An Introduction to Enterprise Public Key Infrastructure (PKI)

February 2001

Introduction

Due to the proliferation of networks, and the Internet in particular, enterprises large and small alike are conducting business in ways that didn't exist just five years ago. With this new way of doing business come added challenges, threats, and risks to the security of the business itself. So why are enterprises embracing this new business paradigm despite the security risks? The answer is simply that the benefits of handling both business processes and the information flows between business partners and customers using public networks appear to outweigh the risks of conducting those transactions. Enterprises are saving significant sums of money and generating new markets by using the Internet and other networking technologies.

To mitigate the security risks of conducting business in an open environment while at the same time maintaining the cost advantages of doing so, enterprises are turning their attention to an emerging segment of the security market known as Public Key Infrastructure (PKI). The purpose of PKI is to provide an environment that addresses today's business, legal, network, and security demands for trust and confidentiality in data transmission and storage. PKI accomplishes these goals for an enterprise through policy and technology components. These components determine and identify the roles, responsibilities, constraints, range of use, and services available.

This paper identifies the key concepts and issues surrounding the technologies and policies required to implement and support an enterprise PKI.

What Is Public Key Infrastructure?

Public Key Infrastructure (PKI) is an environment that consists of policies, protocols, services, and standards that support the applications of public key cryptography to mainstream business functions. PKI is not useful in and of itself, but is instead an enabler of trust that provides strong user identification, cryptographic services, and evidence for non-repudiation among entities that may not have had prior knowledge of each other. To enable trust, a PKI typically embodies a collection of one or more Certificate Authorities (CAs) acting as so-called trusted third parties, Registration Authorities (RAs), associated repositories, and governing policies used to manage the relationship between an enterprise and its users.

The Benefits of PKI

PKI provides an architecture that can centralize the management of digital identity and encryption under one umbrella. Through the use of PKI, enterprise applications supporting digital signatures and encryption can be linked to a central identification service, thereby reducing management effort and overall cost. Some organizations

today use both a secure electronic mail solution as well as a Virtual Private Network (VPN). Each of these technologies can typically maintain its own user repository for identifying organizational members. In addition, each technology is often independently operated and managed, thus significantly increasing the cost of maintenance for the organization. If these technologies were integrated with an enterprise PKI, both technologies could rely upon digital certificates centrally managed by the CA for identification and encryption services, thereby reducing complexity and expense.

An integrated enterprise PKI environment adheres to one set of security policies and practice documents, ensuring that subscribers perform legitimate and authorized data processing transactions.

Through the use of encryption and digital signatures, an enterprise PKI can enable the following important security benefits:

- *Authentication* is the process of confirming the identity of an individual or entity. PKI can provide assurance beyond simple user name and password authentication by requiring that a user or entity possess a valid digital certificate and corresponding private key to successfully authenticate. This provides a higher degree of assurance, since the user or entity must not only *have* something, the private key, they must also *know* the pass phrase associated with that private key. Without both pieces of information, authentication will fail.

- *Confidentiality* is the concept of protecting the privacy of information so that only authorized parties can access that information. PKI enables confidentiality through a combination of public key and secret key encryption. Encrypting data in such a manner provides protection for the data. It also allows for this data to be securely exchanged among entities with no prior relationship, as data encrypted with a given entity's public key can only be decrypted by the corresponding private key.

- *Integrity* provides a mechanism for ensuring that data has not been altered. PKI provides integrity through digital signatures, a mechanism for the detection of tampering. If verification of a digital signature fails, the verifier knows that the data has been altered and that it likely cannot be trusted.

- *Non-repudiation* establishes provides proof-of-participation in an action or transaction. PKI provides technical non-repudiation by establishing that an entity's private key was used to digitally sign a transaction. This digital signature can provide a stronger chain of evidence establishing the parties involved in an action, and when that action occurred.

