Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Business Perspective on PKI: Why Many PKI Implementations Fail, and Success Factors To Consider

This paper is intended to provide an overview of PKI and how a PKI implementation affects the entire organization. Information included in this paper may help business areas understand how PKI can be used to achieve tactical and strategic business objectives, and assist with identifying factors required for a successful PKI implementation.

Copyright SANS Institute

Author Retains Full Rights

AD

A Business Perspective on PKI:
Why Many PKI Implementations Fail, and Success Factors To Consider

---

Overview and Premise of this Practical

This paper is intended to provide an overview of PKI and how a PKI implementation affects the entire organization. Information included in this paper may help business areas understand how PKI can be used to achieve tactical and strategic business objectives, and assist with identifying factors required for a successful PKI implementation.

Included is a high-level overview of PKI:

- technical and non-technical components,
- how PKI works,
- how PKI is used in creating a trusted environment, and
- how it compares to alternative security solutions.

A unique perspective on this topic is provided by emphasizing that the most crucial aspects of a PKI are non-technical. Misjudging the importance of the non-technical components may be a key reason that many PKI implementations are not successful.

This is a broad overview of the major components and issues, intended to familiarize non-technical persons or those new to PKI with some of the basic PKI concepts and functions. It is not intended to be all-inclusive. Each PKI installation is unique, and individually tailored for the technical and cultural environment in which it is implemented. The intention is that this information will generate a discussion of security alternatives and support appropriate business decisions regarding PKI.

Background: PKI Basics

PKI, or Public Key Infrastructure, leverages old technology through the use of new distribution, deployment and management capabilities. As of this writing, the use of *Public/private Keys* to provide confidentiality via encryption is at least 25 years old. It is the relatively recently introduced *Infrastructure* component that allows the public/private keys to be deployed and managed throughout the enterprise. The infrastructure supports the distribution, management, expiration, rollover, backup, and revoking of the public/private keys. These features of a PKI will be discussed in more detail later in this paper.

Public/private keys are issued and operate as 'inverse pairs': an operation performed by one key can be reversed, or checked, only by its partner key. For example, for a pair of keys A and B, information <u>en</u>crypted with Key A can be <u>de</u>crypted ONLY using its partner Key B. [(1)]

As the name suggests, one of the keys is kept as the secret *private* key of the key owner. The other, *public* key is made available as an attachment to email messages, in shared directories, on

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

public key exchange sites, etc., allowing anyone to use the public portion of the key to perform operations that only the private key owner can access.

Operations supported by use of public/private key pairs include

- **encryption** – obscures the contents of files or transmissions to protect against unauthorized viewing;
- **authentication** – verifies the identity of the entity requesting access;
- **data integrity** – reveals any changes to files, programs, transactions, transmissions, etc.;
- **nonrepudiation** – (positive identification between sender and receiver) guarantees that a legal electronic transaction occurred.

The owners/users of these keys can be people, devices or applications:

- **people** generally use public/private keys for encrypting email messages.
- **devices** generally use public/private keys for authentication and encryption.
- **applications** generally use public/private keys for authentication and data integrity.

The following simplified example illustrates how public/private keys are used to send confidential email messages.

Encryption example

The most common use of public/private keys is for **encrypting** email messages between people. If Ann wants to encrypt a message for Clark:

- Clark would make his public key available (via one of the methods mentioned above—as an attachment to an email sent to Ann, via a directory or a public key exchange site accessible to both Ann and Clark, etc.).
- Ann would compose and address the email message and signal the email software to encrypt the message (usually by clicking on an icon or selecting the action from the Toolbar).
- The email software would use Clark's public encryption key, which is stored with his information in Ann's email Address book or available in a shared area, to encrypt the message.
- Ann sends the encrypted message to Clark.
- Clark's email software receives the message and automatically tries to decrypt it using Clark's private encryption key, or via a dialog box offers to decrypt the message.
- If the email message was indeed encrypted using Clark's public key, then Clark's private key will decrypt the message so Clark can read it.

