



WHITE PAPER

---

## How to Simplify SSL Certificate Management





WHITE PAPER



CONTENTS

+ Meeting the Challenge of Multiple SSL Certificate Management	3
+ SSL Certificates Provide Core Web-Transaction Security	4
+ One-by-One Certificate Management Is a Tedious Process	5
SSL Certificate Lifecycle Elements	5
+ Simplifying SSL Management with VeriSign's Web-Based Solution	6
+ VeriSign Certificate Center Enterprise Account Solutions	7
+ Reap the Benefits of a VeriSign Certificate Center Enterprise Account	8
+ Learn More	9
+ About VeriSign	9



# How to Simplify SSL Certificate Management

## + Meeting the Challenge of Multiple SSL Certificate Management

Protecting the confidentiality and integrity of sensitive information transmitted over your organisation'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, from server to server, and among other networking devices such as server load balancers or Secure Sockets Layer (SSL) accelerators. For a complete solution, cross-network security must protect servers facing both the Internet and private intranets.

SSL,<sup>1</sup> the world's standard technology used to protect information transmitted over the Web with the ubiquitous HTTP protocol, 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 VeriSign authentication procedures instill, your company can immediately protect sensitive data transmitted between your servers and your customers, employees, and business partners.

VeriSign® Certificate Center Enterprise Account is an easy-to-use and flexible Web-based service for deploying and managing multiple SSL Certificates across the organisation. Leveraging the company's scalable and highly secure infrastructure, VeriSign® Certificate Center Enterprise Account is a solution that enables you to dramatically reduce much of the cost associated with SSL Certificate deployment while maintaining full local control.

### VeriSign® Certificate Center Enterprise Account

**Simple:** Web-based service for managing all your SSL Certificates—no up-front hardware or software to install

**Efficient:** Enrol, issue, revoke, replace and renew with a few clicks of a mouse

**Time-saving:** Issue SSL Certificates on demand

**Value:** Provides discounted, bulk purchases of SSL Certificates



#### VeriSign Secured® Seal

Be sure to post the VeriSign Secured Seal on your home page or other pages where confidential information exchange takes place. The VeriSign Secured Seal lets your site visitors know that you have chosen leading services to help protect them.

<sup>1</sup>The Internet Engineering Task Force has renamed the Secure Sockets Layer (SSL) protocol Transport Layer Security (TLS) and is working on wider adoption of TLS. "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 that the destination of the data is legitimate, encryption to protect the data against interception or tampering, and message integrity to guarantee that the information isn't tampered with during transmission. Digital certificates from VeriSign use SSL technology to address all three of these requirements. SSL has become a global 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® 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 an SSL Certificate. Leading Web browsers inherently trust SSL Certificates signed by the VeriSign root certification-authority (root CA) certificates, which help provide 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 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 authorised 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 has 256-bit capability, meaning that the SSL session key is 256 bits long. However, browser versions exported outside the United States 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 en route. All parties to the transaction can 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 organisation's choice to deploy numerous SSL Certificates includes a practical management decision: Should you do so manually, or should you use a scalable Web-based service, such as VeriSign Certificate Center Enterprise Account, that automates many certificate-management processes? Managing SSL Certificates ad hoc is appropriate for small organisations managing only a couple of them. However, managing multiple SSL Certificates can be time-consuming and overwhelming.

The enrolment process for the SSL Certificate includes extensive collection and verification of information required by the Certification Authority (CA), an organisation 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 proper documentation, articles of incorporation, and other business documents. Also, separate purchase authorisation 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. Five activities can be performed on an SSL Certificate during its lifecycle:

#### *SSL Certificate Lifecycle Elements*

- **Enrol**—Complete application to purchase an SSL Certificate, including submission of organisation eligibility.
- **Issue**—CA issues the certificate; purchaser installs the certificate on a designated server or device to enable SSL services.
- **Revoke**— If a private key is lost or compromised or if a server crashes and a certificate is deleted.
- **Replace**—When a certificate has incorrect information, loss or destruction of the private key or other malfunction.
- **Renew**—Ensure that each certificate is properly renewed with the CA in a timely manner for uninterrupted service.

