

Managing SSL Security in Multi-Server Environments

VeriSign's Easy-to-Use Web-Based Service Speeds SSL Certificate Management and Cuts Total Cost of Security

VeriSign MPKI for SSL

- **Simple:** Web-based service for managing all your SSL certificates—no upfront hardware or software to install
- **Efficient:** Enroll, approve, issue, reject, revoke, renew with a few clicks of a mouse
- **Time saving:** Issue SSL certificates on demand
- **Secure:** Certificate-secured administrator account access
- **Value:** Provides discounted, bulk purchases of SSL certificates

A SMART STRATEGY FOR MANAGING SSL SECURITY ON MULTIPLE SERVERS

Protecting the confidentiality and integrity of sensitive information transmitted over your organization's network is a crucial step to building customer confidence, securely interacting with business partners and complying with new privacy regulations. Your company's requirements may include securing information exchange between Web servers and clients, server-to-server, and among other networking devices such as server load balancers or SSL accelerators. For a complete solution, cross-network security must protect servers facing both the Internet and private intranets.

Secure Sockets Layer (SSL¹) is the world's standard technology used to protect information transmitted over the Web with the ubiquitous HTTP protocol. SSL protects against site spoofing, data interception and tampering. Support for SSL is built into all major operating systems, Web applications and server hardware. Leveraging both the powerful encryption of SSL and the confidence instilled by VeriSign's authentication procedures, your company can immediately protect sensitive data transmitted between your servers and your customers, employees and business partners.

Managed PKI for SSL is VeriSign's easy to use and flexible Web-based service for deploying and managing multiple SSL certificates across the organization. Leveraging VeriSign's scalable and highly secure infrastructure, **Managed PKI for SSL** is an enterprise solution that allows you dramatically reduce much of the cost associated with SSL certificate deployment while maintaining full local control.

¹ The Internet Engineering Task Force has renamed SSL to Transport Layer Security (TLS), and is working on wider adoption of the TLS protocol. SSL, however, remains the popular nomenclature.

SSL Certificates Provide Core Web Transaction Security

Transmitting sensitive data, such as credit card numbers and health care data, across the Web and intranets requires **authentication**—to ensure the destination of the data is legitimate, **encryption**—to protect the data against interception or tampering and **message integrity**—to ensure the information isn't tampered with during transmission. Digital certificates from VeriSign use Secure Sockets Layer (SSL) technology to address all three of these requirements. SSL has become the world's standard for protecting sensitive information transmitted over the Web as well as intranets via HTTP.

As part of a Public Key Infrastructure (PKI) for Web security, digital certificates activate SSL security capability built into all Web servers, browsers and other Web devices. VeriSign's SSL certificates provide three key benefits:

Business Identity Authentication. VeriSign uses extensive procedures to verify the identity of businesses and authorization of the requestor before issuing a SSL certificate. All Web browsers inherently trust SSL certificates signed by VeriSign's root Certificate Authority (root CA) certificates, providing assurance to Web site visitors that their information is being transmitted to a legitimate business, not an impostor.

VeriSign sets the standard for business identity authentication with the industry's most thorough three-part vetting process:

- The business named in the certificate has the right to use the domain name listed in the certificate
- The business named in the certificate is a legitimate business
- The individual who requested the SSL certificate on behalf of the business was authorized to do so

Encryption. All data transmitted between Web browsers (clients) and servers over SSL is encrypted using sophisticated cryptographic techniques making it virtually impossible for the data to be intercepted and viewed. Each secure connection between client and server gets a unique "SSL session key"; the key length indicates the "strength" of the encryption.

The encryption strength used for a particular SSL session depends on the browser version and the type of SSL certificate installed on the Web server. The strongest SSL encryption available in today's browsers is 128-bit (i.e., the SSL session key is 128-bits in length), which has never been broken. However, browser versions exported outside the US before January 2000 typically support only 40-bit SSL sessions, unless the SSL certificate on the Web server supports Server Gated Cryptography (SGC)—also called "step-up" technology.