Another example illustrates how the use of public/private keys can provide authentication and indicate whether information has been tampered with or corrupted during transmission.

Authentication and Data Integrity example

Signing a message involves using one's own private key instead of the public key of the intended recipient. Signing provides both **authentication** and **data integrity**. Again using the example of sending a message between two people Ann and Clark:

- Ann composes a message for Clark, and signs it by clicking an icon on the Toolbar.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- The email software accesses Ann's private signing key and runs a calculation on the message and any attachments, producing a fixed-length number called a *hash* which is a unique representation of the contents. This number is sent along with the message to Clark.
- When Clark receives the message into his email software, Ann's public signing key is located and used to run the same calculation on the message and attachments.
- If the hashes match, Clark has proof that
    - the message did indeed come from Ann, <u>and</u>
    - nothing in the message had been changed from the time that Ann signed and sent it because only her public signing key could produce the same hash value.

Technical Components of a PKI

Public/private key pairs can be obtained by purchasing them from a vendor such as Verisign, or purchasing the technical components to operate one's own PKI. The perspective taken in this paper is that an organization is considering the purchase and implementation of its own in-house PKI.

PKI is deployed in a client-server environment over a network. The core technical components of a Public Key Infrastructure include

- <u>A Certificate Authority (CA) server</u>
  The CA issues the public/private key pairs.
  Note: most enterprise PKI installations require retaining a backup of the private encryption keys issued to clients to prevent rogue encryption activity. Backup of keys and other CA functions needs to be provided for basic redundancy and business resumption (disaster recovery).
- <u>Personal clients or workstations (PCs) running PKI client software</u>
  Although some PKI implementations do not require client PKI software, in general a method of enabling persons to receive and handle the public/private keys must be provided. In some PKIs a second, separate key pair is issued locally by the client software, to be used for positive proof of identity (signing).
  Note: breaching the security of the client PC on which private keys are stored can provide access to the private encryption and/or signing key, allowing impersonation. It is **critical** that basic security measures (such as protecting the sign-on password) are used to secure personal workstations.
- <u>LDAP or X.500 Directory</u>
  Public keys are made available throughout the enterprise via a shared directory. External business partners and customers may be provided with a separate directory for accessing public keys, likely located outside the corporate firewall.
- <u>Registration Authority (RA)</u>
  Different business divisions may wish to exert more control over the portions of the PKI that enable their particular business processes. These areas can utilize their own Registration Authority server, which collects requests for public/private keys from clients. When the business division has approved the request according to its rules and vetting procedures, the approved request is passed to the CA and keys are issued.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Depending on the size and intended functions of the PKI installation, other technical components may be required. For example, an Authorization Server can store security access profiles and pass authorization clearance on behalf of the user to applications and devices participating in the PKI. This can reduce the number of passwords required to access company resources while increasing security.

An organization can choose to host its own CA, directory, and RA functions, or it can outsource these functions to a third-party. If hosted in-house, the strongest security procedures and controls are required to protect the PKI technical components, particularly the Certificate Authority server(s).

Digital Certificates

Digital certificates provide assurance that a public key does indeed belong to the purported owner by binding the owner's identity to the public key.[(2)] This assurance of authenticity is accomplished when the Certificate Authority digitally signs the public key, creating the digital certificate.

Instead of requesting the userID and password, a PKI-enabled device will ask for the digital certificate of an entity attempting to access it. The digital certificate can be a stronger authentication mechanism than a userID and password if the security of the entity presenting the certificate has not been compromised.

The following example illustrates the use of a digital certificate for authentication, encryption, authorization and data integrity.

<u>Authentication, Encryption, Authorization and Data Integrity Example</u>
Devices that can use public/private keys include personal clients or workstations (PCs), servers (such as application or web servers, etc.), firewalls, and routers. The following simplified example shows how, in a PKI-enabled environment, digital certificates can be used to provide secure access to a corporate web server when accessed remotely.