  Note that the presence of a “valid” digital signature does not guarantee that the legitimate owner of a private key was an actual and willing participant in a

transaction. Compromise of an entity's private key, compromise of the CA, malfunctioning software, or computer virus infection can also lead to a valid digital signature without the actual authorization or knowledge of the private key's owner.

What Services Does PKI Provide?

An enterprise PKI can provide a number of services. Typically, these services include:

- *Certificate issuance and renewal* encompasses the issuing of new, and renewal of old, certificates for entities composed of applications, devices, systems, and users.

- *Certificate distribution* provides for making an entity's digital certificates available to others.

- *Certificate revocation* is the cancellation of a previously issued certificate in the event of compromise or corruption prior to the natural expiration date of the certificate. Notice of revoked certificates is provided through Certificate Revocation Lists (CRLs), the Online Certificate Status Protocol (OCSP), and similar mechanisms.

- *Certificate suspension* temporarily invalidates a certificate in cases where it should temporarily not be used, such as when the certificate owner takes a leave of absence.

- *Encryption key escrow or recovery* provides for the retrieval or recovery of encryption keys in the event that they are corrupt, expired, or lost.

- *Non-repudiation* through the use of digital signatures provides technical proof-of-participation of an entity in a transaction.

- *Time stamping* provides an official time record for all transactions, and proves that an event occurred at a specific date and time.

Figure 1 illustrates the relationship among PKI components and how they provide services to the user community.

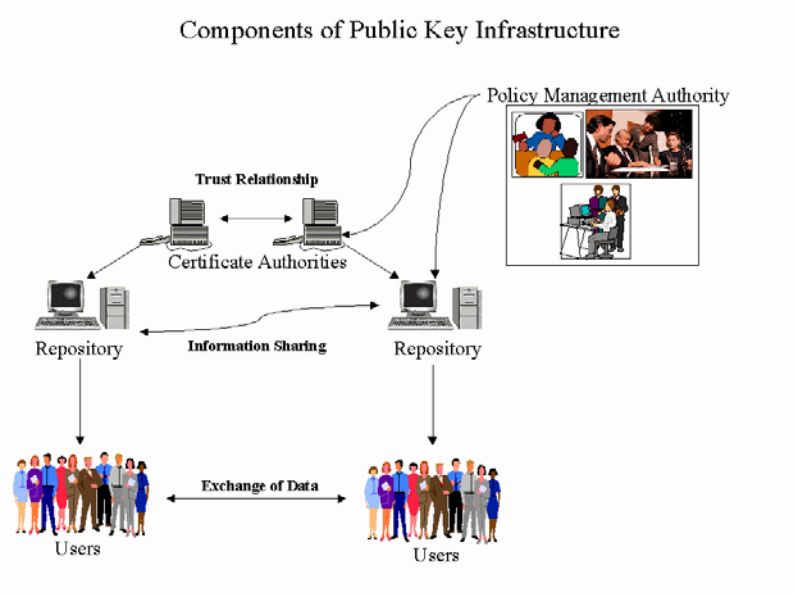

Figure 1: Components of Public Key Infrastructure

The Technology Components of a Public Key Infrastructure

Keys

A key is a sequence of symbols, used with a cryptographic algorithm, that enables encryption and decryption of data. This enables the more secure transfer or storage of data. Two types of cryptographic algorithms, public key and secret key, are used to support the cryptographic operations of a PKI.

Public key, or asymmetric, algorithms make use of two corresponding keys, one called the public key, and the other called the private key. A message encrypted with a given public key can only be decrypted using the corresponding private key. Likewise, a message encrypted with a private key can only be decrypted using the corresponding public key. It is this relationship that enables entities using public key cryptography to identify each other, communicate securely, and ensure the integrity of their communication. Public key cryptography does have a significant drawback -- it is very slow and therefore not suitable for encrypting large volumes of data.