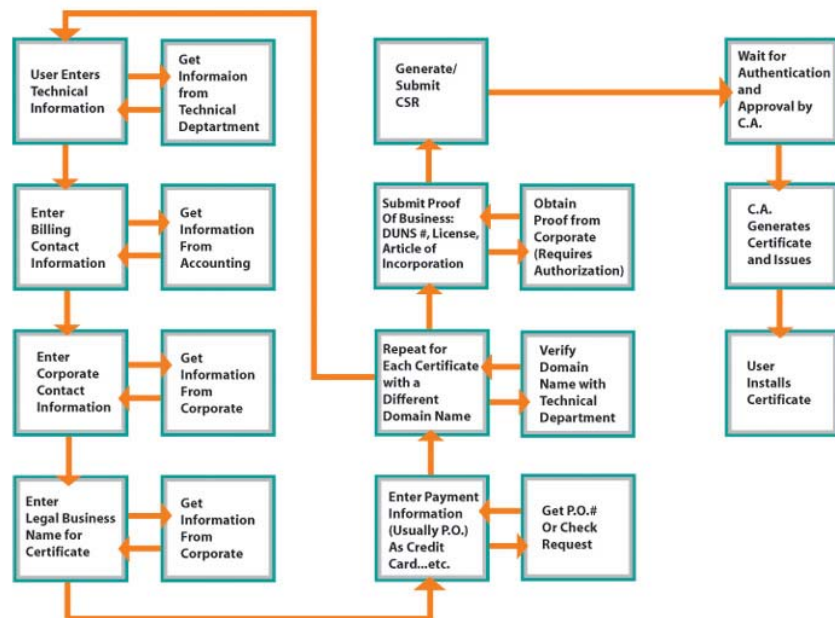
Message Integrity. Contents of all communications between client and server are protected from alteration on route. All parties to the transaction know that the information they have received is exactly what originated from the other side of the SSL connection.

ONE-BY-ONE CERTIFICATE MANAGEMENT IS A TEDIOUS PROCESS

Your organization's choice to deploy numerous SSL certificates includes a practical management decision: Shall you do it manually, or use a scalable Web-based service like **VeriSign MPKI for SSL** that automates many certificate management processes? Managing SSL certificates on an ad hoc basis is appropriate for small organizations where one person is responsible for deploying and managing only a couple SSL certificates. However, deploying numerous SSL certificates across multiple departments and in multiple geographies is a much more complex challenge.

On the surface, the ad hoc deployment strategy seems simple enough. Some decentralized organizations consider the volume discounts offered by other SSL certificate vendors to be sufficient—but they fail to see the "hidden costs" of managing SSL certificates across the organization. The price of the SSL certificate itself is not the only cost to consider, especially in organizations with multiple server types, multiple locations, and multiple server administrators.

Consider the flow-chart diagram below, which shows each step of a typical SSL certificate enrollment process.



SSL CASE STUDY: Finance

A large financial institution used more than 700 certificates – 500 units purchased with VeriSign MPKI for SSL and 200+ retail units. After consolidating all certificates under MPKI for SSL, the company cut annual recurring renewal and management costs for retail certificates by more than \$70,000 – and now controls subscriber-applicants with tight authorization and authentication.

The SSL certificate enrollment process shown above includes extensive collection and verification of information required by the Certificate Authority (CA), which is an organization that authorizes and issues SSL certificates. Some of the required enrollment information is difficult to find—especially when an IT manager starts knocking on executives' doors looking for proof of right documentation, articles of incorporation and other business documents. Also, separate purchase authorization is typically required for each SSL certificate, so delay can thwart

urgent deadlines as the CA conducts its essential authentication and verification procedures on each SSL certificate application. As a result, the total cost of an SSL certificate purchased ad hoc is much higher than the initial purchase price.

Effort and costs spent on deployment are just part of managing an SSL certificate over the life of its validity period, also called the "certificate lifecycle." There are six activities that can be performed on an SSL certificate during its lifecycle:

SSL Certificate Lifecycle Elements

Enroll – Complete application to purchase an SSL certificate, including submission of organization eligibility and administrative data.