- Clark initiates a connection to the corporate network.
- Clark's connection request reaches the corporate firewall.
- The firewall requests **authentication** before allowing the connection.
- Instead of Clark entering a userID and password, Clark's PC provides the firewall with Clark's digital certificate.
- The firewall verifies that the certificate is valid <u>and</u> that Clark is **authorized** to access the corporate network, and allows the connection to proceed through the firewall.
- The firewall may have been instructed to encrypt any connections initiated by Clark; if so, the connection between Clark and the firewall is **encrypted**, creating a VPN.
- Clark attempts to connect to a web server on the corporate network.
- The web server asks for authentication before permitting the connection; again, Clark's PC presents Clark's digital certificate.
- If the server recognizes that Clark has a valid certificate and is an authorized user, the connection is completed.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Note that at several points an Authorization Server was queried to identify what activities Clark is **authorized** to perform. Clark is presented with only the information for which he has been authorized, in accordance with his security profile.

Suppose Clark needs to download a software update. To ensure that the software is indeed authored by the company and has not been altered intentionally or accidentally during transmission, the company can digitally sign the software. When Clark downloads the software, his PKI client will verify the signature to validate that the software came from a trusted source and has maintained **data integrity** (remains unchanged).

Administrative Issues

Another important component of a PKI is the Certificate Revocation List, or CRL. Certificates and keys which have expired or been revoked are listed in the CRL. The *infrastructure* component of the PKI can be set up to support certificate validation before providing access to the PKI-enabled resources or functions. Certificates and keys issued to participants in the PKI (people, devices and/or applications) can then be administered from a single point: revoking the certificate removes access to all resources which use the certificate for validation.

Certificates can be issued to meet specific access requirements. For example, vendors, contractors and other business partners can be issued limited-term certificates that expire at the end of their contract. Different business divisions can establish specific criteria for certificates that provide access to their environment or resources. The ability to issue customized certificates complements the RA (Registration Authority, which supports customized criteria for issuing certificates) to allow the organization to fine-tune the PKI to meet the specific requirements of various business units and functions.

Creating Trust

The security potential offered by PKI is only possible if the keys are *trusted*. An environment of trust is established when the interactions of the technical PKI components operate within a controlled and secure management and administrative environment. Trust is not possible without the appropriate physical, policy and operational controls. These controls are defined and documented in the following:

- The Certificate Policy (CP) defines what the PKI is intended to do, and defines the particular community and/or class of application for which the PKI will be used. It is a business management document, defined independently of the specific details of the operating environment. [(3)]
  *In general, the CP states **what** is to be adhered to.*
- The Certificate Practices Statement (CPS) governs the management and processes supporting the certificates issued by the CA. The CPS interprets the Certificate Policy, tailoring it to the system architecture and operating procedures of the organization. [(3)] The CPS also governs how the Certificate Authority (CA) server is operated and managed.
  *In general, the CPS states **how** to adhere to the Certificate Policy.*

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- The PKI Disclosure Statement (PDS) is a document that may be used instead of the CP and CPS to govern an organization's PKI. It is much more concise than a CP, but still follows the rules for defining the community, purposes and manner by which the PKI will be used.

Management must understand and approve the communities and purposes that are valid for the PKI. The CP and CPS, or the PDS, are legal documents that affect the organization's liability and risk profile. Development of certificate policy and practice documents requires participation from, at a minimum, Human Resources; Finance; Legal; Audit; and IT organizational units to ensure that these documents are defined and maintained in conjunction with related policies in the organization.

