



WHITE PAPER

Managed Public Key Infrastructure

Securing Your Business Applications





CONTENTS

+ Executive Summary	3
+ Protecting Information Assets	3
+ Introducing Enterprise PKI	4
Critical Factors in Running an Enterprise PKI	4
Two Models for PKI Deployment	5
+ The VeriSign Value Proposition	6
+ Elements of Enterprise PKI	7
Managed PKI Functionality	7
Ease of Integration	9
Availability and Scalability	9
Security and Risk Management	9
+ Expertise	11
+ Scope of Operation	11
Broad Community Enablement	11
Cross-Certification	11
Feature Summary	12
+ Conclusion	13



Executive Summary

To operate business-critical applications over the Internet, enterprises need high-level, certificate-based security provided by a public key infrastructure (PKI). PKI protects applications that demand the highest level of security, enabling online banking and trading, Web services-based business process automation, digital form signing, enterprise instant messaging, and electronic commerce. In addition, it protects firewalls, virtual private networks (VPNs), directories, and enterprise applications. The PKI should offer comprehensive functionality, integrate easily with internal and external applications, scale to millions of users, operate flawlessly 24/7, and ensure military-grade physical security. In addition, it should allow enterprises to easily create communities of trust with partners, customers, and suppliers.

In selecting a PKI to provide these critical capabilities, enterprises must choose between deploying PKI software in-house or outsourcing PKI services to a reliable provider. In-house deployments often have inherent drawbacks— proprietary software, limited physical security, and poor redundancy—that impede successful PKI implementation. Outsourced PKIs offer a number of advantages, including lower cost of ownership, rapid deployment, and reduced risk.

The VeriSign® Managed PKI service is an outsourced offering that enables enterprises of any size to rapidly and confidently deploy PKI services. It alleviates the burden of planning, building, and maintaining a PKI, while allowing enterprises to maintain internal control over digital-certificate issuance, suspension, and revocation. Using the Managed PKI service, enterprises can securely move valuable data online to lower costs, streamline processes, and strengthen relationships with partners, customers, and suppliers.

Protecting Information Assets

As financial institutions, manufacturers, government agencies, healthcare organisations, and other enterprises leverage the Internet to link business processes, streamline communications, and conduct commerce, the protection of information assets has become a vital, yet increasingly complex, component of online data exchange. Enterprises not only must safeguard sensitive information and maintain the trust of online trading partners, but also must comply with government and industry regulations related to online data. Meanwhile virus distribution methods have evolved, the hacker arsenal has grown, and technological advances such as wireless communications have created parallel environments that must also be protected. In protecting information assets, enterprise security is now expected to provide gate-keeping functions such as data protection and network isolation, as well as facilitative functions such as exposing enterprise data to outside applications, connecting users for extended collaboration, and enabling online transactions and communications.

Introducing Enterprise PKI

The foundation for providing application and network security in these multi-faceted environments is PKI. Technically, PKI refers to the technology, infrastructure, and practices that support the implementation and operation of a certificate-based public key cryptographic system. The system uses a pair of mathematically related keys—called a private key and a public key—to encrypt and decrypt confidential information and to generate and verify digital signatures. (Digital signatures are used to sign transactions or to authenticate users or machines prior to granting access to resources.) The main function of PKI is to distribute public keys accurately and reliably to users and applications that need them. The process employs digital certificates which are issued to users or applications by an enterprise certificate authority (CA). Issuance of a certificate requires verification of the user's identity, usually by a registration authority (RA).