Approve – Interface with an independent CA, which verifies organization's eligibility and approves granting of the certificate; only available with **VeriSign MPKI for SSL**.

Issue – CA issues the certificate; purchaser installs the certificate on a designated server or device to enable SSL services.

Reject – Immediate administrative rejection of an unauthorized certificate enrollment request; only available with **VeriSign MPKI for SSL**.

Revoke – Immediate administrative revocation of a certificate; only available with **VeriSign MPKI for SSL**.

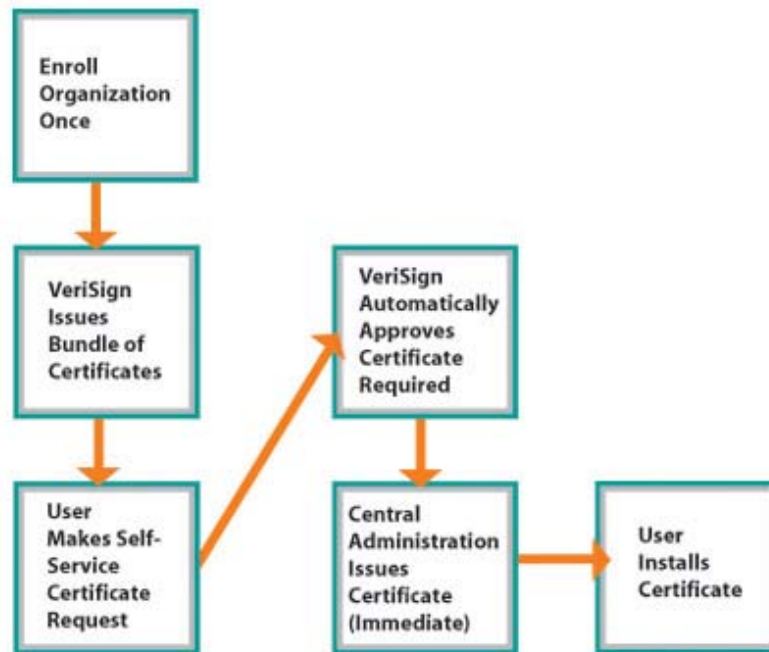
Renew – Ensure that each certificate is properly renewed with the CA in a timely manner.

Using an ad hoc manual process is adequate to manage lifecycles of a handful of certificates. Managing a multitude of certificates is tedious, time-consuming, expensive, and often an overwhelming process – especially in large, distributed organizations. Automating the process with **VeriSign MPKI for SSL** is the logical step to efficient SSL security management.

SIMPLIFYING SSL MANAGEMENT WITH VERISIGN'S POWERFUL WEB-BASED SOLUTION

Companies implementing five or more SSL certificates can significantly ease certificate management processes with the automated benefits of **VeriSign MPKI for SSL**. With Web-based SSL certificate management, your organization gets full visibility into the certificate inventory, centralized operational and financial control, and the assurance of full SSL protection for server transactions.

The flowchart below shows how **VeriSign MPKI for SSL** simplifies the complex certificate enrollment process for immediate, on-demand issuance of SSL certificates.



SSL CASE STUDY: Insurance

A large insurance company used retail SSL Certificates to implement security for Web-based transaction systems. Project development was on weekends and after hours, so the company needed capability to instantly issue certificates to test and implement security on new production servers. Retail certificate issuance took up to four days so the company switched to VeriSign MPKI for SSL. Now, the insurance company can meet its efficiency goals and has cut the costs of certificate acquisition and management.

