



WHITE PAPER

SIMPLIFY SSL CERTIFICATE MANAGEMENT ACROSS THE ENTERPRISE



CONTENTS

- 1 INTRODUCTION
- 1 FIVE STEPS TO TAKE CONTROL OF SSL AND CODE SIGNING CERTIFICATES
- 5 A PLATFORM FOR SINGLE-POINT CONTROL AND FULL VISIBILITY
- 5 CONCLUSION
- 5 LEARN MORE



SIMPLIFY SSL CERTIFICATE MANAGEMENT ACROSS THE ENTERPRISE

INTRODUCTION

The need for SSL Certificates has moved well beyond the “buy” page to core functions of the enterprise. SSL Certificates are used to protect remote employee and partner communications via webmail, chat and IM. Browser-to-server communications for cloud-based services require SSL Certificates when used to display customer account information, business partner transactions and for employee productivity tools. Finally, SSL Certificates are used to secure server-to-server communications for applications and data exchange.

Managing individual Certificates across a large organization quickly becomes complicated with multiple locations, many divisions, and rapidly growing Web-based services. If an SSL Certificate expires, a company not only loses sales and puts customer confidence in jeopardy, employees and business partners may not be able to do their work or risk exposure of confidential information. Managing SSL Certificates across complex networks to ensure protection and prevent unanticipated expirations has become mission critical to all businesses.

This guide provides five simple steps for IT professionals to take control of SSL and Code Signing Certificates across the enterprise, and recommendations for a management platform for full visibility and single-point of control for these Certificates throughout their lifecycle.

FIVE STEPS TO TAKE CONTROL OF SSL AND CODE SIGNING CERTIFICATES

The following five steps will help an IT administrator gain control over all SSL and Code Signing Certificates within the enterprise.

1. Perform an audit of all domains and Certificates.
2. Consolidate all Certificates into a managed account.
3. Define an administrative process for your organization.
4. Set up alerts, run regular reports on available units and renewals.
5. Revoke and replace Certificates as needed.

1. Perform an audit of all domains and Certificates.

Do you know where your SSL Certificates are? Visibility into all SSL Certificates deployed in the enterprise is critical to securing online transactions, communications and Web-based applications. Whether starting from scratch or validating an existing list, a Certificate discovery tool can be used to automate the process and catalogue the location, expiration date, validity period, and key size of SSL Certificates as well as Code Signing Certificates.

However, most Certificate Authority (CA) discovery tools only find SSL Certificates issued by that CA or of a particular type. The audit will miss Certificates purchased outside of the approved process, the very SSL Certificates the administrator should be most concerned about. When choosing an SSL enterprise management platform, look for a universal Certificate discovery tool to save time, reduce risk, and simplify the audit process. The discovery tool should also verify that SSL Certificates have been properly installed.

Output: Real-time reporting of all Certificates on all secured domains.

Scenario: The Mystery Expiration

An e-commerce server goes down and no one knows why. Thousands of sales are lost each hour while IT tracks down the problem. An SSL Certificate purchased from a non-approved vendor expired and the administrator who purchased it left the company. The renewal notice never reached the current administrator and no one knew the SSL Certificate existed on the network. VeriSign® Managed PKI for SSL Certificate enables the administrator to discover all Certificates within the enterprise from **all** CAs for better visibility and control.



2. Consolidate all Certificates into a managed account.

The audit gives you the complete information needed to evaluate your SSL protection and begin consolidating Certificates into a single managed account for better control. In reviewing the audit, consider the following questions:

- Are all Certificates properly installed?
- Do Certificates have the appropriate level of encryption and authentication?
- Are trust marks or security seals displayed on appropriate pages?
- Are all servers that should be protected secured with SSL?
- Are there any unauthorized Certificates that need to be managed?

Today’s SSL Certificates offer a range of encryption strengths and authentication levels. But many SSL enterprise management tools require a different log-in for each type of Certificate. As the organization grows and the number of administrators increases, managing multiple accounts for different types of SSL Certificates will become cumbersome unless you have a single point of control. As current Certificates approach their expiration date, replace them with units from a primary managed account that supports all types of Certificates required. Having a single managed account will also enable you to reduce costs by taking advantage of volume discounts.

Output: A single, managed account for all Certificates within the enterprise.

Scenario: 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 from other integration activities. Purchase multiple Certificates through VeriSign® Managed PKI for SSL for renewal and instant issuance.