Secret key, or symmetric, algorithms make use of only one key that is used to both encrypt and decrypt messages. Secret key cryptography is fast, making it practical for use in encrypting large volumes of data. Distributing the secret key, however, is problematic as anyone that intercepts the key can decrypt any and all messages encrypted with that key. For that matter, anyone that intercepts the key can encrypt a new message and pass that new message off as the original.

PKI combines both public key and secret key cryptography to build a system that allows for the efficient, integral, and secure transmission of data among parties that may have no prior knowledge of each other. Interestingly, this combined approach eliminates the individual drawbacks of both public key and secret key cryptography.

However, it is important to note that in order to preserve the authenticity, confidentiality, and integrity that PKI can provide, private and secret keys must be protected from unauthorized use.

Certificate Authority (CA)

A Certificate Authority (CA) is intended as a responsible, trusted third party that issues, revokes, and manages digital certificates. A CA may directly validate the identity of a public key's owner prior to issuing a certificate, or a CA may delegate this responsibility to trusted Registration Authorities.

Registration Authority (RA)

A Registration Authority (RA) is an optional entity implicitly trusted by a CA to validate another entity's identity prior to the CA issuing a digital certificate for that entity. RAs are typically needed in large PKI deployments where it may be impossible for a CA to itself positively identify each individual entity requesting a certificate.

Digital Certificates

Fundamental to PKI is the digital certificate, a set of digital credentials issued to an entity, such as an employee, by a trusted third party, such as an employer. These credentials are issued in such a way that they uniquely identify a given entity from all others known to the issuer. The trusted third party, or CA, that issues these credentials is responsible for binding a given set of credentials to an individual. Once issued, anyone trusting the CA will trust that the entity identified by a digital certificate is who or what he claims to be. (This assumes that the presenter can prove that she also possesses the private key associated with the certificate, and that the credentials have not been revoked.)

Digital certificates are commonly described as digital passports due to their role in identification. A trusted authority issues digital certificates. Digital certificates contain information used to verify the identity of the digital certificate owner by any entity that trusts the issuer of the digital certificate. Digital certificates are trusted because of the digital signature placed on it by the issuer, much like passports are trusted due to the stamps, seals, and signatures that the issuing authority approves or places on them.

Digital certificates contain a public key that is associated with an entity. It is through the certificate issuance process that a CA binds a public key with a given entity. Once an entity's public key is bound to other identifying information in a digital certificate, that certificate should be freely distributed to any and all parties that need or want to securely communicate with the entity, or verify an entity's identity.

Third Party Trust

Two users possessing digital certificates issued by the same CA can implicitly trust each other due to each user's trust of the CA. As illustrated in Figure 2, the CA has issued the digital certificates of both User A and User B. Since User A has an established trust relationship with the CA, and User B also has an established trust relationship with the CA, the CA can vouch for the identity of each. This confirmation of identity can be accomplished by verifying the CA's signature on each user's digital certificate, making trust between the two users possible.

