



WHITE PAPER

---

## How to Effectively Manage SSL Certificates across the Enterprise





WHITE PAPER



**CONTENTS**

+ Executive Summary	3
+ Managing Growth and Complexity	3
+ Six Steps to Single-Point Control	4
+ SSL for the Enterprise	8
+ Conclusion	9



# How to Effectively Manage SSL Certificates across the Enterprise

## SCENARIO 1: THE MYSTERY EXPIRY

*Your e-commerce server goes down and no one knows why. Thousands of pounds in sales are lost each hour while the IT department tracks down the problem. It turns out that an SSL Certificate expired and the administrator who purchased it two years ago has left the company. The renewal notice never reached the current administrator. VeriSign® Managed PKI for SSL allows up to three e-mail addresses for notifications.*

## SCENARIO 2: THE CONSOLIDATION PROJECT

*A recent merger requires the integration of two network systems. You need to purchase five premium and five standard SSL Certificates and update domain contact information on three existing certificates. Purchasing the certificates individually will take valuable time away from other integration activities. Purchase multiple certificates through VeriSign Managed PKI for SSL for renewal and instant issuance.*

### + Executive Summary

The number of Internet users worldwide passed the one billion mark in 2005 and is expected to reach two billion by 2011.<sup>1</sup> The Internet has become a critical component of operations and sales for organisations large and small, local and global, bargain and premium. Before people share personal and confidential information online, they look for security indicators that the Web site or application can be trusted and that their information will be encrypted. When a Secure Sockets Layer (SSL) Certificate expires, the owner not only loses sales, but also puts customers' confidence at risk. Enabling secure transactions over increasingly complex networks requires a better SSL Certificate management process for the enterprise.

### + Managing Growth and Complexity

SSL Certificates are not just for e-commerce anymore. If an application or a Web site requires a username and password, the transmission of information should be protected by encryption. When securing 10 or more servers, managing individual certificates gets complicated. They may have been purchased at different times, by different people, from different vendors, making it difficult to keep track of which certificate needs to be renewed when and by whom. Authentication for each individual certificate slows down the purchase process for multiple certificates. And some administrators may purchase and install SSL Certificates by working outside of set internal processes.

An enterprise-level certificate management tool helps consolidate information and management. But most management tools only provide access to one type of certificate. A complete security picture requires real-time information about all types of SSL Certificates across multiple domains and departments. While centralising control is ideal for some IT organisations, others prefer to delegate administrative responsibility while retaining an accessible audit trail of changes and updates.

No one wants to have an SSL Certificate expire under their supervision. Tracking renewals by 90-, 60- and 30-day increments helps system administrators plan and budget for renewals. Better notification and contact information management ensures that the right people know when a certificate needs to be renewed. Early renewals and longer validity periods help prevent downtime and reduce cost of ownership.

<sup>1</sup> Computer Industry Almanac, Inc. January 2006. <http://www.c-i-a.com/pr0106.htm>

### SCENARIO 3: LOCAL CONTROL WITH OVERSIGHT

*Your office in India needs to issue a certificate locally to bring a development server online, but the time difference means that they will have to wait 24 hours for your approval. The delay is a costly rubber stamp for a preapproved use of a certificate in an authorised domain by an authenticated user. Delegate administration using VeriSign Managed PKI for SSL to allow instant issuance of the certificate.*

### SCENARIO 4: THE RELOCATION

*In the process of merging data centres, you need to move certificates from one physical location to another. You do not want to purchase new certificates for the new site and lose the validity period of existing certificates, but you cannot afford any downtime. Use the "revoke and replace" feature to move the certificates from one server location to another with VeriSign Managed PKI for SSL.*

## + Six Steps to Single-Point Control

This guide shows IT professionals how to consolidate their SSL Certificates into a single, Web-based management system using VeriSign® Managed PKI for SSL to acquire, issue and manage all types of SSL Certificates across the whole enterprise:

1. Perform an audit of all domains and certificates
2. Confirm contact information on all certificates
3. Migrate all certificates into a managed account
4. Define an administrative process for your organisation
5. Run regular reports on available units and renewals
6. Revoke and replace certificates as needed

### *A Guide to Single-Point Control*

What begins as a single Web server can quickly grow into a server farm, and what began as a local company can quickly become a global enterprise. Such growth requires systems administrators to manage several administrators suddenly. Before such a crisis hits, an organisation should take control of SSL across the enterprise and create a better management system following these six steps:

#### 1. Perform an audit of all domains and certificates

The SSL Certificate audit should note the location, expiry date and validity period, the vendor and the contact listed for every SSL Certificate in your enterprise. Whether starting from scratch or validating an existing list, anyone who might have purchased an SSL Certificate should be notified of the audit and be asked to contribute information. In addition to domain and Web servers, certificates may also be used to secure applications such as mail servers. The NSLookup tool maps domain names to IP addresses to help find the location of missing certificates. If a certificate cannot be found or is no longer needed, be sure to revoke it to prevent misuse.