VeriSign Managed PKI for SSL

FEATURES	BENEFITS
Web-based management portal	A feature-rich interface for Certificate lifecycle management makes setup and deployment easy.
Automated Certificate discovery	Enterprise-wide visibility of all Certificate types from all CAs reduces risk of down time and deployment of rogue Certificates.
Single-point control	Consolidate purchasing and management across business units and locations to reduce costs.
Customizable workflow and audit trails	Delegate administration and pre-approve domains for instant, on-demand issuance with extensive audit trails to track operations.
Full range of SSL Certificates	Manage all Certificate types from one console: Extended Validation (EV), SGC, SAN for Unified Communications, standard SSL and Code Signing.
Robust reporting	Role-based access to real-time, offline, and monthly reports help manage resources and risk.
Customizable alerts and notifications	Prevent missed communications with automated alerts to multiple contacts.
World-class support	Phone, Web, email, and online help, free for 60 days with optional extended plans.



3. Define an administrative process for your organization.

An enterprise Certificate management account enables authorized administrators to purchase multiple Certificate units at one time for issuance, as needed, throughout the organization. The administrator defines a process to streamline management according to the desired level of control, including who has what privileges, how enrollment works, and who receives what type of notifications.

The Certificate management system should have the flexibility and customization necessary to tailor it to your environment. Role-based access and dynamic assignment of privileges help enforce the administrative process. When administrators log in with their unique credentials they are able to manage Certificates based on their role and organization. Audit logs should record a detailed history of all administrator actions related to every issued Certificate.

When an administrator requests an SSL or Code Signing Certificate, the Certificate may be instantly approved, rejected or set as pending, depending on pre-determined administration rules. Domain blocking prevents subscribers from purchasing individual Certificates for managed domains by redirecting them to the managed account enrollment page.

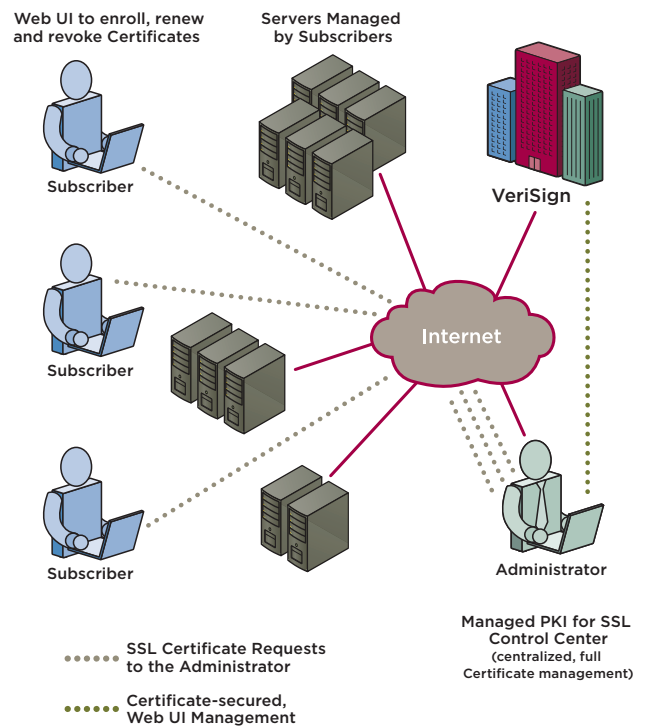
During the enrollment process for most SSL Certificates, the purchaser provides contact information for a Technical Contact, including name, phone number, and email address. Contact information standards and notification settings should reflect your defined administrative process. Expiration alerts, sent as emails or text messages, may be sent to several administrators as well as an alias account such as *ssladmin@yourdomain.com*. Pre-set notifications help streamline the process and keep administrators informed. For example:

- 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 emails notify administrators of instantly-issued Certificates.

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

Scenario: 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 they'll have to wait 24 hours for your approval. The delay is a costly rubber stamp for a pre-approved use of a Certificate in an authorized domain by an authenticated user. Delegate administration using VeriSign® Managed PKI for SSL to allow instant issuance of the Certificate.



WHITE PAPER

USER TYPES	RESPONSIBILITIES
Primary Account Administrator	Assign roles, set administrator privileges and access to wizards for other administrators.
Secondary or Department Administrator	Manage the Certificate lifecycle for a particular domain, department or division: approve and reject Certificate requests, revoke Certificates, assign requests to other administrators.
Read-only Access	View reports such as current requests, Certificate data, and log files.

