# Global Information Assurance Certification Paper

# Implementing a PKI

## Summary

PKI (Public Key Infrastructure) is a technology that is currently in a growth stage. As such, many organizations are either testing it out or are moving past pilot phases into production. To facilitate this move, there is a wide range of vendors selling PKI products. These vendors include Microsoft, RSA Security, and Entrust among others. PKI however is not an out-of-the-box solution. Great care should be given to the development of the policies that regulate the PKI.

If well planned and executed, PKI has the ability to provide a high level of information protection. PKI should be considered as part of an overall security strategy including traditional mechanisms such as firewalls and intrusion detection systems (IDS's). In addition, organizations should understand that the PKI and its components are not immune to risk or attack and should ensure that mitigation procedures are put in place in the event of a system compromise.

## Introduction

PKI (Public Key Infrastructure) is a technology that is currently in a growth stage. It is being used in the healthcare and banking industries to protect client and organizational information. The United States Defense Department is in the process of implementing a massive PKI to protect sensitive and secret information flowing through the nation's military service networks. As we move into 2002, more organizations are moving past PKI pilot phases and into production mode. This paper will address the reasons an organization should or should not stand up a PKI as well as detail some steps to implementing a successful PKI. It is assumed that the reader has some background knowledge of Infosec and PKI technologies.

## Benefits of a PKI

If implemented correctly, a PKI can provide the basic security tenants of confidentiality, authentication/access control, data integrity, and non-repudiation. A PKI can ensure that only legitimate users have access to system resources. It can provide encryption services for employee e-mail communications as well as communications between an organization's customers and its web servers. By using hash and signature algorithms, a PKI helps to ensure that data in transit has not been altered and that it was sent by the person claiming to have sent it. A PKI also has the ability to bind two parties to a transaction by identifying each of them and providing a timestamp.

## Types of Implementation

An enterprise PKI can be stood up to enforce security policy within an organization or between organizational parties (B2B). An enterprise PKI usually comprises encryption keys and signature keys. For better security, dual-key pairs should be used. This will allow for key escrow of only the private encryption key, thereby not negating the benefit of non-repudiation. An enterprise can also assign digital certificates to network resources (i.e., intranet servers, routers) allowing for either one-way or two-way authentication. Two-way authentication is achieved by issuing end-users identity certificates. If this is implemented, then during the SSL (Secure Sockets Layer) handshake both the device and client certificates are validated. An example of a B2B PKI implementation is Identrus (Callan). Identrus is a conglomerate of banks that have joined together to ensure secure transactions with corporate customers. In the Identrus model, each participating bank can trust each other. Under this model, Identrus acts as the root CA (Certificate Authority), or PAA (Policy Approval Authority) while each member bank establishes its own CA. The bank CA's issue digital certificates to their corporate customers who can then be trusted by the entire chain.

A B2C (Business to Consumer) PKI can be implemented that allows secure communication between an organization's customers and its web servers. Again, simple device certificates can be used to enable one-way SSL communication while device and client certificates together can enable two-way SSL communication. An example of a B2C PKI implementation is the CPA (Canadian Payments Association). The CPA acts as the root CA and ensures trust and policy enforcement between it's sub CA's (Stratton). The sub CA's belong to member Canadian banks that wish to participate in the trust model and issue digital certificates to their end-user customers. One of the goals of the CPA PKI project is to instill greater consumer confidence in transacting business over the Internet (Canadian).

**Alternatives**

An organization should ask itself however, if it truly needs a PKI solution or if it only needs to satisfy certain security requirements. Take for example an organization whose sole requirement is the need to send confidential e-mail. A product called HyperSend from Hilgraeve, Inc performs this function by sending messages through HTTP (Hypertext Transfer Protocol) instead of SMTP (Simple Mail Transport Protocol) (Berinato). By installing the HyperSend software on both the sending and receiving machine, a VPN (Virtual Private Network) can be established to send sensitive information within (How To).

An example of an alternative protocol is IPSec (Internet Protocol Security) (see RFC 2401). When used with both the Encapsulating Security Payload (ESP) and the Authentication Header (AH) IPSec can provide source authentication, connectionless data integrity, and encryption services between either hosts or secure gateways. Like Hilgraeve, IPSec can create VPN's between users but it can also encrypt data between network devices. When used with the IKE (Internet Key Exchange), IPSec can provide

organizations with a robust security solution. This is of course if the organization does not need non-repudiation services.

