



DATA SHEET

# VERISIGN® MANAGED PKI FOR INTRANET SSL

Today's private network or intranet communications must be at least as secure as the confidential traffic that crosses the Internet. The information transmission is usually protected with Secure Sockets Layer (SSL) Certificates installed on servers.

However, managing SSL Certificates can be challenging when multiple servers are deployed across various divisions and locations. Also, developing and maintaining own Certificate Authority (CA) for issuing SSL Certificates is a drain on resources and costs. What is needed is a centralized and easy-to-use solution for issuing, renewing, revoking, and managing access privileges for all of your company's SSL Certificates.

## MANAGED PKI FOR SSL CERTIFICATES

VeriSign® Managed PKI for SSL (MPKI for SSL) Certificate Service is designed for managing SSL Certificates throughout even the largest company. MPKI for SSL is ideal for companies that need to deploy SSL Certificates to ten or more servers. MPKI for SSL offers:

- A feature-rich portal that simplifies management of the entire life-cycle of SSL Certificates
  - Web-based management for easy setup, configuration and deployment
  - Issue SSL Certificates to multiple servers instantly and on demand
  - Comprehensive support for SSL Certificates including Extended Validation (EV), SGC, SAN for Unified Communications, and Code Signing Certificates
- Centralized management across multiple business units and/or subsidiaries
  - Consolidate purchasing across the businesses to reduce costs
  - Enterprise-wide visibility to enhance control and reduce risk of down-time
  - Customizable certificate requisition workflow with delegated administration
  - Robust reporting and audit trails
- World-class support options
  - Customers can select support packages to match their business requirements

## KEY BENEFITS

Efficient and Scalable Management

- Manage SSL Certificates on all your company's servers through one easy-to-use and highly secure Web based application. To get started, all you need to do is appoint an administrator who has a browser and an Internet connection; VeriSign does the rest.

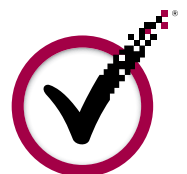
Secures communications across your intranet or private network.\*

- Secures intranet domain names, IP addresses, or host names protecting intranet-based communication for internal Web sites and testing and development environments.

Single Management Interface

- Your administrator can simplify SSL Certificate management by utilizing a single, powerful interface across the entire infrastructure. The industry unique Certificate Discovery module enables administrators to manage SSL Certificates across complex heterogeneous environments that may have SSL Certificates from multiple CAs.

\*Intranet SSL Certificates are not for use on servers or other devices that are publicly accessible from the Internet.





## DATA SHEET

### MANAGING SSL CERTIFICATES IN HETEROGENEOUS ENVIRONMENTS

The Certificate Discovery module within the MPKI enables administrators to track, real-time, all SSL Certificates across multiple CAs and heterogeneous business environments. Without the right tools, managing extensive SSL deployments across complex infrastructures is a manual, time consuming and error-prone process. Oversights, such as an unexpected certificate expiration on a critical server, can have an immediate negative impact on productivity, revenue and operational costs. With the Certificate Discovery module, administrators are able to protect their business from such oversights by:

- Taking a complete inventory of all SSL Certificates and their status
- Identifying renegade certificates and bring them under management

### MPKI FOR SSL ACCOUNT OPTIONS

VeriSign offers two types of MPKI for SSL accounts:

- Managed PKI for SSL Premium Edition utilizes SSL Certificates which support Server Gated Cryptography (SGC) in order to enable 128-bit encryption, the strongest SSL encryption available, regardless of the version of browser version or operating system of the computer visiting the Web site. SGC is used by many leading online retail merchants, banks, brokerages, healthcare organizations, insurance companies, and other businesses that need to guarantee their customers receive the strongest commercially available protection possible.
- Managed PKI for SSL Standard Edition enables 128-bit SSL encryption with newer browser versions while still supporting 40- or 56-bit SSL encryption with older Netscape and Microsoft Internet Explorer browsers and many Windows 2000 systems.

### LEARN MORE

Visit [www.verisign.com/products](http://www.verisign.com/products) for more information. To contact a VeriSign Sales Representative, call 650-426-5115, or send an email to [verisales@verisign.com](mailto:verisales@verisign.com).

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

### KEY BENEFITS

No Up-Front Capital Expense

- There is no need to invest in expensive hardware, software, or overhead you would need to build and maintain your own SSL Certificate Authority (CA). All the back-end services needed to process your SSL Certificate requests are maintained by VeriSign in state-of-the-art facilities designed with high availability and scalability in mind.

Customizable and Extensible Services

- VeriSign provides a host of SSL Certificate bundles and service options, allowing you to take advantage of volume discounts and flexible product support. Choose the quantity, services, and features you need to meet your business requirements.

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 VeriSign's leading services to help protect them.