4. Set up alerts, run regular reports on available units and renewals.

Regular reports generated by the Certificate management platform help system administrators better manage time and resources. Instead of static information in a spreadsheet, real-time reports should show the actual unit inventory across the enterprise by Certificate status: all requests and Certificates, pending, approved, rejected, valid, revoked, deactivated, expired, or expiring. Renewal reports with 90, 60, and 30 day alerts help an administrator plan for SSL Certificate renewals and take advantage of bulk discounts. Historical reports give administrators valuable insight into past usage for future planning and management.

Customization and multiple file formats provide maximum integration into administrative processes and tools. The administrator should have the option to customize detailed Certificate usage reports by organization or administrator and to create automated reports for regular delivery to the key contact. File format options such as pdf, html, and CVS enable information to be shared and integrated into other software for viewing and analysis.

Output: Annual resource allocation and budgeting for SSL.

5. Revoke and replace Certificates as needed.

Consolidated inventory and management tools make it easier to revoke and replace Certificates. When servers are taken offline, moved or replaced, SSL Certificates need to be properly moved using revoke and replace. 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, it should be revoked to prevent misuse. If a private key is lost or compromised or if a server crashes and a Certificate is deleted, the administrator should be able to revoke the Certificate and issue a replacement.

Output: More control over lost or missing Certificates.

Scenario: The Relocation

In the process of merging data centers, you need to move Certificates from one physical location to another. You don't want to purchase new Certificates for the new site and lose the validity period of existing Certificates, but can't afford any downtime. Use "revoke and replace" to move Certificates from one server location to another with VeriSign® Managed PKI for SSL.



A PLATFORM FOR SINGLE-POINT CONTROL AND FULL VISIBILITY

Without the right tools, managing extensive SSL deployments across complex infrastructures can be a manual, time consuming and error-prone process. Most Certificate Authorities offer management tools for their Certificates, however, they lack discovery tools for all Certificates and require IT administrators to manage multiple platforms and logins for different Certificates. Developing a self-signing Certificate Authority (CA) provides better single-point control, however, an in-house solution requires upfront investment, time for development, as well as ongoing enhancements to manage new SSL Certificate types such as Extended Validation.

VeriSign® Managed PKI for SSL combines the best features of a trusted CA and a self-signing solution: single-point control on a highly reliable, scalable infrastructure and automated Certificate discovery of all SSL and Code Signing Certificates across the whole enterprise. In addition, as soon as Certificates are purchased and an account is created, administrators have full access to customize accounts and delegate responsibilities with no infrastructure set-up time or cost.

- **Managed PKI for SSL is a cloud-based service that requires no upfront capital investment with a low total cost of ownership to maintain. As your organization grows, the highly reliable VeriSign infrastructure scales with you.**
- **The Certificate Discovery module within Managed PKI for SSL enables administrators to track all SSL and Code Signing Certificates across multiple CAs and heterogeneous business environments in real time.**
- **Centralized control with flexible delegation allows you to set management controls based on your organization's workflow. Approved administrators managing pre-approved domains may issue SSL Certificates to multiple servers on demand while blocking purchases attempted outside of the approval process.**
- **VeriSign® SSL Certificate options include a range of encryption, authentication and term levels to satisfy your business needs and include the VeriSign Secured® Seal, the most trusted mark on the Internet.**
- **Better visibility and control reduce the risk of downtime for communications and operations due to unexpected expirations, and identify unauthorized SSL deployments.**

1. Includes VeriSign subsidiaries, affiliates, and resellers.

Key Benefits

Lower Total Cost of Ownership Reduce the cost and complexity of managing multiple SSL Certificates across your organization with single-point control, Certificate discovery 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 Find rogue SSL Certificates before they disrupt business operations or put security in jeopardy with Certificate discovery, and track life cycle operations with detailed audit trails.

Increased customer confidence with VeriSign Over 95% 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.

CONCLUSION

Managing SSL Certificates across an enterprise has become complex. VeriSign® Managed PKI for SSL provides a simple yet powerful platform to discover and manage SSL Certificates cost effectively. The cloud-based platform enables IT administrators to automate critical tasks, reduce costs and risks in managing SSL Certificates across the enterprise.

LEARN MORE

For more information about VeriSign® SSL Certificates, please call: +61 9674 5500 or email: sales@verisign.com.au.

