



WHITE PAPER

Managing SSL Security in Multi-Server Environments

Easy-to-Use VeriSign® Web-Based Services Speed
SSL Certificate Management and Cut Total Cost
of Security





CONTENTS

+ A Smart Strategy for Managing SSL Security on Multiple Servers	3
SSL Certificates Provide Core Web-Transaction Security	4
+ One-by-One Certificate Management Is a Tedious Process	5
SSL Certificate Lifecycle Elements	6
+ Simplifying SSL Management with a Powerful VeriSign Web-Based Solution	7
Web Interface Provides Centralised Local Control	7
+ Automated Reports Keep You in Control	9
VeriSign Managed PKI for SSL Certificate Solutions	10
+ Enterprise-Class Service with SSL Expertise at Your Fingertips	11
+ Test the Benefits of Managed PKI for SSL	12
Trial Offer	12



A Smart Strategy for Managing SSL Security on Multiple Servers

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,¹ 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® Managed PKI for SSL 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, Managed PKI for SSL is an enterprise solution that enables you to dramatically reduce much of the cost associated with SSL Certificate deployment while maintaining full local control.

VeriSign® Managed PKI for Intranet SSL, a Web-based companion service for deploying and managing SSL Certificates on hosts used only on private intranets, provides internal hosts with features and benefits identical to Managed PKI for SSL.



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.

VeriSign Managed PKI for SSL

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

Efficient: Enrol, approve, issue, reject, revoke, and renew with a few clicks of a mouse

Time saving: Issue SSL Certificates on demand

Secure: Certificate-secured administrator account access

Comprehensive: Covers hosts facing the Internet or on intranets (optional)

Value: Provides discounted, bulk purchases of SSL Certificates

¹ 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 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 has 128-bit capability, meaning that the SSL session key is 128 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.

SSL CASE STUDY: Finance

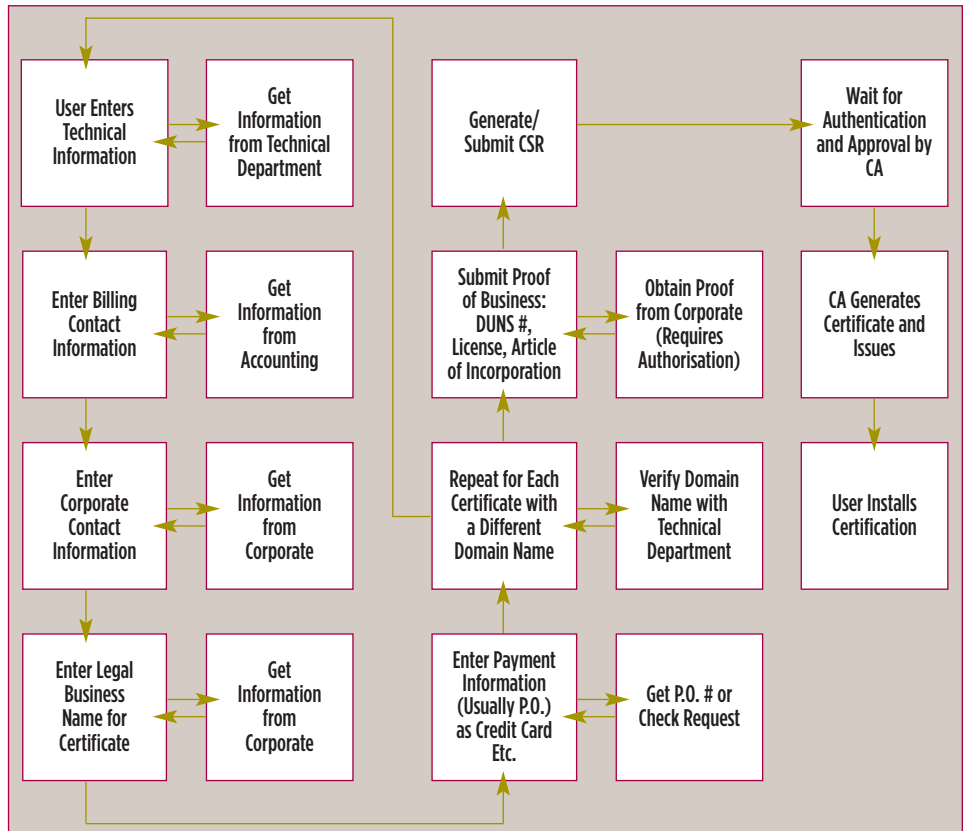
A large financial institution used more than 700 certificates, including 500 units purchased with VeriSign Managed PKI for SSL and more than 200 individually purchased units. After consolidating all certificates under Managed PKI for SSL, the company cut annual recurring renewal and management costs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

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 Managed PKI for SSL or VeriSign Managed PKI for Intranet SSL, that automates many certificate-management processes? Managing SSL Certificates ad hoc is appropriate for small organisations in which one person is responsible for deploying and managing only a couple of them. 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 decentralised organisations consider the volume discounts other SSL Certificate vendors offer to be sufficient, but they fail to see the hidden costs of managing SSL Certificates across the organisation. The price of the SSL Certificate itself is not the only cost to consider, especially in organisations with multiple server types, locations, and server administrators.