An enterprise PKI uses digital certificates to protect information assets via the following mechanisms:

- **Authentication**—Validates the identity of machines and users
- **Encryption**—Encodes data to ensure that information cannot be viewed by unauthorised users or machines
- **Digital signing**—Provides the electronic equivalent of a hand-written signature; also enables enterprises to verify the integrity of data and determine whether it has been tampered with in transit
- **Access control**—Determines which information a user or application can access and which operations it can perform once it gains access to another application; also called authorisation
- **Non-repudiation**—Ensures that communications, data exchanges, and transactions are legally valid and irrevocable

+ Critical Factors in Running an Enterprise PKI

In selecting an enterprise PKI solution, enterprises must consider the following factors, which span PKI technology, infrastructure, and business practices:

- **PKI functionality.** For strong security, easy administration, and hands-on control of certificate management, an enterprise PKI must be based on a modular design that includes reliable, high-performance support for certificate issuance and lifecycle management, protocols and processing capabilities for diverse certificate types, comprehensive administration functions, records retention, directory integration, and key management.
- **Ease of integration.** To minimise costs, leverage existing investments, and ensure compatibility in diverse environments, enterprises should choose a PKI that integrates easily with all the new and legacy applications it is intended to support. The PKI should not lock end users into proprietary PKI desktop software. In addition, it should be able to accommodate the varying desktop policies of not only internal IT departments but also partners, suppliers, and customers.
- **Availability and scalability.** The PKI must be available to its user community around the clock. In addition, it must be able to scale to millions of users, if necessary, to keep up with enterprise growth.



- **Security and risk management.** To preserve trust and minimise financial and legal liability, enterprises running an Internet-based PKI must safeguard the PKI infrastructure, private keys, and other valuable assets from not only network-based attacks but also threats to the physical facility housing the assets.
- **Expertise.** To ensure that the PKI is properly deployed, maintained, and protected, enterprises should employ security professionals who are extensively trained in PKI.
- **Scope of operation.** To maximise Return on Investment (ROI), promote collaboration, and ensure business agility, enterprises investing in PKI should ascertain that the offering can be easily enabled to operate across intranets, extranets, instant-messaging communities, Web-services networks, Internet marketplaces, VPNs, and other communities of interest.

These factors, which are strongly influenced by the PKI deployment model chosen, determine the success or failure of an enterprise PKI and impact an enterprise's immediate and long-range plans for the exchange of high-value data.

+ Two Models for PKI Deployment

When deploying a PKI, enterprises must choose between purchasing standalone PKI software for in-house deployment or outsourcing an integrated PKI platform. Besides their differing capabilities to meet the challenges discussed in the preceding section, the two approaches vary in their total cost of ownership (TCO), time to implementation, likelihood of success, use of in-house talent, degree of risk, and brand value.

In-House Deployment of Standalone PKI Software

In an in-house deployment, an enterprise purchases standalone PKI software and creates a standalone PKI service. In this scenario, the enterprise assumes 100 percent responsibility for provisioning, deploying, and maintaining the PKI itself as well as all the surrounding technology, including systems, telecommunications, and databases. The enterprise is also responsible for providing a secure facility. A secure facility must have physical-site security, Internet-safe network configurations, redundant systems, disaster recovery, viable PKI legal practices, financially sound liability protection, and highly-trained personnel. If any of these components is weak, the enterprise may be compromised.

Regardless of the in-house PKI's capability to address critical success factors, adoption of PKI-enabled services by partners, customers, and suppliers may be hindered by lack of confidence in the unproven PKI or unfamiliarity with the enterprise itself. In addition, non-repudiation—the capability to provide third-party auditing and corroboration of transactions—may not exist in an in-house implementation, further diminishing the PKI's value. Finally, the process of planning, purchasing, implementing, deploying, and testing an in-house PKI can take many months, delaying the deployment of strategic business initiatives as well as the return on existing investments.

Outsourced Deployment to an Integrated PKI Platform

In an outsourced deployment to an integrated PKI platform, an enterprise delegates PKI construction, deployment, and maintenance to a trusted third party whose services include certificate processing, root-key protection, and security and risk management.