Using an ad hoc manual process is adequate to manage lifecycles of a few certificates. Managing a multitude of certificates, however, is tedious, time consuming, expensive, and often an overwhelming process. Automating the process with VeriSign Certificate Center Enterprise Account is the logical step to efficient SSL security management.

**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 Certificate Center Enterprise Account. Now, the company can meet its efficiency goals and has cut the costs of certificate acquisition and management.

**+ Simplifying SSL Management with VeriSign’s Web-Based Solution**

Companies implementing five or more SSL Certificates can significantly ease certificate management processes with the automated benefits of VeriSign Certificate Center Enterprise Account. With Web-based SSL Certificate management, your organisation gets full visibility into the certificate inventory, centralised operational and financial control, and the assurance of full SSL protection for server transactions.

The VeriSign Certificate Center Enterprise Account solution is ideal for businesses that need to manage multiple SSL Certificates but do not require complex, delegated administration capabilities. From within the VeriSign Certificate Center Enterprise Account portal, customers can order, enroll, issue, renew, revoke and replace certificates. They have centralised visibility into pending orders, expiring certificates or any actions that require their attention.

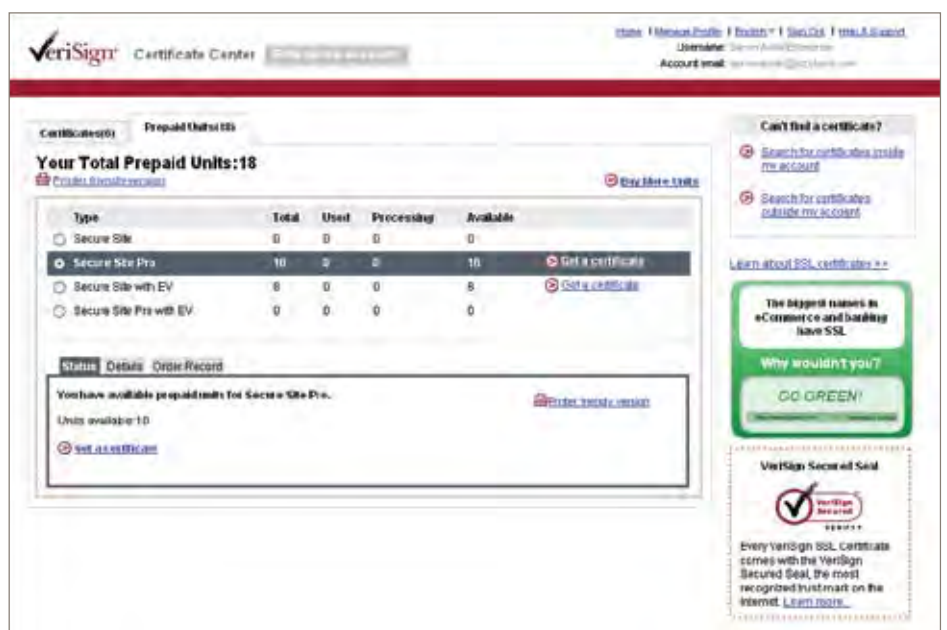
Within the account, customers can pre-authenticate their organisation(s) so that future certificates can be instantly issued, eliminating the bulk of the time typically required for authentication.

Customers acquire prepaid units (certificates), which they redeem for future certificates. By using this system, customers who wish to streamline financial approval of SSL spending can do so, and those who have larger volume purchases can benefit from bulk-pricing discounts.

VeriSign Certificate Center Enterprise Account allows users to:

- Proactively manage certificates quickly and easily from a single portal/console
- Have greater visibility into certificate status for reduced risk of downtime
- Save money by getting bulk discounts from bundling yearly SSL purchases
- Streamline budget approvals by bundling all SSL purchases under a single transaction
- Accelerate certificate purchases and issuance with prepaid units, payment by credit card and organization pre-authorisation

Customers can now easily and cost-effectively administer their portfolio of SSL Certificates from a central tool.





### *Extended Validation (EV) SSL Certificates:*

Your customers are looking for the green address bar so they feel protected online. VeriSign EV SSL Certificates work with high-security browsers to display the green address bar, helping customers feel more confident about the security of your site. This encourages them to do more business with your company.

