Global Information Assurance Certification Paper

Public Key Infrastructure

An Enabler for Secure Trusted Computing

Martin Serauskis

GSEC version 1.4b

Option 1

Abstract

The growth of the Internet has dramatically transformed the ways in which businesses communicate and conduct transactions. To leverage these changes many businesses have deployed partner extranets, e-commerce applications, employee intranets, virtual private networks, and messaging systems. A public key infrastructure (PKI) enables certificate management, authentication, data integrity, dynamic access control, confidentiality and non-repudiation for these technologies. PKI security mechanisms, such as key and certificate management, should be as simple as possible to facilitate. This improves the understanding of the mechanisms, avoids errors in configuration due to unnecessary complexity, and ensures use and compliance of the PKI system. Given the need for interoperability a PKI should be flexible and extensible to open standards, such as the Public-Key Infrastructure (X.509) (pkix) standards and Public-Key Cryptography Standards (PKCS), to ensure components will interact. Use of client and server certificates should be transparent to the end user. The services provided by the PKI can enable seamless authentication, encryption, and signing across all platforms and technologies. A PKI can provide security services for current and evolving Internet technologies, the management of trust models, and the redefinition of common business models.

What is a PKI?

A PKI is the comprehensive system that manages digital certificates. PKI is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet (Verisign). By managing keys and certificates through a PKI, businesses can establish and maintain a trustworthy networking environment. A PKI ensures a secure foundation of network security through the following key and certificate management services:

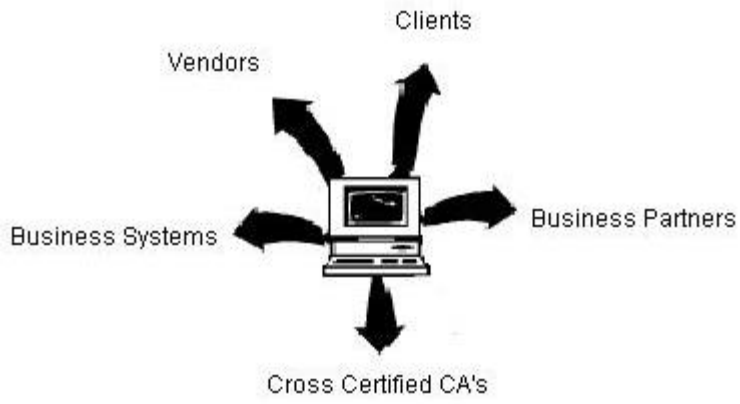
- Public Key Certificate Generation
- Certificate Repository
- Certificate Revocation
- Key Backup and Recovery
- Support for Non-Repudiation of Digital Signatures
- Update of Key Pairs and Certificates
- Management of Key Histories
- Support for Cross-Certification
- Directory Integration
- Client-Side software interacting with all of the above in a secure, consistent, and trustworthy manner

PKI Core

At the core of a PKI is the Certificate Authority or CA. A CA is a secure server that signs end-user certificates and publishes revocation data (Fratto, p.7). It represents the people, processes, and tools to create digital signatures that securely bind the names of users to their public keys. As long as users trust a CA and its business policies for issuing certificates, they can trust certificates issued by the CA.

The CA's signature on a certificate ensures that any tampering with the contents of the certificate can be detected easily. Since the integrity of a certificate can be determined by verifying the CA's signature, certificates can be distributed in a completely public manner. Users retrieving a public key from a certificate authority 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. 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 corresponding to the public key in the certificate may be compromised. Alternatively, an organization's security policy may dictate that the certificates of employees must be revoked in certain situations. An example is an affiliation change where a user changes their name due to marriage. In these situations, users of the system must be informed that continued use of the certificate is no longer considered trustworthy. The revocation status of a certificate should be checked prior to each use. As a result, a PKI can incorporate a scalable certificate revocation system. The CA must be able to securely publish information regarding the status of each certificate to an accessible directory. The combination of publishing and consistently using certificate revocation information constitutes a complete revocation system.

The use of a trusted certificate authority and PKI services enables the creation, maintenance, and enforcement of stronger trust models. The CA becomes the cornerstone of the trust model. Certificates allow businesses to build trust relationships with clients, business partners, systems, foreign CAs, and vendors for secure data communications such as e-mail. In addition, certificates provide the means to enforce the trust models through stronger authentication and encrypted communications.



