Entrust® Technologies

Guide to the Business Impact of PKIs

Version 2.0

Date: September 1998
© Entrust Technologies Limited, 1998. All rights reserved.

No part of this document may be reproduced, stored in a retrieval system or database, or transmitted, in any form or by any means, electronically, mechanically, photocopying, recording, or otherwise, without the prior written permission of Entrust Technologies Limited.

Entrust is a registered trademark of Entrust Technologies Limited. All other product and company names may be trademarks of their respective owners.

This booklet is intended to provide general information about the use of PKI in business today. It is not intended to provide specifications advice for the design of a PKI system.

Table of Contents

Overview

Organizations are increasingly becoming dependent on Internet-based communications. The Internet is a low cost networking solution providing a standard medium for communication. An Enterprise's use of applications such as e-mail, Web servers, remote access, and other e-commerce applications are prone to a variety of computer attacks. A recent survey by the FBI and CSI (Computer Security Institute) polled over 500 companies and found that over 64% of organizations suffered an attack in the last 12 months[1]. These attacks were due to saboteurs, viruses, laptop thefts, financial fraud, and stolen proprietary information. The FBI also reported that US industries loss due to theft of intellectual property stored on computers totaled $63 billion in 1997. As people continue to rely on the Internet, intranets, and extranets for mission-critical communication, the need for easy-to-use yet sophisticated security tools is vital.

[1] Computor Security Issues & Trends; vol. IV no.1, winter 1998.

Introduction

The purpose of this guide is to explain the business need for using a public-key infrastructure (PKI) and the benefits a PKI can provide in improving the operational effectiveness of your organization while providing an attractive return on your security investment.

A public-key infrastructure is a critical solution to ensure secure electronic business communication incorporating digital signatures and encryption technology. A PKI transparently manages keys and certificates enabling an organization to create and use a trustworthy networking environment. A trusted network allows organizations to take advantage of the following benefits:

- confidential communication - ensures only intended recipients are able to read files. Files could not be intercepted.
- authentication - validates the creation of a file by the sender. Recipients need to know the sender created the file.
- non-repudiation - prevents the sender from denying involvement in the creation of a file.
- integrity - guarantees the file was not altered during transmission.

The benefits of digital signatures and security of information is a mandatory option to enable e-commerce applications. With a PKI, organizations can take advantage of these benefits to gain competitive advantages by improving products and services. According to a 1998 CSI/Zona Information Security Market survey, 58% of respondents use encryption in a variety of ways, while 43% plan to buy encryption products this year.

This paper will elaborate on the elements that allow businesses to take advantage of a public-key infrastructure. In particular, this paper concentrates on the following items:

- the concept of a public-key infrastructure
- the requirements for implementing an effective, comprehensive public-key infrastructure.

What Can a Business do with a PKI

A PKI can provide security solutions for a range of business applications. Solutions are available for Web security, e-mail, remote access, e-forms, or other e-commerce applications. Security features within applications are transparent to end users and easy-to-use.

Administration of all these business applications is simple with a PKI. A PKI enables you to administer security only once for all the business applications you intend to use. The end user will only have to remember one password for all applications, leading to savings in helpdesk support costs. You will also be able to manage and administer all the security of the applications with one infrastructure — the PKI.

There is a wide range of applications that can leverage the power of a PKI on your existing network. Here are some examples:

Secure E-mail Applications. Expanding global business has created the need for cost-effective and confidential methods of communication. Previous attempts at secure communications have included confidential faxes, diskettes via courier and closed-door meetings. These methods are not convenient nor sufficient to meet the pressures of time and budget constraints. Secure e-mail (using your existing e-mail messaging system) alleviates the requirements to use inadequate communications methods and enables confidential information to be shared between enterprises, customers, employees and partners over private and public networks.

Desktop Security. You can often find volumes of confidential data — that has been communicated securely — stored in locked cabinets and storage rooms. We recognize the need to lock our filing cabinets and desks, but we often leave our desktop or laptop computer data unsecured and unprotected. Protection of the information on the desktop encompasses a wide variety of activities including automatic encryption/decryption of files and folders, restricting sensitive information from unauthorized individuals, secure deletion of sensitive information (temporary files and

Windows SWAP files), controlling access to your computer at start-up (i.e. boot-up protection) and during temporary absence from your desk (i.e. screensaver locks).