An organization's existing security policies may already address some of the CP/CPS or PDS requirements. In these cases, additional policies specific to the PKI will need to be developed to fill in the policy gaps. Refer to RFC 2527 for a framework for these documents. [(4)]

Functions that underpin the PKI and therefore need to be addressed in the CP/CPS or PDS include key handling issues such as

- Key distribution – how will keys be securely provided to workers, partners, devices, etc.
- Key management – who should receive keys, and under what circumstances
- Key expiration – the default length of time that keys are valid, e.g. 2 years
- Key 'rollover' – re-issue of keys after a default expiration date is reached
- Key history – retaining a history of all keys issued to an entity can be important to ensure future access to items or functions protected by expired or revoked keys
- Key backup – essential for private encryption keys; not recommended for private signing keys due to the resulting risk of compromising nonrepudiation. (If someone else, for example a system administrator can access private signing keys, reliable authentication via the private signing key is no longer possible. However, organizations are advised to retain backups of private encryption keys to protect against technical failures or rogue encryption activity.)

Technology comprises only one component of an implemented PKI. Note that crucial elements of the PKI include the

- underlying security policy implemented by the PKI
- policies and procedures for issuing and revoking certificates
- business processes of tracking and managing certificates
- administrative activities related to key management.

How PKI Is Used Within the Security Architecture

IT security should always start with architectural considerations first. A security architecture refers to a plan and set of principles that describe (a) the security services that a systems is required to provide to meet the needs of its users, (b) the system elements required to implement the services, and (c) the performance levels required in the elements to deal with the threat environment.[(5)]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The security architecture supports business initiatives and processes and addresses vulnerabilities to reduce the organization's liability and risk profile. Organizational elements which must be coordinated to derive a strong and complete security architecture include

- senior management commitment
- organizational policies, standards and procedures
- security policies, standards and procedures
- information security management structure
- corporate security awareness and training programs
- technical strategy, architecture, standards and procedures
- administrative and end-user standards and procedures
- monitoring, enforcement, and recovery processes.

The activities required to implement a PKI involve all of the above security architecture elements. The decision to implement a PKI therefore clarifies and solidifies an organization's security infrastructure by requiring coordination, consensus and buy-in amongst all the elements. The decision to implement a PKI is a business, not technical, decision addressing business and asset protection issues.

⇒ **PKI <u>uses</u> technology to implement the security policy infrastructure by which a company steers and manages its electronic business relationships.**

⇒ **PKI will fail in an enterprise if it is handled solely as a technological implementation.**

A successful implementation depends more on creating or encouraging a supportive political and policy environment rather than just hooking together the technologies. The PKI infrastructure includes policies, practices, procedures, and ongoing administration as well as the technical components. Its challenge, and its benefit, is that it is arguably the most pervasive and comprehensive enterprise-wide security infrastructure that can be achieved.

The Case for PKI

PKI security requires a comprehensive coordination among business, technology, and administrative areas of an organization in order to develop the political, policy and procedural supportive climate. This pervasive, "total-organization" involvement, wrapped around the solid technology of public/private keys, has defined a new security standard for organizations. An organization may decide that its business assets, initiatives and strategies require this high a level of protection, or that its customers will accept nothing less.

There are many reasons to protect confidential data:

- legislative requirements, both existing and pending, particularly in regards to customer privacy, social security numbers, and health information;
- insider attacks and accidental destruction of data (the 2001 FBI/Computer Security Institute study shows that the majority of data loss originates from inside an organization);
- outsider attacks are rising due to internet-based technologies (i.e. IP vs. SNA);

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- easy availability of downloadable “point-and-click” hacking / exploitation tools;
- threat of civil or criminal litigation if confidentiality is compromised;
- dangers of making critical business decisions based on invalid data;
- the need to demonstrate due diligence should a breach of confidentiality occur;
- consequences of negative publicity, loss of credibility and goodwill;
- surveys show customers are more willing to do business with companies that protect their privacy.