Web Interface Provides Centralized Local Control

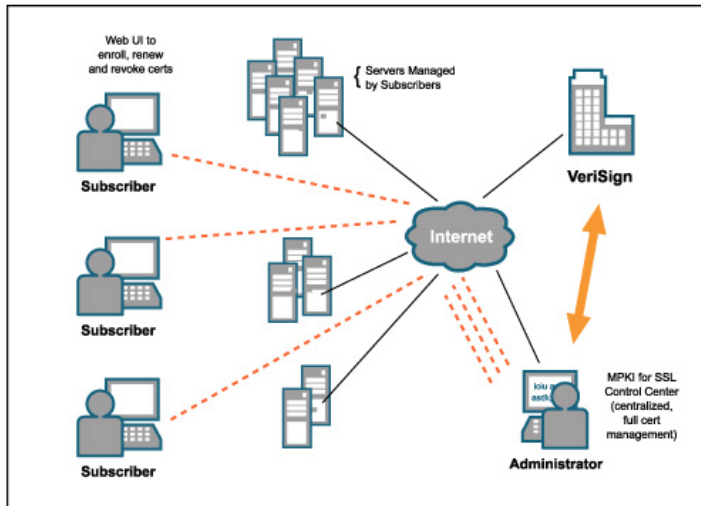
The key to **VeriSign MPKI for SSL** process automation is a hosted Web-based infrastructure. Your organization's local administrator centrally manages all aspects of the SSL certificate lifecycle with a Web-based "Management Tools" interface called Control Center. Authenticated administrators use Control Center to manage and control certificate enrollment, approval, issuance, rejection, revocation, and renewal. Control Center provides:

- Full PKI management
- Centralized administration and control
- Access to specialized reports to track certificate details
- Audit log of all certificates issued and all administrator actions
- Email alerts
- Download CRL
- Interactive online help

Management tools also include a "Subscriber Tools" element, permitting role-based task delegation for distributed administration. Certificate subscribers interact with the system via customizable screens. All data is automatically processed in the VeriSign hosted, carrier-class data center, which acts as a behind-the-scenes relay hub between the administrator, users and the CA. The diagram below shows workflow between these entities:

VeriSign Managed PKI for SSL

----- SSL Certificate Requests to the Administrator
←→ Certificate-secured, Web UI Management



The customizable Web interface screens enable users to request certificates and do other tasks without requiring human intervention. For example, the illustration below shows a typical **VeriSign MPKI for SSL** browser screen used for entering certificate request information.

The screenshot shows a web browser window titled 'Managed PKI for SSL (Premium Edition) Subscriber Enroll - Microsoft Internet Explorer'. The address bar shows the URL: <https://onsite.verisign.com/VeriSignIncWebTrustServicesGroupGlobalServer/serverEnroll.htm>. The main content area is titled 'Step 2: Enter Authentication Information'. Below the title is a paragraph of instructions: 'The information that you enter here will be used to help your Managed PKI administrator approve your request for a Premium SSL ID. Please complete all of the fields, and use only the English alphabet with no accented characters.' The form contains several input fields: 'First Name', 'Middle Initial', 'Last Name', 'Email Address', 'Title', 'Employee ID Number', 'Mail Stop', 'Department No', 'Server IP', 'Application Server Type' (a dropdown menu with 'Select Application Server Vendor' selected), and 'Certificate Validity' (set to '2 Years'). Below the form is 'Step 3: Choose a Challenge Phrase', which includes instructions on how to choose a challenge phrase and a note to use only the English alphabet with no accented characters and no punctuation.

VERISIGN MPKI FOR SSL CUSTOMERS SAY:

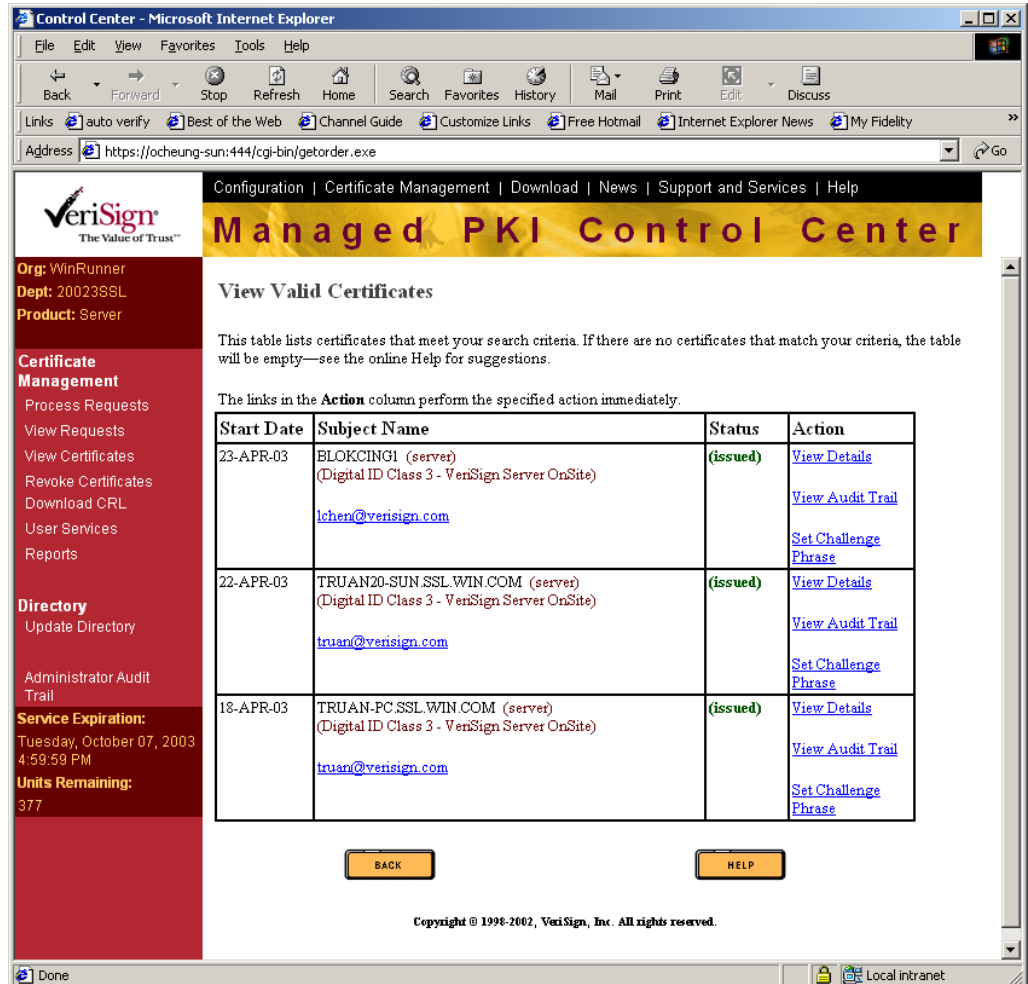
- 94% centrally control cert. management and costs
- 59% use one admin.; 27% use two
- 53% estimate internal costs are less than 5% more as a percentage of cert. price; 41% estimate 5-25% more
- 64% use some certificates for internal, behind-the-firewall applications

(From 2003 Survey; 76% have 1000+ employees.)

AUTOMATED REPORTS KEEP YOU IN CONTROL

Control Center provides a complete history of all certificate activity. Comprehensive Web-based reports automatically generated by **VeriSign MPKI for SSL** give you a precise, real-time view of certificate status throughout the enterprise. Reports also act as a third-party security audit trail for certificate activity.

Reports include certificates requested, approved, issued, rejected, and revoked. The illustration below shows a typical report view of valid certificates.



With Control Center, your administrator also can filter reports by date range and view all data, or search for specific granular details. Administrators view search results on demand by downloading a comma-delimited report file generated by VeriSign for import into any popular spreadsheet application.

VeriSign Managed PKI for SSL Certificate Solutions

VeriSign offers two **Managed PKI for SSL** solutions to meet all of your SSL security needs:

Premium Edition – True 128-bit SSL security for protecting the most sensitive data on your network.

VeriSign's Managed PKI for SSL Premium Edition (Global Server ID) Certificates, use Server Gated Cryptography (SGC) technology to enable 128-bit SSL encryption in all browsers, including 40-bit export browser versions.

- Premium Edition SSL certificates guarantee a 128-bit SSL session in all current browsers. Other Certificate Authorities promote their SSL certificates as "128-bit", but these do not use SGC and cannot ensure 128-bit SSL encryption regardless of browser version.
- VeriSign is the only Certificate Authority authorized by the U.S. Department of Commerce to distribute 128-bit SGC SSL Certificates outside the U.S.