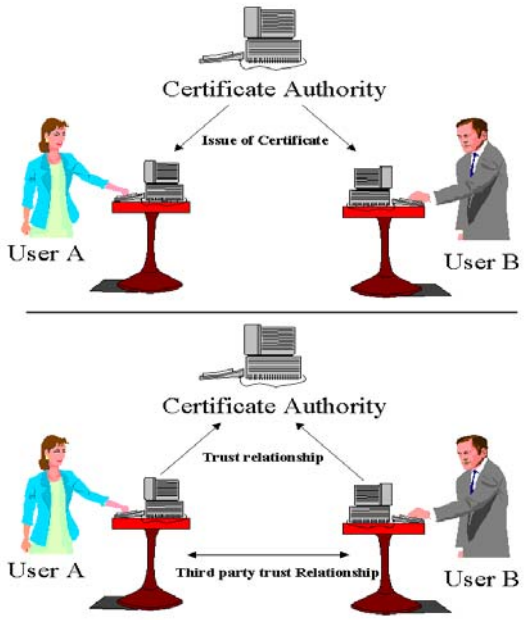

Figure 2: Third Party Trust

Repository

The repository is the workhorse of PKI, storing certificate and entity information and making the data available to an enterprise upon request. The most common repositories are built upon industry standard X.500 Directory Access Protocol (DAP) or Lightweight Directory Access Protocol (LDAP) services that provide lookup and retrieval services to an enterprise. Alternatively, there is the option of using various built-in repositories, typically fashioned after a common address book, found embedded in applications such as Internet Explorer and Netscape Communicator browsers. These built-in repositories require that the certificates of intended recipients be imported, usually by the user, and are generally associated with workgroups and not enterprise environments.

A common misconception about PKI is that CAs provide constant service and require uninterrupted communication with the user community. This is not true. Instead, it is the repository that services virtually all day-to-day PKI-related requests, including entity certificate lookup and certificate revocation list checking. Once a CA issues a digital

certificate to an entity, that entity will typically only communicate with the CA for actions such as certificate issuance, renewal, recovery, and revocation of certification. Research indicates that the repository typically supports greater than 80 percent of all PKI transactions within an enterprise.

The Critical Role of Policy

At present, there is no single global PKI model. Instead, there are numerous independent architectures with varying degrees of coexistence and interoperability. Various governments, industries, and standards bodies are working towards the goal of a global, standardized PKI. However, it is far more likely that these standardization efforts will result in multiple, independent PKIs with increased levels of coexistence and interoperability, much as currently exists with network operating systems such as NetWare, UNIX, and Windows.

It is for these goals that the trust mechanisms and certificate formats used in PKIs are defined in an open and scalable manner. Likewise, coexistence and interoperability issues explain why PKI is a relatively young technology, despite the fact that some of the underlying components have been around for 30 or more years. Within 3 to 5 years, we envision better definition of, and interoperability among, various PKIs, as well as the establishment of global “root” CAs.

Although technology plays a critical role in implementing and operating PKI, PKI is ultimately a policy-based environment. The policy drafting process, which typically requires the involvement of people or functions from across the enterprise, including management, HR, legal, and IT, will make such decisions as what the certifications are used for, who gets them, and how quickly revocation information must be disseminated, etc. Without formal policy and planning prior to implementation, the trust placed in an enterprise PKI can easily be undermined. An example might be lapses in identity verification during the certificate registration process. In brief, policy development and planning is vital in tailoring the PKI to meet the environmental and functional needs of an enterprise.

Policy development and maintenance decisions made during the planning, implementation, and duration of a PKI are often difficult and can have a direct effect upon the use, flexibility, and trust level of the resulting environment. Policy development can be expensive, with some estimates attributing 75 percent of enterprise investment in PKI to policy development. The Government of Canada, for example, invested over 1.5 man-years of effort in the creation of the Government of Canada PKI CP. Note that a single set of appropriately crafted policies can apply to more than one CA within an enterprise.

It is evident that policy development and maintenance decisions require the skill of experts in a variety of fields. Many organizations enlist legal, operational, business,

policy, and technical experts to develop the PKI policies that support the implementation and operation of their PKI.

The bodies of experts that create and govern PKI policies are referred to as the *Policy Management Authority (PMA)*. In some instances, the PMA is divided into the roles of the *Policy Approval Authority (PAA)* and the *Policy Creation Authority (PCA)*. The PAA is the arm of the PMA that develops the policy governing the PKI, whereas the PCA is the arm of the PMA that implements the PKI policy through establishment of one or more CAs. In essence, this split makes a distinction between the decision-makers and the active technology participants.

The primary policies of an enterprise PKI are the *Certificate Policy (CP)* and the *Certification Practice Statement (CPS)*. Collectively, these two policy documents can be compared to, or serve as, a traditional security environment Concept of Operations (CONOP). Although the need for such policy documents may initially not be evident, larger enterprises considering PKI cross-certification between CAs will find that legal requirements make both policies necessary. This need is centered in the fact that business partners do not necessarily have the same security requirements, nor do they necessarily instill equal levels of trust into their PKI. Therefore, trusting certificates issued by a less-secure business partner can undermine the security of an enterprise PKI. Policy can identify these issues, insulate an enterprise from their ill effects, and provide grounds for legal remediation if necessary.

