



## DATA SHEET



### KEY BENEFITS

#### *Enables Rapid, Widespread Deployment of Digital Certificates*

By leveraging a highly scalable managed service based on open standards, enterprises can easily issue and manage certificates to thousands of end users and network devices.

#### *Minimizes PKI Costs*

The VeriSign Managed PKI service lowers the total cost of ownership when compared to standalone PKI software implementations.

#### *Supports Compliance with Government Mandates*

Enterprises can leverage digital certificate services such as authentication, encryption, digital signing, and non-repudiation to promote compliance with industry-specific regulations regarding data privacy.

#### *Reduces Risk Exposure*

By delegating key security tasks and processes to a proven industry leader, enterprises minimize the risks and penalties associated with improper deployment or operation of an in-house PKI.

## VeriSign® Managed Public Key Infrastructure (PKI) Service

As online commerce, communication, and collaboration become established—and often preferred—modes of business, network security becomes as much a function of letting the “good guys” in as keeping the “bad guys” out. To facilitate tighter integration with business partners, provide secure access to users, ensure business continuity, and maintain compliance with government regulations, enterprises must be able to authenticate internal and external users, and reliably secure online data exchanges, transactions, and communications.

The VeriSign® Managed Public Key Infrastructure (PKI) service is a fully integrated enterprise solution designed to secure intranet, extranet, and Internet applications while enabling fluid interaction with business partners, mobile workers, Web services devices, and other users. This highly scalable service allows enterprises to rapidly establish a robust PKI and certificate authority (CA) system while alleviating the burden of PKI deployment, maintenance, and oversight. Enterprises retain complete control over security policy, authentication models, and certificate lifecycle management. Built on open standards to ensure maximum flexibility, the VeriSign Managed PKI service allows interoperability with virtually any application or device, and is pre-integrated with leading off-the-shelf solutions, including Microsoft® applications and Windows® operating systems. By leveraging the Managed PKI service to deploy digital certificate services, enterprises can reduce the cost and complexity of PKI implementations while providing globally trusted, state-of-the-art authentication, encryption, digital signing, and non-repudiation services within and beyond the enterprise.

### + Comprehensive Functionality

The VeriSign Managed PKI service allows enterprises to quickly, securely, and cost effectively issue digital certificates not only to employees, customers, and business partners, but also to Web services applications and network devices such as servers, routers, and firewalls. Centralized, auditable root key generation; key escrow; and distributed key recovery ensure maximum security and protection of private keys. The service also supports dual key-pair generation, allowing the separate issuance of encryption and signing key pairs. Internationalization features include support for UTF-8 encoding, which allows enterprise users to enroll for and display digital IDs in languages that require non-ASCII characters (such as Japanese, Chinese, and several European languages).



Where it all comes together.™



## DATA SHEET

### *Securely Opens the Enterprise to Trading Partners*

Digital certificates enable enterprise users to conduct secure transactions and communications with virtually anyone, anywhere.

### *Promotes Adoption by Partners, Customers, and Suppliers*

VeriSign offers a proven platform that is recognized and trusted throughout the world, encouraging rapid adoption of PKI-enabled services, both within and outside the enterprise.

## MANAGED PKI FEATURES

### *Core Features*

Common authentication mechanism for multiple applications:

- Trusted Messaging (Microsoft Exchange, Lotus Notes®, AOL® Instant Messenger™)
- Secure VPN (Check Point, Cisco, and Nortel)
- Two-Factor Authentication (Aladdin™, Authenex™, ActivCard®, Schlumberger™)
- Secure Forms (Adobe®, Evincible™)
- Web Services (Trust Gateway service)

### *Local Hosting*

- Customer may localize, brand, and host end-user enrollment pages

### *Full certificate lifecycle management*

- Control Center which gives enterprise administrators full control over enrolling, approving, revoking, and renewing digital certificates

### *Flexible authentication methods:*

- Manual authentication
- Passcode authentication
- Automated administration

### *Hosted Certification Authority*

- VeriSign hosts and operates the CA infrastructure on behalf of the customer
- 24/7/365 Data Center operations
- Disaster recovery

### **+ Fast, Scalable Implementation**

Easy-to-use toolkits and pre-integration with leading applications and platforms ensures rapid deployment of the VeriSign Managed PKI service on virtually any system, network, or device, whether located within the enterprise or externally. The Managed PKI service has been proven under real-world conditions to scale smoothly from thousands to hundreds of thousands of users, allowing enterprises to deploy digital certificates on an as-needed basis. In addition, because all services are hosted on VeriSign's existing infrastructure, implementation can be completed in a matter of weeks.

