VeriSign Strategy White Paper #98-01

Public-Key Infrastructure – The VeriSign Difference

Public Key Infrastructure (PKI) – The VeriSign Difference

Operating secure, business-critical applications over the Internet requires an advanced enterprise PKI. Selecting the right approach to enterprise PKI can dramatically affect the bottom-line.

Introducing Enterprise PKI

Enterprises around the world are deploying a new generation of distributed, business-critical applications—enabling delivery of new products and services on an unprecedented scale—over intranets (employees), extranets (trading partners), and the Internet (worldwide customers and prospects). These applications must be operated in a high-availability, high-security environment, in order to gain customer confidence and allow enterprises to exploit the advantages of the electronic marketplace—faster time-to-market, lower distribution costs, and greater access to global customers.

One element has now emerged as the foundation for secure distributed applications, including supply chain management, secure messaging, e-commerce, virtual private networks, and intranet applications—that element is Public Key Infrastructure (PKI). An enterprise's PKI constitutes the core of its Internet security infrastructure—the key to ensuring authenticated, private and non-repudiable communications and transactions. The success of an enterprise's PKI will have a major impact on its core business operations.

Critical Success Factors in Running an Enterprise PKI

In the online-all-the-time world of the Internet, one of the biggest challenges you will face in operating a PKI is satisfying your customer expectations for a highly-available, highly-secure, PKI service. From the perspective of a customer, business partner, or internal client, the end-result of a successful PKI is measured by the ease of obtaining and using digital certificates—trusted electronic credentials that enable access control, secure messaging, and transaction security for business-critical applications. From the enterprise perspective, running a PKI operation means running a trusted online service for end users. Managers may be staking their jobs—and enterprises their business reputations—on the success of their PKI solution.

The foundation for secure Internet applications is a Public Key Infrastucture (PKI). An enterprise's PKI constitutes the core of its Internet security infrastructure—the key to ensuring authenticated, private and non-repudiable communications. The success of an enterprise's PKI will have a major impact on its core business operations.

In selecting an enterprise PKI solution, there are five critical success factors that will likely determine the success or failure of your trusted PKI operation—spanning PKI technology, infrastructure, and business practices:

- ***Proven PKI Technology*****:** Full PKI functionality includes support for certificate issuance and life-cycle management, processing and protocols for diverse certificate types, comprehensive administration functions, records retention, directory integration, and key management. How do you run state-of-the-art PKI technology, but ensure that it won't fail under high-stress, real-world conditions? What operational proving-grounds has it been tested under?

- ***Open Architecture with Best-of-Breed Applications***: Your enterprise PKI needs to be integrated with all the applications it supports. How do you deploy PKI that can support your own choice of new and legacy applications? How do you avoid forcing your end-users to be locked into proprietary PKI desktop software that they must install, update, and troubleshoot? How do you deal with the desktop policies mandated by IT departments outside your control (e.g., business partners) when moving beyond the intranet?

- ***High Availability and Scaleability***: Your PKI needs to be available to its user community around-the-clock. How can you guarantee 7x24 service availability to business partners, internal clients, or external customers—including systems, networks, customer support, and disaster recovery—without massive up-front capital investment? How do you handle unexpected peak loads in demand? How can you start your PKI small but be confident it can scale effectively to millions of users ultimately?

- ***Secure Operating Infrastructure***: Operating your PKI presents a new, unique set of risk management challenges. How do you ensure that you don't "go it alone" in risking company reputation, financial, and legal liability when running an Internet-based PKI? How can you safeguard precious corporate information assets with the most hacker-proof PKI security protection?
- ***Extranet/E-commerce Readiness***: Your PKI may have to support different user communities, both inside and beyond the enterprise. How do you architect your PKI to operate and scale successfully across such communities—intranets, extranets, industry trading groups, and large-scale Internet commerce? Will proprietary approaches derail these efforts?

If these questions apply to your enterprise's decision to provide business-critical PKI services, please read on. This white paper compares two radically different approaches to deploying enterprise PKI, focusing on their respective abilities to meet these five critical challenges.

There are many crucial elements to running an enterprise PKI that standalone PKI software vendors don't like to talk about. Why*? Because they make their money by selling software*—not by ensuring that a PKI is up and running day-in and day-out, through security emergencies, overnight service interruptions, customer crises, hacker attacks, and rapid-fire technology changes.

Two Models for PKI Deployment

Based on recent advances in the PKI industry, there are now two very different approaches to building an enterprise PKI**:**

- **Purchase** ***standalone PKI software***, and create a standalone PKI service—where the enterprise alone assumes 100% responsibility for provisioning all the surrounding technology, including systems, telecommunications, and databases, in addition to providing physical site security, Internet-safe network configurations, high-availability redundant systems, disaster recovery, PKI specialists, viable PKI legal practices, and financially safe PKI liability protection; or
- **Deploy an** ***integrated PKI platform***—which combines enterprise-controlled and operated PKI software/hardware, compatibility with popular applications, and the certificate processing services and infrastructure of a high-availability, high-security *PKI backbone*—with shared liability and independently audited business processes.

The downside of the standalone PKI software approach is that it leads to *standalone enterprise PKI*— where the enterprise assumes 100% of the investment and 100% of the risk. By contrast, an enterprise deploying an integrated PKI service platform—with 7x24 PKI services, shared investment, and shared risk—is far more likely to succeed in providing reliable and trustworthy PKI services, at lower cost and with faster deployment of the dependent applications.

