

341RGF;IXZRSD})98:><()YU^\$
\$*CVLKW\$JFVD98-423TNBJK
CX V;;ZJPEROG9UCV N'JWEFU
Y1 "THE4L3:1703S4}5HKL165
79GFD3T4809#\$OJ90E2QTOI
H34QLTIFYUSIGN341RGF;IXZR
SD})98:><()YU^\$OF341\$*CV
LKW RGF;IXZRSD})98:><()YU^\$
*CV@TRUST:LKW\$JFVD98-423
BJK\$*CVLKWHONISDG{JFV23
98-423TNBJKW2E<THE-R=12
SDG;IXZR2~SD})98:>D<2(7)YU
;I7&XNETZRSD})9B8<(LUY)YU
CV:>LKW\$JFVDKW\$JF#VD&S
<W3<RGF;IXZRSD})9%F*Z)YU^
*CV@:LK4W\$JF9VD98-42I!53
RJK\$*CVLKWHONISDG{JFV23

Guide to Securing

Intranet and Extranet Servers

Table of

Contents

Summary	1
Benefits of the Intranet and Extranet	3
New Security Concerns	6
Goals of Intranet and Extranet Security Systems	10
Certificates and PKI: The Optimal Technology Solution for Achieving Your Security Objectives	12
The Central Role of the Certificate Authority	18
Getting Started	26
Next Steps: Using Client IDs and VPN IDs	31
Conclusion	32
Case Studies	34

Summary

Over the last four years, organizations have embraced Intranets and Extranets enthusiastically. This is not surprising. Intranets and Extranets offer clear cost savings and ease of installation compared with older leased line networks or WANS based on proprietary technology. Furthermore, they enable highly productive and cost effective new ways of working. Organizations can use Intranets and Extranets to distribute information more cost effectively and in a more timely manner. They can use them to build a wide range of self-service applications that help reduce administrative costs. And, they can use them to improve collaboration among employees across the organization and with business partners.

As Intranets and Extranets have become more widely deployed, new security challenges have emerged. While many organizations have deployed firewalls and access control technology to improve security, these technologies leave many security issues unaddressed.

This guide will give an overview of the main security risks of deploying Intranets and Extranets and will discuss the five fundamental goals of a security system: Privacy, Authentication, Content Integrity, Non-repudiation, and Ease-of-use. The guide will also describe how an intelligently

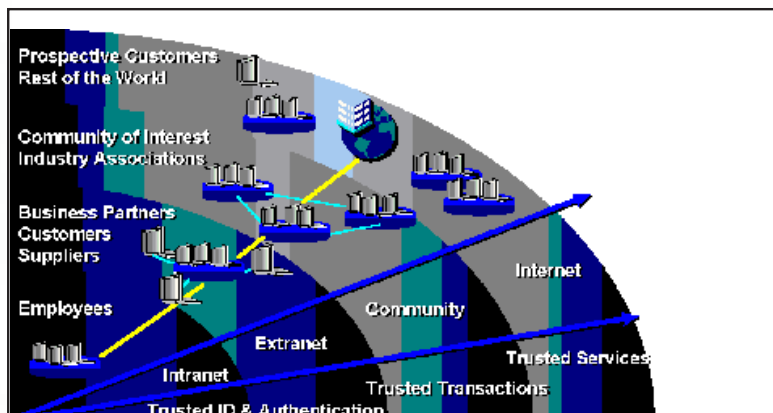
deployed Public Key Infrastructure (PKI) system, based on the digital certificate technology, addresses these security goals. Finally, the guide will give an overview of how VeriSign's OnSite family of products can help your organization quickly and effectively deploy a PKI.

The Growth of the Intranet and Extranet

Few technologies have been accepted as rapidly as Intranets within organizations. Virtually unknown four years ago, Intranets are now ubiquitous. Analysts at Zona Research predict that the Intranet market will exceed the Internet market by a ratio of 2 to 1 by 1999. Killen & Associates estimated the market for Intranet software, equipment, and services in the US would exceed \$20 billion by the year 2000. Early in 1997, Booz Allen & Hamilton reported that nearly every member of the Fortune 500 had deployed an Intranet or was in the process of doing so.

Many of these organizations are now extending their Intranets to reach key customers and/or business partners via Extranets. A 1998 survey of 1,400 chief information officers by market research firm RHI Consulting showed that 38 percent of respondents expect the popularity of Extranets to "increase significantly" during the next three years. Another 44 percent said they expect their popularity to "increase somewhat" during the same period.

Figure 1: The Expanding Network



Benefits of the

Intranet and Extranet

The reasons for this growth are clear. Compared with earlier wide area networks (WANs) based on proprietary technology or expensive leased lines, Intranets and Extranets are significantly easier and less expensive to set up and operate. Intranets can offer organizations numerous operational efficiencies, and, as a result, they can generate staggering returns on investment.

Where WANs required expensive leased lines, Intranets and Extranets allow users to communicate over vast distances using inexpensive public Internet lines. When organizations tried to link local area networks (LANs) over the WAN, diverse communications protocols (including ipx/spx, netbios, netbui, and DECnet) often limited applications' ability to talk to each other. By adhering to TCP/IP, the standard Internet protocol, Intranets and Extranets make it easy for different computer systems within or even outside an organization to speak to each other. Using the hypertext language and browser model of the World Wide Web, Intranets provide users with tools that are graphic and easy to operate.

Once up and running, Intranets and Extranets reduce costs and improve operations in many ways, including:

- **Reducing costs of distributing information.** Intranets make it faster and easier to distribute policies, procedures, and company news to employees; Extranets make it easy and inexpensive to distribute online catalogs and price lists
- **Lowering administrative costs.** The interactive capabilities of the Intra/Extranet allow users to complete many tasks themselves that once required administrative assistance. For example, Intranets now allow employees to enroll in their own 401(k) or health plans, while business-to-business customers can order their own supplies over the Extranet
- **Improving collaboration.** Users become more productive by using the Intra/Extranet to form virtual, online teams. These virtual teams can collaborate without the expense of frequent travel or the delays of sending information via the postal service. Within an organization, the Intranet can flatten hierarchies, giving more employees access to the information they need to make strategic decisions. Extranets allow businesses to collaborate more closely with each other as well. For example, Extranets can be used to integrate the supply chain, replacing expensive and proprietary systems such as electronic data interchange.

