Global Information Assurance Certification Paper

Public Key Infrastructure (PKI) – 101

Ellen Kennedy
March 15, 2001

Introduction

Digital certificates are managed through an architecture called public key infrastructure (PKI). A digital certificate can be thought of as an online identification or driver's license. The purpose of a digital certificate is to establish the basis for asymmetric encryption.

Asymmetric encryption uses two keys, a private key and a public key. A public key is bound to the owner's digital certificate and is available for anyone to use. A private key is ideally protected by and available only to the owner of the key. Asymmetric encryption allows a user to encrypt a message with their private key and the recipient to decrypt it using your public key. The public key can be used to decrypt any messages encrypted by the private key. [1] That is, a message encrypted ($M_{encrypted}$) with the private key ($K_{private}$)

$$M_{encrypted} = K_{private}(M)$$

can be decrypted (M) with the public key (K_{public})

$$M = K_{public}(M_{encrypted})$$

If a message is altered after it has been encrypted, the message cannot be decrypted. This provides the basis for non-repudiation and integrity assurance. Non-repudiation is the ability to establish the source of an interaction so that the claim that a user did not create the interaction cannot be upheld. Integrity assurance is the ability to ensure data is valid and has not altered.

PKI is made up of technology, standards, and policies. This paper will discuss the components of the PKI and the critical pieces that need to be in place to establish a level of trust.

Components of a PKI

While PKI implementation is complex, PKI processes and procedures are logical and often common sense. Most are familiar with portions of the user certificate request process, therefore we will use this process to identify some of the major components of a PKI.

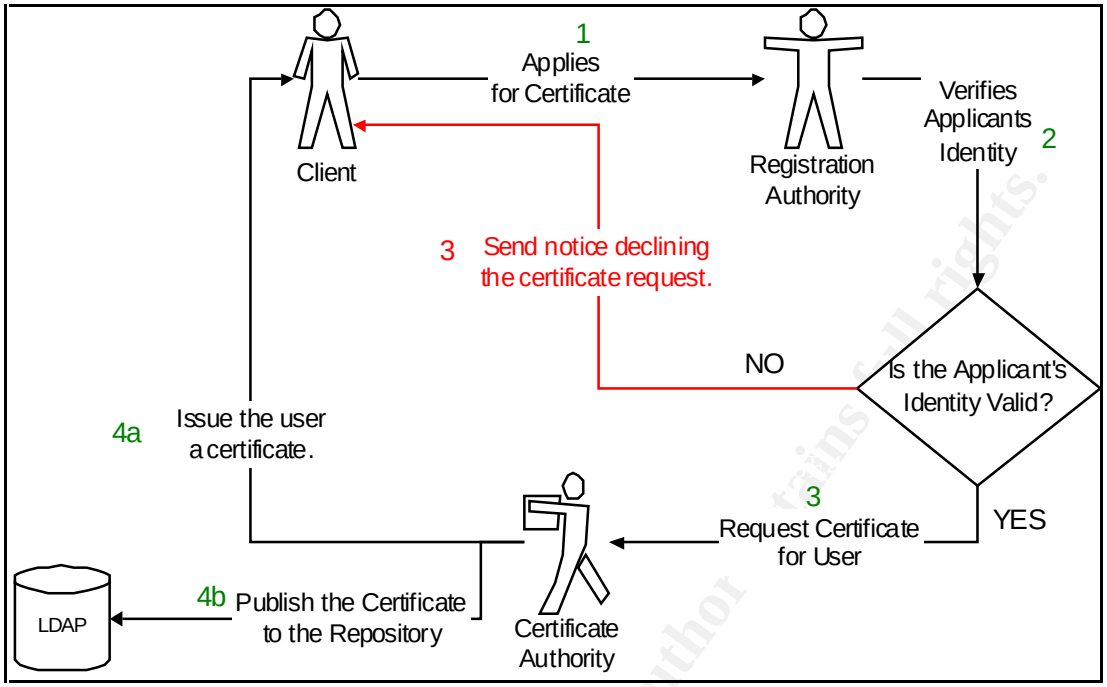

Diagram 1: Requesting a Certificate

1) An individual would like to obtain a digital certificate. The individual fills out a web-based form and submits it. The request is added to a queue of certificate requests.