The CP is a more publicly available document that describes what is happening from an operational standpoint, and allows partners to make the business and technical decisions required to establish trust in another organization's PKI. The CPS is typically treated as an internal document detailing the functions of the PKI. Studying the CPS can often give a first indication of vulnerabilities or susceptibilities in the PKI. In essence, the CP is a descriptive document that identifies *what* the PKI environment does, and the CPS is a descriptive document that identifies *how* the PKI environment does it.

For example, an enterprise's CP may state that the system is backed up twice daily, and the CPS may identify the backup times as 6 AM and 6 PM. Since the CP is a more external document, and the CPS is an internal document, the CP can provide a business partner assurance that adequate backups are being performed without providing the specific implementation details in the CPS.

Another document required for an enterprise PKI is the *Subscriber Agreement*. This document usually serves as a contractually binding agreement between the operator of the PKI and the user. Typically, this document is published on the Internet, intranet, or through other means for user review. The Subscriber Agreement identifies the responsibilities of the user concerning the PKI, and identifies the limits of liability of the PKI operator regarding the use of a user's digital credentials.

Possible Pitfalls of PKI Implementation

Security practitioners have identified a number of significant pitfalls related to PKI implementation. In no particular order, these pitfalls include:

- *Failure to properly identify the business requirements for PKI* can result in the implementation of a system that has little or no present value to an enterprise, and that is unlikely to scale to meet future needs. The needs of the organization must be clearly identified. Since PKI is intended to be a security framework from which other solutions hang, the PKI should also be expected to scale to the needs of the organization.

- *Miscalculation of resources required for implementation.* Organizations have been shown to gauge the level of effort required to deploy an enterprise PKI on previous experience with enterprise applications. While this may seem like a sensible metric, experience has demonstrated that the knowledge and support required to deploy an enterprise PKI is very different from other applications. As a result, enterprise PKI deployments typically take longer or cost more to implement than initially anticipated.

- *Weak registration process, including entity identification and certificate distribution*. The PKI registration process is the single most important element to maintaining the integrity of an enterprise PKI. Without strong processes for entity identification and the subsequent distribution of digital certificates, trust in an enterprise PKI is easily undermined, thereby providing little or no benefit to the organization.

- *Misconception of the purpose and use of PKI.* A major pitfall for organizations that are looking to implement PKI is the misconception that PKI is a "silver bullet" that will end all security woes. PKI provides a set of tools that support authentication, confidentiality, integrity, and evidence of non-repudiation. It is up to the organization to use these tools properly to achieve better security. Indeed, real security is the result of many different processes and technologies. Education and training is typically required for organizations to describe the true purpose and role of a PKI environment.

- *Lack of protection for the CA and user private keys.* The security of the CA and entity private keys is paramount to the overall integrity of the PKI. Compromise a user's private key, and trust in that user is violated. Compromise a CA's private key, and trust in *every* certificate issued by that CA is violated. Unfortunately, mainstream key storage media, such as those provided by default under Netscape Communicator and Microsoft Internet Explorer, offer little or no protection from illegitimate use. Solutions offering higher protection for private keys, such as hardware tokens and smart cards, do exist, but financial and technological barriers often prevent their widespread use.

- *Lack of protection for workstations.* Private keys stored on or accessible to user workstations are susceptible to illegitimate use. Such use can range from an unauthorized user sitting down at another person's computer, to the installation of a computer virus or remote control program that can access a user's private key without the owner's knowledge.

