualified domain name, such as www.samplecompany.com). This task is performed by the browser during authentication and is a fundamental feature of browsers using SSL.

When the client performs URL-to-certificate name matching, it will detect that the URL of the site it is visiting is different from the common name in the certificate. Most browsers are programmed to alert users of this potential security risk and will present a dialog box similar to the one shown in the following figure.
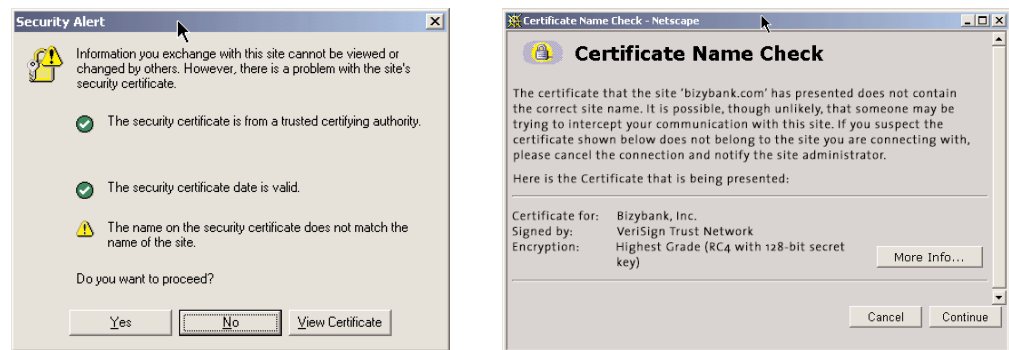
Certificate mismatch error message

This dialog box may create the impression that the site is not secure and dissuade prospective customers from doing business with the site.

This situation can also occur in configurations where multiple hostnames resolve to the same machine, such as https://ww1.verisign.com and https://www.verisign.com.

Enterprise Authentication (Site Name-to-Certificate Name Matching)

The organization listed in the certificate must be tightly bound to the organization running the site. In practice, this means that the organization listed in the certificate should have the right to use the domain name in the common name of the Server ID and should be the entity with which the client is ultimately communicating or conducting business. It also means that the organization must have authorized the issuance of the certificate for a particular site. To meet these requirements, before issuing the Server ID, VeriSign strongly validates the identity of the business and that the applicant is authorized to request the ID. The browser then performs site name-to-certificate name matching during the authentication step of an SSL session with the Server ID.

Many online retailers, banks, brokerage houses, healthcare organizations, insurance companies, and other online businesses choose VeriSign's Server IDs to protect the sensitive information of their customers. These organizations understand the vital role business identity verification (or "authentication") plays in maintaining trust in online transactions. VeriSign's extensive authentication procedures set the standard for the Certificate Authority industry.

Private Key Protection

Private key protection is fundamental to ensuring security with digital certificates. In an SSL session, the client uses the certificate's public key to send confidential information to the server. Because any information encrypted with the server's public key can be decrypted using the server's private key, whoever possesses the private key—or a copy of the key—can access the information. When a private key is created and stored in a single server, or preferably in a FIPS-140 Hardware Security Module (HSM), the key is reasonably well contained and auditable. The enterprise must carefully safeguard the certificate's private key as well as avoid any network configuration that compromises it. To ensure the highest level of security, VeriSign recommends using a unique private key on each server in a multi-server deployment and having the hosting server generate the private keys.

Dedicated Certificates

One of the most common violations related to private key protection—and also one that is most likely to seriously compromise security—is certificate sharing, in which the same certificate and private key are copied to multiple machines or enabled for multiple users. Using the same certificate on multiple physical servers requires generating multiple copies of the same private key and storing that key in multiple locations. When private keys are moved among servers, either by network or disk, accountability and control decrease, and auditing becomes more complex, increasing the risk of exposure and complicating the process of tracing who had access to a key in the event of compromise. The chance of problems increases significantly in relation to the number of servers or users sharing a given certificate. In an article providing RSA prescriptions for applications that are vulnerable to the adaptive chosen ciphertext attack on PKCS #1 v1.5, prescription #1 included the recommendation that "different servers should have different key pairs." Please visit http://www.rsasecurity.com/rsalabs/pkcs1/prescriptions.html.

SHARED CERTIFICATE LICENSING SCENARIOS IN MULTI-SERVER CONFIGURATIONS

VeriSign recommends following best practices by not copying or sharing certificates (and private keys) among servers. However, due to redundancy, load balancing, and other performance and availability considerations, some customers have unique Web infrastructure configurations that require sharing certificates among multiple servers or other devices.