Table 1 summarizes the fundamental differences between standalone PKI software and a PKI service platform. The balance of this white paper further explores the factors underlying these crucial issues.

Success Factor	**Integrated PKI Platform**	**Standalone PKI Software**
Proven PKI technology	Fully-featured PKI, proven in world's largest 7x24 PKI service centers. Leveraged experience from 100s of enterprises.	Enterprise designs, builds, and deploys supporting infrastructure, and assumes 100% implementation risk. Software vendor has no PKI operating experience.
Open architecture with best-of-breed applications	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.
High availability and scaleability	Contractually guaranteed PKI backbone services & disaster recovery. On-demand scaleability. Leverages high capacity, fault-tolerant infrastructure.	Enterprise provides 100% services infrastructure & disaster recovery. Assumes 100% operational risk.
Secure operating infrastructure	Contractually guaranteed PKI backbone security. Externally audited. Shared liability.	Enterprise provides 100% of security infrastructure; must design own operational policies and practices; assumes 100% of risk.
Extranet/e-commerce readiness	Enterprise can select private and/or public trust networks (largest in world).	Private cross-certification only. Enterprise builds 100% custom solution each time. Partners assume 100% of risk.

The VeriSign Value Proposition

At VeriSign, we've learned from the successes and failures of earlier approaches to PKI deployment. As a result, our approach is to build industrial-strength PKI service platforms for enterprises of all sizes, leveraging the largest and most reliable PKI backbone in the world.

As the world's largest PKI processor, we've gained unequaled real-world experience which serves as the foundation for the design and support-readiness of our enterprise PKI service platform—VeriSign centers support a rapidly growing customer base of millions of consumers, 80,000 websites, and hundreds enterprises. You can leverage our expertise and capitalize on our infrastructure—an investment of over $40 million in building the world's largest PKI backbone—so that you don't have to build that infrastructure for your enterprise.

VeriSign enterprise PKI customers include some of the largest enterprises in the world—including:

Banks—NationsBank, Bank of America, Federal Reserve of NY, Sumitomo Bank

Brokerage Firms—Merrill Lynch, Morgan Stanley Dean Witter

Electronics—Hewlett Packard, Texas Instruments

Telecommunications—AT&T, British Telecom, US West, Ameritech,

Transportation—United Parcel Service (UPS)

Government Agencies—Internal Revenue Service, civil & defense agencies

Why go it alone in enterprise PKI when you can be supported by the acknowledged leader in mission-critical PKI services?

Protecting Information Assets

The goal of an enterprise PKI is to protect information assets through:

- Authentication—validating the identity of parties in communications and transactions;
- Confidentiality—ensuring that information is not intercepted during transmission;
- Non-Repudiation—ensuring that transactions, once committed, are legally valid and irrevocable;
- Availability—ensuring that transactions or communications can be executed reliably upon demand.

Technically, PKI refers to the technology, infrastructure, and practices needed to enable use of public-key encryption and/or digital signatures in distributed applications on a significant scale. The main function of PKI is to distribute public keys accurately and reliably to those needing to encrypt messages or verify digital signatures (used to sign transactions or to authenticate people prior to granting access to resources). This process employs digital certificates issued by an enterprise *certification authority* (CA) to users who register with that CA. Issuance of a certificate requires authentication of the user, usually by a *registration authority* (RA). The scope of PKI also extends to functions such as certificate renewal, certificate revocation/status checking, and user private key backup/recovery.[1]

PKI is now the foundation for all application and network security, including access control to information resources from web browsers, secure e-mail, digital forms signing and workflow, firewalls, routers supporting virtual private networks (VPNs), directories, and single-sign-on to corporate applications (including legacy applications).

A PKI implementation needs to be highly secure – security requirements generally exceed those for typical secure transaction processing system, since issuance of just one bad certificate or penetration of a CA's security can result in an unlimited number of bad transactions or issuance of an unlimited number of bad certificates.

VeriSign OnSite—Industrial-Strength Enterprise PKI

VeriSign OnSite is a unique, state-of-the-art PKI service platform for the enterprise. It integrates:

- **Enterprise PKI administration software**—enterprise-operated and controlled ; with expert wizards for step-by-step installation, configuration, management, and report generation; installs on standard web browsers and server platforms; with interfaces to enterprise business systems for automated user administration and directory integration;
- **Guaranteed back-end processing services**—contractually guaranteed 7x24 data processing, customer support, and disaster recovery services, leveraging investment in the industry's only global PKI backbone;
- **Scaleable and unquestionably secure infrastructure**—modular, high-capacity processing and database systems, with audited, state-of-the-art network, physical, and cryptographic security;
- **Shared financial and legal liability**—managed risk, so you don't "go it alone" in running your PKI service;
- **Pay-as-you-go, volume-based pricing**—with costs for additional users, including operational costs, incurred only as those users activate; avoids large up-front capital expenses and gives the lowest cost of ownership of any PKI deployment.

[1] For a comprehensive description of PKI, see: Warwick Ford and Michael S. Baum, "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption," Prentice-Hall, 1997.

PKI Security and the Need for Distributed Functionality

Any PKI implementation should be designed with high-grade security built-in from day one. Even if the *initial* PKI deployment does not protect critical assets, remember that PKIs will likely be later leveraged to protect precious information assets—extending to the *crown jewels* of Internet-based commerce.