Standard Edition – for protecting sensitive data on Intranets and public Web sites. Standard Edition SSL certificates from VeriSign enable:

- 128-bit SSL encryption when communicating with newer Microsoft and Netscape browser versions.
- 40-bit SSL encryption when communicating with older, export-version, Microsoft and Netscape browsers.

Extensive Server Platform Support. VeriSign's Managed PKI for SSL Standard and Premium Edition certificates are compatible with a comprehensive list of server platforms. (See <http://www.verisign.com/products/onsite/ssl/compatibility.html> for details.)

Strongest Authentication Process. VeriSign protects businesses with the strongest, 3-step certificate authorization process. We verify and insure the veracity of the organization and Internet domain – double-checking facts with research and personal calls by VeriSign staffers.

Strongest Warranty Protection. Each Managed PKI for SSL certificate is backed by VeriSign's NetSure Warranty Protection Program, that protects VeriSign SSL Certificate customers against economic loss resulting from the theft, corruption, impersonation, or loss of use of a certificate. Warranty limits are \$250,000 of protection for MPKI for SSL Premium certificates and \$100,000 for Standard certificates.

VeriSign MPKI for SSL Hosted Solution Provides Built-In Infrastructure:

- PKI expertise
- Trained IT staff
- Trained security staff
- Redundant servers
- Redundant networking
- Disaster recovery/backup
- Hardened data center
- Hardened network operations control center
- Redundant power, HVAC
- Physical and digital access controls
- Digital authentication
- Root key management
- Third-party security audits
- Liability insurance

ENTERPRISE-CLASS SERVICE WITH SSL EXPERTISE AT YOUR FINGERTIPS

A major benefit of VeriSign's hosted **MPKI for SSL** solution is continuous access to the company's rich store of security expertise. VeriSign has issued more than 400,000 SSL certificates, which makes it the leading provider worldwide. As part of the solution, customers get a broad range of enterprise support services, including:

- World-class 24x7 data center
- 24x7 support organization
- Complete Web-based resources
 - Technical Web seminars
 - "Knowledge Base"
 - Troubleshooting tips
 - Tutorials
 - FAQs
- Tiered support plan options: Standard, Gold, Platinum
- Response times: Service Level Agreements for each support plan and severity level
- Highest CA physical security
 - Tier 7 security facility
 - No single point of failure and Hot-site disaster recovery facility
 - Maintain performance levels and scale capacity

Along with the support options available, your organization's administrator gets a designated point of contact at VeriSign. No other CA is as experienced or provides services as comprehensive as VeriSign.

TEST THE BENEFITS OF MPKI FOR SSL

The **VeriSign MPKI for SSL** solution will simplify management of your organization's SSL certificates, requiring no upfront hardware or software to install or operate. With a few clicks of a mouse, you can efficiently enroll, approve, issue, reject, revoke and renew SSL certificates across the enterprise from one central administration point. VeriSign's solution saves you time because all actions occur on-demand. All management activity is secured by authentication and encryption. The solution includes discounts for bulk purchases of SSL certificates.

Trial Offer

VeriSign invites your organization to test the benefits of using a hosted, automated Web-based service for managing SSL certificates. To request a free demonstration of **VeriSign MPKI for SSL**, please call one of our SSL Security Specialists at (650) 426-5115, option 2.

ABOUT VERISIGN, INC.

VeriSign, Inc. (NASDAQ: VRSN) is the leading provider of digital trust services that enable everyone, everywhere to engage in commerce and communications with confidence. VeriSign's digital trust services create a trusted environment through our core offerings – telecommunications services, security services, and registry services – powered by a global infrastructure that manages billions of network connections and transactions a day.

VeriSign, Inc.

487 E. Middlefield Rd.
Mountain View, CA 94043
650.961-7500
www.verisign.com

VERISIGN IS A REGISTERED TRADEMARK OF VERISIGN, INC. ALL OTHER TRADEMARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.(C) 2003 VERISIGN, INC. ALL RIGHTS RESERVED.