PKI solutions begin to make great sense when there is a need for technical non-repudiation (it is still to be seen how these systems will stand up to legal non-repudiation requirements). By providing each end-user his or her own private signature key, the PKI can reasonably assure that participants in a transaction are who they say they are and that they truly did participate in the transaction.

**PKI Class Levels**

Or can it? PKI certificates are divided into different classes (Verisign). Class one PKI certificates cannot offer the assurance of non-repudiation or authentication. This is because the method of registering end-users is not face-to-face. In this case, an organization would most likely be only concerned with obtaining confidentiality and integrity services. A class one PKI can be relatively easy to stand up but the rewards are minimal when compared to a class three PKI. Class three certificates address this problem by requiring an in-person registration with an identification check. This would seem to solve the issue, however not all class three implementations can guarantee technical non-repudiation. The policies and processes put in place to protect a user's private signature key are directly related to the assurance level of non-repudiation provided by a PKI.

**Authentication Techniques and Smart Cards**

Two-factor authentication attempts to address this problem by requiring the end-users to authenticate using something they have (e.g., a token) with either something they know (e.g., a password) or something they are (biometrics). The most secure implementation requires that private keys be stored on a smart card and as such, zeroization should occur if the card is tampered with or if password authentication fails after a set amount of attempts. Biometric authentication is generally more secure than password authentication however passwords can suffice when strong-password policies are enforced. In high-level assurance environments (e.g., Secret Military and Intelligence over unsecured networks) care should be taken that signing and encryption occur only on the cards. This prevents the private keys from ever being exposed to the computer operating system. This is a standard for class four PKI (high value data over an insecure network) but is probably not a need for a standard commercial implementation.

**Usage Concerns**

Many employees feel that there is no need to either encrypt or sign their e-mail communications. This feeling can be a result of not understanding the inherent risks of communications over the Internet or the employee may simply feel that his or her work is not important enough to encrypt. Care should be taken to ensure that employees

realize the need for the PKI. Bits of important information from ordinary, everyday e-mail traffic can be compiled by an attacker into a profile of an organization or department. This information could then be used to launch social engineering attacks or even direct attacks against system resources. Some organizations by their nature have more sensitive information flowing through their systems than others, however most organizations should be concerned about keeping internal information confidential.

**PKI Vendors**

There is a range of choices available to organizations looking for a PKI vendor. While each of these vendors offer similar functionality in their products, there are some differences. We will first look at a PKI product architecture by examining Baltimore Technologies and then discuss offerings from some of the other well-known players in the PKI market.

*Baltimore Technologies*
Baltimore Technologies offers the Unicert 3.5 PKI product. Active Directory is supported as well as smart-cards. There is also a built-in capability for user pre-authorization. A key archive server is included which works by encrypting a user's private encryption key with 3DES and then encrypting the result with 3DES again.

Unicert is designed modularly. The Core Layer has five modules: CA, CAO (CA Operator), RA (Registration Authority), RAO (RA Operator), and a Gateway (Unicert). The gateway's function is simply to either receive certificate requests and forward certificates (acting as a middleman between the RA and end-user) or to receive certificate requests and forward informational messages to the end-user (Gateway).

The Advanced Technology Layer consists of four modules: Key Archive Server, Advanced Registration Module (ARM), Advanced Publishing Module (APM), and WebRAO (Unicert). The Key Archive Server is used to store encrypted private encryption keys. The ARM provides an interface to smartcard management systems and also allows an enterprise to pre-authorize its users (i.e., issue passwords to each employee) for faster certificate registration operations. It should be noted however that the means of transmitting the passwords to employees would determine how trustworthy and secure the system is. According to Unicert, the APM allows an organization to keep its existing directory system in place. It publishes certificates to directories using the LDAP (Lightweight Directory Access Protocol) standard and is easily integrated with Microsoft Active Directory. Finally, the WebRAO provides for remote RA administration from a web browser over the Internet.

The Extended Technology Layer consists of only two modules: Timestamp Server and Unicert Roaming (Unicert). The Timestamp Server attaches a timestamp with the server's digital signature to documents. The Unicert Roaming component is optional and stores keys on a centralized server. Users wishing to use their keys do not need to

be in possession of them. Instead, a password is supplied to the roaming server via an Internet browser and the user is given access to his or her keys. The user can then access the intended application. Unicert has made this process transparent to the user.