The sum total of these benefits can mean a staggering boost to an organization's bottom line. A recent article in the Intranet Journal cites dramatic returns on companies' Intranet and Extranet investments. For example, Lockheed Martin's implementation of an Intranet gave a staggering 1,562% return on investment; Cadence, Inc. 1,766%; and US West more than 1,000%.

Industry Extranets show similar promise. For example, within the automotive and retail industries, many companies are establishing Extranet-based supply chain networks, allowing real-time inventory, order, and delivery information to be communicated between retailers, distributors, manufacturers, and suppliers. This helps dramatically improve the ability of all organizations within the supply chain to match the supply of goods for the demand of goods, while simultaneously decreasing inventories. This improves efficiency, inventory management, and, ultimately, profitability throughout the entire supply chain.



New

Security Concerns

As the use of Intranets and Extranets has grown, so has the need for security. The TCP/IP protocols and technology are inherently designed to be open. TCP/IP is a connectionless protocol; data is broken up into packets which travel freely over the network, seeking the best possible route to reach their final destination. Therefore, unless proper precautions are taken, data can readily be intercepted and/or altered—often without either the sending or the receiving party being aware of the security breach. Because dedicated links between the parties in a communication usually are not established in advance, it is easy for one party to impersonate another party.

Figure 2: Expanding Networks Increase Possible Points of Attack

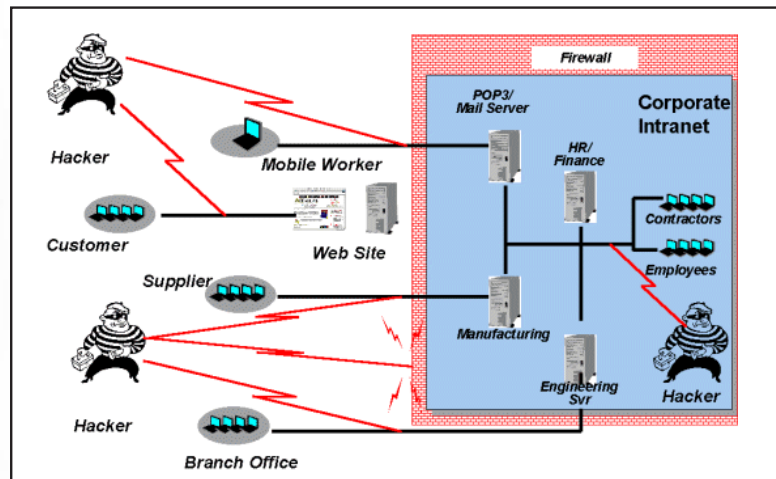


Figure 2 illustrates the growth in network complexity has increased the potential points of attack both from outside and from within organizations. Fortunately, the methods of protecting against these attacks have also expanded.

Two of the most common security precautions in use today are firewalls and passwords. Passwords are designed to prevent unauthorized individuals from directly gaining access to sensitive data stored on servers. Firewalls, by contrast, are designed to provide a perimeter defense mechanism, preventing unauthorized individuals outside the organization from gaining access to sensitive data inside the organization. According to a recent IDC study, virtually 100% of Fortune 500 organizations have already deployed firewalls.

Despite their important role in network security and widespread adoption, firewalls provide only a partial solution. As shown in Figure 2, perimeter defenses can do little to prevent against attacks by insiders (e.g. disgruntled employees, contractors, or others). Passwords are also largely ineffective against inside attacks. Most passwords are notoriously easy to guess; where passwords are not guessed, they can often be discovered on sticky pads on employee's computers or intercepted as they pass, in the clear, over corporate networks.

Even when passwords are not guessed, or when more sophisticated access control methods are used, it is important to note that access control alone can not ensure that information remains confidential. While a good password system might prevent someone from directly entering a server to obtain confidential information, passwords do not protect data as it passes "over the wire" between the server and the client.

The same general problem applies to data that passes outside the firewall, between corporate servers and branch offices, customers,

suppliers, and remote employees. Any time that data is sent between your servers and organizations outside your firewall, the data can be intercepted using “sniffers.” Hackers do not need to get “in” to your system, if you are sending data outside the perimeter.

Types of Security Risks Encountered on an Intranet and Extranet

Intranet and Extranet security breaches can take a variety of forms. For example,

- An unauthorized person, such as a contractor or visitor, might gain access to a company's computer system.
- An employee or supplier authorized to use the system for one purpose might use it for another. For example, an engineer might break into the HR database to obtain confidential salary information.
- Confidential information might be intercepted as it is being sent to an authorized user. For example, an intruder might attach a network sniffing device to the network. While sniffers are normally used for network diagnostics, they can also be used to intercept data coming over the wire.
- Users may share documents between geographically separated offices over the Internet or Extranet, or telecommuters accessing the corporate Intranet from their home computer can expose sensitive data as it is sent over the wire.
- Electronic mail can be intercepted in transit.

These are not merely theoretical concerns. While computer hackers breaking into corporate computer systems over the Internet have received a great deal of press in recent years, in reality, corporate insiders—such as employees, former employees, contractors working onsite, and other suppliers—are far more likely to attack their own

company's computer systems over an Intranet. In a 1998 survey of 520 security practitioners in U.S. corporations and other institutions conducted by the Computer Security Institute of San Francisco with the participation of the FBI, 44 percent reported unauthorized access by employees compared with 24 percent reporting system penetration from the outside.

Such insider security breaches are likely to result in greater losses than attacks from the outside. Of the organizations that were able to quantify their losses, the Computer Security Institute survey found that the most serious financial losses occurred through unauthorized access by insiders, with 18 companies reporting total losses of \$50,565,000 as compared with losses of \$86,257,000 for the remaining 223 companies that were able to put a dollar value on their losses. As organizations increasingly install Intranets and Extranets, therefore, it is becoming critical for them to secure these systems from inside attacks.