VeriSign's licensing policy contains provisions for sharing certificates in the following configurations:

- Redundant server backups
- Server load balancing
- SSL acceleration
- Shared hosting

The following sections provide a detailed discussion of these shared certificate configurations and the VeriSign licensing policies that apply to each of them.

REDUNDANT SERVER BACKUPS

To maximize revenue and increase customer satisfaction, the Web servers running e-commerce and other business-critical applications must maintain high availability. To accomplish this goal, customers commonly use a redundant or "standby" server to back up their primary Web servers. The standby server typically has the same configuration and contains identical files as the primary server. If the primary server fails for any reason, the customer quickly deploys the standby server in its place, avoiding extended Web server downtime.

If a customer has a standby server offline and brings it online only when the primary server fails, it is a "cold standby" server. If a customer has a standby server online and ready to receive traffic when the primary server fails, it is a "hot standby" or "failover" server.

Licensed Certificate Option

The VeriSign subscriber agreement prohibits the customer from using a certificate "on more than one physical server or device at a time, unless the customer has purchased the Licensed Certificate Option." However, customers with multiple server configurations may have a requirement to share certificates among servers or other devices. The Licensed Certificate Option allows the customer to obtain additional licenses to use the certificate on multiple servers with the identical Common Name. Due to the increased risk of private key compromise associated with copying certificates and private keys from server to server, this option is less secure than deploying unique certificates per server. For this reason, VeriSign offers only $10,000 in NetSure warranty protection for each additional license purchased under the Licensed Certificate Option.

VeriSign Licensing Policy

VeriSign encourages customers to make one backup copy of the certificate and associated private key and store them both in a secure location. Although not recommended by VeriSign (due to the increased risk of private key compromise described herein), it is also permissible for the customer to maintain the backup copies of the certificate and associated private key on one cold standby server. If the customer requires backup copies on (a) more than one cold standby server or (b) one or more hot standby servers, the customer must purchase additional licenses using the Licensed Certificate Option described at left.

SERVER LOAD BALANCING

To improve Web site performance and availability, it is becoming increasingly common for customers to distribute Web site traffic across multiple servers using load balancing devices. Those servers may reside at one location or in geographically diverse locations. Load balancers can be configured to distribute Web site traffic to available servers based on several factors, including load or operational state of the servers, load or operational state of the network, and client browser location.

There are two basic load balancing configurations:

- Dynamic Hostname
- Identical Hostname

Dynamic Hostname Configuration

In this configuration, the Web site has multiple physical servers, each of which hosts a virtual server with a slightly different hostname (for example, ww1.mycompany.com, ww2.mycompany.com, and ww3.mycompany.com). Sharing a certificate between servers in   a configuration where there are multiple physical servers with different hostnames should be avoided. During

the SSL handshake, the client browser will detect that the URL of the Web site ww2.mycompany.com is different from the common name of the certificate ww1.mycompany.com and display a warning to the end user.

VeriSign Licensing Policy
VeriSign recommends either unique certificates or wildcard certificates for dynamic hostname configurations:

- Unique certificates - VeriSign recommends customers purchase individual certificates for dynamic hostname configurations. If the configuration contains more than five physical servers, VeriSign recommends Managed PKI for SSL. Managed PKI for SSL allows customers to conveniently manage multiple SSL certificates and provides discounted pricing for volume purchases. For more information, visit: http://www.verisign.com/products/onsite/ssl/option.html.

- Wildcard certificates - If individual certificates are not an option, VeriSign offers wildcard certificates. A wildcard certificate is a special form of certificate that contains an asterisk in the hostname portion of the certificate's common name (for example, .*.mycompany.com). This allows the certificate to secure multiple physical servers with different hostnames. Customers must purchase Wildcard certificate licenses based on the number of unique hostnames in their dynamic hostname configurations.

  To request a wildcard certificate price quote, please send an e-mail request to: wildcard-request@verisign.com. For a discussion of wildcard compatibility issues, see the "Wildcard Certificates" box at right.

Identical Hostname Configuration

In this configuration, the Web site has multiple physical servers, all of which share the same hostname (for example, three servers all named www.mycompany.com).

VeriSign Licensing Policy
VeriSign recommends either unique certificates or the Licensed Certificate option for configurations where there are multiple physical servers, all of which share the same hostname:

- Unique certificates—Create a different certificate for each different server. Because good PKI practices (and VeriSign's internal policies) prohibit the issuance of two certificates with exactly the same name, VeriSign recommends that each certificate

Wildcard Certificates

Wildcard certificates are special certificates that are issued with an asterisk in the form of CN= *.verisign.com that are used to secure environments that feature dynamic hostnames.