2) The Registration Authority (RA) is responsible for confirming the identity and authorization of the individual to obtain a certificate. The RA is an optional component on a PKI. Smaller scale PKIs uses the Certificate Authority (CA) to perform this function. Ultimately, the CA has the responsibility of ensuring the individual issued the public key is whom they claim to be. In order to achieve this level of identification, an out-of-band process must be established. The approach to this out-of-band process differs from PKI to PKI. A High assurance PKIs may require an applicant to go to a local registration authority (RA) and display a physical form of identification, for instance a passport or driver's license. Low-assurance PKIs take approaches to validate pieces of information regarding the applicant. Verisign (www.verisign.com) offers three classes of certificates based on the level of validation required to obtain the certificate.[2]

3) The RA confirms the identity of the individual to the CA and requests a certificate on behalf of the user.

4) The CA validates the requests from the registration authority.
   a) The CA signs the certificate with its private key and issues the individual the certificate.

b) The CA then publishes the public key to the appropriate LDAP (Lightweight Directory Access Protocol) directories or alternate data stores.

The CA can be thought of as a digital notary. If the notary is corrupt then the identification cannot be trusted. It is often assumed that a level of security is reached if someone has implemented a PKI or holds a digital certificate. This assumption is inaccurate. Technology alone does not achieve security. The certificate policy specifies the levels of assurance the PKI is to provide and the Certificate Practice Statement (CPS) specifies the mechanisms and procedures to be used to achieve a level of assurance.

The PKI policy exists within the overall security policy of an organization. The PKI policy defines the requirements of what is to be done to maintain the security of the PKI. How those requirements are met is defined in the certificate practice statement (CPS). The CPS includes procedures to be followed to provide a level of assurance for the PKI. Development of the CPS is the most time-consuming and essential component of establishing a PKI. Issues such as those documented in Ellison and Schneier's paper *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure*[3] can and should be addressed in the PKI policy and CPS. The planning and development of the certificate policies and procedures will require the definition of requirements, such as key escrow, and processes such as certificate revocation.

Key escrow is a very important and controversial aspect of PKI. Key escrow is the storage and retrieval of private keys to recover data in the absence of the private key owner. Key escrow goes against the very idea of a private key. The private key may be accessed by more than the owner of the key and thus lessens the case for non-repudiation. While key escrow is often frowned on, it is often considered a necessary evil. Requirements for key escrow/recovery systems may stem from customer support, legal or policy requirements. International PKI implementations may require key escrow to comply with government and law enforcement restrictions. Key escrow processes/policies normally require two individuals to obtain a key. The process can be related to the missile launch process, two keys entered at a distance from each other, simultaneously to obtain the forbidden.

Another challenging issue surrounding PKI is the implementation of a certificate revocation method. While key escrow is an optional feature, certificate revocation is a necessary part of the certificate process. Authentication of clients and servers requires a way to verify each certificate within the chain, as well as a way to determine if a certificate is current or if it has been revoked. Some reasons why a certificate would be revoked are key compromise, loss, modification of privileges, misuse, or termination. It is essential that near real-time revocation of certificates is achieved. The most commonly used method of certificate revocation is through a Certificate Revocation List (CRL). This method proves challenging due to the challenges in distributing large lists in near-real time.

> A CRL is a list of certificate serial numbers signed by the CA. Every certificate has a unique serial number assigned to it by the CA; this number is part of the signed certificate and cannot be altered. When an application attempts to validate the certificate, it needs only to look up the serial number in the CRL associated with the signing CA.[4]

In practice, the implementation of a successful certificate revocation process has been a major challenge. While the challenges surrounding certificate revocation are interesting, they are out of scope of this paper.

Using the Certificate

Presently the primary use of digital certificates is to implement Secure Socket Layer (SSL). A smaller number of applications are beginning to use digital certificates for authentication of the user. An even smaller number of applications use the information (attribute name-value pairs) contained within the digital certificates DN for authorization decisions.

Prior to determining how the certificate will be used, it is important to understand the validating information contained within a certificate. Diagram 2 displays a subset of a server certificate's Distinguished Name (DN) attribute values.