### **+ Secure, User-Friendly Remote Access**

Pre-integrated with leading Virtual Private Network (VPN) solutions (e.g., Check Point®, Cisco®, Nortel™) and support for Wireless LAN via EAP-TLS, the VeriSign Managed PKI service provides the ability to transparently use digital certificates for strong authentication in wired and wireless access environments. Roaming capabilities enable mobile end users, working from any Internet-enabled PC or device, to seamlessly use digital certificates when accessing intranets, extranets, Web applications, and Web portals. Depending on business requirements, enterprises can choose an entry-level, single-server model roaming service or a more robust, multi-server model service. Finally, integration with smart cards, USB tokens, and Trusted Platform Modules on Intel® Centrino™-based PCs enables the use of a variety of two-factor authentication solutions for remote access.

### **+ Long-Range Flexibility**

VeriSign is committed to open standards, innovative technology, and strategic collaborations, to promote the flexibility and ease of use that enterprises need to not only operate freely in diverse environments, but also to maximize return on existing investments. The VeriSign Managed PKI service supports standard certificate types including S/MIME, SSL, and IPSec, as well as industry standards such as X.509v3, LDAP, and PKCS 7, 10, and 12. Managed PKI operates on current versions of popular browsers such as Internet Explorer and Netscape®, and a variety of operating systems, including Windows, Solaris™, and AIX.® A Java™-based or ActiveX® plug-in—the VeriSign® Personal Trust Agent (PTA)—enables enterprises to present a common, brand-able user interface for digital certificate services, even in heterogeneous subscriber platform environments.

### **+ Tight Integration with Microsoft Applications**

VeriSign has teamed up with Microsoft to offer security services based on Microsoft Windows Server™ 2003. Built on Microsoft Windows Server 2003 and VeriSign Managed PKI services, this next-generation managed PKI platform allows enterprises to easily deploy digital identity management solutions to thousands of end users and enables seamless interoperability across heterogeneous systems and enterprise networks. The new platform will utilize the auto-enrollment capabilities in Microsoft Windows Server 2003 and Windows XP to enable rapid deployment of applications, such as secure email, file protection, and digital signatures. In addition, the solutions are particularly well suited to supporting secure access to corporate networks through wireless LANs, VPNs, and other applications.

### **+ Industry Compliance**

The VeriSign Managed PKI service is the first managed PKI to achieve Federal Bridge Certification Authority compliance, allowing enterprises to interoperate easily with federal agency PKIs. In addition, the VeriSign Managed PKI service helps enterprises comply with industry-specific government mandates regarding the protection, availability, and audit-



## DATA SHEET

### Gold support program

- Service Level Agreements with optional NetSure® warranty program

### VeriSign Trust Network<sup>SM</sup>

- Customers who have a public CA can leverage the VTN which is governed by VeriSign's Certificate Policy and Certification Practices Statement (CP/CPS)

### Value-Added Features

#### Key Management Services

- Secure escrow and recovery of private keys

#### Roaming Services

- Enables users to access their digital certificates from any machine—single or multi server model entirely hosted at customer site, split between customer site and VeriSign data center, or entirely hosted at VeriSign data center
- Support for existing LDAP directory (customer hosted model)

#### Premium Validation

- CRLs that are updated hourly
- OCSP for real-time certificate validation

#### Platinum Support Program

- 24/7/365 help desk support
- Pre-production system for testing and development
- Assigned support manager

ability of sensitive data. Using Managed PKI services, healthcare services providers, financial institutions, government agencies, insurance companies, and other organizations can authenticate, encrypt, sign, and audit data exchanges to support compliance with federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill 1386, the Gramm-Leach-Bliley Act, and 21 CFR Part 11.

### + PKI Modernization Program

In response to the growing trend of companies moving away from proprietary PKI software systems, VeriSign is offering a program to enable enterprises and government agencies using proprietary PKI vendor software to quickly, easily, and cost-effectively migrate to next-generation VeriSign Managed PKI services. Special pricing incentives and technical assistance is available for customers looking to upgrade from proprietary software to next-generation PKI service solutions.

### + For More Information

For more information about VeriSign Managed PKI, please call 650-426-5310, or visit [www.verisign.com/products/pki](http://www.verisign.com/products/pki).

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

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, NetSure, VeriSign Trust Network, "Where it all comes together," 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. Microsoft, ActiveX, Windows Server, and Windows are trademarks of Microsoft Corporation. Check Point is a trademark of Check Point Software Technologies Ltd. Cisco is a trademark of Cisco Systems, Inc. Nortel is a trademark of Nortel Networks Limited. Intel and Centrino are trademarks of Intel Corporation or its subsidiaries. Netscape is a trademark of Netscape. Java and Solaris are trademarks of Sun Microsystems, Inc. Lotus Notes and AIX are trademarks of IBM. Aladdin is a trademark of Aladdin Knowledge Systems. Authenex is a trademark of Authenex. ActivCard is a trademark of ActivCard Corporation. Schlumberger is a trademark of Schlumberger Smart Cards & Terminals. Adobe is a trademark of Adobe Systems Incorporated. Evincible is a trademark of Enverus, L.L.C. AOL and Instant Messenger are trademarks of America Online, Inc.