Web-based Security. As the World Wide Web (WWW) grows in popularity, more and more organizations and individuals see the Web as an efficient, inexpensive means of distributing information, products and services. While the WWW is an attractive distribution channel for this new generation of on-line services, those wishing to take advantage of the Web's presence must ensure security concerns are addressed. Organizations that wish to use the Internet to share information with employees, partners and clients must implement security that prevents electronic fraud such as data tampering, eavesdropping and masquerading.

E-Commerce. Electronic commerce is used widely in organizations around the world. Everything from e-mail, e-forms, electronic data interchange (EDI) applications, and financial transactions over the Internet, is oftentimes referred to as electronic commerce (EC). To secure your EC data, organizations must implement security that works seamlessly across applications and platforms such that it is transparent to users and easy for organizations to manage. Security that provides privacy to ensure the confidentiality of data, access control to authorize data access, integrity to assure data originality, authentication to provide proof of identity, and non-repudiation to prevent denial of transactions.

Access Control. Access control ensures that only those who are authorized to view data can access that data. An aspect of the PKI is to function as an access control device by identifying the user to all those that recognize its validity.

Virtual Private Networks. Secure virtual private networks (VPNs) enable business users to exchange information over internal and public networks with complete privacy, integrity and user authentication. A secure Virtual Private Network (VPN) is a solution for Internet remote access, branch office internetworking (intranets), and communications with business partners (extranets).

Business Case Studies

The benefits of implementing a comprehensive PKI solution have yielded tangible returns for many organizations. The applications range from extending personalized banking services to reducing the turnaround time of application forms. Organizations are using PKI technology for a secure and cost-effective means of communicating with customers. Organizations are also realizing that the technology can provide a quick return on investment.

It is often thought that security is expensive, with very little visible payback. However, according to Forrester Research a PKI could provide annual savings of $4.4 million based on a 20,000 user population. The cost of setting up can be quickly recovered from a dramatic reduction of helpdesk costs (up to 40%). This reduction is attributed to a decreased request for password assistance. Focusing on particular business applications and the potential cost savings will enable you to establish a return on the PKI investment[2].

End-to-End Online Banking Solution - Scotiabank®

The Bank of Nova Scotia, one of Canada's Big Six banks, wanted to provide a unique end-to-end on-line banking security solution which enables customers to pay bills, view account balances, and move between banking and brokerage services. The Entrust® PKI solution gives customers convenient, personalized services via a secure, easy-to-use solution that is more cost effective than other security technologies.

"We looked at the competition and what they were doing with traditional PC banking with software diskettes and upgrades. But we saw that there were low costs and ease of use with the Internet. There was a void in the market in Internet security, and Entrust was the first to come up to bat. We expect to have 100,000 users within a year". Albert Wahbe, executive vice president, Scotiabank.

[2] The Forrester Report: Network Strategies; February 1998.

Transmission of Confidential Customer Information - J.P. Morgan
J.P. Morgan used their Entrust PKI to better communicate sensitive financial statements to customers. Prior to the use of a PKI, J.P. Morgan used a combination of custom hardware encryptors via private lines and regular dial access. The links were point-to-point and as the links went down the transaction would be discontinued. J.P. Morgan was able to eliminate the hardware encryptor yielding a saving of $1 million. This does not include the maintenance costs of the hardware and the dial-up access costs.

J.P. Morgan has also expanded their Entrust PKI to its commercial mortgage underwriting business. Previously, documents were hand-delivered but now they can securely e-mail the documents.

"That will cut the time it takes to negotiate the terms of a transaction from three weeks to no more than three days". Charles Blauner, vice-president at J.P. Morgan. [source; Information Week, March 23, 1998]

Posting and Bidding of Surplus Electricity - U.S. Electric Utilities
The Federal Energy Regulatory Commission (FERC) mandated that all electric utilities post surplus electrical transmission capacity on the Internet so the bidding and the exchange of information is public.