- *Directory or repository design and implementation.* Building an enterprise directory to support PKI is tricky, and differs from most other enterprise-wide application deployments. In many cases, organizations have only a single opportunity to deploy the directory correctly. Once deployed and integrated into the lifeblood of the enterprise, it is very difficult to substantially change how the directory is implemented. Thus, thorough up front design and planning is critical.

- *Policy decisions and documentation.* It is difficult to determine what information should actually be captured in the policy documents supporting an enterprise PKI. Too little information can render the policies incomprehensible, and degrade the enterprise's security. All too often, policy statements, particularly in outsourced solutions, have become mere glorified disclaimers that disavow responsibility and liability. On the other hand, too much information can make the policies difficult to understand and implement. The extent to which policy is spelled out often depends on how much security an organization requires. Some enterprises, for example, can live with a 24-hour lag time in getting out information about revoked certifications, while others, such as banks, require such information right away.

- *Poor certificate verification mechanisms.* Trust in a PKI dissolves if the identity of another entity isn't verified for each and every transaction. Without such verification, the recipient of confidential data, for example, may very well be an imposter who has compromised another's private key. However, real-time verification of entity credentials is not presently common, and falls short in two areas. First, verification of credentials is a voluntary process that is up to the client-side application to enforce. If the application, such as a Web browser, doesn't make the effort to check the validity of credentials, then the user will never know if they are valid or not. Second, even if the application does validate the credentials, the Certificate Revocation List (CRL) -- a list of known "bad" certificates -- may not be up-to-date.

Attempting to work around these pitfalls has cost many enterprises much time and money. And for some organizations, avoiding these pitfalls has been impossible, causing the PKI implementation to stop dead in its tracks. Careful up-front planning and prototyping can mitigate most, if not all, of these risks.

Who is Using PKI Today?

Numerous government agencies, industries, and standards bodies have been exploring the proposed benefits of PKI for the past several years. Many of these initiatives still exist as small, pilot deployments. Some organizations have successfully moved beyond the pilot phase and have deployed an operational PKI, if only for a specific division or project.

Government Agencies

The US Government has established a Public Key Infrastructure Steering Committee consisting of subordinate working groups (for example, legal and technical working groups), whose purpose is furthering the understanding and use of PKI throughout the federal government. Some of the US government agencies actively exploring or using PKI include:

- Department of Defense (DoD)
- Department of Energy (DoE)
- Department of Justice (DoJ)
- Federal Deposit Insurance Corporation (FDIC)
- Immigration and Naturalization Service (INS)
- National Security Agency (NSA)
- US Postal Service (USPS)

The US government isn't alone in its exploration and use of PKI. Many other governments are also working with PKI, notably the governments of Australia, Canada, Ireland, and the United Kingdom.

Industry

Many private-sector industries are exploring or using PKI, either voluntarily or as a result of government regulation. Some of these industries include:

- *Automotive* - The automotive industry has created the Automotive Network Exchange (ANX), a virtual private network used to securely exchange mission-critical information, such as just-in-time inventory data, among subscribers. The ANX does allow connectivity from the Internet, provided that the Internet Service Provider (ISP) is granted certification from the ANX central authority responsible for monitoring the performance levels of the ISP.

- *Banking* - The banking community has established an industry-specific CA, Identrus, acting as a trusted third party for authenticating bank and financial transactions for businesses and banks. Specifically, the mission of Identrus is to

provide a global framework for trusted business-to-business electronic commerce.

- *Health Care* - The Health Insurance Portability and Accountability Act (HIPAA) places stringent security and privacy requirements upon health care and insurance providers, all but mandating that these organizations implement PKI. As a result, numerous health care agencies have a PKI plan. However, few have reached even a pilot implementation phase. An example of a health care PKI is PCS Health Systems, Inc. of Scottsdale, AZ, which makes prescription records available over the Web to insurance subscribers and other clients.

- *Shipping* - The shipping industry is quickly putting PKI technology to use, and provides perhaps the best examples of fully deployed PKIs used to provide both transaction integrity and confidentiality. Federal Express was one of the first to implement a PKI within its organization, and PKI enables the USPS Information-Based Indicia Program (that is, print-your-own electronic postage).

