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.

Key and Certificate Management in Public Key Infrastructure Technology

The intent of this paper is to provide an overview and briefly discuss the various phases involved in Key and Certificate management. Anyone interested in understanding this specific process will find this paper useful. A basic understanding of PKI Technology is assumed.

Copyright SANS Institute

Author Retains Full Rights

AD

Key and Certificate Management in Public Key Infrastructure Technology

Sriram Ranganathan

August 20, 2001

Introduction

Key and Certificate life cycle management is an essential and crucial process in Public Key Infrastructure technology. There are several stages involved in this process and how it is managed will determine the success or failure of a particular deployment whether using a vendor's services and expertise or building one's own (a rare scenario).

Thus, it is necessary to gain a good understanding of this aspect of PKI, to be able to participate and contribute to a successful implementation.

Audience

The intent of this paper is to provide an overview and briefly discuss the various phases involved in Key and Certificate management. Anyone interested in understanding this specific process will find this paper useful. A basic understanding of PKI Technology is assumed.

Ample references to some excellent resources are cited at the end and readers are encouraged to refer to them for additional details.

Overview

The Key and Certificate Management process, hereinafter K/CM, distinctly differs from the actual usage. Whereas usage deals with the operations involved in creating and verifying digital signatures using the key pair and encrypting or decrypting messages, K/CM deals with the administration tasks such as creation, publication and management of keys and certificates.

All parties (CAs, RAs, vendors, end-entities and users) involved in the infrastructure operation have their own set of individual and shared responsibilities during the various phases.

Key(s) and Certificate(s)

Throughout this paper, the term *key* specifically refers to the *public key* and *certificate* refers to the *X.509 Version 3.0 certificate,* unless otherwise noted.

Basic Requirements in the Key/Certificate Management Environment

A comprehensive K/CM requires (a) an automated, seamless process with minimum end-entity intervention, (b) a well-defined and audited operations procedure with appropriate controls in the CA's environment (c) a coordinated approach among the

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

different players (CAs, RAs and the end-entity) and (d) the secure operation of the client-end software that interacts with several other components in the process.

Life Cycle Management

The following three main phases define the key and certificate life cycle management process [1]:

- Set-up or Initialization
- Administration of Issued Keys and Certificates and
- Certificate Cancellation and Key History / Archival services

Each one of the above phases in turn consists of several sub-phases. Depending on the type and scale of a particular deployment the requirements vary and hence the associated services. However, a PKI should be able to offer all these as part of a comprehensive, scalable solution.

- The End-entity set-up and initialization consists of the following steps (usually in sequence):

  a) Registration
  b) Key Pair Generation
  c) Certificate Creation
  d) Key/Certificate Distribution
  e) Certificate Dissemination and
  f) Key Backup

Registration process starts when an end-entity approaches an RA/CA with a specific request. Upon verification of the identity and credentials, the RA, if involved, forwards the request to the CA and the entity is appropriately registered. This process also involves a shared-secret assignment to the end-entity to authenticate it to the CA at a later stage within the initialization phase.

Depending on the Certificate Practice Statement, Certificate Policy and privileges associated with the requested certificate, the identity verification may require a physical appearance and/or submission of appropriate authorization documentation.

Key Pair Generation involves the creation of one or more key pair(s) using well-established algorithms – like RSA, DSA or the more recent Rijndael algorithm popularly known as Advanced Encryption Standard or AES.

Dual or multiple key pairs are often utilized to perform different roles to support distinct services. For e.g. one key pair may be used for signing and another for encrypting messages. A key pair can also be restricted by policy to certain roles based on usage factors like type, quantity, category, service and protocol. For instance a certificate and

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

therefore the key can be restricted to purchase computer hardware worth only a certain dollar amount.

Multiple key pairs usually require multiple certificates, due to the fact that the X.509 certificate format does not support multiple keys. Multiple certificates can contain the same public key, although this is not advisable due to the inherent security risks (substitution attacks) associated with erroneous privileges for the same key in different certificates.

An important consideration with respect to multiple keys is the location of key generation and storage facility. Especially within the context of keys being used for non-repudiation services, the owner of the private key is entrusted with generating and storing such keys. In other scenarios performance, usage, legalities and algorithm specifications are the factors affecting the choice of location.

Certificate C**reation** responsibility is with the CA regardless of where the key is generated. A certificate binds an *entity's unique distinguished name (DN)* and other additional attributes that identifies an entity with a *public key associated with its corresponding private key.* The *entity DN* can be an individual, an organization or organizational unit or a resource (web-server/site). Creation and issuance of certificates is governed by appropriate certificate policies. The public key needs to be transmitted securely to the CA in case if it was generated elsewhere by a party other than the CA. Certificates can be used to verify a digital signature or for encryption purposes.