A fundamental requirement of a CA supporting business-critical applications is that it must employ hardware cryptographic modules for certificate signing, since software-based cryptography implementations are prone to tampering or misuse. *Root keys* that provide the basis for linking together multiple CAs and generally have longer lifetimes require special precautions, including storing the private key in a secure, off-line hardware unit and requiring multiple key share holders to enable the key for signing in a tightly controlled, audited process.

The full complement of strong security controls must also be employed, including physical security of the facility (room, building, and equipment) housing the CA, personnel security measures (including screening and specialized training of all staff with access to the CA), and procedural controls to enforce such policies as dual control over all sensitive functions. The secure facility typically needs to be operational on a 24x7 basis, and needs full disaster recovery backup.

While all CAs need strong security, the costs of building and operating a secure facility and the up-front financial commitment are daunting to many enterprises. Outsourcing the CA function to someone else is not necessarily the answer either, since enterprises frequently want full policy control over their PKIs, in terms of deciding who receives a certificate, what the certificate contents are, how and when certificates are revoked, and day-to-day operation of the CA.

VeriSign OnSite is the only PKI offering to address these seemingly irreconcilable needs. With VeriSign OnSite, the enterprise controls the CA and can administer and audit the operation continuously. However, day-to-day back-end, secure data processing functions, such as certificate-signing cryptographic hardware and records retention, are delegated to VeriSign and operated out of a VeriSign secure data center. This is achieved through the VeriSign's WorldTrust distributed PKI architecture, components of which are operated by both VeriSign and the enterprise.

All **PKIs implemented through VeriSign OnSite employ hardware-based cryptography, screened and trained personnel, a military-grade secure facility, and a rigidly audited system of procedural controls. With a do-it-yourself PKI product, security is left entirely to the enterprise.**

Elements of Enterprise PKI

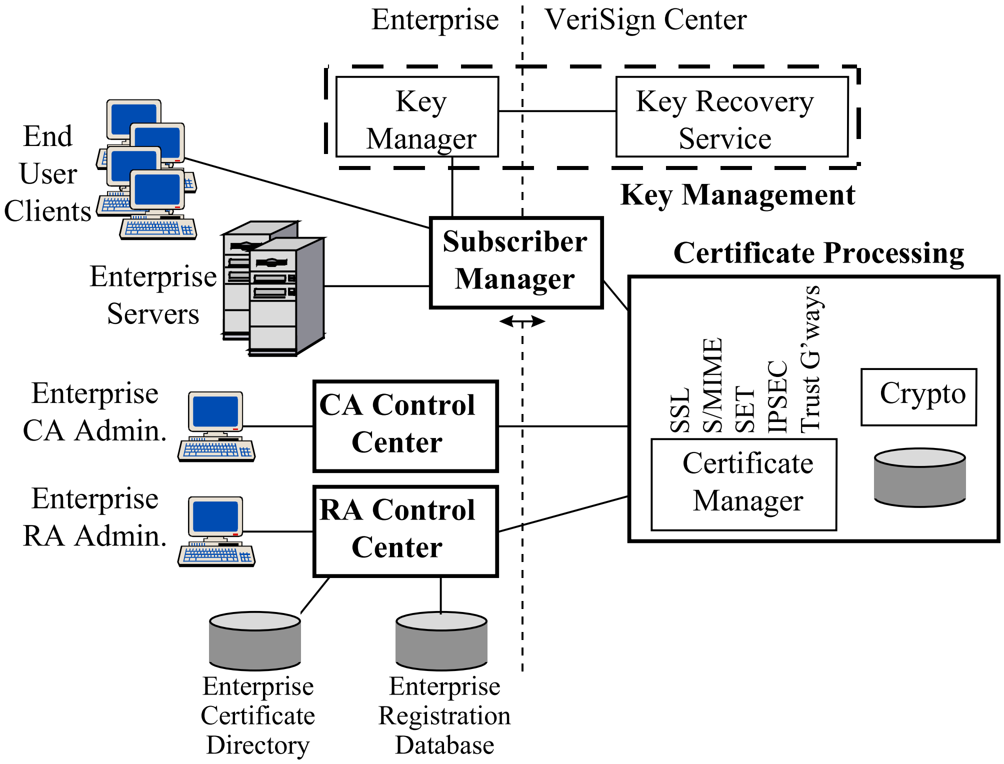
Provision of an enterprise PKI service has many facets, including secure infrastructure establishment and maintenance, specialist staff training and screening, 7x24 operations, application-interfacing, etc. The VeriSign approach to enterprise PKI distinguishes itself from the build-it-yourself approach using standalone PKI software, by giving the customer control over policy and day-to-day decision making, but delegating back-end processor tasks to VeriSign. To explain the VeriSign difference, let us consider the complete PKI solution in terms of the five critical success factors already identified: *technology, open architecture, availability and scaleability, security and risk management*, and *extranet/e-commerce readiness*.

Technology

At the core of PKI lies technology—software and hardware that implement the functions of a certification authority (CA), registration authority (RA), enrollment processes, certificate renewal and status-verification services, application interfaces, directory services and interfaces, private key management, and so on. The demands on this technology are considerable – it must support strong security, high availability, multiple certificate types for different applications, and multiple application product 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 WorldTrust architecture stands out as today's most robust and comprehensive PKI architecture.[2] It supports the PKI service center needs of enterprises, commercial CAs, and websites worldwide, satisfying the most stringent security, commercial, and legal/practices requirements.