Diagram 2: Viewing Server Certificate Information

The important things to notice in the certificate details are:

- Who the certificate was issued to (red arrow – top left)
- Which certificate authority issued the certificate (blue arrow – top right)
- When the certificate expires (green arrow – lower right)

Diagram 3: Viewing Personal Certificate Information

Diagram 3 displays a personal certificate. Please note the disclaimer 'Persona Not Validated' which indicates there was no out-of-band contact with the individual and therefore this certificate should not be considered a high assurance form of identification.

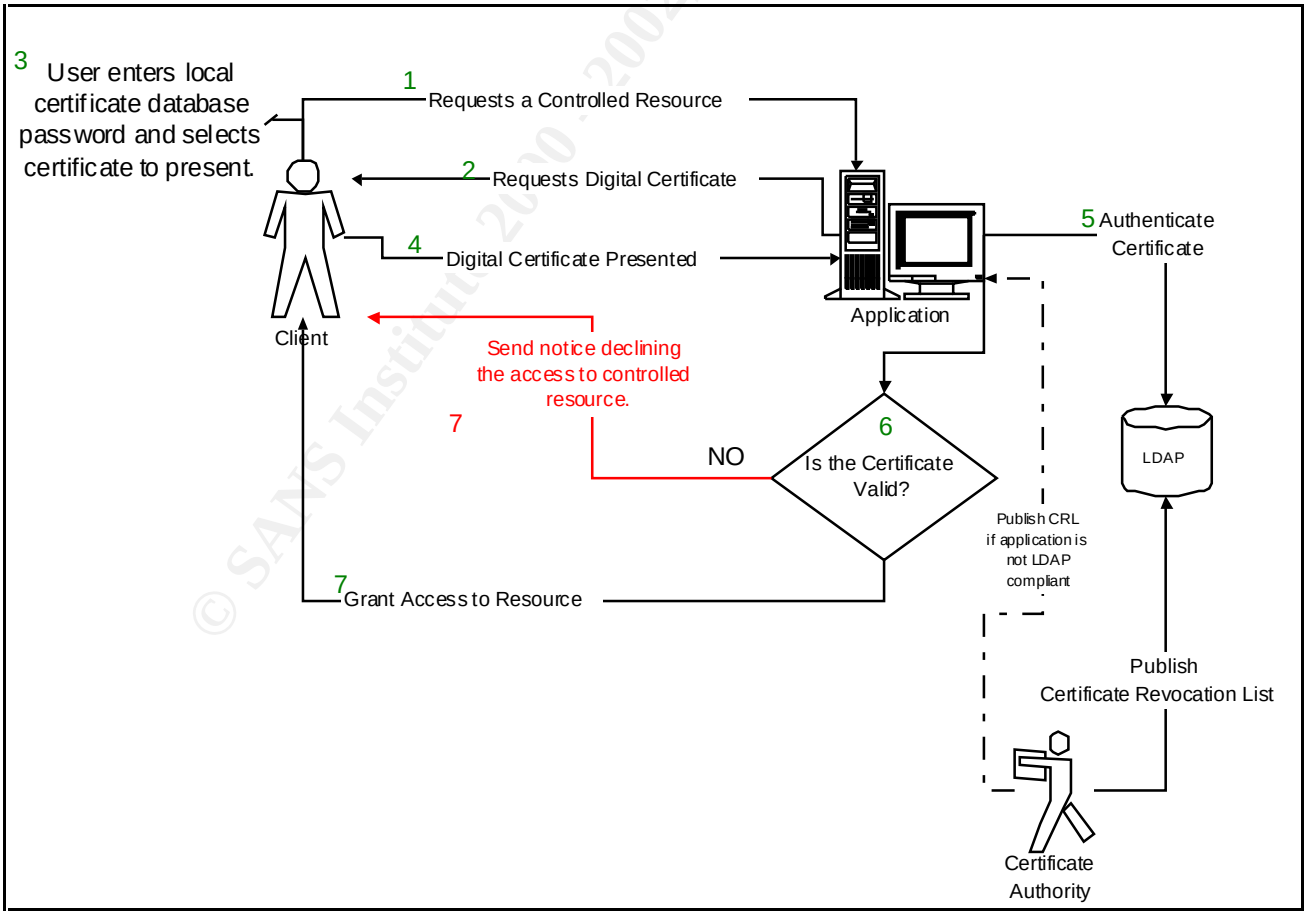

Diagram 4: Requesting a Secured Resource

Regardless of how the certificate is used there are steps that must be taken to validate the certificate (reference Diagram 4). When a certificate is presented, the DN is used to lookup the certificate containing the public key that signed the certificate. If the presented certificate is valid, the certificate used to verify the signature must be checked. If the signing public key is not trusted the process continues until a trusted certificate is read. If the verifying certificate is trusted, the certificate is deemed valid and the Certificate Revocation List (CRL) is checked and if not revoked the certificate is used. If another CA signs a CA's root certificate, it is part of what is known as a CA chain or hierarchy. If CA certificate is self-signed, the CA is known as a stand-alone CA.[5] The stand-alone CA is PKI's solution to the chicken and egg dilemma.

Hosting versus Hosted

Establishing a PKI is not as easy as hosting a web server. The root certificate signs all other certificates, thus the golden apple, and must be protected at all costs. A level of security above and beyond the typical hosting facility must be reached to protect the CA. Qualified PKI implementers/integrators are very difficult to find.

An alternative to establishing an in-house PKI is to out-source the hosting. This has many advantages to it. Many times the scope of a PKI effort is underestimated. The level of security and support required for a high assurance PKI cannot be met by organizations. A trusted third-party can be advantageous from many aspects. Major PKI hosting providers, such as Baltimore Technologies and Entrust, have already established:

- Policies, procedures, and CPSs that vary in levels of assurance.
- Secure environments.
- Skill sets to establish and maintain a high security level.
- Audit and certification methods.
- Customer support and help desks.

The option of using a hosted PKI should be considered from business, financial, legal, marketing, and operational standpoints.