PKI Trust Model

The certificates issued by the CA are the electronic counterpart to a driver license, passports, and membership cards. A digital certificate binds an identity to a pair of electronic keys that can be used to encrypt and sign digital information and authenticate a user.

A certificate typically contains the:

- Owner's public key
- Version
- Owner's name
- Expiration date of the public key
- Name of the issuer (the CA that issued the Digital ID)
- Serial number of the Digital ID
- Digital signature of the issuer

Not all certificates are the same.

The most widely accepted format for certificates is defined by The International Telecommunications Union, ITU-T (formerly known as CCITT), is X.509. The initial version of X.509 was published in 1988, version 2 was published in 1993, and version 3 was proposed in 1994 and published in 1995. Version 3 addresses some of the security concerns and limited flexibility that were issues in versions 1 and 2 (RSA Security).

The X.509 standard is important for two reasons:

- Defines a framework for authentication services
- Defines a standard certificate format

Example of a Certificate

There are generally two types of certificates: client side and server side.

Client side certificates can reside on the user's laptop and/or desktop or be stored on a hardware token, such as a smart card, that is accessible to an end user via password or PIN. The end user utilizes the certificate to authenticate with certificate enabled applications, encrypt and sign e-mail, and to encrypt data residing on the laptop or desktop.

Server side certificates reside within the certificate-enabled application such as a web server or firewall. The server side certificate is used to authenticate the server to users and encrypt and sign communications with the end client. It is imperative that the CA issues standards based certificates to ensure interoperability with other certificate enabled technologies.

To obtain a certificate one must be authorized by a Registration Authority or RA. The RA acts as the verifier for the certificate authority before a digital certificate is issued to a requestor. The user requests a certificate that is sent to the registration authority. At this point, an operator verifies the claimant's identity and the opportunity of the request. It is crucial for the verification to be operated through an acknowledged "secured" channel, be it face to face meeting, online verification, or telephone. Without it, a person could request and obtain a certificate on someone's behalf.

The PKI system should support a dual key pair architecture to provide encryption and digital signature functionality (Entrust). The encryption key pair allows users to encrypt data in order to keep the data private. The

signing key pair allows users to digitally sign data, which provides authentication (guarantees who signed the data), data integrity (recipients of signed data are alerted if the data has been tampered with), and non-repudiation (a user cannot deny having signed the data). The most effective way to provide these security features is to separate the encryption and digital signature functionality into two key pairs. This is because the encryption key pair and the signing key pair require separate considerations with respect to:

- creation, storage and backup requirements
- expiry and key lifetime requirements

Cryptographic key pairs and certificates should not be used forever. They must be updated over time, to ensure the certificate and keys are not compromised. The process of updating key pairs and certificates should ideally be transparent but at a minimum should be painless to the end user. 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. Key pairs must be updated when certificates are updated to ensure key roll over.

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. The key history must also be securely managed by the key backup and recovery system. This ensures that encrypted data can be recovered securely.

Businesses must be able to retrieve encrypted data when users lose their decryption keys. Therefore, a system for backing up and recovering the decryption keys is required. There are two reasons why key backup and recovery are important to a solid PKI.

The first reason is users forget passwords. Valuable information would be lost if there was no ability to securely recover keys. Furthermore, unless users know they can always recover their encrypted data (even if they forget their password), 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 (Entrust).

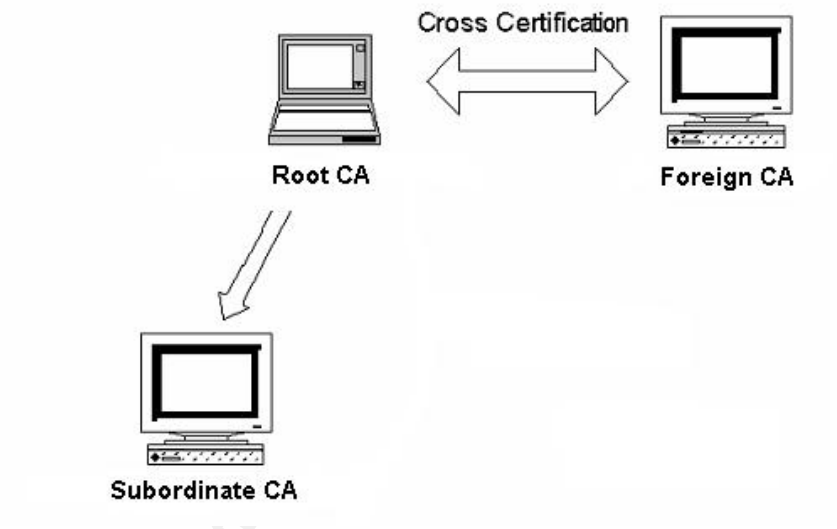
Since users keys were backed up they can be retrieved and used.