Because it is their core business, integrated PKI platform providers can devote a greater percentage of their resources to state-of-the-art PKI technology, security, and training than is feasible for most enterprises. In addition, security practices, procedures, and infrastructure



have been tested over time. This accelerates deployment and helps ensure that the PKI operates at the highest levels of availability and security. Because billing for outsourced services is based on flat rates, number of digital certificates issued, or a combination of the two, the enterprise can predict costs more accurately and simply add PKI capability as business expands.

An important differentiator among outsourced PKI platforms is the enterprise's capability to control and execute its security policies with respect to user authentication and certificate lifecycle management.

The VeriSign Value Proposition

VeriSign operates Intelligent Infrastructure Services that enable businesses and individuals to find, connect, secure, and transact across today's complex global networks. As an industry leader in Internet security and PKI, VeriSign builds state-of-the-art integrated PKI service platforms for enterprises of all sizes. Real-world experience serves as the foundation for the design and support-readiness of the VeriSign Managed PKI service. By leveraging VeriSign expertise and infrastructure, enterprises alleviate the burden of building, deploying, and maintaining an in-house infrastructure while retaining complete control over certificate lifecycle management, including issuance, renewal, and revocation. Enterprises can rapidly secure Web services, instant messaging, online forms exchange, legacy, and other applications, yielding faster return on investment and enabling an agile response to evolving business strategies.

The VeriSign Managed PKI service meets all the critical requirements of a successful PKI deployment, while providing the following advantages:

- **Lower TCO**—VeriSign invests millions of dollars in building, maintaining, updating, securing, and externally auditing its PKI platforms, as well as in staffing its operating centers. By leveraging the VeriSign Managed PKI service, enterprises save significantly on secure facilities, infrastructure, and staffing. In fact, TCO of an in-house PKI system is greater than outsourcing to VeriSign, even if the insourcer's software costs are zero.¹
- **Rapid deployment**—Because the platform, policies, and procedures are already in place, the VeriSign Managed PKI service can be implemented in less than one-third the time of a typical in-house, software-based PKI.
- **Proven success**—The VeriSign Managed PKI service is based on a proven back-end infrastructure, helping to ensure the implementation's success.
- **Minimum impact on staff**—Day-to-day operation and maintenance of the PKI is handled by VeriSign's security professionals, allowing in-house IT resources to focus on core business.
- **Strong security**—VeriSign leverages military-grade facilities and industry-leading certificate practices to ensure the highest level of security.
- **Brand value**—By using a recognised, trusted brand, enterprises more easily gain the confidence of suppliers, partners, and customers.



The following table summarises the fundamental differences between standalone PKI software and the VeriSign Managed PKI services platform.

Success Factor	Integrated PKI Platform	Standalone PKI Software
PKI functionality	Fully-featured PKI, proven in world's largest 24/7 PKI service centers. Leveraged experience from hundreds of enterprises.	Enterprise designs, builds, and deploys supporting infrastructure, and assumes 100 percent of the implementation risk. Software vendor has no PKI operating experience.
Ease of integration	Seamless integration with standard best-of-breed applications, including standard Web browsers, mail clients, and enterprise applications.	Requires proprietary client software for all users and applications.
Availability and scalability	Contractually guaranteed PKI backbone services and disaster recovery. On-demand scalability. Leverages high-capacity, fault-tolerant infrastructure.	Enterprise provides 100 percent of services infrastructure and disaster recovery. Assumes 100 percent of the operational risk. Redundancy difficult. Scalability limited.
Security and risk management	Contractually guaranteed PKI backbone security. Mature, industry-leading certificate practices. Externally audited.	Enterprise provides 100 percent of security infrastructure; must design own operational policies and practices; assumes 100 percent of risk.
Personnel	Rigorous screening process. Highly-trained security professionals; core focus is security and PKI; up-to-the-minute knowledge base and skill sets.	Personnel must receive regular training to keep up with evolving technology, standards, and risks. Inexperience may slow deployment, cause downtime, and create gaps in security.
Scope of operation	International network of CAs. Enterprise can select private and/or public trust networks (largest in world.)	Private cross-certification only. Enterprise builds 100-percent custom solution each time. Partners assume 100 percent of risk.