Consider the flow-chart diagram below, which shows each step of a typical enrolment process for an SSL Certificate.



SSL Certificate Management Service for Internal Hosts

VeriSign Managed PKI for Intranet SSL secures communications across your intranet or private network. The following are key benefits:

- Same features and benefits as Managed PKI for SSL
- Simple, efficient, time saving, secure, and provides value
- Useful for securing internal business operations, company portals, and testing development environments

The enrolment process for the SSL Certificate shown above includes extensive collection and verification of information required by the certification authority (CA), an organisation that authorises and issues SSL Certificates. Some of the required enrolment 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. Six 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 and administrative data
- **Approve**—Interface with an independent CA, which verifies the organisation's eligibility and approves granting of the certificate; available only with VeriSign Managed PKI for SSL and VeriSign Managed PKI for Intranet 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 unauthorised certificate-enrolment request; available only with VeriSign Managed PKI for SSL
- **Revoke**—Immediate administrative revocation of a certificate; available only with VeriSign Managed PKI for SSL and VeriSign Managed PKI for Intranet 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, however, is tedious, time consuming, expensive, and often an overwhelming process—especially in large, distributed organisations. Automating the process with VeriSign Managed PKI for SSL and VeriSign Managed PKI for Intranet SSL is the logical step to efficient SSL security management.

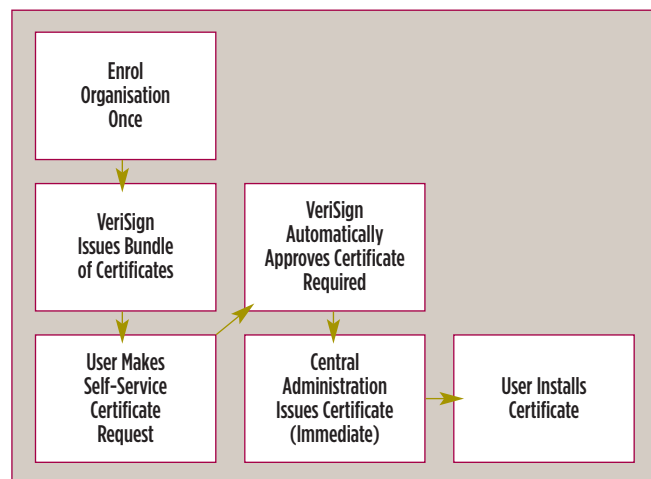
SSL CASE STUDY: Insurance

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 Managed PKI for SSL. Now, the company can meet its efficiency goals and has cut the costs of certificate acquisition and management.

Simplifying SSL Management with the Powerful VeriSign Web-Based Solution

Companies implementing five or more SSL Certificates can significantly ease certificate-management processes with the automated benefits of VeriSign Managed PKI for SSL and VeriSign Managed PKI for Intranet SSL. 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 flow chart below shows how VeriSign Managed PKI for SSL and VeriSign Managed PKI for Intranet SSL simplify the complex certificate-enrolment process for immediate, on-demand issuance of SSL Certificates.