One or more of the following security elements may be required to provide the required level of protection:

- **authentication** to ensure that only the correct users can access confidential or proprietary resources;
- **authorization** to restrict access for anyone other than those with a business need;
- **encryption** of sensitive information to protect against unauthorized viewing;
- **data integrity** to prevent changes to data files and agreed-upon transactions;
- **nonrepudiation** (positive identification between sender and receiver) to guarantee that a legal electronic transaction occurred.

These security requirements can be addressed using ‘point solutions’ (individual components installed as-needed), or through an enterprise-wide security infrastructure such as that required by PKI. In any case, the solution must address the system and network environment, the political and procedural environment, and supporting applications such as email, Web applications, and business applications.

Advantages of ‘point’ solutions are that

- they can be deployed relatively quickly and inexpensively;
- many software choices are available;
- each area can select their own most suitable solution.

Disadvantages of ‘point’ solutions include:

- the required elements of data integrity and nonrepudiation are not provided;
- recovering encrypted information may be difficult or impossible;
- only select segments of the information distribution system are secured;
- frequent failure to integrate with other security tools for the purposes of auditing and access control;
- inability to scale sufficiently to meet expanding opportunities;
- increased technical complexity;
- difficulty standardizing, making integration between applications and/or system components difficult or impossible;
- increased costs of additional maintenance, redundancy and administrative overhead with multiple solutions;
- individual solutions are more vulnerable to exploitation;
- security gaps can occur when data moves between protection schemes.

Advantages of a PKI solution for the enterprise include:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- PKI allows positive identification between senders and receivers, computers, and applications through the use of digital certificates, providing an improved layer of authentication and access control;
- sensitive information is encrypted using public/private keys;
- PKI leverages an existing X.500 or LDAP directory to store public encryption keys;
- encryption keys are backed up (escrowed) so encrypted data can be recovered;
- PKI provides a legal basis for electronic business transactions (nonrepudiation);
- the PKI infrastructure is created based on a trust hierarchy;
- once the infrastructure is built, additional applications 'snap in';
- the infrastructure becomes cheaper the more it is used;
- the infrastructure provides a consistent interface for administration;
- properly implemented, the infrastructure handles new key 'rollover' and revocation of outdated keys;
- end-to-end security protection is possible.

Disadvantages of a PKI security infrastructure include

- initially expensive to install, configure and implement;
- proper implementation to ensure ease of use can be complex and time consuming;
- PKI is not commonly understood by developers at this time;
- lack of PKI deployment expertise.

Summary and Conclusion

PKI is a scaleable security solution consisting of a set of well-established techniques and standards that provides authentication, privacy, tamper detection and nonrepudiation. PKI uses public/private keys and includes the infrastructure to manage and maintain the keys, resulting in an electronic environment that is private, confidential, and legally binding. The security industry is moving to PKI and certificates for safe internet transactions. PKI is currently the only technology that provides the required level of data integrity and protection to support electronic commerce.

---

1 - Netscape Communications Corp. "How Digital Certificates Work."
URL: http://home.netscape.com/security/techbriefs/certificates/howcerts.html?cp=stbmid

2 - Netscape Communications Corp. "Digital Certificates".
URL: http://home.netscape.com/security/techbriefs/certificates/

3 – Entrust White Paper, Certificate Policies and Certificate Practice Statements, Sharon Boeyen, February 1997, p. 2 URL: http://www.entrust.com/resources/pdf/cps.pdf

4 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC2527, March 1999 URL: http://www.ietf.org/rfc/rfc2527.txt

5 – Computer Security Alert, May 2001 pg. 1, article by Rolf Oppliger, Ph.D.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Additional resources contributing to this paper include:

PriceWaterhouseCoopers, information on Security Architecture

The E-Business Advantage: Making the Most of PKI, February 2000, Hurwitz Group white paper

ComputerWorld security research links: Digital Certificates. URL http://www.computerworld.com/itresources/rclinks/0,4167,KEY73_RLI743,00.html

The PKI Page: URL http://www.pki-page.org/

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**