Figure 3: Average Losses from Various Types of Attacks

Type of Attack	Average Loss
Unauthorized Insider Access	\$ 1,363,915
Theft of Proprietary Info	1,307,146
Financial Fraud	656,927
Telecom Fraud	595,766
Sabotage of data or networks	164,817
Spoofing	128,000
System penetration by outside	110,944
Telecom eavesdropping	96,833
Denial of Service	77,417
Virus	65,997
Active Wiretapping	49,000
Insider Abuse of Net Access	38,744
Laptop Theft	35,348
Average Loss	215,753

Source: CSI/FBI 1998 Survey of Computer Security

Goals of Intranet and Extranet Security Systems

Fortunately, there are a variety of techniques available to address these security holes within Extranets and Intranets. Before choosing a particular technology, however, it is important to understand the full range of issues that security systems should address:

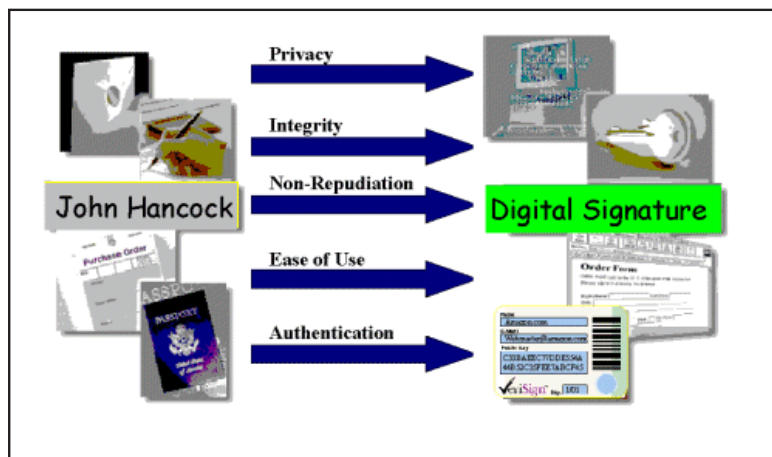
- **Authentication**—ensuring that entities sending messages, receiving messages, or accessing systems are who they say they are, and have the privilege to undertake such actions
- **Privacy**—enabling only the intended recipient to view an encrypted message
- **Content Integrity**—guaranteeing that messages have not been altered by another party since they were sent
- **Non-Repudiation**—establishing the source of a message so that the sender cannot later claim that they did not send the message
- **Ease of use**—ensuring that security systems can be consistently and thoroughly implemented for a wide variety of applications without unduly restricting the ability of individuals or organizations to go about their daily business

This last goal is frequently overlooked. Organizations must not only develop sound security measures, they must also find a way to ensure consistent compliance with them. If users find security measures cumbersome and time consuming to use, they are likely to find ways to circumvent them— thereby putting your Intranet and Extranet at risk. Organizations can ensure the consistent compliance to their security policy through:

- **Systematic application.** The system should automatically enforce the security policy so that security is maintained at all times.
- **Ease of end-user deployment.** The more transparent the system is, the easier it is for end-users to use—and the more likely they are to use it. Ideally, security polices should be built into the system, eliminating the need for users to read detailed manuals and follow elaborate procedures.
- **Wide acceptance across multiple applications.** The same security system should work for all applications a user is likely to employ. For example, you should be able to use the same security system whether you want to secure e-mail, e-commerce, server access via a browser, or remote communications over a virtual private network.

Certificates and PKI: The Optimal Technology Solution for Achieving Your Security Objectives

Figure 4.
Public Key Infrastructure Provides Tools for Achieving Security Objectives



Fortunately, a set of technologies have been developed over the past fifteen years that are particular well suited to meeting these five security goals. Broadly called Public Key Infrastructure (PKI), this technology allows organizations using open networks, such as TCP/IP Intranets and Extranets, to replicate or even improve on the mechanisms used to ensure security in the physical world. Envelopes and secure couriers are replaced with sophisticated methods of data encryption, which can ensure that messages are only read by their intended recipients. Physical signatures and seals are replaced with digital signatures which, in addition to ensuring that messages came from a

particular entity, can also ensure that message was not altered by as much as one bit during transit. Identity documents, such as passports, employee ID cards, and business licenses, can be replaced with digital certificates (also known as Digital IDs). Finally, the various mechanisms for centralized control, audit, and authorization, such as those provided by corporate governance structures, industry boards, or trusted third parties such as accountants, can be replicated in the digital world through the infrastructure used to managed encryption, digital signatures, and Digital IDs.

What is a Digital Certificate

Understanding digital certificates is central to understanding public key infrastructure systems. A digital certificate, also known as a Digital ID, is the electronic equivalent of a passport or business license. It is a credential, issued by a trusted authority, that individuals or organizations can present electronically to prove their identity or their right to access information.

When a Certification Authority (CA) such as VeriSign issues Digital IDs, it verifies that the owner is not claiming a false identity. Just as when a government issues a passport, it is officially vouching for the identity of the holder, when a CA gives your business a digital certificate, it is putting its name behind your right to use your company name and Web address.

How digital certificates work

In physical transactions, the challenges of identification, authentication, and privacy are solved with physical marks, such as seals or signatures. In electronic transactions, the equivalent of a seal must be coded into the information itself. By checking that the electronic “seal” is present and has not been broken, the recipient can confirm the identify of the message sender and ensure that the message content was not altered

in transit. To create an electronic equivalent of physical security, digital certificates use advanced cryptography.

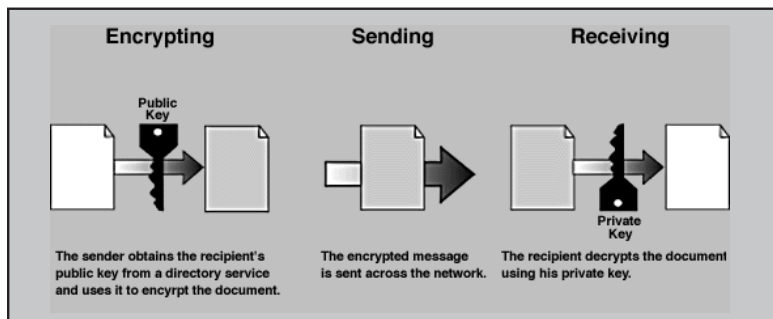
Cryptographic systems have been used to protect valuable information for thousands of years. Traditionally, cryptographic systems have attempted to ensure security using some variant of the secret key system. Secret key systems require that both parties in a communication scheme have a copy of the same secret code or "key." When two people wanted to share information, the sender would encrypt the information using his copy of the secret key. The recipient could decrypt the message only by using her copy of the same key. If somebody intercepted the message, that person could not decipher it without the key.

Despite their widespread use, secret key systems have several critical limitations. First, simply transmitting the secret key poses risks, because the key can be intercepted in transit by unauthorized parties. Second, if one of the sharing parties uses the key maliciously, that party can deny or repudiate, the transaction. Alternatively, the malicious party can impersonate the sender, or can use the secret key to decrypt other sensitive information. To prevent against this sort of attack, organizations must require users to have different secret keys for each party with whom they communicate. If an organization has a hundred people, literally millions of different secret keys will need to be used to accommodate all possible combinations.