Elements of Enterprise PKI

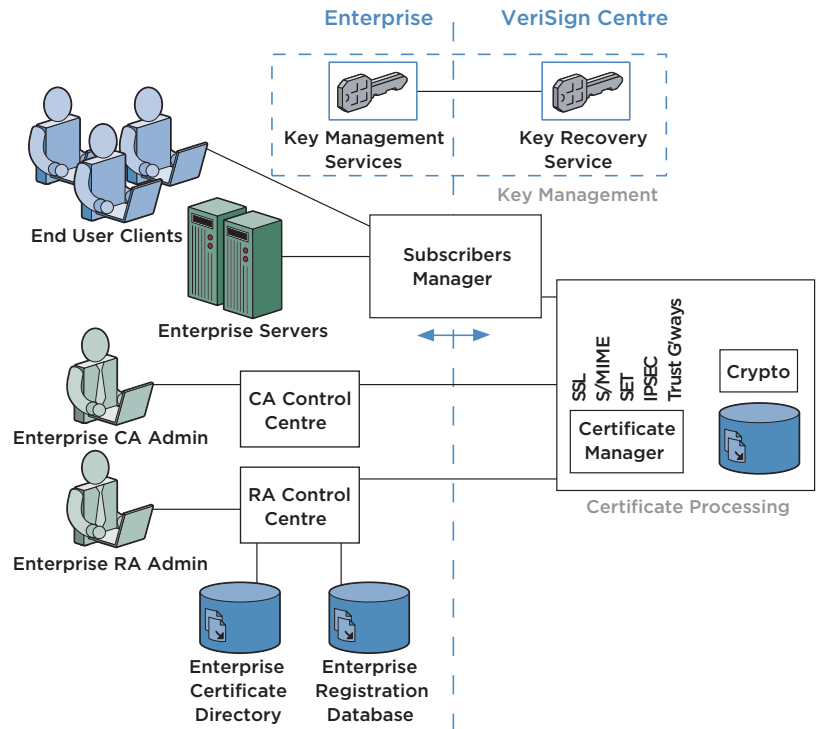
The VeriSign approach to enterprise PKI distinguishes itself from the build-it-yourself approach by giving enterprises control over policy and day-to-day decision-making but delegating back-end processor tasks to VeriSign. To explain the VeriSign difference, the following sections discuss the complete PKI solution in terms of the critical success factors already identified: functionality, ease of integration, availability and scalability, security and risk management, expertise, and scope of operation.

+ Managed PKI Functionality

At the core of PKI lies software and hardware that implement CA and RA functions, enrollment processes, certificate renewal and status-verification services, directory and application interfaces, private-key management, and so on. This technology must support strong security, high availability, and multiple application interfaces. Most importantly, it must have a modular design, permitting PKI functions to be distributed between enterprise premises and a supporting, secure data center.

The VeriSign Trust NetworkSM architecture, on which VeriSign Managed PKI services are based, is robust and comprehensive. It supports the PKI service-center needs of enterprises, commercial CAs, and Web sites worldwide, satisfying the most stringent security, commercial, legal, and best-practices requirements.

VeriSign's WorldTrust Architecture



The VeriSign Trust Network architecture is comprised of the following module families:

- **End-User Enrolment Pages**—Provides localisable and brandable enrolment pages for end-user registration and other end-user services such as certificate renewal.
- **Managed PKI Control Centre**—Provides in-house certificate-management functions, such as certificate issuance approval, revocation approval, and general administration functions; can be fully automated.
- **CA Control Centre**—Enables enterprises to establish local CA policy, such as certificate content rules and administration authorisations.
- **Certificate Processing**—Includes certificate issuance, certificate lifecycle compliance and protocol support, premium validation services such as online certificate status protocol (OCSP), cryptographic key management, records storage, and other core functions.
- **Certificate Manager**—Allows enterprises to choose the types of certificates to be issued, for example, SSL, S/MIME, IPsec, or VeriSign Trust Gateway certificates.
- **Key Management Services**—Provides maximum-security generation, backup, and recovery of user-key pairs; includes dual-key (separate key pairs within a single application) support.