[2] For a full description, see: "The VeriSign WorldTrust PKI Architecture," VeriSign White Paper #98-05, 1998.



VeriSign's WorldTrust Architecture

The WorldTrust architecture compromises the following module families:

- **Subscriber Manager:** Support for end-user registration and other end-user services such as certificate renewal, typically through web servers located on enterprise premises or at a VeriSign center. The *look and feel* are tailored to the enterprise.
- **RA Control Center:** Certificate management functions, such as certificate issuance approval, revocation approval, and general administration functions, located at the enterprise. These functions can be software-interfaced to local management systems, such as an employee or customer database, to allow them to be fully automated.
- **CA Control Center:** Establishment of local CA policy, such as certificate content rules and administration authorizations. These functions are typically located at the enterprise.
- **Certificate Processing:** Certificate issuance (based on RA approval), certificate life-cycle compliance and protocol support, cryptographic key management, secure records retention, data base mirroring for disaster recovery purposes, and other core functions. These functions are built around a high-performance transaction engine located at a secure facility operated by VeriSign or one of VeriSign's worldwide affiliates. Cryptographic functions are embedded in government-certified hardware

cryptographic modules, with enabling keying materials split between multiple independent responsible persons.

- **Certificate Manager:** The component of OnSite where the customer chooses the different types of certificates to be issued, for example, SSL S/MIME, IPSEC, or Trust Gateway certificates.
- **Key Management:** Software components and a supporting service to provide maximum-security generation, backup, and recovery of user key pairs.
- **Enterprise Integration Software Modules:** Software modules that provide interfaces to enterprise databases to support automated certificate issuance and other administration functions, automated posting of certificates to enterprise directory or database, and access to certificate revocation information by enterprise web servers.
- **Application Integration Toolkits:** For use by commercial application vendors or enterprise customers for enabling PKI-ready applications.

Administration Options

Flexibility is needed in how enterprises administer PKIs, for example, how certificate issuance or revocation is initiated and approved. Organizations with modest-sized certificate communities or while in technology piloting stages are best served with a manual administration system which does not require any special software integration. With OnSite, this is available instantly, via administrator access to administrative web pages hosted by VeriSign; the administrator uses a standard web browser with smart-card add-on for added security. Organizations with large client communities, however, need the option of driving certificate administration from other administrative systems or corporate database updates occurring in real time. For example, as new employees are entered in the corporate human resources database, certificate issuance is automatically approved and, as employees terminate, certificates are automatically revoked.

It should be possible to integrate PKI administration with enterprise systems administration – not add a new administrative burden. VeriSign OnSite's automated administration allows issuance and revocation of certificates to be transparently driven by pre-existing administrative systems or databases of any type. Standalone PKI software, on the other hand, requires the enterprise to create and depend day-to-day upon a new, specialist "PKI administrator" job function.

All options are made available with VeriSign OnSite. OnSite's Automated Administration option exposes a simple API for interfacing to any of the popular DBMS or other administrative systems, with support for firewall separation of functional components as necessary for security purposes. Our experienced Professional Services Organization will do the software integration if desired.

Key Backup and Recovery

When a public-private key pair is used to protect stored encrypted data, it may be necessary to recover the private key if the primary copy of that key is lost or otherwise becomes inaccessible. Without such a capability, loss of a private key may mean loss of valuable data.

VeriSign addresses this requirement with OnSite Key Manager—an option which allows an enterprise administrator to centrally generate user key pairs and control the backup and recovery of the private keys. Centralized generation of key pairs facilitates batch pre-authentication and key distribution in large communities. Support for the management of full user key histories is included.

OnSite Key Manager operates in conjunction with a VeriSign Key Recovery Service. Private keys are stored on the enterprise premises in a non-vulnerable, enveloped form, allowing for strong protection of the private keys without the need for a bulletproof secure facility. Recovery of a private key requires retrieval from VeriSign of a unique key which can unlock the envelope. This system has major security advantages over the vulnerable key-backup databases offered by standalone PKI software product vendors.[3]

When an enterprise needs to back up private keys, the paramount requirements are enterprise control and high security. With VeriSign's state-of-the-art key management solution, private keys are held by the enterprise but can only be exposed after a confirming transaction with a highly secure PKI processing center. PKI built on standalone PKI software is vulnerable to disclosure of all the enterprise's private keys in one attack, and leaves all the costs of security, and all the risk, with the enterprise.

Dual-Key Support

When a public-private key pair is the basis for protecting stored encrypted data, there may be a requirement, by enterprise administration, to keep a backup copy of the encryption private key, to be sure that encrypted data can be recovered in the event the original copy of the private key was lost or

[3] "VeriSign Public-Key Infrastructure – Enterprise Key Management," VeriSign White Paper #98-02, 1998.

became inaccessible. However, if a public-private key pair is to be used for creating legally binding digital signatures, that is, for transactions with *non-repudiation*, then it may be beneficial if no copy of the signature private key is ever made. (In theory, if signature private key copies exist, an alleged signer might claim that the copy—not the original key—made the signature, and thereby repudiate a transaction.) If both the encryption-key-backup and non-repudiation requirements need to be satisfied in one application, a user may need to have two separate key pairs—one with the private key backed-up (for encryption purposes) and one not (for non-repudiable digital signatures).