Digital certificates employ the more advanced public key cryptography system, which does not involve the sharing of secret keys. Rather than using the same key to both encrypt and decrypt data, a digital certificate uses a matched pair of keys that uniquely complement each other. When a message is encrypted by one key, only the complementary key can decrypt it.

In public key cryptography systems, when your key-pair is generated, you keep one key private. This key is called the “private key,” and nobody other than you, as the rightful owner, should ever have access to it. However, the matching “public key,” can be freely distributed as part of a digital certificate. You can share your digital certificate with anyone, and can even publish your certificate in directories. If someone wants to communicate with you privately, they use the public key in your digital certificate to encrypt information before sending it to you. Only you can decrypt the information, because only you have your private key.

Figure 5. Encrypting Information Using Digital Certificates



Conversely, you can use your key pair to digitally sign a message. To sign a message, you simply encrypt the message with your private key. The message can be decrypted using the public key contained within your certificate. While many people have access to your certificate, only you could have signed the message, because only you have access to your private key.


A digital certificate is a binary file. Your digital certificate contains your name and your identifying information along with your public key—it tells correspondents that your public key belongs to you. Digital certificates generally also contain a serial number, an expiration date, and information about the rights, uses, and privileges associated with the certificate. Finally, the digital certificate

contains information about the certificate authority (CA) who issued the certificate. All certificates are digitally signed using the private key of the Certificate Authority. (Generally, the Certification Authorities' own certificate (called a root certificate) is widely deployed in software packages, allowing people to seamlessly identify legitimate certificates issued by the certification authority.) If the CA maintains good security protection of their private key, it is virtually impossible for anyone to forge a digital certificate.

It is important to note that certificates are not only issued to individuals. Organizations, as well as entities such as servers and routers, can also be issued certificates.

Figure 6. Secure Communications Using Certificates

- Before sending a secret message--ask to see the other party's certificate--to get their public key
- When signing a document--encrypt using your private key, and send encrypted document plus *your* certificate
- Before trusting a document, verify signature using the sender's certificate
- Before doing anything with a certificate, be sure you trust the Certificate Authority who issued it



Digital certificates meet your security objectives

Given the ease and versatility of PKI, security technology based on Digital Certificates has been deployed widely over the past several years. These widely used security protocols include:

- **S/MIME:** The Secure, Multipurpose Internet Mail Extension protocol allows for sending signed and encrypted e-mail
- **SSL:** The Secure Sockets Layer protocol allows for authenticated and encrypted communication between browsers and servers, or between different servers. This is a very important protocol, which will be discussed in greater detail later in this paper.
- **IPSEC:** The IP Security Protocol is a newly developing protocol, allowing authenticated and encrypted communication between routers, between firewalls, and between routers and firewalls. This protocol will play an important role in Extranets in the coming years.

The following table provides a summary of how these various protocols can be deployed in securing your Intranet or Extranet.

Figure 6: Security Protocols for Various Types of Secure Communications

	Privacy/ Encryption	Authentication	Signing Content Integrity <i>(sometimes optional)</i>
Internal employee to server, remote employee server	- SSL 2.0 or 3.0 (provided by Secure Server ID)	- Server authenticated by Server ID - Client authenticated by passwords (phase 1, or by SSL 3.0 with client IDs (preferred)	Signed documents and controls (S/MIME, form signing). Signing done using Client IDs
Customer to web server	- SSL 2.0 or 3.0 (provided by Secure Server ID)	Same as above	NOT USUALLY NEEDED
Remote employee using e-mail	- SSL or POP3 or IMAP mail Server - S/MIME Client IDs (Phase 2) or VPN using IPSEC	- Server authenticated by server ID Passwords (not recommended)	- S/MIME Client IDs - S/MIME (using client IDs)
Communication with branch offices	- SSL (phase 1) - VPN using IPSEC	- Server authenticated by Server ID - Router/firewall authenticated by IPSEC ID - Clients authenticated by passwords or by SSL 3.0 with Client IDs	Signed documents and controls (S/MIME, from signing)

The Central Role of the

Certificate Authority

Requirements for CA's: Technology, Infrastructure, and Practices

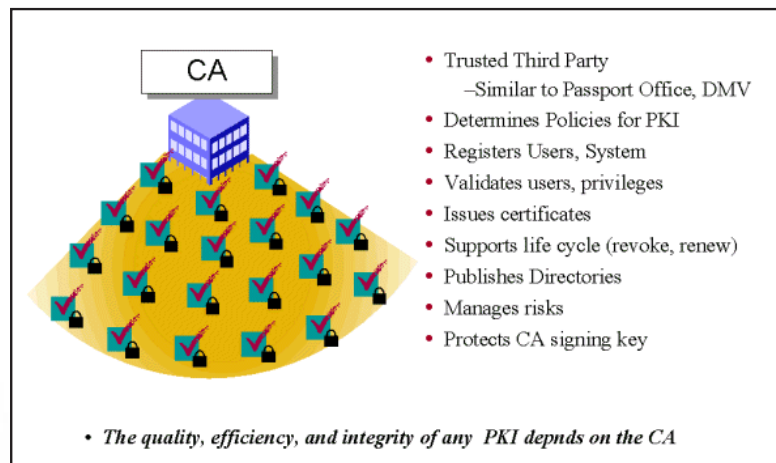
Deploying a successful Public Key Infrastructure requires looking beyond technology. As you might imagine, when deploying a full scale PKI system, there may be dozens or hundreds of servers and routers, as well as thousands or tens of thousands of users with certificates. These certificates form the basis of trust and interoperability for the entire network. As a result, the quality, integrity, and trustworthiness of a public key infrastructure depends on the technology, infrastructure, and practices of the Certificate Authority who issues and manages these certificates.

Certificates Authorities have several important duties. First and foremost, they must determine the policies and procedures which govern the use of certificates throughout the system. These policies and procedures are generally encapsulated in a document called a Certification Practices Statement (CPS). A CPS will generally determine how the CA fulfills the following duties:

- Registering and accepting applications for certificates from end users and other entities

- Validating entities' identities and their rights to receive certificates
- Issuing certificates
- Revoking, renewing, and performing other lifecycle services on certificates
- Publishing directories of valid certificates
- Publishing lists of revoked certificates
- Maintaining the strictest possible security for the CA's private key
- Ensure that the CA's own certificate is widely distributed, so that
- Establishing trust among the members of the infrastructure
- Providing risk management

Figure 7: The Role of the Certificate Authority



As the leading provider of certificates and certificate-based services, VeriSign helps meet these requirements in two different ways. First, VeriSign itself serves as a Certificate Authority for the Internet. Second, VeriSign has a broad range of solutions to allow other organizations to establish themselves as Certificate Authorities for their Intranets and Extranets.