Unicert supports RSA keys of up to 2048 bits and DSA keys of 1024 bits. Unicert also supports EC/DSA (Elliptic Curve/DSA) for key generation and signing and uses Blum Blum & Shub as the psuedo-random number generator.

*RSA Security*

RSA Security offers the RSA Keon Advanced PKI as their PKI solution. Keon takes a bit of a different approach than Baltimore's Unicert. The main focus is on the Security Server and the credential stores. The credential stores host user certificates and keys as well as network logon information (user names and passwords). These stores can be placed on smartcards or on the centralized Security Server. When the credentials are placed on the Security Server, users authenticate to the server using either one, two, or three-factor authentication (set by administrator). The store is then downloaded to the user's computer (via SSL) where he or she can transparently use its contents to log onto networks and applications (Single Sign-On support). RSA uses this technique because smartcards require a buildup of infrastructure (readers) that many organizations have not yet invested in. Private keys in the credential store are encrypted using 3DES and logon information is encrypted using the RC4 algorithm (RSA Keon).

Keon Advanced supports legacy applications that are not yet PKI aware by using Public Key Wrappers. The wrappers store application logon information within the credential store thereby allowing the PKI to work in the background to log users on to the application.

*Entrust*

Entrust has released the Entrust Authority Security Manager v6.0 as its PKI product. Entrust stresses the need for transparent security for the end-user. Security Manager offers support for both single and dual key pairs (Entrust) as well as support for up to 20 million users per CA. In addition, the key recovery database can be encrypted using the new AES (Advanced Encryption Standard).

Security Manager v6.0 has added directory support for Microsoft's Active Directory. Certificates may also be stored in a standard LDAP directory. Entrust also offers the option of customizable user certificates. This allows administrators to specify access controls in certificates. In addition, Entrust allows administrators to change the DN (Distinguished Name) and CA fields in a user's digital certificate, thereby allowing administrators the ability to change a user's identity. It is assumed that audit trails are in place to mitigate the risks associated with this feature. The cost of the Entrust Authority consists of a $25,000 base fee plus $27 per certificate for 10,000 of them (Messmer).

*iPlanet*
iPlanet is an alliance between Netscape Communications and Sun. iPlanet CMS (Certificate Management System) 4.2 is their latest PKI product release. This offers support for millions of users and is priced at $10 per extranet user and $40 per intranet user (Phillips). The operating platforms that CMS runs on include Windows NT 4.0, Solaris, AIX, and HP-UX.

*Microsoft*
Microsoft has entered the PKI market by including a PKI solution in its Windows 2000 operating system. Under the Microsoft model, there are two types of CA's. The first is the enterprise CA. This is mainly used in a tight environment where everyone receiving certificates is using Windows 2000. The second type is the stand-alone CA. This CA is used when an organization wishes to issue certificates to outside partners or customers. Certificates from the stand-alone CA can be used on non-Microsoft operating systems. Microsoft allows integration of both CA types with its Active Directory. This allows the directory to store certificates and revocation lists and also allows the stand-alone root CA to be run offline from the network. By doing this, the root CA can still sign sub-CA certificates using a manual floppy disk transfer process. This can ensure an even greater level of security for the root CA (De Clercq-Frame E). A policy module in a stand-alone environment is used to accept certificate requests and mark them as pending. In an enterprise environment, the policy module is intelligent enough to be able to automatically approve or deny certificate requests. After approval, private keys are stored on either a smartcard or in a user's Windows profile (Hayday).

**Some Steps to Implement a Successful PKI Solution**

These steps are in addition to normal program management and systems analysis procedures used in an IT project implementation.

- Know the reason the organization is looking to implement the PKI. Is it possible that a simpler solution can meet the requirements? Scalability should also be considered here however. If an organization is only in need of confidentiality services today, will it need non-repudiation, authentication, and integrity services at a later date?

- Know what business processes will be affected by the PKI implementation. Meet with line managers to advise them of this and gain insight into their concerns. It is important that user acceptance of the PKI be obtained.

- Spend time developing the Certificate Policy (CP) and Certificate Practice Statements (CPS's). These are of paramount importance to the PKI. It should be understood that a PKI implementation is much more a policy-based issue than a technology-based one. The setup of a certificate authority and the ability to issue certificates can be achieved

in a matter of minutes. Policy on the other hand should go through several iterations and be developed in conjunction with many organizational departments. These departments can include I.T., Security, Legal, Finance, Operations, and others.