Business:	Can the organization establish a PKI within the required timeframe? Is the organization willing to establish a PKI support structure/organization?
Financial:	Is it likely, due to the complexity, that a ROI will be realized?
Legal:	Is the organization willing to take the liability risks inherent in PKIs?

Marketing:	Can it be used as a marketing point when targeting eMarketplace prospects?
Operational:	Can we hire, contract or establish the skill sets required to establish and maintain the PKI?

Conclusion

A PKI can provide the level of trust necessary to achieve consumer confidence while providing means to achieve message integrity and non-repudiation. A PKI deployment is complex and challenging from a business perspective as well as a technical perspective. The key to deploying a successful PKI is sound planning; do not underestimate the effort or the required security level for a PKI. It is essential to attain experienced PKI professionals to guide an organization through the process of deploying a PKI. The experienced PKI professional will be able to provide insight and value that one cannot obtain from books.

References

1) Luotonen, Ari "Web Proxy Servers, 1/e: Encryption and Authentication Security | Page 1". April 2, 1999. URL: http://www.networkcomputing.com/netdesign/1007part2a.html

2) Verisign, Inc.. CPS Section 5: "Validation of Certificate Applications". May 30, 1997. URL: http://www.verisign.com/repository/CPS/CPSCH5.HTM

3) Ellison, Carl and Schneier, Bruce. "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure". Computer Security Journal, v 16, n 1, 2000, pp. 1-7. URL: http://www.counterpane.com/pki-risks-ft.txt

4) Fratto, Mike. (June 26, 2000) "Certificate Revocation: When Not To Trust" URL: http://www.networkcomputing.com/shared/printArticle?article=nc/1112/1112ws1full.html&pub=nwc

5) Cearley, Kent and Winsor, Lindsay. "Securing IT Resources with Digital Certificates and LDAP". URL: http://www.cu.edu/%7Esecurity/pki/Cause97.htm

6) Public Key Infrastructure Steering Committee, Government Information Technology Services Board, Office of Management and Budget. "Access with Trust". September, 1998. URL: http://www.cio.gov/fpkisc/documents/AccessWithTrust.pdf

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
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 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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 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
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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