VeriSign as the Internet's CA

As the Certificate Authority for the Internet, VeriSign has issued over 3,000,000 Digital IDs to individuals for use in identifying themselves on the Internet and in sending signed and encrypted e-mail. VeriSign has also issued more than 75,000 IDs for use on servers, which enable people to conduct secure and authenticated e-commerce and other forms of communication with those servers. The Public Key Infrastructure that VeriSign has helped establish for the Internet will secure billions of dollars in transactions this year. In order to maintain the trustworthiness of this commerce, VeriSign has invested heavily in its own infrastructure and practices, as summarized in Figure 8. VeriSign has published the industries leading Certification Practices Statement, available on line at www.verisign.com/repository. VeriSign is regularly audited by a professional accounting firm to ensure compliance with this CPS and all certificate issuance and management takes place within a 5-tier military grade secure facility, by employees who have undergone rigorous background checks. As an example of this security, all VeriSign CA private keys are stored using the same technology that is used to protect nuclear missile codes. To build the acceptance of the PKI, VeriSign has gone to great lengths to ensure that its CA public keys are embedded in all of the major browsers, servers, and other applications. VeriSign has also worked with legislatures around the world to promote the legal acceptance of digital signatures and digital transactions. Finally, to promote trust, VeriSign introduced the NetSure ™ program, which backs each VeriSign Server IDs with \$100,000 of coverage against theft, loss, or impersonation.

Figure 8: VeriSign's Technology, Infrastructure, and Practices

Technology	Infrastructure	Practices
<ul style="list-style-type: none"> • RSA crypto • X.509 formats • 1024 bit signing • SSL, S.MIME, SET, IPSEC • Secure Messaging • Web-based service • Life cycle mgmt • Transaction engine • Trusted by default by over 100 ISV apps 	<ul style="list-style-type: none"> • 24x7 Operations • Secure facilities • Secure networks • Scalable systems • Redundant telecom • Call centers • 300+ employees • US, Japan, Europe • 75,000 Server ID's • 3M client Ids (as of Sept '98) 	<ul style="list-style-type: none"> • Certification Practice Statement • W3C, NIST, IETF • Bonded operators • Liability coverage • Legal expertise • Int'l localization • Regularly audited by KPMG (SAS 70)

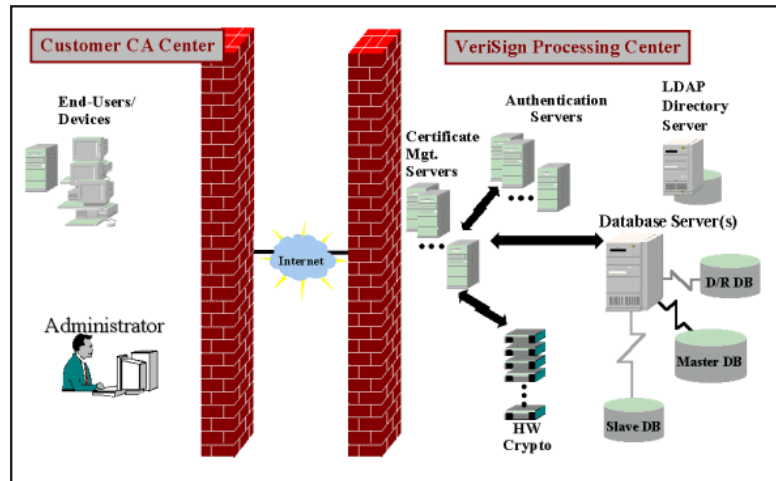
Establishing the PKI for your Intranet or Extranet

When your organization looks to establish its own Public Key Infrastructure, it is important that you be able to establish a high quality set of technology, infrastructure, and practices. While there are several products on the market today that purport to offer stand-alone solutions for generating and managing certificates, these “software-only” solutions can at best offer only the technology that is needed for a robust PKI. As a result, an independent study by the Aberdeen group recently concluded that organizations buying off-the-shelf certificate software solutions end up spending \$1M-\$11M to hire the personnel and build the surrounding infrastructure and practices necessary for a complete solution.

By contrast, VeriSign OnSite offers a more cost-effective and practical solution, called VeriSign OnSite. As indicated in Figure 9, OnSite allows your organization to leverage VeriSign's existing infrastructure and practices. Your organization maintains complete control over the front-end functions—determining who gets certificates, whose certificates get revoked, etc. However, all of the back-end functions of generating certificates, managing security, maintaining systems,

backing up data, auditing security, etc. is handled by VeriSign within VeriSign's secure facilities.

Figure 9: The VeriSign OnSite Solution



How OnSite Works

VeriSign OnSite consists of customized end-user enrollment Web pages, administrative control and management of Web pages, and a certificate directory distribution service. End users interact with customized, Web-based enrollment forms to request and receive their certificates. These forms support the latest browsers from Microsoft and Netscape, as well as a rapidly growing list of other networked software products. The enrollment forms, along with the other lifecycle Web pages, can be hosted at the customer's site or optionally by VeriSign.

Administrators utilize a second set of Web pages to control user authentication, to approve certificate requests and renewals, to revoke certificates, to view reports on CA activity, and other management tasks. Administrators are authenticated before they access the system, using specialized certificates and VeriSign-provided smart cards and readers.

VeriSign OnSite also includes a complete certificate directory and the ability to interface that directory with a customer's corporate directory in a number of ways. A customer can choose to have VeriSign download certificate information directly into their LDAP-compliant directory, or they can periodically fetch that information from VeriSign and integrate it with their directory themselves.

All of the computer and telecommunications infrastructure, cryptographic software and hardware, and on-going key management services required is hosted and operated by VeriSign in our highly secure Operations facilities. In addition, for customers desiring the easiest possible solution, VeriSign can host all of the necessary Web pages. Customers seeking more control over, or full customization of, their pages can host them locally with a minimum of effort.