An integral part of a PKI is to integrate it with a directory. The Directory should be an LDAP (Lightweight Directory Access Protocol) compliant Directory. Since LDAP is an open protocol, applications need not worry about the type of

server hosting the directory. The Directory contains the name of each person in the CA domain, public certificates of each user, and certificate revocation lists (list of certificates that have been revoked). In cross-certified systems, the Directory also stores cross-certificates and revocation lists of foreign CAs.

Cross-Certification

Cross-certification is the process in which each CA signs another's certificate to signify trust (Fratto, p.7). Cross-certification extends third-party trust relationships between Certification Authority domains. For example one company and its trading partner, each with their own CA, may want to validate certificates issued by each other'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.



An Example of Cross Certification

As you can see in the picture above the Root CA is the trust anchor in the hierarchy. The Root CA manages the trust relationships among the CAs by establishing a single point of trust.

Certificate Policy and Practice Statements

A PKI must adhere to certain rules governed by its role in an organization. Two very important documents must be created that govern a way a PKI operates.

> A Certificate Policy is a named set of rules that indicates the applicability of a Certificate to a particular community and/ or class of applications with common security requirements. A Certificate Practice statement is a statement in which a CA employs in issuing and

revoking Certificates, and providing access to same. The Certificate Practice Statement defines the equipment and procedures the CA uses to satisfy the requirements specified in the Certificate Policy that are supported by it (Andersen).

These documents should be kept up to date and be readily available for potential cross certification opportunities and audit purposes.

PKI Offerings

A PKI leverages the use of security services across a wide variety of applications and platforms. PKI is one mechanism to provide the foundation for network security through these security services. These security services can be leveraged by new and existing technologies that require strong security in the following manner:

- Confidentiality - Data is obscured and protected from view or access by unauthorized individuals.
- Data Integrity – The verifier of a digital signature can easily determine whether or not digitally signed data has been altered since it was signed.
- Access Control - Data can only be accessed in a comprehensible form by those specifically identified when data is encrypted.
- Authentication – Users can securely identify themselves to other users and servers on a network without sending secret information (for example passwords) over the network.
- Non-Repudiation – Users who digitally sign data cannot successfully deny signing that data.

The PKI also leverages enterprise services to provide many offerings that can be integrated into a secure technology infrastructure. These offerings provide security functions that can seamlessly leverage this framework in order to accept and embrace businesses changing technology models. These PKI offerings include:

- Desktop Security
- Secure Messaging
- Secure Server Hosting
- Virtual Private Networking

- Developer/Application Toolkits

The inability to secure and protect confidential data on desktops and laptops is a widely understood problem. Protection of this information encompasses a wide variety of activities including automatic encryption/decryption of files and folders, restricting information from unauthorized individuals, secure deletion of sensitive information, and controlling access to the computer during startup and temporary absence. The PKI can provide these services while seamlessly and transparently integrating with a secure desktop solution.

The ability to securely communicate via E-mail between employees, clients, business partners, and vendors is becoming an essential business requirement. These communications can be provisioned via the PKI infrastructure that will integrate a businesses messaging solution with client and server certificates. These certificates, provided by the PKI, ensure communications across trusted networks such as an intranet and untrusted networks such as the Internet. Trust models should be developed to establish trust relationships between untrusted and trusted domains via some form of cross-certification, direct trust or third party trust. Direct trust implementation will be dependent upon the worldwide community adoption of the emerging PKI technology.

An important element of the business strategy is the establishment of public servers that provide knowledge sharing mechanisms. A PKI will provide enhanced security with the use of certificates for encryption and digital signatures and certificate based authentication. Users can utilize client side certificates to authenticate with the server. The server will only accept certificates that are signed by trusted CA's. If the end user presents a certificate from a trusted CA then the server will verify that the client certificate is valid by checking its revocation status. After certificate verification the user can only access the areas to which he has permission to as defined by the access control lists. All communications between the client and server are encrypted. The use certificate services can enable businesses to continue to provide security sensitive services to external clients and business partners such as private discussion areas.