A typical X.509 Certificate contains several standard fields and additional policy-related extension fields. There are several groups that are working on the standards for a specific application area, and hence there exists a number of certificate profiles or formats for different requirements. SPKI, PGP and SET formats are popular versions. Most of them derive from the X.509 Version 3.0 specification. Though certificates enable the PKI, there are several privacy issues surrounding an individual's certificate usage [2].

Requests and subsequent d**istribution** of keys and certificates require secure transmission modes. The IETF PKIX working group has defined management and request message format protocols (CMP / CRMF) specifically for this purpose. Alternatives such as Public Key Cryptography Standards (PKCS) also exist.

Dissemination involves securely making the certificate information available to a requestor without too many hassles. This is done through several techniques, including out-of-band and in-band distribution, publication, centralized repositories with controlled access, etc. Each has its own benefits and drawbacks. Depending on the client-side software, certificate usage, privacy and operational considerations, the information requirements and dissemination method varies. Several protocols are available that facilitate secure dissemination of certificates and revocation information.

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

Enterprise domains widely use LDAP repositories with appropriate security controls along with in-band distribution through S/MIME based e-mail. This hybrid approach maximizes the benefits. Even within the repository model several configurations like direct-access, inter-domain replication, guard mechanism, border and shared repositories are possible and often used.

Key Backup is an important service that is provided either by the CA or a trusted third-party. In some cases the end-entity also engages in backing up its keys but this is generally not reliable due to the complexities involved. Except for keys that are used for non-repudiation purposes, all other keys are usually backed up. Key backup is the only solution that addresses lost keys and helps recover encrypted data and is an essential element of business-continuity and disaster recovery planning.

Key backup is different from key escrow, in that the backup is not meant for a trusted third party access to encrypted data, be it law enforcement or other government agencies. Key escrow and recovery has several implications on individual privacy. This is neatly brought out by a 1997 report published by a group of renowned scientists in cryptography, titled "The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption". [http://www.cdt.org/crypto/risks98/]

- The issued keys and certificates need to be administered properly after the initialization phase. This phase involves the following:

  a) Certificate Retrieval and Validation
  b) Key Recovery and Key Update

As the name implies, **Certificate Retrieval** involves access to certificates for general signature verification and / or for encryption purposes. Retrieval is necessary as part of the normal encryption process for key management between the sender and the receiver and in the case of verification, as a reference where the certificate containing the public key of a signed private key is retrieved and sent along with the signature or is made available on demand. It is imperative to have an easy and simple mechanism to retrieve certificates. Otherwise the whole infrastructure will not make much sense.

Validation is performed to ensure a certificate is issued by a trusted CA in accordance with appropriate policy restrictions and ascertain its integrity and validity (whether expired/revoked) before its actual usage. In most cases all of this is achieved transparently by the client-software before cryptographic operations using the certificate are carried out.

Key Recovery complements the key backup process. The recovery of backed up keys allows access to encrypted messages and avoids permanent loss of business-critical information. This process is also automated to minimize user intervention and errors.

Key Update is the process of issuing new keys and the corresponding certificate prior to an expiration of an existing certificate and its keys. Ideally key updates are

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

recommended to occur automatically and transparently when a key approaches three-quarters of its intended lifetime to facilitate smooth transition and prevent service breakdowns. Key Update is a much simpler process as opposed to certificate update, which requires starting all over.

3. The final phase in the life cycle management deals with cancellation procedures. This includes:

a) Certificate Expiration
b) Certificate Revocation
c) Key History
d) Key Archive

Certificate Expiration occurs when the validity period of a certificate expires. Every certificate has a fixed lifetime and expiration is a normal occurrence. Upon expiry a certificate can be renewed provided the keys are still valid and remain un-compromised. As part of the renewal process, a new certificate is generated with a new validity period. In this case, the same public key is placed into the new certificate. Alternatively, a certificate update can also be done which is essentially a new certificate, with new key pair and new validity period. Certificate update, like key update must take place before the certificate expires. In this case, the policy restrictions may remain the same as of the expired certificate.

Certificate Revocation implies the cancellation of a certificate prior to its natural expiration. Several situations warrant revocation. For instance, it could be due to privilege changes for the certificate owner, key loss due to hardware failure, private key compromise, etc. Cancellation per se is an easier process when compared to properly notifying and maintaining the revocation information. The delay associated with the revocation requirement and subsequent notification is called revocation delay and this is clearly defined in the Certificate Policy as it determines how frequently or quickly the information is broadcast and used for verification.

There are several ways in which the notification is accomplished. The primary method is through Certificate Revocation Lists (CRL). There are several flavors of CRLs including Delta CRLs, Partitioned CRLs, Indirect CRLs etc. Essentially CRLs are data structures containing revoked certificates. To maintain integrity and authenticity CRLs are signed. Other methods include CRL Distribution points, Certificate Revocation Trees (CRTs), and Redirect/Referral CRLs.