- Plan for both technical and physical security of the PKI components (PAA, PCA, CA, RA, etc…). Additionally, ensure that trusted roles (RA, LRA, TA, etc…) be staffed with reputable persons.

- Develop a Key Recovery Infrastructure (KRI). The KRI should be used only to recover private encryption keys. Key escrow of signature private keys undermines non-repudiation.

- Develop policies for key expiration and revocation. Determine the frequency of CRL (Certificate Revocation List) checking needed and ensure the selected software can meet the requirements. Also, determine the method and frequency that the CRL is updated.

- Plan for integration of the PKI with the existing directory structure. Is the organization's existing directory structure LDAP compliant? DAP compliant? What will need to be done to allow end-users to obtain certificates in the most convenient manner?

- Determine the need for cross certification with industry partners or others. Will the organizations PKI "talk" to and trust it's partners' PKI? Plan out options for the future. If the organization is using the PKI strictly for internal uses today, will it want to expand certificate issuance to customers or partners tomorrow?

- Don't think of PKI as a security panacea. Organizations must still employ traditional security methods such as firewalls, intrusion detection systems, host-level security (i.e., patches and O/S hardening) and auditing.

- Provide the most convenient and cost-effective registration possible to end-users provided that the process meets the requirements of in-person registration. This could be accomplished by using TA's (Trusted Agents) at each organizational site to verify identity and register users.

- Develop a disaster recover policy. What will the procedures be in the unfortunate event of a CA compromise? What will happen if the CA signing key is lost or destroyed. Where are the primary and backup keys stored and who has access to them?

- Develop audit policies and perform tests to be sure the PKI is secure. Have Penn Test Teams try to circumvent security procedures on an annual or biannual basis to ensure that illegitimate users are not granted digital certificates.

**PKI Risks and Mitigation Procedures**

A PKI, like any security solution, is only as strong as its weakest component. Much attention is paid to the key size of the encryption algorithm however this is not the biggest concern one should have. A much more pressing concern is how user's private keys are protected.

*Password or Biometric Security Features*

Are your user's utilizing one or two-factor protection? Some PKI implementations protect private keys with only a password and store them on a host computer. Smartcards with strong password policies or with biometric authentication (even better) should be used to achieve a trusted PKI. Most smartcards today offer tamper resistance features. If an attacker attempts to log-in over an administrator-set number of times, the smartcard erases all critical data stored on it (zeroization). This prevents brute-force password attacks. Smartcards that utilize biometric settings sometimes utilize low-end optical scanners. These scanners may be tricked to allow a system compromise by using a reprographic of a user's fingerprint (Raikow). Another concern with biometrics is the security of the minutia files (stored on a centralized authentication database). Attackers must not be able to gain access or decrypt these files. Doing so could allow an attacker to copy the file and forever compromise a user's biometric (Raikow).

*Protection of the CA and signing keys*

An issue with iPlanet CMS is that the CA administrator's password is stored by default in clear-text in the admin-serv/config/adm.conf file on the Windows NT 4.0 platform (Vulnerability). Since the admin server is accessible via the Internet, this should pose a security concern. If the CA sits on a network, it should be protected by a firewall and an intrusion detection system (IDS). Also, it is imperative that the CA signing key be stored in a secure manner. For physical security, CA's can be placed in a "cage" with access granted to only those who are authorized.

*User Registration Process*

As mentioned earlier in this document, the registration process is integral to the trust of a PKI. The risk of issuing certificates to an un-trusted party can be mitigated relatively easily in a PKI supporting a single organization, however there is much more concern when trust relationships are established with outside organizations. Again, policy development is critical in this situation. Organizations should only trust other organizations that meet their policy requirements for identification verification. Also, there should be mechanisms in place to ensure that the policies are being enforced and followed by each organization in the trust chain.

*CRL Checking and Certificate Lifetime*
An important aspect of PKI is the ability to communicate an invalid certificate to subscribers. If a private key is compromised, the CRL will need to be updated as quickly as possible. The other half of the equation involves the method an application uses to check the CRL. Is there an automatic check or does the user need to manually check to see if a certificate is revoked? The use of the OCSP (Online Certificate Status Protocol) can be used to mitigate this risk. OCSP requires an OCSP responder to be set up which contains up to date revocation information (Myers). When an application requires a certificate verification it queries to the responder and then waits for a response of either "good," "revoked," or "unknown."