The World Wide Web (WWW) was chosen as the means of communication and doing business because it was accessible and easy to use. However, the lack of security that is inherent in an unmanaged and unaffiliated network like the Web was a serious concern.

To resolve this problem a task force representing over 200 electric utilities and utility cooperatives (Joint Transmission Services Information Network - JTSIN), responded to the FERC mandate by hiring companies to create and maintain the network and its applications. Using an Entrust-Readyproduct (TradeVPI by TradeWave) a solution was designed that provided the needed security. "There isn't another solution that offers the level of security, information access, and performance that the Entrust/TradeWave vendors are providing today," said Jeff Geltz, of All Energy, Inc., former Chairman of the JTSIN Management Committee.

The business benefits for implementing a PKI on your network are numerous. These benefits range from improved customer service and improved business processes to reduced costs. These benefits can be realized by focusing a PKI solution to particular business applications. Many organizations have benefited from an Entrust PKI providing tangible returns on their PKI investment. Realize the potential of your network — use an Entrust PKI!

What is a PKI?

What is a public-key infrastructure?

The comprehensive system required to provide public-key encryption and digital signature services is known as a public-key infrastructure (PKI).

The purpose of a public-key infrastructure is to manage keys and certificates. By managing keys and certificates through a PKI, an organization establishes and maintains a trustworthy networking environment. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

What is an effective public-key infrastructure?

There are a number of requirements that businesses have with respect to implementing effective public-key infrastructures. First and foremost, if users cannot take advantage of encryption and digital signatures in applications, a PKI is not valuable. Consequently, the most important constraint on a PKI is transparency. The term transparency means that users do not have to understand how the PKI manages keys and certificates to take advantage of encryption and digital signature services. An effective PKI is transparent.

In addition to user transparency, a business must implement the following items in a PKI to provide the required key and certificate management services:

- public key certificates
- a certificate repository
- certificate revocation
- key backup and recovery
- support for non-repudiation of digital signatures
- automatic update of key pairs and certificates
- management of key histories
- support for cross-certification
- client-side software interacting with all of the above in a secure, consistent, and trustworthy manner.

Note: In this paper, the term client-side refers to application clients and application servers. PKI requirements are the same for both application clients and servers, and both are "clients" of the infrastructure services described in this paper.

The remaining sections of this paper define each of the requirements listed above. All of these requirements must be met for an organization implementing a PKI to establish and maintain a trustworthy environment. All of these requirements must also be met to have an automatic, transparent, and usable PKI.

Certificates and Certification Authorities

For public-key cryptography to be valuable, users must be assured that the other parties with whom they communicate are "safe"—that is, their identities and keys are valid and trustworthy. To provide this assurance, all users of a PKI must have a registered identity. These identities are stored in a digital format known as a public key certificate. Certification Authorities (CAs) represent the people, processes, and tools to create digital certificates that securely bind the names of users to their public keys.

In creating certificates, CAs act as agents of trust in a PKI. As long as users trust a CA and its business policies for issuing and managing certificates, they can trust certificates issued by the CA. This is known as third-party trust. For more information on third-party trust, refer to the Entrust Technologies White Paper titled "The Concept of Trust in Network Security". This White Paper is available on the Entrust Technologies Web site at *http://www.entrust.com/library.htm.*

CAs create certificates for users by digitally signing a set of data that includes the following information (and additional items):

- the user's name in the format of a distinguished name (DN). The DN specifies the user's name and any additional attributes required to uniquely identify the user (for example, the DN could contain the user's employee number).
- a public key of the user. The public key is required so that others can encrypt for the user or verify the user's digital signature.
- the validity period (or lifetime) of the certificate (a start date and an end date).
- the specific operations for which the public key is to be used (whether for encrypting data, verifying digital signatures, or both).