Few applications currently require dual key pairs. VeriSign supports dual key pairs for those applications that do. Standalone PKI software vendors who have built their architectures around "universal dual key-pairs" unnecessarily lock the enterprise 100% into proprietary client software.

With RSA-based technology, dual key pairs are very rarely a real requirement in today's applications, and many application products neither implement, nor need to implement, support for dual key pairs. However, as deployment of PKI technology advances, real needs for this feature will likely emerge.

The VeriSign infrastructure inherently supports dual key pairs and multiple active certificates per user. VeriSign's application partners are adding dual key capabilities as customer needs arise. For instance, Microsoft's Outlook 98 supports dual key pairs as an option and Netscape has announced that it will be implementing dual key pairs in its clients this year. VeriSign's application-integration toolkit supports both single and dual key-pair options today and the VeriSign OnSite platform can manage both today.

Open Architecture

Open vs Closed PKI

One PKI can serve multiple applications, thereby reducing administrative burdens and improving the end-user experience, for example, by reducing the number of passwords a user must remember. One of the biggest challenges is how to PKI-enable the applications—especially the *best-of-breed applications* demanded by enterprise customers generally. Two approaches are used by PKI vendors:

- **Closed PKI:** Proprietary PKI software is installed on every desktop. Applications which use the PKI require a proprietary software interface from the PKI vendor.

- **Open PKI:** Native applications interface to the PKI using industry standard interface protocols or tailored interfaces agreed through PKI-application vendor partnerships. No proprietary PKI software is needed on the desktop.

Closed PKI does not extend easily beyond the corporate intranet to extranet applications serving customers or partners. If all certificate-using desktops are not under enterprise control, it is impractical to require special-purpose software, such as a proprietary PKI client, on those desktops. In an extranet, desktop systems in their *native mode* must interoperate with the central PKI.

Closed PKI means that the PKI vendor dictates what desktop software must be used throughout a complete PKI community, including customers, partners, etc. All users must assume the burden and cost of installing, updating, and troubleshooting this special software. A major pitfall of Closed PKI is illustrated by the following real-life example: A prominent PKI software vendor recently released a variant of a popular web browser, customized to interface to that PKI vendor's products through a proprietary software interface. However, subsequent upgrades of the browser would not work with the same PKI—unwitting customers were stranded with an obsolete browser release.

An enterprise PKI must support all of the enterprise's preferred applications, without requiring the burden of proprietary PKI products on all desktops. VeriSign works with over 100 independent software vendors, including all the big names, to give you Open PKI—applications that are VeriSign-PKI-enabled as shipped from their vendors. Closed PKI limits PKI-enabled applications to those from vendors prepared to build to a proprietary PKI software interface. Worse, it does not work in extranets where the enterprise does not control all desktops.

Closed PKI also does not extend easily beyond the corporate intranet to extranet applications serving customers or partners. If all certificate-using desktops are not under enterprise control, it is impractical to require special-purpose software, such as a proprietary PKI client, on those desktops. In an extranet, desktop systems in their *native mode* must interoperate with the central PKI.

VeriSign is committed to the concept of Open PKI which averts the above problems. VeriSign has partner relationships with over 100 independent software vendors, including Microsoft, Netscape, Lotus, Oracle, Hewlett-Packard, SECUDE (PKI for SAP R/3), Intuit, Jetform, Cisco, and Lucent. VeriSign's enterprise PKI solutions work effectively with standard products from these vendors. Since VeriSign's PKI offerings totally complement the offerings of these software vendors, we can readily work with them all as partners to make Open PKI a reality.

VeriSign also contributes heavily to the formulation of industry standards for PKI; for example, we provide the Co-Chair for the IETF PKIX committee that develops such standards plus Editors for five of the PKIX standard drafts.

VeriSign's Open PKI strategy also includes a software toolkit for PKI-enabling customer-written applications, or customers can choose from a range of VeriSign-enabled toolkits from other vendors, including Entegrity, Baltimore, RSA, and Xeti. The Open PKI program extends also to partnership relationships with systems integrators, such as KPMG and Ernst and Young. Such partnerships facilitate the building of highly integrated enterprise PKI solutions.

Directory/Database Technology

Enterprises operate a variety of corporate directory/database systems, which potentially need to be integrated with their PKIs. These directory/database systems include: X.500-technology directories, Web-based LDAP directory servers, DBMS systems from the traditional suppliers, and various legacy systems. Certificates (and, if applicable, CRLs) needed by enterprise applications can be distributed by any of the above systems.

VeriSign recognizes the need to accommodate all of the above technologies, as opposed to binding an enterprise PKI offering to one specific technology (e.g., X.500) only. Enterprises are moving to common directory architectures and want directory integration – not directory separation. Accordingly, VeriSign OnSite includes a customizable Directory Integration Module which supports the delivery of certificates to local enterprise directories and databases. It directly supports LDAP-based directory systems but is also designed for rapid adaptation to interface to any desired directory or database technology. This OnSite option comes packaged with VeriSign Professional Services resources to adapt it to satisfy any particular customer's needs.