- **Enterprise Integration**—Provides interfaces to enterprise databases to support automated certificate issuance and other administration functions, automated posting of certificates to enterprise directories or databases, and access to certificate-revocation information by enterprise Web servers.
- **Application Integration Toolkits**—Enables commercial application vendors and enterprises to enable PKI-ready applications.

+ Ease of Integration

One of the biggest challenges in a PKI deployment is PKI-enabling applications, both within and outside the enterprise. The architecture that the PKI vendor uses—proprietary or standards-based—influences the ease and cost of integration.

- **Proprietary.** Proprietary PKI software is installed on every desktop. Applications that use the PKI require a proprietary software interface from the PKI vendor, making it costly, complex, and usually unfeasible to extend applications to other areas of the intranet or to partners, customers, and suppliers. In addition, upgrades to any application may be incompatible with the existing PKI.
- **Standards-based.** Native applications interface to the PKI using industry-standard interface protocols or tailored standards-based interfaces provided through PKI-application vendor partnerships. No proprietary PKI software is needed on the desktop.

VeriSign uses a standards-based approach to PKI and works with over 100 independent software vendors to provide built-in support for the VeriSign Managed PKI service; applications are PKI-enabled as shipped from these vendors. To further ensure seamless operability with virtually any application, the VeriSign Managed PKI service also includes easy-to-use application programming interfaces (APIs) for PKI-enabling customer-written applications.

+ Availability and Scalability

A PKI supporting mission-critical applications must be available around the clock and must be able to smoothly scale to support large numbers of users and applications.

Availability

To ensure continuous availability, the VeriSign Managed PKI service has a fully redundant infrastructure with guaranteed 24/7 service levels for all critical components. Backup disaster recovery sites operate 24/7 in geographically separate locations. By contrast, standalone PKI products frequently are not designed for redundancy, predisposing them to unplanned downtime. In addition, disaster-recovery capabilities may be limited, unless arrangements are made for a separate secure location.

Scalability

VeriSign digital certificate issuance has been proven under real-world conditions to scale smoothly from hundreds to millions of users. Standalone PKI software is known to encounter scaling limits at the tens of thousands due to lack of a transaction-optimised architecture and scaling and resiliency limits with database and directory systems.

+ Security and Risk Management

Protecting root and private keys and providing continuous service are two critical aims of enterprises deploying a PKI. To ensure strong security and 24/7 availability, an enterprise must have airtight physical security and sound certificate practices. However, physical security is one of the largest expenses in a PKI deployment, and well-designed certificate



practices require a mature, carefully-delineated approach to security and risk management. VeriSign makes significant investments in security technology and offers an industry-leading certificate practices statement that ensures a level of security exceeding the capabilities of most enterprises operating standalone PKIs. Leveraging the VeriSign Managed PKI service, enterprises can alleviate not only the costs, but also the risks of establishing and operating a high-security, high-availability facility.

Physical Security

Because software-based cryptography implementations are prone to tampering or misuse, a fundamental requirement of a CA supporting business-critical applications is that it employ hardware cryptographic modules for certificate signing. In addition, root keys (which provide the basis for linking together multiple CAs) require special precautions. Their private key must be stored in a secure, offline hardware unit; multiple key shareholders must be employed to enable the key for signing; and all processes must be tightly controlled and audited. Besides the specific mechanisms used to protect keys, the facility housing critical PKI functions must be impenetrable. In addition, it must have redundant power, redundant heating, air conditioning, and ventilation (HVAC), and specialised fire systems to prevent heat and water damage.