The CA's signature on a certificate ensures that any tampering with the contents of the certificate can be easily detected. (The CA's signature on a certificate is like a tamper-detection seal on a bottle of pills—any tampering with the contents of a certificate is easily detected) As long as the CA's signature on a certificate can be verified, the certificate has integrity. Since the integrity of a certificate can be determined by verifying the CA's signature, certificates are inherently secure and can be distributed in a completely public manner (for example, through publicly-accessible directory systems).

Users retrieving a public key from a certificate can be assured that the public key is valid. That is, users can trust that the certificate and its associated public key belong to the entity specified by the distinguished name. Users also trust that the public key is still within its defined validity period. In addition, users are assured that the public key may be used safely in the manner for which it was certified by the CA.

Key backup and recovery

A business must be able to retrieve encrypted data when users lose their decryption keys. This means that the enterprise to which the user belongs requires a system for backing up and recovering the decryption keys. There are two reasons why key backup and recovery are so important to businesses.

The first reasons is that users forget passwords. It is potentially catastrophic for a business to lose data when users forget the passwords required to access their decryption keys. Valuable information would be lost forever if there was no ability to securely recover those keys. Furthermore, unless users know they can always recover their encrypted data (even if they forget their passwords), some users will not encrypt their most valuable and sensitive information for fear of losing it—even though that information needs to be protected the most.

The second reason is that users may lose, break, or corrupt the devices in which their decryption keys are stored. For instance, if a user's decryption keys are stored on a magnetic card, the magnetic field on the card can become corrupted. Again, permanent loss of those decryption keys can be disastrous. Users are prevented from recovering encrypted data unless their decryption keys are backed up.

The difference between key backup and key escrow

This paper's discussion of commercial requirements for key backup and recovery can be completely separated from law enforcement requirements for "key escrow"—a topic widely discussed in the media. Key escrow means that a third party (such as a federal agent) can obtain the decryption keys required to access encrypted information. The purpose of key escrow is to help with law enforcement, and key escrow is a heavily-debated topic because of the fine lines between issues of public interest (such as national security) and individual freedom and privacy. Key backup and recovery requirements, as discussed above, focus on fundamental commercial needs that exist regardless of law enforcement requirements.

Which keys require backup?

Earlier, this paper introduced the notion of different functions for keys pairs. One key pair is used for encrypting and decrypting data. This is called the "encryption key pair". Another key pair is used for digitally signing data and verifying signatures. This is called the "signing key pair". Note that there is no discussion above regarding backup and recovery of signing key pairs. The only keys requiring backup are users' decryption keys. As long as a trusted agent (for example, the CA) securely backs up users' decryption keys, security is not compromised and the user's data can always be recovered. However, signing keys have different requirements from decryption keys. In fact, as the next section describes, backing up signing keys destroys a basic requirement of a PKI.

Support for non-repudiation

Repudiation occurs when an individual denies involvement in a transaction. (For instance, when someone claims a credit card is stolen, this means that he or she is repudiating liability for transactions that occur with that card anytime after reporting the theft). Non-repudiation means that an individual cannot successfully deny involvement in a transaction. In the paper-world, individuals' signatures legally bind them to their transactions (for example, credit card charges, business contracts, …). The signature prevents repudiation of those transactions. In the electronic world, the replacement for the pen-based signature is a digital signature. All types of electronic commerce require digital signatures because electronic commerce makes traditional pen-based signatures obsolete.

The signing private key

The most basic requirement for non-repudiation is that the key used to create digital signatures—the signing key—be generated and securely stored in a manner under the sole control of the user at all times. It is not acceptable to back up the signing key.

Unlike encryption key pairs, there is no technical or business requirement to backup or restore previous signing key pairs when users forget their passwords or lose, break, or corrupt their signing keys. In such cases, it is acceptable for users to generate new signing key pairs and continue using them from that time forward.

The need for two key pairs

It is difficult to simultaneously support key backup and recovery and non-repudiation. To support key backup and recovery (as discussed in a previous section), the decryption keys must be backed up securely. To support non-repudiation, the keys used for digital signature cannot be backed up and must be under the sole control of the user at all times.

To meet these requirements, a PKI must support two key pairs for each user. At any point in time, a user must have one current key pair for encryption and decryption, and a second key pair for digital signature and signature verification.