Deploying a PKI should not force an enterprise to adopt a particular directory strategy. VeriSign OnSite adapts to a customer's installed directory/database technology, including LDAP, X.500, SQL, or legacy technology. Standalone PKI software that requires a particular directory interface protocol and/or dictates a particular directory schema will not integrate easily with pre-existing directory systems due to feature and schema conflicts.

Revocation

A certificate may need to be revoked by a CA if a user private key is compromised or the CA is no longer willing to support the certification. Different application environments demand different revocation mechanisms, dependent on their risk scenarios, timeliness requirements, and the sizes and distributions of the subscriber and relying party communities. Established revocation mechanisms include certificate revocation lists (CRLs), interactive (WWW) real-time certificate status interrogation, and on-line certificate status checking (OCSP). VeriSign is committed to supporting all of these revocation mechanisms in accordance with customer demand.

Daily CRLs and interactive real-time certificate status determination are supported by standard VeriSign OnSite policy choices. Hourly CRL-issuance is available as an option. VeriSign also supplies a revocation plug-in for Microsoft's IIS and Netscape's Enterprise Server that checks the revocation status of a presented client certificate, automatically fetching CRLs as needed. This gives a fully-automated revocation environment for web servers which, unlike Closed PKI offerings, will operate with standard web browsers.

For applications requiring real-time status checking, VeriSign pioneered the development of the OCSP protocol and was the first vendor to demonstrate OCSP in operation in the 1998 National Automated Clearinghouse Association (NACHA) PKI trials. VeriSign will provide OCSP for enterprise customers as application vendors release support for this protocol.[4]

Enterprise PKI must support various revocation requirements of different applications. VeriSign generates CRLs daily or hourly for all enterprise customers. It provides turnkey revocation status-checking for enterprise web servers that can operate with standard web browsers. OCSP will also be supported for OCSP-enabled clients. PKI software vendors support only CRLs, usually only in conjunction with their proprietary client software.

[4] Netscape Communications Corporation's foreshadowed its implementation of this protocol in an announcement in August, 1998.

Availability and Scaleability

Redundancy and Disaster Recovery

A PKI used for mission-critical purposes requires 7x24 availability, redundant systems, and full disaster recovery backup. With VeriSign OnSite, a fully redundant infrastructure is already in place, with 7x24 service levels guaranteed for all critical components. There are redundant systems for servers, database, Internet service providers, telecommunications, and power. Disaster recovery operates 7x24 using a geographically separated site operated in conjunction with ComDisco.

An enterprise building its own PKI from standalone PKI software vendor products must establish and finance its own redundant configurations, and its own disaster recovery strategy and sites. This often proves difficult since these PKI products are not designed for redundancy.

A PKI supporting mission critical applications must have fully redundant systems and backup sites for disaster recovery purposes, otherwise business is at risk. VeriSign OnSite includes built-in redundancy in all of the critical components that are located at the VeriSign center. An enterprise that takes the PKI software product approach must establish and finance its own redundant systems and disaster recovery site.

Scaleability

Enterprises want to be able to start small—set up a PKI initially with hundreds or a thousand users, then progressively scale that PKI to tens of thousands, hundreds of thousands, and ultimately millions of users.

A VeriSign-supplied enterprise PKI can scale smoothly across this full range, with the customer paying only for the scale of PKI needed at any time. Furthermore, it is the only PKI technology in the world proven under real-world conditions to be capable of issuing certificates to the scale of millions. The scaleability comes from the use of multi-processor server architectures, high-performance transaction engines, multi-unit cryptographic hardware banks, and scaleable Oracle database technology. Standalone PKI software is known to encounter scaling limits at the tens of thousands due to lack of a transaction-optimized architecture and scaling and resiliency limits with their database and directory systems.

An enterprise must be able to smoothly grow its PKI from modest beginnings to a platform supporting large numbers of customers, employees, and e-commerce business partners. The VeriSign solution has been proven to scale smoothly from hundreds to millions of users, and the customer pays for the scale of PKI needed at any time. PKI software vendor products suffer degradation at or before tens of thousands of users.

Security and Risk Management

Facility and Personnel Security

In a PKI service deployment, the full complement of strong security controls need to be employed, including hardware cryptographic modules, physical security of the facility housing the CA, personnel security measures (including screening and specialized training of all CA staff), and procedural controls to enforce such policies as dual control.

The costs of establishing and operating a high-security, high-availability facility can be prohibitive. The VeriSign PKI solution removes this burden from the enterprise customer by locating critical functions in a secure data center operated by VeriSign or an affiliate on a 7x24 basis. Each data center has multi-tiered physical security, security-screened personnel, and is subjected to stringent security audits. 7x24 service levels are guaranteed. Customer service operates on a three-shift basis. VeriSign's infrastructure is backed up by the operators of the world's largest network of PKI centers, supporting over 3 million consumers and 65,000 websites.

This state-of-the-art security infrastructure has been leveraged by hundreds of enterprises, whose management cannot afford to take the security risks created by standalone PKI installations. This is especially true as enterprises expand their PKI beyond initial pilot installations to full-scale production systems.

A mission-critical PKI needs a high-security, high-availability (7x24) facility with specially trained and screened personnel, redundant systems, full disaster recovery, and round-the-clock customer support. The enterprise that builds its own PKI from software products is responsible for all this. With VeriSign OnSite, the security-critical functions link to VeriSign secure data centers, allowing the enterprise to focus on core business operations. By contrast, standalone PKI requires the enterprise to create 100% of its own secure environment.