The need to communicate with clients, business partners and vendors over public clients continues to increase. The issues with communication over external networks are authenticity of end entities and confidentiality and integrity of data. The use of Virtual Private Networks (VPN) enables the end entities to strongly authenticate with one another and encrypt all communications between themselves. VPNs can benefit from deploying a Public Key Infrastructure (PKI) to create, distribute, and track digital certificates on a per-user basis (Phifer). Each VPN entity will possess a certificate created by the CA and will enforce the trust models developed

by the PKI. For example trust can be established between the client side application and the firewall. The client side certificate used to authenticate the end user will be the same certificate utilized by the user to authenticate to each of the other certificate enabled applications.

End users can utilize their client side certificates to strongly authenticate with the proxy server for outbound services. A proxy server sits between a client application, such as a Web browser, and a server. It intercepts all outgoing requests to see if it can fulfill the requests itself. If not, it forwards the request to the server. The Proxy Server can utilize a server side certificate to authenticate with the end user for outbound services.

In addition to providing desktop security, e-mail security, public server hosting security, and virtual private networks, the PKI needs to integrate directly into custom designed and built applications so that security does not become a burdensome extra step in the process for creating and using information. Consequently, the PKI will provide a set of Application Programming Interfaces or API's that allow all custom applications to "plug in" to the infrastructure and utilize the services provided by the PKI.

Summary

PKI is essential for supporting evolving Internet technologies, the maturing of Industry standards, the distribution of models of trust, and the redefinition of business and technology models. These new models require the infrastructure to support the new methods of collaboration, coordination, and sharing among business partners, clients, and vendors. A PKI is an enabler for providing secure commuting technologies by providing the following:

- Enabling secure communications with business partners, clients, vendors, and other personnel.
- Creation of a core infrastructure for new and existing technologies that require strong security (Confidentiality, Access Control, Authentication, Data Integrity, and Non-Repudiation).
- Foundation for stronger security internally and externally for all services.
- Enable the creation and enforcement of trust models.
- Central and comprehensive certificate management
- Open standards based and interoperable with many existing and future technologies.

Once truly enterprise wide, the PKI can function as the enterprise service required for the implementation and enforcement of secure trusted computing. The PKI will be the central point of integration to secure the infrastructure and all communications amongst all clients, business partners, and vendors.

Sources

Andersen. "Certificate Policy." State of Illinois Digital Signature Project. 21 May 2002. URL: http://www100.state.il.us/tech/pki/cert_policy_definitions.cfm (5 Feb. 2003).

Verisign. "Understanding PKI." What is PKI?
URL: http://verisign.netscape.com/security/pki/understanding.html (3 Mar. 2003).

pkcs-editor@rsasecurity.com. "Public-Key Cryptography Standards."
URL: http://www.rsasecurity.com/rsalabs/pkcs/ (20 Feb 2003).

Sanchez, Eric Bhatt, Anand, Fenner, Joe. "Securing Your E-Business." Aug. 2001. URL: http://www.collectionsworld.com/08tec01.htm (22 Mar. 2003).

RSA Security. "5.3.2 What are the ITU-T (CCITT) Standards?"
URL: http://www.rsasecurity.com/rsalabs/faq/5-3-2.html (25 Feb 2003).

Hontañón, Ramón J. "Keeping PKI Under Lock and Key." 05 Oct. 2000. URL: http://www.networkmagazine.com/article/NMG20001004S0015 (17 Mar. 2003).

Fratto, Mike "PKI: Struggling for Interoperability." 07 Aug. 2000.
URL: http://www.networkcomputing.com/1115/1115f2.html (05 Feb. 2003).

Phifer, Lisa "VPNs: Virtually Anything?" 12 April 2001.
URL:
http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci540868,00.html (20 Feb. 2003).

Scheier, Robert "Digital Signatures: Use with care, if at all." 20 Feb. 2002.
URL:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci803325,00.html (15 Feb. 2003).

Baczewski, Dr. Philip "The Network Connection." URL:
http://www.unt.edu/UNT/departments/CC/Benchmarks/julaug94/bitcon.htm (25 Feb. 2003).

Entrust "Key Update and the Complete Story on the Need for Two Key Pairs." August 2000. URL: http://www.entrust.com/resources/pdf/2keypairs11.pdf (15 Feb. 2002).

PKIX Working Group "Public-Key Infrastructure (X.509) (pkix)." 14 Jan. 2003.
URL: http://www.ietf.org/html.charters/pkix-charter.html (20 Feb. 2003).

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event