OnSite Benefits

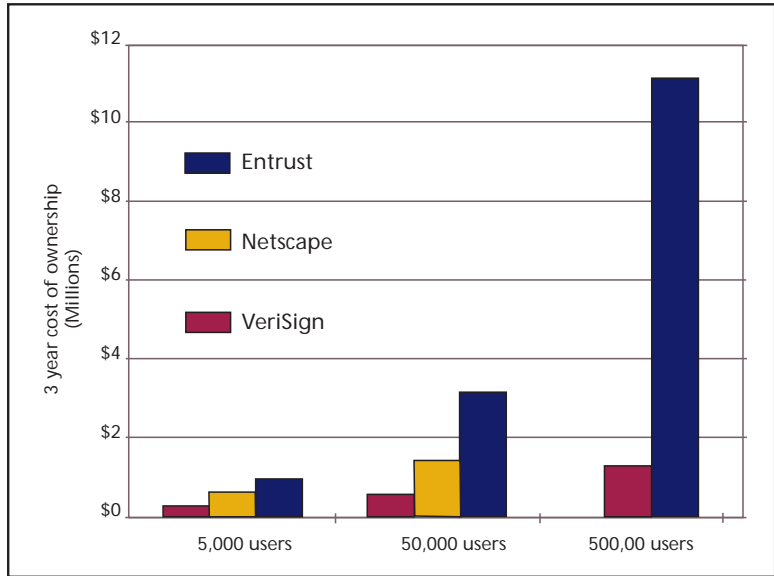
OnSite benefits include:

- **Control.** With OnSite, you immediately become a Certificate Authority with complete control over the entire authentication and certification management process. OnSite also gives you the option to host and customize your Web pages and to augment VeriSign's normal procedures for issuing certificates using your own unique policies and procedures. For example, you can require that your end users submit departmental billing numbers, managers' names, secret codes, or any other type of identifying information that you feel is necessary before issuing a certificate. In addition, OnSite automatically maintains a full audit log of all actions taken by end users and administrators in the issuance and management of certificates.
- **Consistency.** OnSite allows organizations to issue and manage server certificates across a large organization in a consistent

manner by providing a single administrative interface for all certificates—Secure Server IDs, as well as certificates for use with the S/MIME protocol for securing electronic mail and the IPSec protocol for securing the routers used in VPNs.

- **Ease.** OnSite is easy to set up. All you need to get started with OnSite is a PC with an Internet connection and a smart card and smart card reader provided by VeriSign. While OnSite allows you to control who gets certificates, VeriSign performs the actual issuance and management of those certificates, allowing you to leverage the technology, infrastructure, and security practices of VeriSign's secure certificate issuing facility. Furthermore, VeriSign's certificates are compatible with hundreds of applications, including all major browsers, more than 50 Web servers, and dozens of applications for form signing, secure e-mail, and other applications.
- **Cost Savings.** VeriSign OnSite's back-end systems are operated by VeriSign in our secure Operations center. Organizations can leverage this existing security infrastructure, rather than having to build one from scratch. You can take advantage of the sophisticated facilities, security, and practices created by VeriSign to support all VeriSign services. Complete offsite backup and disaster recovery is also included as part of the service. Providing a similar level of support for an in-house solution would be prohibitively expensive. Indeed, a recent study by the Aberdeen Group found that OnSite currently provides users with the lowest cost of ownership compared with its competitors due to lower startup and on-going operational costs .
- **Faster Deployment.** By using VeriSign's existing security infrastructure, rather than building a new one of your own, your organization can deploy your PKI solution more quickly. In some cases, OnSite has been deployed by organizations within 1 week.

Figure 10: High Level Result from Aberdeen cost of ownership study



Getting Started

When deploying Security for your organization, VeriSign recommends you proceed in the following stages:

1. Phase One: Assess Your Business Needs and Security Risks:

VeriSign recommends that you start out any "Security Assessment" by thinking critically about the business needs of your Intranet and Extranet. Understand the nature of the communications that are needed, and the security goals (content integrity, non-repudiation, etc.) that your communications goals imply. VeriSign then recommends getting an objective assessment of the security gaps in your existing infrastructure.

2. Phase Two: Make a long-term Plan for Deploying PKI:

Many organizations start embracing certificate technology without considering the long-term needs for deploying robust technology, infrastructure, and practices. Many of the companies with whom VeriSign works initially tried to deploy stand-alone "software-only" solutions, but quickly came to realize that long-term support, scalability, and total cost of ownership factors lend themselves more readily to VeriSign's OnSite solutions than to the "software-only" solutions.

3. Phase Three: Start by Securing your Servers:

Most organizations face a critical security issue with communications between their

servers and their internal and external users. One single technology solution—deploying SSL on your servers using Server IDs—provides an easy and effective first step to dramatically improving security throughout your system. This step will be discussed in detail in the following section of this guide.

4. Phase Four: Continue by deploying Client ID and VPN solutions:

These solutions take somewhat more effort to deploy than Secure Server IDs and SSL. However, these steps are necessary to achieve the goals of authenticating users on your network and to ensure non-repudiation of transactions or communications. With the OnSite solution, your organization can use the same interface and infrastructure to issue Server IDs for SSL, Client IDs for SSL, S/MIME, and other applications; and IPSEC IDs for router, firewalls, and other parts of your Virtual Private Network.

Deploying SSL across your Intranet and Extranet Servers

Digital certificates allow Intranet and Extranet servers to implement the Secure Sockets Layer (SSL) protocol, the standard technology for secure Web-based communications. SSL support is built into virtually all web server software. To enable this server security, though, you must install a digital certificate on your Web server