The audit is a good time to evaluate the type of certificate used and make sure it meets your current needs. Would a highly visible, public Web server benefit from an upgrade to a new SSL Certificate that meets the CA/Browser Forum Extended Validation Standard? Does the intranet need SSL protection?

Output: a complete list of all domains and certificates.

#### 2. Confirm contact information on all certificates

During the enrolment process for most SSL Certificates, the purchaser provides contact details for a Technical Contact, including name, telephone number and e-mail address. The Technical Contact plays an important role in the authentication and renewal process. If that person leaves the company without reassigning his or her responsibilities, renewal notices may go to the wrong address. If a certificate expires, a critical service may be disrupted. Updating contact information with an alias, such as [ssladmin@yourdomain.com](mailto:ssladmin@yourdomain.com), ensures that messages will reach an active administrator.

Output: up-to-date contact information on all certificates.

**KEY BENEFITS**

**Lower Cost of Ownership**  
*Reduce the cost and complexity of managing multiple SSL Certificates across your organisation with single-point control and volume pricing.*

**Flexible management options**  
*Achieve the right level of control for certificate lifecycle management with delegated administration capabilities, role-based access control and dynamic assignment of privileges.*

**Better risk management and control**  
*Extensive audit trails track certificate lifecycle operations. Retail blocking prevents business units and subsidiaries from purchasing individual certificates.*

**Increased customer confidence with VeriSign**  
*Over 93% of the Fortune 500 and the world's 40 largest banks choose VeriSign as their SSL provider. They trust our encryption technology and rigorous business authentication practices.*

**3. Migrate all certificates into a managed account**

If the enterprise requires 10 or more SSL Certificates, consolidating certificates into a single, managed account may save time and money. As current certificates approach their expiry date, replace them with units from the primary managed account. Select a primary management account for consolidation that supports all types of certificates required. Today's SSL Certificates offer a range of encryption strengths and authentication levels. But many SSL enterprise management tools require a different login for each type of certificate. As the organisation grows and the number of administrators increases, managing multiple accounts for different types of SSL Certificates will become cumbersome unless you have single-point control.

Output: a single, managed account for all certificates within the enterprise.

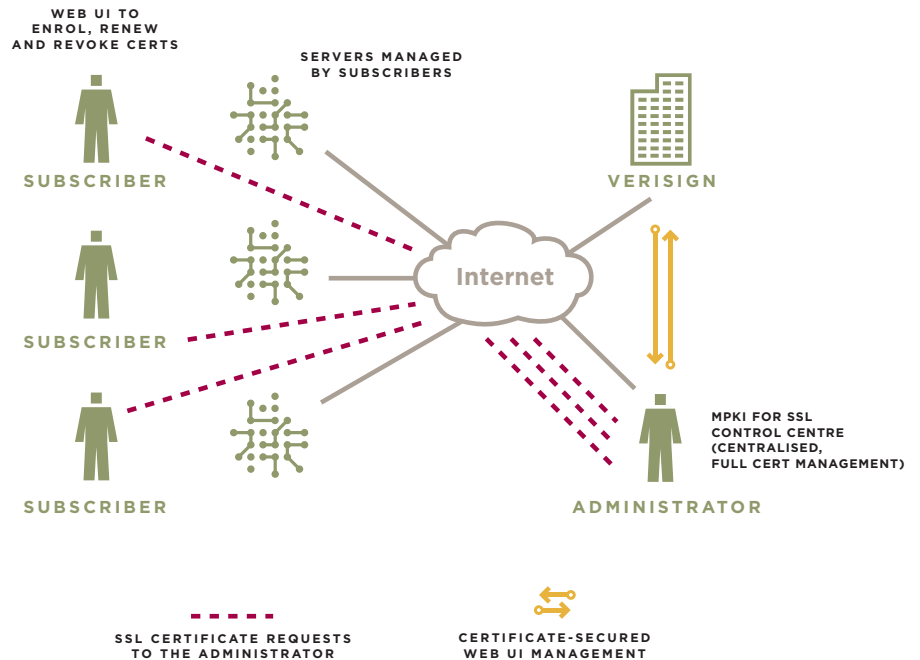
**4. Define an administrative process for your organisation**