VeriSign locates critical PKI functions in a secure data center operated by VeriSign or an affiliate on a 24/7 basis. To ensure the highest levels of security and availability, all PKIs implemented through the VeriSign Managed PKI services employ hardware-based cryptography, highly screened and trained personnel, a military-grade secure facility, and a rigidly audited system of procedural controls. Round-the-clock service levels are supported.

Customer Practices Support

To guarantee non-repudiation and win the trust of partners, customers, and suppliers, enterprises must have well-defined, audited processes for cryptographic PKI management, day-to-day operations, and recordkeeping. This is particularly important when enterprises use PKI-based digital signatures to electronically sign electronic transactions, documents, and other information. In this case, sound practices and independently audited processes are essential to ensure that transactions are legally binding.

VeriSign is a world leader in the development of PKI practices, with audited business processes that meet the most stringent industry standards. VeriSign's Certification Practices Statement (CPS), which delineates the practices underlying the VTN public CA services, is recognised as the most comprehensive document of its type and is used internationally as a foundation for enterprise PKI practices.

VeriSign's practices include witnessed and audited processes for CA key establishment and management, and rigid multi-party controls over all key materials. VeriSign undergoes an annual, independent security audit against established WebTrust for CA and SAS-70 security guidelines, and has been approved to issue certificates consistent with the policies and procedures defined by the Department of Defence. VeriSign processes are certified by KPMG in accordance with AICPA SAS-70.

Expertise

Proper planning, implementation, and maintenance of a PKI require highly-trained personnel with hands-on experience. To assemble a security team for an in-house PKI deployment, enterprises must divert development and IT staff from their core strengths, train existing personnel for the job, and/or screen and hire new resources. Once the PKI is deployed, ongoing staff training is necessary in order to keep current on rapidly changing security trends and technology. Overall inexperience, unfamiliarity with specific technology, and untested security policies may expose an in-house deployment to delays, unexpected downtime, and flawed security.

By outsourcing PKI deployment to VeriSign security professionals with in-depth experience, enterprises minimise personnel costs, reduce risks, and speed deployment. As the leading provider of Internet trust services, VeriSign has extensive experience developing, implementing, and maintaining a PKI. The VeriSign Managed PKI team focuses solely on security and PKI, and its skill set is updated constantly to incorporate state-of-the-art technology and security practices.

Scope of Operation

PKI can potentially span communities of any size, from enterprise extranets that include select partners, to industry-specific Web services networks that span multiple enterprises, to global communities that include all comers, for example, instant messaging. VeriSign facilitates the development of communities beyond the intranet through broad community enablement and cross-certification.

+ Broad Community Enablement

While some enterprises require closed, private PKIs, others want their certificates to be recognised and trusted by out-of-the-box commercial Web browsers or other desktop applications. This greatly facilitates the establishment of extended PKI communities, by obviating the need for special software installation or configuration in the desktop systems of organisations that are not under the administrative control of the PKI-operating enterprise. The VeriSign Managed PKI service gives enterprises the option of establishing an isolated private PKI, a community or industry-wide PKI, or a PKI linked into the VTN. The VTN is a global, cross-certified PKI operated by VeriSign and its worldwide affiliates. Root keys of the VeriSign Trust Network are pre-installed in all major commercial desktop products, including Microsoft® and Netscape® clients, allowing the certificates issued in the PKI to be immediately recognised by the users of these products. With an in-house PKI, community building can be unwieldy, involving manual exchange and installation of cross-certificates or root keys.

+ Cross-Certification

Cross-certification is the process whereby one CA issues a certificate for another CA, allowing certificate chains to link PKI communities that may span multiple enterprises.