## **+ VeriSign Certificate Center Enterprise Account Solutions**

VeriSign offers a variety of SSL Certificate solutions to meet all your SSL security needs—inside and outside the firewall:

### *Secure Site Pro with Extended Validation (EV)*

Give your customers the confidence to make their purchases online with the most trusted and secure option for SSL: VeriSign® Secure Site Pro with EV SSL Certificates. Extended Validation triggers the display of the green address bar in the latest high-security browsers, and true 128-bit SSL Certificates enable every site visitor to experience the strongest SSL encryption available to them. Plus:

- Extended Validation, green address bar
- 128-bit minimum to 256-bit encryption
- US\$250,000 warranty
- VeriSign Secured® Seal
- Installation Checker

### *Secure Site with EV*

Give your customers the confidence to make their purchases online with VeriSign® Secure Site with EV SSL Certificates. Extended Validation triggers the display of the green address bar in high-security browsers. Plus:

- Extended Validation, green address bar
- 40-bit minimum to 256-bit encryption
- US\$100,000 warranty
- VeriSign Secured® Seal
- Installation Checker

### *Secure Site Pro*

Show your customers that you're taking every step to protect their private information with strong encryption: VeriSign Secure Site Pro SSL Certificates. True 128-bit SSL Certificates enable every site visitor to experience the strongest SSL encryption available to them. Plus:

- 128-bit minimum to 256-bit encryption
- US\$250,000 warranty
- VeriSign Secured® Seal
- Express delivery
- Installation Checker

### *Secure Site*

VeriSign® Secure Site SSL Certificates protect the transfer of sensitive data on Web sites, intranets, and extranets using a minimum of 40-bit and up to 256-bit encryption. Plus:

- 40-bit to 256-bit encryption
- US\$100,000 warranty
- VeriSign Secured® Seal
- Installation Checker



### *Strongest Authentication Process*

VeriSign protects businesses with the strongest three-step certificate-authorisation process. We verify and ensure the veracity of the organisation and Internet domain, doublechecking facts with research and personal calls by VeriSign staffers.

### *Strongest Warranty Protection*

Each VeriSign SSL Certificate is backed by the VeriSign® Netsure® warranty protection program, which protects VeriSign SSL Certificate customers against economic loss resulting from the theft, corruption, impersonation, or loss of use of a certificate. Warranty limits are US\$250,000 of protection for Secure Site Pro certificates and US\$100,000 for Secure Site certificates.

### **+ Reap the Benefits of a VeriSign Certificate Center Enterprise Account**

The VeriSign Certificate Center Enterprise Account SSL solution will help simplify management of your organisation's SSL Certificates, requiring no up-front hardware or software to install or operate. With a few clicks of a mouse, you can efficiently enroll, issue, revoke, replace and renew SSL Certificates across the enterprise from one central point.

A VeriSign Certificate Center Enterprise Account gives users:

- Faster certificate enrolment and issuance
- Greater visibility into certificate status for more proactive management for reduced risk of down-time
- Cost-effective spending on bulk purchases
- Maximum flexibility with:
  - + Single certificate and bulk purchases
  - + Payment by credit card, purchase order or check

The VeriSign solution saves you time because all actions occur on demand, and all management activity is secured by authentication and encryption. The solution includes discounts for bulk purchases of SSL Certificates. It's a cost-effective and simple solution for managing all your SSL Certificates. To learn more about VeriSign Certificate Center Enterprise Account, please call one of our SSL security specialists at +61 3 9674 5500.

VeriSign is the leading Secure Sockets Layer (SSL) Certificate Authority enabling secure e-commerce, communications, and interactions for Web sites, intranets, and extranets. Choose the most trusted mark on the Internet and enable the strongest SSL encryption available to every site visitor.



## WHITE PAPER

### + Learn More

For more information about VeriSign® Certificate Center Enterprise Account, please call +61 3 9674 5500 or email: [sales@verisign.com.au](mailto:sales@verisign.com.au)

### + About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

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

©2008 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

00020913 09-11-2008