Over time, users will have numerous key pairs that must be managed appropriately, as discussed in the following section.

Key update and management of key histories

Cryptographic key pairs should not be used forever. They must be updated over time. As a result, every organization needs to consider two important issues:

- updating users' key pairs, and
- maintaining, where appropriate, the history of previous key pairs.

Updating users' key pairs

The process of updating keys pairs should be transparent to users. This transparency means users do not have to understand that key update needs to take place and they will never experience a "denial of service" because their keys are no longer valid. To ensure transparency and prevent denial of service, users' key pairs must be automatically updated before they expire.

Maintaining histories of key pairs

When encryption key pairs are updated, the history of previous decryption keys must be maintained. This "key history" ensures that users can access any of their prior decryption keys to decrypt data. (When data is encrypted with a user's encryption key, only the corresponding decryption key—the paired key—can be used for decrypting). To ensure transparency, the client-side software must automatically manage users' histories of decryption keys.

The key history must also be securely managed by the key backup and recovery system. This ensures that encrypted data can be recovered securely, regardless of what encryption public key was used to originally encrypt the data (and, by extension, regardless of when the data was encrypted).

When a signing key pair is updated, the previous signing key be securely destroyed. This destruction prevents any other person from gaining access to the signing key and is acceptable because there is no need to retain previous signing keys.

Certificate repositories and certificate distribution

As mentioned earlier in this paper, the CA acts as a trusted third-party issuing certificates to users. Businesses also must distribute those certificates so they can be used by applications. Certificate repositories store certificates so that applications can retrieve them on behalf of users. The term repository refers to a network service that allows for distribution of certificates.

Over the past few years, the consensus in the information technology industry is that the best technology for certificate repositories is provided by directory systems that are LDAP (Lightweight Directory Access Protocol)-compliant. LDAP defines the standard protocol to access directory systems.

Several factors drive this consensus position:

- storing certificates in directories and having applications retrieve certificates on behalf of users provides the transparency required for use in most businesses
- many directory technologies supporting LDAP can be scaled to:
- support a very large number of entries
- respond efficiently to search requests due to their information storage and retrieval methods, and
- be distributed throughout the network to meet the requirements of even the most highly-distributed organizations

In addition, the directories that support certificate distribution can store other organizational information. As discussed in the next section, the PKI can also use the directory to distribute certificate revocation information.

Certificate revocation

In addition to verifying the CA's signature on a certificate (as discussed in the section titled Certificates and Certification Authorities), the application software must also be sure that the certificate is still trustworthy at the time of use. Certificates that are no longer trustworthy must be revoked by the CA.

There are numerous reasons why a certificate may need to be revoked prior to the end of its validity period. For instance, the private key (that is, either the signing key or the decryption key) corresponding to the public key in the certificate may be compromised. Alternatively, an organization's security policy may dictate that the certificates of employees leaving the organization must be revoked. In these situations, users in the system must be informed that continued use of the certificate is no longer considered secure.

The revocation status of a certificate must be checked prior to each use. As a result, a PKI must incorporate a scalable certificate revocation system. The CA must be able to securely publish information regarding the status of each certificate in the system. Application software, on behalf of users, must then verify the revocation information prior to each use of a certificate. The combination of publishing and consistently using certificate revocation information constitutes a complete revocation system.

The most popular means for distributing certificate revocation information is for the CA to create secure certificate revocation lists (CRLs) and publish these CRLs to a directory system. CRLs specify the unique serial numbers of all revoked certificates. Prior to using a certificate, the client-side application must check the appropriate CRL to determine if the certificate is still trustworthy. Client-side applications must check for revoked certificates consistently and transparently on behalf of users.

Cross-certification

Cross-certification extends third-party trust relationships between Certification Authority domains. For example, two trading partners, each with their own CA, may want to validate certificates issued by the other partner's CA. Alternatively, a large, distributed organization may require multiple CAs in various geographic regions. Cross-certification allows different CA domains to establish and maintain trustworthy electronic relationships.