Standards Bodies

Standards bodies have been instrumental in the development and formalization of PKI, and are also using it internally for both development and production applications. Such standards bodies include:

- Internet Engineering Task Force (IETF)
- The Institute of Electrical and Electronics Engineers (IEEE)
- International Telecommunications Union – Telecommunications Standardization (ITU-T)
- National Institute of Standards and Technology (NIST)

Which Vendors Provide PKI Software?

The PKI market is growing, with several dozen commercial vendors providing PKI solutions. Vendor PKI offerings include both products and services designed to provide the technology required to implement a PKI solution. Not all solutions are created equal, however, and each solution has its own particular strengths and weaknesses that must be evaluated against an enterprise's PKI requirements. Larger product vendors include:

Vendor	PKI Product(s)	Web Site (URL)
Baltimore Technologies	UniCERT CA	www.baltimore.com
Cylink	NetAuthority PKI	www.cylink.com
Entrust Technologies	Entrust/PKI	www.entrust.com
Microsoft	Microsoft Certificate Services	www.microsoft.com
Netscape	Netscape Certificate Server	www.iplanet.com

Novell	Novell Certificate Server	www.novell.com
RSA Security	Keon	www.rsasecurity.com
Spyrus	Spyrus PKI	www.spyrus.com
Tivoli	Secure Way Public Key Infrastructure	www.tivoli.com
Verisign	Verisign Onsite	www.verisign.com

Does My Enterprise Need PKI?

PKI is an emerging environment of policies, protocols, and standards with great promise for establishing trust and long-term potential savings through added integrity and confidentiality. That promise of greatness, however, comes at some cost. The price is exacted in terms of up front cost for PKI development and deployment, as well as the implicit costs of adopting an emerging technology such as expenses related to retraining, interoperability constraints, and eventual standardization requirements.

Implementing PKI simply for the sake of having one is nonsensical. As stated earlier, PKI is an enabler and not a solution itself. Prior to investing in PKI, an enterprise must determine whether or not PKI is needed by assessing needs, defining requirements, and determining which applications and processes should be, and can be, PKI-enabled.

Thus, when considering PKI, enterprises must ask themselves questions such as the following:

- What degree of trust is needed?
- How is that trust measured and reported?
- What policies are required?
- How does policy selection affect PKI selection and deployment?
- How will business partners be included in an enterprise PKI initiative?
- What are the development and implementation costs associated with an initiative?
- What will the continuing operational costs be?
- And, ultimately, will the enterprise meet its objectives after implementing PKI?

In the end, an enterprise wants to find itself in an environment that establishes a higher degree of trust and enhanced security controls that encompass applications, networks, and systems, as well as users.

Summary

In short, PKI is an enabler of trust within an enterprise and among business partners. A properly implemented PKI can greatly enhance the confidentiality, integrity, and overall security of PKI-enabled applications, services, and systems. Despite its benefits, however, PKI is not a “silver bullet” that will magically solve every Information Security problem. A significant up-front effort is required to determine and establish policies, procedures, and technologies that will lead to a successful enterprise PKI deployment.

PKI is an emerging technology that continues to mature. Enterprises that are interested into successfully deploying PKI must view PKI as a long-term solution, and not a short-term patch for existing security problems. Implementation of PKI requires planning and policy that significantly affect the way organizations conduct business and communicate with their customers and business partners.

META Security Group Can Help

META Security Group is a leader in Information Security. For assistance in determining the feasibility of PKI to your enterprise, in crafting policy, and in executing deployment, contact META Security Group:

META Security Group
20464-A Chartwell Center Drive, Charlotte NC 28236-6862
704-895-0837 fax: 704-895-8165
World Wide Web site at http://www.metasecuritygroup.com

```
http://www.metaseurity group.com
```