Figure 11: A Sample Secure Server ID

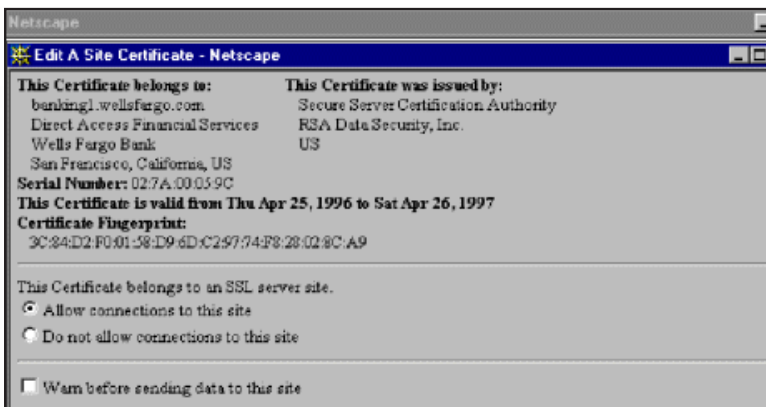
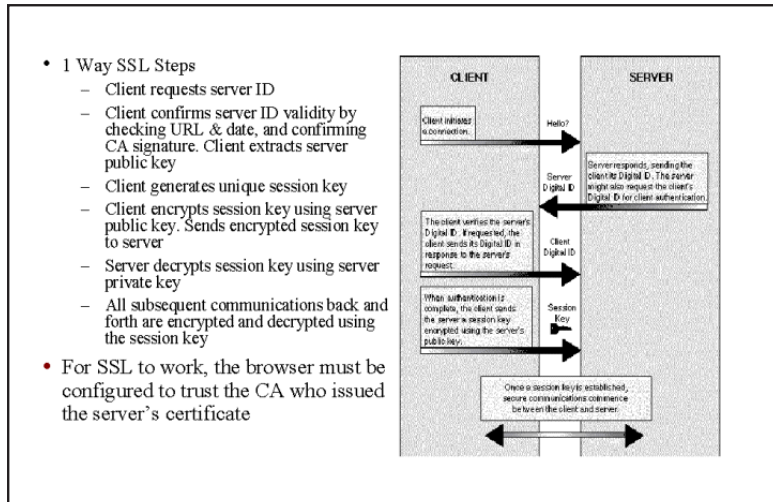


Figure 11. shows a typical digital certificate for a server. As you will note, certificates are issued to a particular web address (in this example: banking1.wellsfargo.com) run under the auspices of a particular, legally incorporated organization (in this example: Wells Fargo Bank of San Francisco, CA). The certificate contains a serial number, and expiration date, various cryptographic extensions and, of course, the public key for the web server. The certificate is then signed with the private key of the CA who issued the Certificate. (Note: Most Secure Server IDs are signed with the private key of VeriSign's, parent company, RSA Data Security, Inc.)

Together with SSL, Digital certificates secure Intranet communications through:

- Authentication. When a Server uses an SSL ID, all browsers know that they are dealing with a legitimate source. SSL also supports 2-way authentication through the use of both server and client IDs. By exchanging digital certificates, clients and servers can verify each other so that each knows exactly who is on the other end of the transaction.
- Message privacy. All traffic between the server and browser is encrypted using a unique "session key." Each session key is only used with one customer during one connection, and that key is itself encrypted with the server's public key. These layers of privacy protection guarantee that information cannot be intercepted or viewed by unauthorized parties. (Note: Encryption is provided in both directions even if only the server has a Digital ID.)
- Message integrity. The contents of all communications between the server and the browser are protected from being altered en route. All those involved in the communication know that what they're seeing is exactly what was sent from the other side.

Figure 12 shows the technical detail of what happens during an SSL session.



VeriSign Solutions for Implementing SSL

VeriSign offers a range of solutions that meet the needs of organizations wishing to secure their Intranet and Extranet applications.

Retail Certificates

Organizations requiring certificates for just a handful of servers can obtain their certificates directly from VeriSign. VeriSign offers a full set of lifecycle services for these Secure Server ID customers.

- A search function helps you determine whether a Server ID is Valid, Expired, or Revoked.
- A Renew function lets you renew a server ID that is expiring or which has already expired.
- A revoke option lets you revoke a server ID in case of any suspected compromise such as: lost or stolen private keys, corrupted key pairs, change in site ownership, or suspected fraud.
- Replace allows you to replace your existing Server ID with a new one if your Server ID becomes corrupted or if you must revoke your original ID.

As of September 1998, VeriSign has issued more than 75,000 Server IDs had been issued, to organizations across the retail, health care, education, automobile, government, and manufacturing industries. 95 of the Fortune 100 companies and all of the 20 leading e-commerce sites on the web use a VeriSign Secure Server ID to secure communications and transactions. You can secure your servers one-by-one by obtaining Secure Server IDs for them from the VeriSign website (www.verisign.com/server)

OnSite

Organizations that wish to secure 10s or 100s of secure Intranet or Extranet servers across multiple departments or geographic regions will want to consider VeriSign's Server OnSite. OnSite for Secure server IDs provides organizations with an easy way to manage the issuance, renewal, revocation, and usage of Server IDs. Using the OnSite model discussed above, organizations can request, approve, and install their certificates in minutes, providing the utmost in flexibility. Furthermore, because Server OnSite allows organizations to order multiple Server IDs for multiple servers, you can avoid multiple

Purchase Orders and expiration dates. (For more information, please visit www.verisign.com/serveronsite).

Next Steps:

Using Client IDs and VPN IDs

Since SSL does not require that the client have a certificate, some organizations initially limit access to servers using passwords. However, many organizations find that assigning Digital IDs to end users provides a much better long-term solution. Your organization can centrally administer the issuance, revocation and renewal of Digital IDs. Unlike passwords, you can use Digital IDs to enable document signing, secure e-mail, and other useful applications. In addition, you can easily augment the web servers that have been configured for SSL using Server IDs to require Client IDs for end-user authentication.

Over the next year, organizations deploying Extranets may also wish to consider the use of VeriSign OnSite to deploy that enable the IPSEC protocol within Virtual Private Networks (VPN's). IPSEC enables secured, authenticated communication between routers and firewalls.

Conclusion

As your organizations moves to Intranet and Extranet solutions, you will need to be careful to ensure that your organization implements a robust security solution. Industry standards solutions based on Public Key Infrastructure can provide a framework for ensuring that the goals of privacy, authentication, content integrity, non-repudiation, and ease of use. To implement a proper PKI requires, however, that your Certificate Authority function is implemented with the highest quality technology, infrastructure, and practices.

VeriSign PKI solutions have allowed hundreds of organizations across multiple industries to quickly and effectively deploy PKI solutions. In particular, VeriSign's OnSite solution allows your organization to gain the benefits of a full-scale PKI at a fraction of the normal cost and investment, by leveraging VeriSign's existing technology, infrastructure, and practices.