An enterprise certificate management account enables authorised administrators to purchase multiple certificate units in one go for issuance, as needed, throughout the organisation. The administrator defines a process to streamline administration according to the desired level of control, including: who has what privileges, how enrolment works and who receives what type of notifications.

Administrator Type	Allowed Tasks
Security Administrator	Assign roles (administrator privileges and wizard access) to other administrators.
Configuration Administrator	Configure VeriSign Managed PKI for SSL, specify enrolment page contents, and manage the database and reporting features.
Certificate Management Administrator	Approve and reject certificate requests, revoke certificates, assign requests to other administrators and manage the certificate lifecycle. To facilitate the authentication process, it may be helpful to assign the Certificate Management Administrator role to an administrator who knows a particular group of subscribers well.
Read-only	View current requests, certificate data and log files. This is the default role for all administrators after the first administrator.

The certificate management system should have the flexibility and customisation tools necessary to tailor it to your environment. Role-based access control and dynamic assignment of privileges help enforce the administrative process. Administrators log in to the system with unique credentials to perform the lifecycle tasks available to them based on their role and organisations.

Figure 1: VeriSign Managed PKI for SSL Model



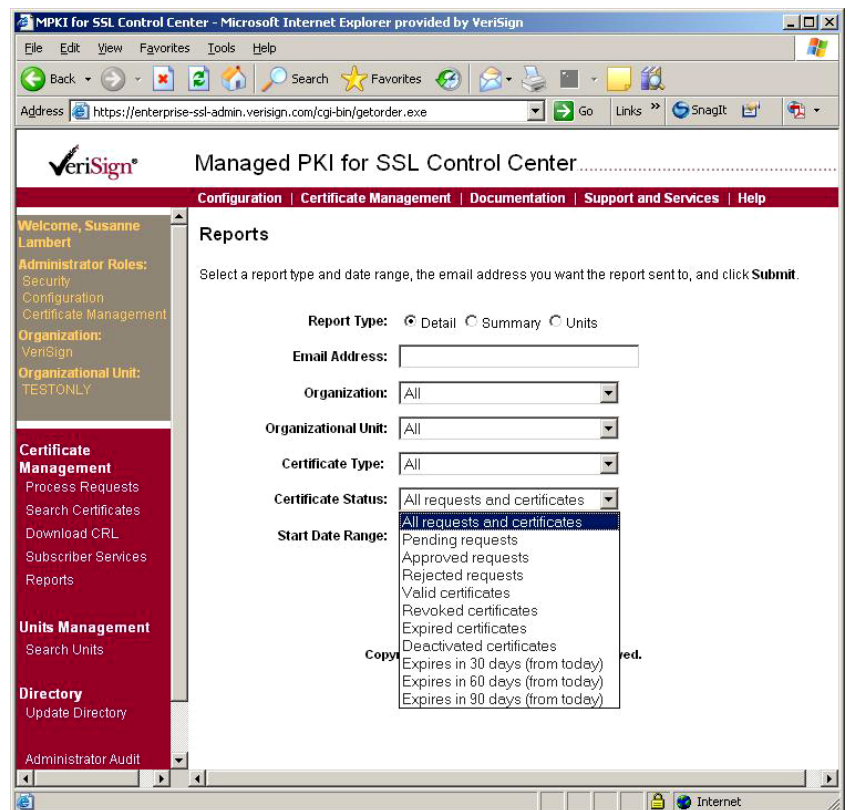
To request an SSL Certificate, a subscriber visits an enrolment page and completes a Web-based form. The certificate may be approved or rejected instantly or set as pending, depending on the predetermined administration rules. Domain blocking prevents subscribers from purchasing individual certificates for managed domains by redirecting them to the managed account enrolment page.