Customer Practices Support

PKI operators need to establish and enunciate practices that allow the entire PKI community to trust the infrastructure and be confident that risks are controlled. This applies particularly to a PKI community that spans multiple organizations, and most particularly when the PKI supports digital signatures used in support of electronic commerce, that is, in replacing business-to-business or consumer-to-business paper transactions with electronic transactions. With such a PKI, sound practices are essential to ensure that transactions will be legally binding and have non-repudiation, that is, signers cannot falsely deny originating messages. Practices statements also need to establish fair and non-onerous means for apportioning liability in the event of a failed transaction that causes material damage.

VeriSign is a world leader in the development of PKI practices. In particular, VeriSign's Certification Practices Statement (CPS),[5] which enunciates the practices underlying the VeriSign Trust Network (VTN) public CA services, is recognized as the most comprehensive document of its type in the world. It is used as a foundation for enterprise PKI practices internationally. VeriSign OnSite customers may choose to establish their own, private PKI hierarchies and define their own practices. In this case, VeriSign practices consultants are available to assist. Alternatively, the enterprise CA may be certified into one of the VeriSign Trust Network public hierarchies, in which case the provisions of the VeriSign CPS will apply.

To achieve non-repudiation and multi-party trust in PKI, you need specialized, audited processes covering cryptographic PKI management, day-to-day operations, and record-keeping. VeriSign leads the development of PKI practices internationally, with audited business processes that meet the most rigid industry standards, including liability-sharing and insurance protection. Build-it-yourself PKI means build 100% of your own practices, liability coverage, insurance policies, and audit.

VeriSign's practices include witnessed and audited processes for CA key establishment and management and rigid multi-party controls over all key materials. VeriSign's processes have been certified by KPMG in accordance with AICPA SAS-70. VeriSign's practices are backed up by $50 million E&O insurance, the industry's only NetSure extended warranty program for enterprises joining VeriSign Trust Network, and liability-sharing agreements.

Non-repudiation

Non-repudiation refers to the generation and secure storage of evidence to support the resolution of disagreements as to the outcome of electronic transactions. Ultimately, the evidence must be able to prove convincing to a third party arbitrator, who can resolve a dispute without needing to rely entirely on the words of the disputing parties. Non-repudiation depends on the use of digital signatures, created by parties who keep their private keys secure. In addition, non-repudiation depends upon the issuance of digital certificates by a trusted and independently audited CA system, and the maintenance of

[5] Available at: http://www.verisign.com/repository/CPS.

secure records of certificate issuance and life-cycle management, including all steps occurring in the revocation of such certificates in the event of private key compromise or other circumstances leading to certificate revocation.

With VeriSign OnSite, while the enterprise has full control over the issuance and revocation of digital certificates, complete records of the issuance and life cycle management of certificates are maintained by VeriSign in a high security, independently audited data center. Disaster recovery services operate around-the-clock at a geographically separated backup site.

Non-repudiation means independently verifiable evidence. Unless operated under independent supervision, enterprise-operated PKI products do not give non-repudiation, since no third party can offer corroboration of process and records integrity. VeriSign's independently evaluated and audited cryptographic PKI management processes and secured records provide a solid basis for swift and final dispute resolution.

Extranet/E-commerce Readiness

PKI can potentially span a community of any size, for example, a corporate intranet, an extranet that links an organization with its business partners or customers, a community-of-interest that spans multiple organizations (such as corporations in the same industry), or a global community that includes all-comers, for example, for the greater Internet mail community. VeriSign facilitates the development of communities beyond the intranet in several unique ways.

Broad Community Enablement

While some enterprises require closed, private PKIs, others want their certificates to be recognized and trusted by out-of-the-box commercial web browsers or other desktop application products. This greatly facilitates the establishment of extranet PKIs or community-of-interest PKIs, by obviating the need for special software installation or configuration in the desktop systems of organizations that are not under the administrative control of the PKI-operating organization.

With VeriSign OnSite, these requirements are satisfied by giving the enterprise customer the option of establishing an isolated private PKI, a community or industry-wide PKI, or a PKI linked into the VeriSign Trust Network. The VTN is a global, integrated PKI operated by VeriSign and its worldwide affiliates such as British Telecom, AT&T, CertPlus in France[6],

[6] CertPlus is a joint venture of France Telecom, GemPlus, Matra, and VeriSign.

HiTRUST in Taiwan, SACA in South Africa, and VeriSign Japan. 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 recognized by the users of such products.

While enterprise PKI may start with just intranet applications, proper planning will allow it to later scale to extranets or larger community structures. Communities can be built instantly when the members already recognize common root keys. VeriSign OnSite customers are offered the options of private PKI, extranet PKI, industry PKI, or a PKI cross-certified into the global VeriSign Trust Network, whose roots are pre-installed in all popular client products. With a PKI built from standalone software, community building is much more unwieldy, involving manual, pairwise 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 together PKI communities that may span multiple organizations. VeriSign has led the development of cross-certified structures, including the VeriSign Trust Network global public PKI community, private PKI certification structures for enterprises or communities-of-interest, the global SET infrastructure which involves cross-certification of multiple vendors' CA products, and cross-certification of the most popular CA software products—Netscape's Certificate Server and Microsoft's Certificate Server—into VeriSign's infrastructures.