The term cross-certification refers to two operations. The first operation, which is generally executed infrequently, is the establishment of a trust relationship between two CAs. In the case of bilateral cross-certification, two CAs securely exchange their verification keys. These are the keys used to verify the CAs' signatures on certificates. To complete the operation, each CA signs the other CA's verification key in a certificate referred to as a "cross-certificate".

The second operation is done by the client-side software. The operation, which is executed frequently, involves verifying the trustworthiness of a user certificate signed by a cross-certified CA. The operation is often referred to as "walking a chain of trust". The "chain" refers to a list of cross-certificate validations that are "walked" (or traced) from the CA key of the verifying user to the CA key required to validate the other user's certificate.

When walking a chain of cross-certificates, each cross-certificate be checked to ensure that it is still trusted. User certificates must be able to be revoked; so must cross-certificates. This requirement is frequently overlooked in discussions regarding cross-certification.

For more information on third-party trust and cross-certification, refer to the Entrust Technologies White Paper titled "The Concept of Trust in Network Security". This White Paper is available on the Entrust Technologies Web site at *http://www.entrust.com/library.htm.*

Client-side software

When discussing requirements for PKIs, businesses often neglect the requirement for client-side software. (For instance, many people only focus on the CA component when discussing PKIs). Ultimately, however, the value of a PKI is tied to the ability of users to use encryption and digital signatures. For this reason, the PKI must include client-side software that operates consistently and transparently across applications on the desktop (for example, e-mail, Web browsing, e-forms, file/folder encryption, ...). A consistent, easy-to-use PKI implementation within client-side software lowers PKI operating costs.

In addition, client-side software must be technologically enabled to support all of the elements of a PKI discussed earlier in this paper. The following list summarizes the requirements client-side software must meet to ensure that users in a business receive a usable, transparent (and thus, acceptable) PKI.

- **public key certificates**
  To provide third-party trust, all PKI-enabled applications must use certificates in a consistent, trustworthy manner. The client-side software must validate the CA's signature on certificates and ensure that the certificates are within their validity periods.

- **key backup and recovery**
  To ensure users are protected against loss of data, the PKI must support a system for backup and recovery of decryption keys. With respect to administrative costs, it is unacceptable for each application to provide its own key backup and recovery. Instead, all PKI-enabled client applications should interact with a single key backup and recovery system. The interactions between the client-side software and the key backup and recovery system must be secure, and the interaction method must be consistent across all PKI-enabled applications.

- **support for non-repudiation**
  To provide basic support for non-repudiation, the client-side software must generate the key pairs used for digital signature. In addition, the client-side software must ensure that the signing keys are never backed up and remain under the users' control at all times. This type of support must be consistent across all PKI-enabled applications.

- **automatic update of key pairs**
  To ensure transparency, client-side applications must automatically initiate updating of users' key pairs. This activity must be done in accordance with the security policies of the organization. It is unacceptable for users to have to know that their key pairs require updating. To meet this requirement across all PKI-enabled applications, the client-side software must update key pairs transparently and consistently.

- **management of key histories**
  To ensure that users can easily access all data encrypted for them (regardless of when it was encrypted), PKI-enabled applications must have access to users' key histories. The client-side software must be able to securely recover users' key histories.

- **a scalable certificate repository**
  To minimize the costs of distributing certificates, all PKI-enabled applications must use a common, scalable certificate repository. Transparent support for certificate retrieval from a common repository improves usability. It is costly and cumbersome for applications to require different certificate repositories.

- **certificate revocation**
  PKI-enabled applications must interact with a common, scalable certificate revocation system. Because certificate revocation is central to trust management, client-side software must interact with the certificate revocation system in a consistent manner across all applications.

- **support for cross-certification**
  To ensure consistent application of trust management policies, all PKI-enabled applications must use a common cross-certification model. As mentioned in the section titled "Cross-certification," cross-certification allows the PKI to determine the trustworthiness of a certificate issued by a foreign Certification Authority. For example, the client-side software must check to ensure that none of the cross-certificates in a "chain of trust" is revoked.

