



DATA SHEET

KEY BENEFITS

Enables Rapid, Widespread Deployment of Digital Certificates

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

Minimises PKI Costs

The MPKI service delivers lower cost of ownership when compared to stand-alone PKI software implementations.

Supports Compliance with Government Mandates

Enterprises can gear 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 minimise the risks and penalties associated with improper deployment or operation of an in-house PKI.

VeriSign® Managed Public Key Infrastructure (MPKI) Service

As online commerce, communication, and collaboration become expected, 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 integrate with business partners, provide secure access to users, ensure business continuity and comply with government regulations, enterprises must be able to authenticate internal and external users and reliably secure online data exchanges, transactions and communications.

The VeriSign® MPKI 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. The highly scalable service enables enterprises to rapidly establish a robust public key infrastructure (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-life cycle management. Built on open standards to ensure maximum flexibility, the MPKI service enables 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 gearing the MPKI 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 MPKI service enables enterprises to issue digital certificates quickly, securely and cost-effectively not only to employees, customers, and business partners, but also to Web service applications and network devices such as servers, routers and firewalls. Centralised, auditable root-key generation, key escrow and distributed key recovery ensure maximum security and protection of private keys. Dual key-pair generation is also supported, enabling the separate issuance of encryption and signing key pairs. Internationalisation features include support for Unicode transformation format (UTF)-8 encoding, which enables enterprise users to enrol for and display digital IDs in languages that require non-ASCII characters (such as Japanese, Chinese and most European languages).



Where it all comes together.™

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's proven platform is recognised and trusted throughout the world, encouraging rapid adoption of PKI-enabled services, both within and outside the enterprise.

+ Fast, Scalable Implementation

Easy-to-use toolkits and pre-integration with leading applications and platforms ensure rapid deployment of the MPKI service on virtually any system, network or device, whether located within the enterprise or externally. The MPKI service has been proven under real-world conditions to scale smoothly from thousands to hundreds of thousands of users, enabling 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 (Check Point,[®] Cisco,[®] Nortel Networks[™]) and supporting wireless local area networks (LANs) via extensible authentication protocol (EAP)-transport layer security (TLS), the MPKI service provides the ability to use digital certificates transparently for strong authentication in wired and wireless access environments. Roaming capabilities enable mobile end users, working from any Internet-enabled PC or device, to use digital certificates seamlessly 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, universal serial bus (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's commitment to open standards, innovative technology and strategic collaborations ensures the flexibility and ease of use that enterprises need not only to operate freely in diverse environments but also maximise return on existing investments. MPKI supports standard certificate types, including Secure Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL) and Internet Protocol Security (IPSec), as well as industry standards such as X.509v3, Lightweight Directory Access Protocol (LDAP) and public-key cryptography standards (PKCS) 7, 10, and 12. MPKI operates on current versions of popular browsers, such as Internet Explorer and Netscape[®] and 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, brandable user interface for digital certificate services, even in heterogeneous subscriber platform environments.

+ Tight Integration with Microsoft Applications

VeriSign has teamed with Microsoft to offer security services based on Microsoft Windows Server[™] 2003. Built on Microsoft Windows Server 2003 and VeriSign MPKI services, this next-generation PKI platform enables 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 uses the auto-enrolment capabilities in 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

MPKI is the first managed PKI to achieve Federal Bridge Certification Authority (FBCA) compliance, enabling enterprises to interoperate easily with US federal agency PKIs. In addition, MPKI helps enterprises comply with industry-specific government mandates regarding the protection, availability and auditing of sensitive data. Using MPKI, healthcare services providers, financial institutions, government agencies, insurance companies and other organisations 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 Code of Federal Regulations (CFR) Part 11.

+ VeriSign® PKI Modernisation Programme

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

+ MPKI Features

Core Features

Common authentication mechanism for multiple applications:

- Trusted messaging (Microsoft Exchange, IBM® Lotus Notes,® AOL® Instant Messenger™)
- Secure VPN (Check Point, Cisco and Nortel Networks)
- Two-factor authentication (Aladdin,™ Authenex,™ ActivCard,® Schlumberger™)
- Secure forms (Adobe,® Evincible™)
- Web services (VeriSign® Trust Gateway service)

Local hosting:

- The customer may localise, brand and host end-user enrolment pages.

Full certificate-life cycle management:

- The VeriSign® Control Center gives enterprise administrators full control over enrolling, approving, revoking and renewing digital certificates.

Flexible authentication methods:

- Manual authentication
- Passcode authentication
- Automated administration

Hosted CA:

- CA infrastructure hosted and operated by VeriSign on behalf of the customer
- 24/7/365 VeriSign® Data Centre operations
- Disaster recovery



VeriSign® Gold Support Programme:

- Service level agreements (SLAs) with optional VeriSign® NetSure® warranty programme

+ VeriSign Trust NetworkSM

- Customers who have a public CA can gear the VeriSign Trust Network, which is governed by VeriSign® Certificate Policy and Certification Practices Statement (CP/CPS).

Value Added Features

Key management services:

- Secure escrow and recovery of private keys

Roaming services:

- Single or multi-server model entirely hosted at customer site, split between customer site and VeriSign Data Centre or entirely hosted at VeriSign Data Centre
- Support for existing LDAP directory (customer-hosted model) Premium Validation
- Certificate revocation lists (CRLs) updated hourly
- Online certificate status protocol (OCSP) for real-time certificate validation

VeriSign® Platinum Support Programme:

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

Visit us at www.verisign.co.uk for more information.