Cross-certification structures may be made as simple (i.e., hierarchical) or as complex (i.e., unbounded web-of-trust) as the user community requires. VeriSign cross-certification supports all of these structures.[7]

Cross-certification comprises two essential steps:

1. **Practices establishment:** The establishment of appropriate agreements as to risk-management practices and business terms and conditions between the cross-certifying organizations.
2. **Certificate request/issuance:** Transfer of a certificate signing request from one CA to the other, and issuance of a cross-certificate by the latter CA.

Certificate request/issuance is straightforward, reflecting the same process as issuance of a user certificate. This process uses industry standard certificate-request protocols such as the widely-deployed PKCS#7 and PKCS#10 standards or the emerging IETF PKIX standards.

[7] Not all certificate-using application products support all structural configurations.

The practices establishment step presents a greater challenge, but VeriSign's customers can benefit from the unique expertise in VeriSign's Practices Department, led by Michael Baum, renowned electronic commerce attorney. VeriSign customers have the option of cross-certification into a structure with established practices in place or, alternatively, establishing a new structure with new practices. In the latter case, customers are offered access to VeriSign's unique practices expertise on a consulting basis or by sublicensing proven practices statements.

The critical issue with building cross-certified structures is that the approach of establishing many networked, bilateral cross-certification arrangements does not scale into workable communities—the overall trust level would end up reflecting the lowest common denominator of all of the bilateral relationships. VeriSign works with communities-of-interest to establish a communal approach to PKI practices from day one, using extensive real-life experience as the basis.

Cross-certification means much more than just issuing another certificate – it is a special business arrangement, involving agreements on such points 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 organizations worldwide. VeriSign helps its customers establish cross-certification practices and agreements. With a PKI software product, where cross-certification is concerned, you are on your own.

Feature Comparison – VeriSign & Entrust

VeriSign is the only vendor in the PKI space offering a *complete* enterprise PKI solution—based on the PKI service platform concept. As an example, the following table summarizes some major differentiators between VeriSign and Entrust PKI offerings.

PKI Component	***VeriSign OnSite 4.0*** ***Integrated PKI Platform***	***Entrust*** ***Standalone PKI Software***
Technology		
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)	Base product uses software cryptography (hardware option at additional expense)
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 by intruders/administrators if private root key held in on-line, operational environment)	Root keys held in on-line, operational environment
User key management	User encryption keys backed up at enterprise; full key histories; strong protection using distributed key recovery technology	User encryption keys backed up at enterprise; full key histories; held in single-point-of-failure online database
User dual-key support	Supports single or dual key pairs for any application (dependent on application requirements and capabilities)	Supports single or dual key pairs (dual key pairs supported only with proprietary client and applications interfaced via proprietary toolkits)
Open Architecture		
Open vs closed PKI	Open PKI; no proprietary software on desktops; 100+ ISV partners; 120+ applications enabled	Closed PKI; many features require proprietary desktop client or toolkit; limited to 29 ISV partners; 45 applications enabled[1]
Directory/database technology	Enterprise choice of LDAP, X.500, SQL, or legacy DBMS; no directory schema restrictions	LDAP/X.500 directory required with special schema restrictions that may conflict with other enterprise directory schema
Revocation	CRLs issued regularly; revocation enabled for web servers and standard browsers; OCSP support for key clients, e.g., Netscape	CRLs issued regularly; revocation limited to Entrust proprietary client & server plugins; no OCSP; no revocation for other client applications without proprietary desktop or toolkit
Availability and Scaleability		
Redundancy	Guaranteed 7x24 service levels, redundant servers, database, ISPs, telecommunications	None provided by vendor; enterprise provides its own
Disaster recovery	Guaranteed 7x24 disaster recovery backup at remote secure site	None provided by vendor; enterprise provides its own
Scaleability	Proven, seamless scaleability from 100s to millions; guaranteed peak loading service levels	Scaleability problems start at 10s of thousands; product unproven at 100s of thousands+

Security and Risk Management		
Facility security	Fortified construction, 5-tier security; dual biometric access control, 24-hour monitoring, motion detect, network security audit	None provided by vendor; enterprise provides its own
Personnel security	Investigative screening, specialist training, retraining	None provided by vendor; enterprise provides its own
Independent audit	Independent SAS-70 audit by KPMG; VISA audited and approved	None provided by vendor; enterprise arranges its own
Customer practices support	Enterprise CA may join VTN with proven established practices, or may establish own practices; VeriSign offers practices consulting and/or CPS	None provided by vendor; enterprise must develop its own practices and legal expertise
Non-repudiation	Evaluated/audited cryptographic materials management and secured records retention provide independently verifiable evidence for dispute resolution	No non-repudiation, unless PKI is operated under full supervision of an independent authority
Extranet/E-Commerce Readiness		
Global Community Enablement	Enterprise has option of joining PKI structure with roots pre-installed in all commercial web/mail clients	Enterprise must configure web/mail clients to recognize CA
Cross-certification	Can cross-certify enterprise OnSite 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	Mechanical certificate issuance only; no assistance with practices; vendor has no operating experience; no cross-certification with Netscape/Microsoft

NOTES:

1. Based on current Entrust Website information.

For Further Information...

...see the VeriSign website at www.verisign.com, contact your local VeriSign Account Representative, or call VeriSign at (650) 961-7500.