Each of the issues discussed above relates to interactions between the client-side software and the infrastructure elements of a PKI. There are additional requirements of the client-side software that are independent of the infrastructure elements. For example, the client-side software should allow users to encrypt and decrypt information even when they are disconnected from the infrastructure elements of the PKI. To maximize usability and minimize cost, the client-side software should support multiple types of key storage devices (for example, smart cards, PC cards, secure files, …). Users should be able to use a single key storage device across all PKI-enabled applications.

Total Cost of Ownership of a PKI

An investment in any technology for enterprise-wide use would not be prudent without a thorough understanding of all the associated costs. Any technology purchase requires an up-front investment and a certain amount of ongoing support. The technology investment decision is typically based on the ability of a product to provide operational efficiencies and cost savings. The same considerations apply for a PKI purchase as any other technology purchase. The total cost of the purchase needs to be understood before the investment is made.

A key factor in determining the payback and Return on Investment of a PKI investment is a full understanding of the Total Cost of Ownership (TCO). The ideal PKI solution should provide ease of use, low administrative overhead, simplicity in enforcing and auditing a security policy — and a flexible and scalable architecture. This solution allows an organization to leverage its existing network and realize tangible benefits from the adoption of a security infrastructure which effectively manages the communication and storing of confidential and proprietary information.

A recent Giga Group report[1] analyzes the total cost ramifications of a PKI on an organization. This analysis goes beyond the traditional product acquisition and maintenance costs to include the level of operator support and administrative overhead necessary for managing a PKI. The report analyzes three different product scenarios focused on three unique business applications — each with an increased level of sophistication. These scenarios are taken one step further by comparing user deployments of 5,000 and 20,000 users. The business applications assessed include:

1. **Basic Certificates for Web Authentication** - uses a digital certificate to deliver strong authentication in a pure Web browser environment.
2. **Managed Certificates for Web Authentication** - builds on the previous application but provides for encryption, automatic certificate rollover, and automatic CRL (Certificate Revocation List) checking.
3. **Managed Identities for Enterprise Applications** - implements a security system for organizations that require desktop file encryption and secure e-mail all managed and maintained using a PKI. A PKI delivering key backup and recovery and automatic certificate rollover is vital for the Enterprise.

The results show that Entrust yielded a 36-42% cost savings advantage over a CA service (i.e. VeriSign). These savings are attributed primarily to the significantly lower operating support costs incurred by the customer to maintain and administer a PKI. The Entrust/PKI ensures lower operating support costs with built-in features such as key backup and recovery, automatic update of key pairs and certificates, and the management of the key histories. These advanced capabilities lower the total cost of ownership of a PKI.

TCO/User for 20,000 Users

Business Applications	Entrust	VeriSign
Basic Certificates	$11	$17
Managed Certificates	$20	$18
Managed Identities	$79	$124

Source: Giga Information Group

"We want best of breed security where we control the trust model. We want a platform for future e-commerce. A very high standard of security went into our design. Entrust has all the bases covered for our trust model. Having VeriSign control our security and trust model doesn't meet our standards."

Global 500 Financial Service Company

1 "A Total Economic Impact Analysis of Two PKI Vendors: Entrust and VeriSign", Giga Information Group, September 1998

Summary

A comprehensive PKI must implement the following items:

- public key certificates
- a certificate repository
- certificate revocation
- key backup and recovery
- support for non-repudiation of digital signatures
- automatic update of key pairs and certificates
- management of key histories
- support for cross-certification
- client-side software interacting with all of the above in a secure, consistent, and trustworthy manner.

Only a comprehensive PKI can achieve the goal of establishing and maintaining a trustworthy networking environment, while at the same time providing an automatic and transparent system that is usable.

The business benefits of reduced costs, streamlined business processes, and improved customer service provide tangible returns on an investment in PKI. Organizations have already realized cost savings of $1-$5.4 million per year. A focus on particular business applications will ensure your PKI provides the returns you seek. Your existing network can be leveraged to provide secure e-mail, desktop security, Web-based security, e-commerce, access control, or virtual private networks. Realize the potential of your network — use an Entrust PKI.