As a first step, VeriSign recommends securing all of the servers within your Intranet and Extranet with Server IDs and the SSL protocol. This can be done quickly and efficiently using VeriSign's OnSite for Server ID product. This product provides organizations with large numbers of Intranet and Extranet servers the utmost control over the issuance

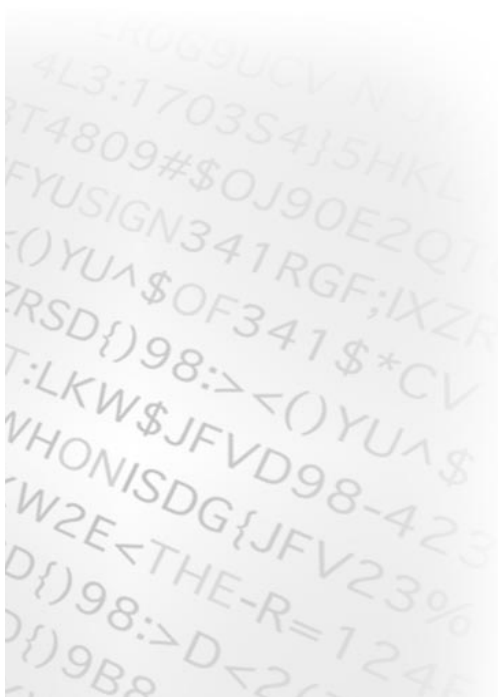
and management of these servers in a way that is easy to use, rapid to deploy, and relatively inexpensive to operate.

To learn more about VeriSign's OnSite for Server ID solutions, you may obtain trial certificates, white papers, data sheets, and pricing information at www.verisign.com/onsite/server

To speak to a VeriSign account representative, please call 650-429-3522

For more information about VeriSign's OnSite offerings for Client IDs and VPN's, visit www.verisign.com/onsite

Finally, to schedule an in-depth security assessment for your company, please visit VeriSign's newest subsidiary, SecureIT, at www.secureit.com. This group of 40 professional security consultant can help you organization develop its long range security plans.



Case Studies

VeriSign OnSite Secures

Pyxis Automated Medication Dispensing System

More than 10 years ago, San Diego-based Pyxis Corporation pioneered a new product category in healthcare—automated medication dispensing—which enables pharmacies and hospitals to streamline the process of distributing medications and medical supplies. One of Pyxis' products is the MEDSTATION System 2000 Rx System, which Pyxis operates on a turnkey basis for nearly 2,500 customers. Pharmacists stock the MEDSTATION with the medications required by patients in a particular area of the hospital. By logging onto the MEDSTATION with a secure password, nurses assigned to that area can access a patient file detailing the medications and dosages that patient is to receive. The MEDSTATION then physically dispenses the medication and tracks the medications the patient has received for billing purposes.

Recently, Pyxis added a new module to the system that keeps track of medications for patients who come into the hospital unconscious and unidentified—once the patient is identified, his or her record is sent to the main MEDSTATION database. This new module, which resides on a server called Procar, can be accessed from desktop workstations

equipped with a browser. Communications between the workstations and Procar are secured with digital certificates using VeriSign's Onsite. "Since we knew that for some time, our application would be used only on the hospital's on-premises Intranet, we were tempted to build it to run in that highly secure environment. But then we thought, 'wouldn't it be nice for pharmacists to eventually be able to dial in and access the system from home.' So we built in the maximum security we would get for a Web enabled application," says James H. King, Pyxis' Director of Interface Development.

Pyxis selected VeriSign Onsite for its digital certificates says King, "Because of the volume of digital certificates we needed. We plan to deploy 500 of these systems in the next 12 to 18 months, so OnSite's volume certificate issuing features were an attractive feature, trying to acquire those one by one takes too long. We also got a big volume discount."

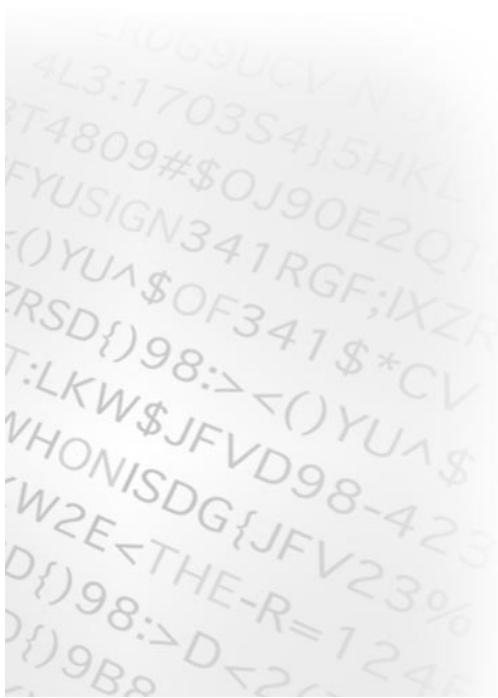
In the future, Pyxis has even bigger plans for Onsite. Pyxis plans to use the Procar server as a gateway between the hospitals main patient database and a new data warehouse that will provide online analytical processing. The new system will allow hospitals to access that data warehouse through a Web enabled application. And VeriSign Onsite's digital certificate's will be there to secure it.

Deere & Company Secures Intranet with VeriSign OnSite

Deere & Company of Moline, Illinois is the world's leading provider of agricultural equipment and a major producer of equipment for a wide range of industries. The company also provides financial services such as credit, insurance, and managed health care plans. With 35,500 employees and offices in 160 countries, Deere & Company's total sales and revenues were \$12.79 billion in 1997.

Deere & Company uses OnSite to secure its Intranet systems because, says Farhan Ahmed Siddiq, a consultant at Deere, "For information about salary and benefits that we would not want employees to get unauthorized access to, personal IDs and passwords do not provide enough security. A network administrator could put a network sniffer on the wire and start sniffing to get that information. SSL provides encryption to prevent a sniffer from deciphering confidential information."

The company uses VeriSign OnSite for Secure Server IDs to issue and manage the Digital certificates that enable SSL on its Intranet systems because VeriSign offers the most complete solution on the market. "We wanted to be able to issue certificates quickly and have more control over them," explains Siddiq. "Previously, requesting certificates introduced a lag time of about a week, as POs were cut, and so on. It was a hassle. Using VeriSign Onsite lets us manage the certificates ourselves. And since we request a couple of certificates every week, it made sense to purchase them in bulk."





The Sign of Trust on the NetSM

1350 Charleston Road • Mountain View, CA 94043

phone 650.961.7500 • fax 650.961.7300

www.verisign.com

VeriSign is a registered trademark exclusively licensed to VeriSign, Inc. All other trademarks are properties of their respective owners. © 1999 VeriSign, Inc. All rights reserved. 7/99