When adopting a wildcard certificate solution, keep in mind the following compatibility issues:
- Netscape browsers work with wildcards, but not with Microsoft IIS servers. Microsoft IIS uses Unicode as the character set for the common name field of wildcard certificates, and Netscape browsers do not support Unicode characters in certificates. For more information on wildcard compatibility with Microsoft products, visit http://support.microsoft.com/support/kb/articles/Q258/8/58.ASP.
- Apache Web servers use printable string as the character set for the common name, which violates the X.208 specification.
- Many deployed versions of Internet Explorer do not work with wildcard certificates, especially if running on a Windows 2000 platform. Internet Explorer will correctly connect to these hosts, but end users will get a warning that the server certificate does not match the hostname to which they are connecting.

have the same common name and the same organizational name, but a different organizational unit, as illustrated in the following table.

	Certificate 1	Certificate 2	Certificate 3
Hostname	www	www	www
Common Name	www.mycompany com	www.mycompany com	www.mycompany com
Organization	Mycompany, Inc	Mycompany, Inc	Mycompany, Inc
Organizational Unit	Server 1	Server 2	Server 3
For server farms containing more than five servers, VeriSign recommends Managed PKI for SSL (www.verisign.com/products/onsite/ssl/index.html).			

- Licensed Certificate Option (see box on page 7)—The VeriSign subscriber agreement prohibits the customer from using a certificate "on more than one physical server or device at a time, unless the customer has purchased the Licensed Certificate Option." However, customers with multiple server configurations may have a requirement to share certificates among servers or other devices. The Licensed Certificate Option allows the customer to obtain additional licenses to use the certificate on multiple servers with the identical Common Name. Due to the increased risk of private key compromise associated with copying certificates and private keys from server to server, this option is less secure than deploying unique certificates per server. For this reason, VeriSign offers only $10,000 in NetSure warranty protection for each additional license purchased under the Licensed Certificate Option.

SSL ACCELERATION

SSL acceleration devices are becoming an increasingly critical tool for enhancing and optimizing the performance of secure Web sites. Deployment configurations for these devices vary depending on the topology of the customer's network, server configuration, and the specific SSL acceleration device being deployed. For a list of VeriSign supported SSL accelerator partners, go to: http://www.verisign.com/products/site/accelerator/index.html.

There are two basic SSL accelerator configurations:

- SSL sessions terminate at the Web server
- SSL sessions terminate before the Web server

SSL session terminates at the Web Server

Some vendors offer SSL acceleration solutions in which each server has its own accelerator card with a unique certificate. In this case, deployment configurations and associated licensing policies are the same as those described in the Server Load Balancing section above.

SSL session terminates before the Web server

SSL accelerators that terminate the SSL session before the Web server will either (a) re-encrypt the SSL session data being sent to the server or (b) send the SSL session

data to the server unencrypted. In the latter case, customers should be aware that sending data unencrypted from the point where the SSL session terminates to the server exposes their Web site visitors to increased security risks (see the "SSL Session Terminates Before the Server Farm" box at right).

VeriSign Licensing Policy

Regardless of whether SSL session data terminates at or before the Web server, if the SSL accelerator contains a certificate pointing to multiple servers, the customer must use the Licensed Certificate Option to purchase additional licenses for each additional server the SSL accelerator is pointing to in the server farm.

- Licensed Certificate Option (see the box on page 7)— The VeriSign subscriber agreement prohibits the customer from using a certificate "on more than one physical server or device at a time, unless the customer has purchased the Licensed Certificate Option." However, customers with multiple server configurations may have a requirement to share certificates among servers or other devices. The Licensed Certificate Option allows the customer to obtain additional licenses to use the certificate on multiple servers with the identical Common Name. Due to the increased risk of private key compromise associated with copying certificates and private keys from server to server, this option is less secure than deploying unique certificates per server. For this reason, VeriSign offers only $10,000 in NetSure warranty protection for each additional license purchased under the Licensed Certificate Option.

Note: Most SSL accelerator vendors have the built-in capability to support hundreds of certificates. If the configuration contains more than five physical servers, VeriSign recommends Managed PKI for SSL. Managed PKI for SSL allows customers to conveniently manage multiple server certificates and provides discounted pricing for volume purchases. For more information, visit: http://www.verisign.com/products/onsite/ssl/option.html.

SHARED HOSTING

On the Internet, the largest percentage volume of Web sites are hosted in a shared environment; that is, several sites are hosted on a single server. These shared hosted sites typically belong to entry-level customers who do not need the expanded functionality offered by dedicated hosting plans or to customers who want to start with a less expensive shared hosting option before graduating to a dedicated plan.