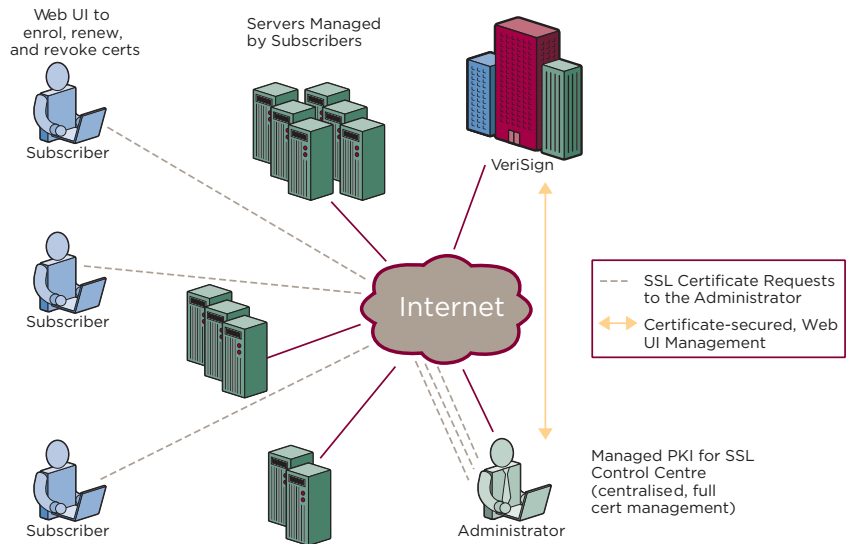


+ Web Interface Provides Centralised Local Control

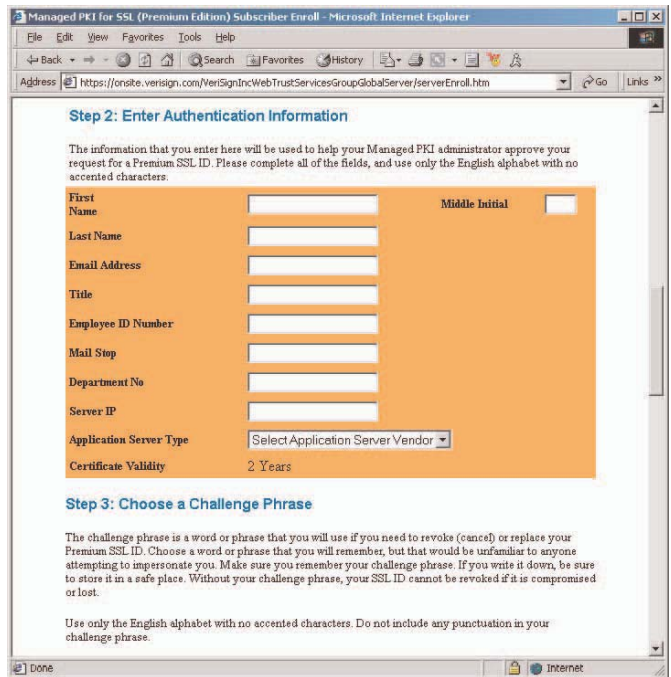
The key to VeriSign Managed PKI for SSL and VeriSign Managed PKI for Intranet SSL process automation is a hosted Web-based infrastructure. Your organisation's local administrator centrally manages all aspects of the SSL Certificate lifecycle with a Web-based management-tools interface called Control Centre. Authenticated administrators use Control Center to manage and control certificate enrolment, approval, issuance, rejection, revocation, and renewal. Control Center provides:

- Full PKI management
- Centralised administration and control
- Access to specialised reports to track certificate details
- Audit log of all certificates issued and all administrator actions
- Email alerts
- Download of certificate-revocation list (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 customisable screens. All data are automatically processed in the VeriSign hosted, carrier-class data centre, which acts as a behind-the-scenes relay hub between the administrator and users—the diagram below shows workflow between these entities:



The VeriSign Managed PKI for SSL and VeriSign Managed PKI for Intranet SSL customisable Web-interface screens enable users to request certificates and carry out other tasks without requiring human intervention. For example, the illustration below shows a typical VeriSign Managed PKI for SSL or VeriSign Managed PKI for Intranet SSL browser screen used for entering certificate-request information.