**Conclusion**

Information Security should be a major concern of all organizations. A PKI, along with traditional physical and technical security mechanisms can enhance an organization's security posture dramatically. PKI has been around for a while mainly in concept and in pilot phases but is beginning to be implemented in more production environments. In order to successfully implement a PKI, it is essential to first realize the underlying security and business needs of the organization. Analysis can then be conducted to determine if the organization would be best served by a PKI or if a less complicated system would be more beneficial. It is also important for the PKI implementers to focus a majority of their time and thought on policy creation. PKI is simply a means to enforce that policy using technical tools. By carefully examining an organization's current and future needs and spending time and thought on PKI policies, organizations can reap the widespread benefits of a successful PKI implementation. As the technology moves past its growth stage to a more mature and stable level, many more organizations will realize these same benefits.

**Bibliography**

Berinato, Scott., and Dennis Fisher. "Cheaper Techniques Take on PKI." *EWeek*. 21 Aug. 2000. ZDNet. (26 Dec. 2001).
<http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2617314,00.html>

Callan, Eoin. "ENCRYPTION: Leading Institutions Back New Global Security System." *FT.com*. 1 Mar. 2000 (27 Dec. 2001).
<http://specials.ft.com/ln/ftsurveys/sp9aa6.htm>

"Canadian Payments Association and e-Scotia Announce CPA Root Certification Authority Hosting Agreement." Scotia Bank Website. News Release. 5 Apr. 2001. 30 Dec. 2001 (30 Dec. 2001).
<http://www.escotia.com/escotia/new_20010405.htm>

De Clercq, Jan. "Running a Windows 2000 PKI Project". Microsoft TechNet. March 2001. (2 Jan. 2002).
<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/smrtcard/smartc04.asp>

Entrust Authority-Security Manager Features and Benefits. Entrust. 2002. (30 Dec. 2001).
<http://www.entrust.com/authority/manager/features.htm#lifecycle>

Gateway Page. Baltimore Technologies. 2002 (28 Dec. 2001).
<http://www.baltimore.com/unicert/unicert/gateway.html>

Hayday, John. "Microsoft Windows 2000 Technical Reference." Internet Security Systems. 16 Aug 2000. Microsoft Press Online. (2 Jan. 2002).
<http://www.microsoft.com/mspress/books/sampchap/3873c.asp>

How to Use HyperSend Page. HyperSend. 2001. (30 Dec. 2001).
<http://www.hypersend.com/HyperSend/Model/Home/Welcome/How>

Messmer, Ellen. "Entrust Answers Microsoft Users' Security Needs." *Network World Fusion*. 6 Aug. 2001. (26 Dec. 2001).
<http://www.nwfusion.com/archive/2001/123597_08-06-2001.html>

Myers, Ankney, et all. "Online Certificate Status Protocol." IETF. June 1999. (2 Jan. 2002).
http://www.ietf.org/rfc/rfc2560.txt

Phillips, Ken. "iPlanet CMS Boosts Extranet Security." *EWeek*. 8 Sep. 1999. ZDNet. (26 Dec. 2001).
<http://www.zdnet.com/products/stories/reviews/0,4161,2327162,00.html>

Raikow, David. "Biometrics: The Worst-Case Scenarios." ZDNet US. 1 Feb 2001. (30 Dec. 2001).
<http://www.zdnetindia.com/techzone/resources/security/stories/13111.html>

"RSA Keon Advanced PKI: A Security Architecture for Enabling E-Business." RSA. 2000. (26 Dec. 2001).
<http://www.rsasecurity.com/products/keon/whitepapers/advpkiwp/KEAPKI_WP_0200.pdf>

Stratton, Jennifer. "The Keys to The Lock: The Public Key Infrastructure Initiative Builds Confidence in E-Commerce." *Canadian Central News and Views*. March 2001 (2 Jan. 2002).
<http://www.cucentral.ca/Private/industry/article_pki.htm>

Unicert Technical Details Page. Baltimore Technologies. 2002. (27 Dec. 2001). <http://www.baltimore.com/unicert/unicert/details.html>.

"Verisign PKI Disclosure Statement." v1. Verisign. 1999. (27 Dec. 2001). <http://www.verisign.com/repository/disclosure.html>

"Vulnerability Report for Netscape CMS and Netscape Directory Server." Core Security Technologies. 26 Oct. 2000. (29 Dec. 2001). <http://www.core-sdi.com/pressroom/advisories_desplegado.php?idxsection=10&idx=123>