A number of mechanisms are available for hosting a Web site in a shared environment. The use of SSL certificates in these environments has been ad hoc for several reasons:

- Typical shared hosting customers are extremely price sensitive, want ease of use, and are not interested in the technical aspects of their Web site.
- An SSL certificate requires a unique IP address/port combination, and available public IP addresses are scarce.

SSL Session Terminates Before the Server Farm

Using an SSL accelerator can pose a security risk, because in many cases the SSL session is terminated before the server farm, meaning that clear text is sent between the accelerator device and the server farm without encryption. Sending this portion of the client-to-server communications through clear text exposes enterprises to the risk of a security breach behind the firewall. For this reason, VeriSign's NetSure Protection Plan is limited when deploying a certificate in an acceleration architecture. SSL accelerators featuring "back-end encryption" is recommended in all instances.

- Some server software does not provide the functionality to support dedicated certificates for virtual hosted customers.

To circumvent the limitations imposed by shared hosting environments, Web hosts may offer "Shared SSL" plans. In a typical shared SSL plan, the Web host or ISP requests a certificate for its own domain (e.g., https://secure.isp.com) and then lets its customers use that certificate for securing their own transactions through a site redirection. This scenario allows other domains to use the encryption capabilities of the Web host's certificate but prevents authentication of individual organizations.

Without authentication, online customers do not know to whom they are sending their information, creating the potential for a serious breach in security and exposing Web hosts to liability claims if their certificates are used to legitimize fraudulent transactions. Because this practice violates the basic principles of digital certificate trust, as well as the terms of VeriSign certificate licensing, enterprises employing this practice automatically forfeit the NetSure protection provided with their certificate.

VeriSign Licensing Policy

If customers can be issued individual IP addresses, they should apply for individual SSL certificates, which will simplify authentication and encryption. If individual IP addresses cannot be assigned, license the SSL certificate to encrypt information for specific, authenticated customer domains. VeriSign's Shared Hosting Security Service (SHSS) program provides the solution for this scenario.

Specific solutions for each type of hosting environment follow:

Directory based
In this configuration, the ISP hosts customer Web sites under its own domain name, such as www.isp.com/cust1, www.isp.com/cust2, and www.isp.com/cust3. So, if an SSL certificate is issued to https://www.isp.com, there is a single hostname but multiple organizations using the same certificate.

VeriSign Licensing Policy

The ISP validates the identity of and provides information about each certificate user, and then licenses the certificate for the appropriate number of users/organizations. VeriSign's SHSS program provides the solution for this scenario.

Name based
In this scenario, the ISP hosts Web sites under their own domain names, such as cust1.isp.com and cust2.isp.com.

VeriSign Licensing Policy

Obtain a wildcard SSL certificate with a common name such as *.isp.com licensed for use with a specified number of domains. This license allows individual customers to be authenticated and issued seals. For a discussion of wildcard compatibility issues, see the "Wildcard Certificates" box on page 8.

Domain based

In this scenario, the ISP and each customer have their own domain name, such as www.isp.com, www.cust1.com, and www.cust2.com, but the secure pages for cust1 and cust2 are hosted under www. isp.com. In this case, authentication of customer domains is possible and must be performed before encryption. VeriSign's SHSS program provides the solution for this scenario.

Product Summary

For more information about licensing agreements, please refer to the following documents:

Certification Practice Statement (CPS)	http://www.verisign.com/repository/cps
End User Subscriber Agreement	http://www.verisign.com/repository/ssid_agree.html
VeriSign ISP Program Agreement	http://www.verisign.com/repository/isp/agree_isp.html
Secure Site Seal Licensing Agreement	https://www.verisign.com/repository/sslicense_agree.html

For more information about VeriSign products and services, please refer to the following sites:

VeriSign Shared Hosting Security Service	http://www.verisign.com/isp/shss/index.html
VeriSign OnSite® for Server IDs	http://www.verisign.com/onsite/server/index.html
VeriSign Server IDs	http://www/products/site/index.html
Secure Site Seal	https://www.verisign.com/repository/sslicense_agree.html

CONCLUSION

SSL certificates form the basis for trust and security in high-value Web applications by providing strong data encryption as well as reliable authentication of the site and the company with which a client is communicating. As the Internet evolves and enterprises and service providers require increasingly complex server configurations to secure their high-volume Web sites, VeriSign is committed to providing solutions that provide a solid trust infrastructure for the Internet, while addressing the specific needs of these new environments. VeriSign looks to continued participation from its customers, technology partners, and service provider channels to guide future development of products and services that allow each Internet end user to confidently use the Internet as a secure medium for high-value online business, communications, and commerce.

VeriSign, Inc.
487 E. Middlefield Road
Mountain View, CA 94043
Phone: (650) 961-7500
Fax: (650) 961-7300

VeriSign®