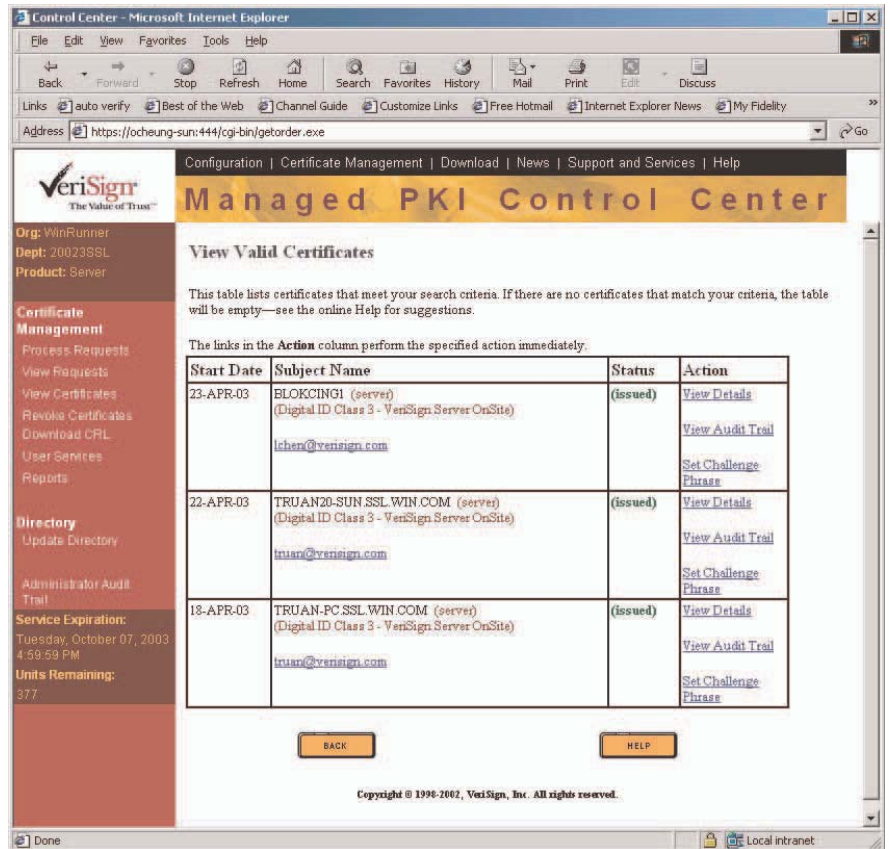
VeriSign Managed PKI for SSL Customers Say:

- 94 percent centrally control certificate management and costs
- 59 percent use one administrator; 27 percent use two
- 53 percent estimate internal costs are less than 5 percent more as a percentage of certificate price; 41 percent estimate 5 to 25 percent more
- 64 percent use some certificates for internal, behind-the-firewall applications (From: 2003 survey; 76 percent of businesses surveyed have more than 1,000 employees)

Automated Reports Keep You in Control

Control Centre provides a complete history of all certificate activity. Comprehensive Web-based reports automatically generated by VeriSign Managed PKI for SSL and VeriSign Managed PKI for Intranet 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 Centre, 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 Managed PKI for SSL and Managed PKI for Intranet SSL solutions to meet all your SSL security needs—inside and outside the firewall:

Premium Edition—128-bit SSL security for protecting the most sensitive data on your network. VeriSign Managed PKI for SSL Premium Edition Certificates use SGC technology to enable 128-bit SSL encryption on almost all computers in use today, including older browsers and all Windows® 2000 systems.

- Premium Edition SSL Certificates guarantee a 128-bit SSL session in all current browsers. Other CAs promote their SSL Certificates as having 128-bit capability, but these do not use SGC and therefore will actually experience reduced encryption levels on older, export version browsers and on many Windows 2000 computers, regardless of the version of Internet Explorer installed on these systems.
- VeriSign is the only CA authorised by the U.S. Department of Commerce to distribute 128-bit SGC SSL Certificates outside the United States.

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 and many Windows 2000 systems

Extensive Server Platform Support

The VeriSign Managed PKI for SSL Standard Edition and Premium Edition certificates are compatible with a comprehensive list of server platforms. (See details at www.verisign.com/products-services/security-services/ssl/ssl-certificates/)

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, double-checking facts with research and personal calls by VeriSign staffers.

Strongest Warranty Protection

Each Managed PKI for 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 Premium Edition certificates and US\$100,000 for Standard Edition certificates.

VeriSign Managed PKI 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 centre
- 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 the VeriSign hosted Managed PKI for SSL and Managed PKI for Intranet SSL solutions is continuous access to the company's rich store of security expertise. VeriSign has issued more than 450,000 SSL Certificates, which makes it the leading provider worldwide. As part of the solution, customers get a broad range of enterprise support services, including:

- A World-class 24/7 data centre
- A 24/7 support organisation
- Complete Web-based resources
 - + Technical Web seminars
 - + Knowledge Base
 - + Troubleshooting tips
 - + Tutorials
 - + List of frequently asked questions
- 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 or hot-site disaster recovery facility
 - + Recovery facility
 - + Maintenance of performance levels and scale capacity

Along with the support options available, your organisation'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 Managed PKI for SSL

The VeriSign Managed PKI for SSL and Managed PKI for Intranet SSL solutions 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 enrol, approve, issue, reject, revoke, and renew SSL Certificates across the enterprise from one central administration point. 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.

+ Trial Offer

VeriSign invites your organisation to test the benefits of using a hosted, automated Web-based service for managing SSL Certificates. To request a free demonstration of VeriSign Managed PKI for SSL or to learn more about VeriSign Managed PKI for Intranet SSL, please call one of our SSL security specialists, at +61 3 9674 5500

Visit us at www.VeriSign.com.au for more information.