Preset notifications help streamline the process and alerts keep administrators informed. Expiry alerts, sent as e-mails or text messages, may be sent to several administrators and an alias account. When the number of available certificate units drops below a set number, the administrator receives a replenishment alert to purchase more. Pending alerts let administrators know when they need to log in and review requests. Confirmation e-mails notify administrators of instantly-issued certificates.

Output: a clearly articulated administrative process integrated into the management system.

5. Run regular reports on available units and renewals

Access to real-time information about enterprise-wide SSL Certificates helps system administrators better manage their time and resources. Instead of tracking certificates in a spreadsheet, summary and detail reports show the actual unit inventory across the enterprise by certificate status: all requests and certificates, pending, approved, rejected, valid, revoked, deactivated, expired or expiring. A renewal report with 90-, 60- and 30-day alerts helps an administrator plan the quarterly budget for SSL Certificate renewals. Administrators may customise detailed certificate usage reports by organisation or administrator. Audit logs record detailed history of all administrator actions related to every issued certificate.



Output: better resource allocation and oversight.

6. Revoke and replace certificates as needed

Consolidated inventory and management tools make it easier to revoke and replace certificates. If a private key is lost or compromised, or if a server crashes and a certificate is deleted, the administrator can revoke the certificate and issue a replacement.

Output: more control over lost or missing certificates.



### + SSL for the Enterprise

The cost and complexity of managing individual SSL Certificates escalates quickly as organisations grow and expand their online services. Installing and managing your own Certificate Authority (CA) for issuing SSL Certificates is resource-intensive and inefficient. VeriSign Managed PKI for SSL is an easy-to-use, Web-based application for issuing, renewing, revoking and managing SSL Certificates. Administrators can customise enrolment pages for their enterprise and VeriSign manages the back-end services in our state-of-the-art facilities.

#### VeriSign Managed PKI for SSL Features

Purchase	Purchase all types of VeriSign certificates for multiple organisations from one account
Enrolment	Customisable enrolment pages, branded subscriber enrolment pages and instant enrolment options
Alerts	Replenishment alerts, renewal notification
Issuance	Instant issuance of certificates
Unlimited Replacement	Unlimited certificate replacement and free 30-day revocation
Web-based Interface Management	Manage all types of VeriSign certificates for multiple organisations from a single portal
Certificate View	Query certificate status across organisations, domains and administrators
Reporting	Summary and detailed reports on certificates by type, status, organisation, expiry date and usage
Audit trails	Audit log of all certificates and administrator actions across organisations and certificate types
Delegated Administration	Delegate administrator responsibilities and privileges by organisation and organisational unit
Security	Two-factor authentication for administrators, role-based access control and retail blocking
Validity Period	1-year, 2-year, 3-year or 4-year validity periods
Domains	Issue certificates to multiple domains, add domain names, assign domains to organisations
Support	Telephone, Web, e-mail and interactive online help included for 60 days. Optional extended plans.
Usage	Web sites, intranets, extranets, e-commerce sites, multiple logical servers
Browser Compatibility	Compatible with virtually every browser in use



VeriSign Managed PKI for SSL offers access to all VeriSign SSL Certificates, offering strong encryption, rigorous authentication, the VeriSign Secured™ Seal and a NetSure® Protection Plan with up to \$250,000 in extended warranty protection. VeriSign is the leading SSL provider of SGC-enabled SSL Certificates, enabling 128- or 256-bit encryption for over 99.9 per cent of Internet users.

### VeriSign Managed PKI for SSL Certificates

Extended Validation SSL Certificates	True 128-bit or 256-bit SSL with the most stringent authentication process to provide the green address bar and the VeriSign Secured Seal
Premium SSL Certificates	True 128-bit or 256-bit SSL and the VeriSign Secured Seal
Standard SSL Certificates	High-quality encryption and the VeriSign Secured Seal
Premium Intranet SSL	True 128-bit or 256-bit SSL for internal security
Standard Intranet SSL	High quality encryption for internal security
Code Signing Certificates	Assure the integrity and authorship of code and content
Financial SSL Certificates for OFX and Subject Alternative Names (SAN) Certificates	Authenticate and secure transactions on the Internet for qualifying financial institutions

### + 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. VeriSign Managed PKI for SSL provides enterprises and service providers with SSL Certificates from the Web's most trusted security provider and the tools to manage them across the organisation.

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

© 2009 VeriSign Sarl. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle, and other trademarks, service marks and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. All other marks are trademarks of their respective owners.