Performance, timeliness and scalability are some of the key factors that influence the revocation mechanisms.

Instant access methods through Online Certificate Status Protocols (OCSP) are also available. However, there is no guarantee that the 'real-time' service is indeed providing 'fresh' status. It is possible that the service might respond based on poorly updated database.

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

There are also exceptions where such notification is deemed unnecessary. Two such exceptions involve short certificate lifetimes and single-entity approvals. In the former case, the accepted revocation delay might be more than the certificate lifetime and hence may not require revocation at all. In the latter case, as requests are always approved by a single entity it may not be necessary to publish revocation separately. One e.g. involves web-based credit card authorizations where a relying-party (merchant, in this case) processes the charge by verifying the account with the issuer bank and the revocation information can be obtained at that point directly. Here the revocation was verified through a different approach other than CRLs or OCSP.

Key History deals with secure and reliable storage of expired keys for later retrieval to recover encrypted data. This process applies more to encryption keys than signing keys. The storage facility is usually located at the end-entity premises. CAs and third parties may also assume responsibility for this service.

Key Archive is a service typically undertaken by a CA or third-party to store the keys and verification certificates for an extended period of time. When used with additional services like time stamping and notarization, key archive serves audit requirements and dispute resolution purposes. For e.g. it can be used to verify a digital signature created using keys that has subsequently expired.

Evaluating CAs and PKI Vendors

CAs and third party vendors form the backbone of a typical PKI implementation and therefore it is imperative to assess and evaluate them to ensure they have proper controls in place.

One initiative in this area is a consulting and certification process called WebTrust for CAs Program[3], a joint effort developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) to audit, evaluate and certify a CA, using independent consulting agencies. The goal is to reduce the business risks and provide an assurance to the customers. This also helps in differentiating a CA from its competitors.

This program is consistent with the American National Standards Institute's PKI Practices and Policies Framework (ANSI X9.79) standard for financial institutions, containing a set of broadly accepted criteria including Certification Authority Control Objectives that serve as a reference for the assessment of CAs operations. There are also several other co-operative efforts under development by organizations like IETF and ISO.

Summary

Setting up an enterprise Public Key Infrastructure is an extremely complex task with enormous demands on financial, human, hardware, and software resources, in addition to the time-factor.

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

It is very important to understand the concepts, processes and products involved, and ask pertinent questions right at the beginning.

In addition to basic support, training and documentation issues some of the areas that need to be explored in detail include, but not limited to [4]:

- Support for standards, protocols, and third-party applications
- Issues related to cross certification, interoperability[5] and trust models
- Multiple key pairs and key pair uses
- Toolkit to PKI-enable applications and client-side software availability
- Impact on end-user for Key Backup, Key/Certificate Update and Non-repudiation services
- Performance, scalability and flexibility issues regarding distribution, retrieval and revocation systems
- Physical access control to facilities

Certificate Policy (CP) and Certificate Practice Statements (CPS) are two primary documents that address the intended use of the certificates and operating procedures of a CA and/or PKI, respectively. Guidelines for writing these documents are defined in IETF RFC 2527[6.] Having a good policy framework is a deciding factor for the successful deployment and operation of PKI.

Most of the core standards related issues have been addressed by research and standards organizations like IETF. The security awareness in the IT industry has grown considerably and the business-community is beginning to understand the seriousness of security implications and the benefits of PKI. Even the governments of many countries, for their part, have framed e-commerce laws. Some of the key issues that remain to be addressed include making existing applications PKI-aware, skills training, and CA-CA cross-certification. With the growth in e-commerce, PKI deployments are expected to grow significantly over the next couple of years despite questions on standards, policies, products, legalities and return on investment, aside from the technology itself.

References

1. Understanding Public-Key Infrastructure Concepts Standards and Deployment Considerations, August 1999 - Carlisle Adams, Steve Lloyd - [Primary source for this paper]

2. Private Credentials, Zero-Knowledge Systems, November 2000 http://www.zks.net/media/credsnew.pdf

3. WebTrust sm/tm Program For Certification Authorities August 25, 2000 http://ftp.webtrust.org/webtrust_public/certauth_fin.doc

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

4. Technical PKI Evaluation Guide, Entrust Inc. December 1998
http://www.entrust.com/resources/pdf/pkiguide.pdf

5. PKI Interoperability Framework, March 2001
http://www.pkiforum.org/pdfs/PKIInteroperabilityFramework.pdf

6. IETF RFC 2527 Certificate Policy and Certification Practices Framework, March, 1999 http://www.ietf.org/rfc/rfc2527.txt

7. The PKI Page – by Stefan Kelm contains links to PKI sites 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 22nd, 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**