Cross-certification involves more than just issuing a certificate. It is a special business arrangement, involving agreements on issues such as security practices and liability apportionment. VeriSign has built numerous multi-enterprise cross-certified CA structures, linking groups of financial institutions, commercial CAs, and other enterprises worldwide. In addition, its Managed PKI service is certified by the Federal Bridge Certificate Authority (FBCA), allowing government agencies to securely exchange information. VeriSign can help enterprises establish and/or integrate cross-certification practices and agreements that address the security requirements of all participants. With a standalone PKI software product, enterprises must develop and execute cross-certification processes on their own.

+ Features Summary

VeriSign is the only vendor in the PKI space offering a complete enterprise PKI solution—based on the PKI service-platform concept.

The following table summarises some major features of the VeriSign offering.

PKI Component	VeriSign Managed PKI
PKI Functionality	
Cryptographic hardware for certificate signing	All CAs use hardware cryptography, FIPS 140-1 level 3 endorsed (averts risks of tampering and disclosure of private CA key inherent in software cryptography)
Root-key protection	Root keys always network isolated and in secure facility; activation by regimented, audited secret sharing (averts risks of penetration and disclosure of private information by intruders/administrators if private root key held in online, operational environment)
User-key management	User encryption keys backed up at enterprise; full key histories; strong protection using distributed-key recovery technology
Dual-key support	Supports single- or dual-key pairs for any application (dependent on application requirements and capabilities)
Revocation	Certificate revocation lists issued regularly; revocation enabled for Web servers and standard browsers; supports OCSP
Ease of Integration	
Standards-based vs. proprietary PKI	Standards-based PKI; no proprietary software on desktops; 100+ ISV partners; 120+ applications enabled
Directory/database technology	Enterprise choice of LDAP, X.500, SQL, or legacy DBMS; no directory schema restrictions
Availability and Scalability	
Redundancy	Guaranteed 24/7 service levels, redundant servers, database, ISPs, telecommunications
Disaster recovery	Guaranteed 24/7 disaster-recovery backup at remote secure site
Security and Risk Management	
Facility security	Fortified construction, five-tier security; dual biometric access control, 24-hour monitoring, motion detect, network security audit
Personnel security	Investigative screening, specialist training, retraining
Independent audit	Independent SAS-70 audit by KPMG
Customer practices support	Enterprise CA may join VTN with proven established practices, or may establish own practices; VeriSign offers practices consulting and/or CPS
Non-repudiation	Evaluated/audited cryptographic materials management and secured-records retention provide independently verifiable evidence for dispute resolution
Expertise	
Dedicated staff	Highly-screened and trained security professionals focus solely on security and PKI
State-of-the-art skill set	Refresher courses and ongoing updates to maintain proficiency
Scope of Operation	
Global community enablement	Enterprise has option of joining PKI structure with roots pre-installed in all commercial Web/mail clients
Cross-certification	Can cross-certify enterprise Managed PKI CA into established VTN or private network; can cross-certify private Netscape or Microsoft certificate server; cross-certification includes all phases, including support for practices establishment

Conclusion

As the role of Internet security has evolved to include gate-keeping functions as well as network facilitation, protecting information assets has become more costly and complex. The foundation for providing application and network security in this dynamic environment is PKI. Because a successful PKI requires state-of-the-art technology, sophisticated certificate practices, and highly-trained personnel, in-house deployment of PKI services involves significant investments of time and money. In addition, enterprises deploying standalone, in-house PKIs often cannot provide the same levels of security as service providers dedicated solely to PKI and security.

The VeriSign Managed PKI service is an outsourced offering that alleviates the burdens and risks of building, deploying, and maintaining an in-house PKI while allowing enterprises to maintain internal control over vital aspects of security such as certificate issuance, suspension, and revocation. By leveraging VeriSign industry-leading technology and expertise, as well as its comprehensive certificate practices statement, enterprises not only reduce costs, speed time to deployment, and strengthen security, but also win the confidence of partners, customers, and suppliers who recognise and trust the VeriSign name.