Summary of Protocols for PKI Interoperability

ATTENTION

1. Enterprise Environment

The Enterprise environment is typified by organizations seeking to provide consistent, transparent security across all end-user applications. The organization has the greatest amount of control in this environment, allowing it to leverage investment in interoperable PKI solutions for both infrastructure and end-users.

Certificate Generation - X.509, PKIX Part 1

X.509 defines the format of a public key digital certificate as well as Certificate Revocation Lists (CRLs). PKIX Part 1 provides profiles for each of these two standards.

Certificate Distribution - Lightweight Directory Access Protocol (LDAP)

LDAP defines the protocol used to publish and access digital certificates and CRLs from a repository.

Certificate Management - PKIX Certificate Management Protocol (PKIX-CMP)

PKIX-CMP defines the protocol for managing keys and certificates. Extends beyond simple certificate request to support PKI lifecycle functions required in the Enterprise.

2. Inter-Enterprise Environment

The Inter-Enterprise environment is typified by organizations seeking to provide trusted and secure means for business-to-business electronic commerce. The organization has control over its own resources, both infrastructure and end-user, that must interoperate with others' PKIs.

Certificate Generation - X.509, PKIX Part 1

These standards also apply to cross certificates and CRLs used in establishing one to one or hierarchical trust between enterprises.

Certificate Distribution - LDAP, S/MIME

LDAP provides the access protocol for enterprises wishing to share full or partial certificate repositories. S/MIME defines a protocol that is used for the direct exchange of digital certificates between end users.

Certificate Management - PKIX CMP, PKCS #7/#10

PKIX-CMP provides protocols for the request and management of cross-certificates, as well as keys and certificates as in the Enterprise model. PKCS #7/#10 provides protocols for requesting and receiving keys, certificates and cross-certificates without any management once created and distributed.

3. Consumer Environment

The Consumer environment is typified by organizations seeking to enable electronic commerce with consumers over the Internet. While controlling its infrastructure, the organization must interoperate with consumers using a wide variety of applications, typically web browsers and associated e-mail.

Certificate Generation - X.509 v3

These standards provide the profile definition of a public key digital certificate. While no standards have been approved for revocation checking in this environment, proposed schemes (ex. OCSP) are under review.

Certificate Distribution - S/MIME

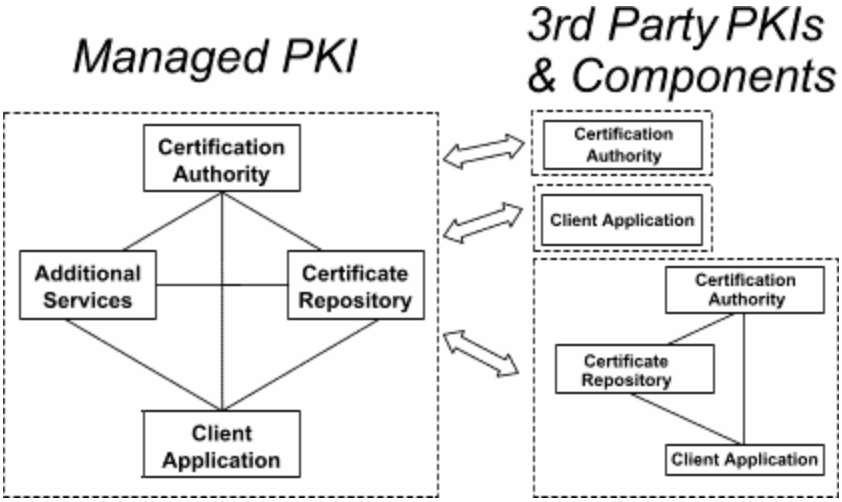
Distribution of certificates in this environment is currently limited to direct user to user communication with S/MIME.

Certificate Management - PKCS #7/#10

PKCS #7/#10 supports certificate request and receipt but does not provide for any key or certificate management. While no standards have been approved for key and certificate management in this environment, proposed schemes (ex. PKIX-CMC) are under review.

4. Elements of PKI Interoperability

Regardless of the environment in which it operates, a Managed PKI is made of up several components that must interoperate. As shown in the figure below, these include interfaces within a single PKI as well as to external environments.



A brief summary of the purpose of each component is as follows:

- Certification Authority. The Certification Authority (CA) represents the trusted third party that issues keys and certificates to end users and manages their life cycle including generation, revocation, expiry and update.
- Certificate Repository. The Certificate Repository provides a scalable mechanism to store and distribute certificates, cross-certificates and Certificate Revocation Lists (CRLs) to end users of the PKI.
- Client Application. The Client Application is the end user software that requests, receives and uses public key credentials for conducting secure electronic commerce.
- Additional Services. Additional services are required by a Managed PKI that will interoperate with the other three components listed. These provide particular services that enable many electronic commerce applications. Typical services include Timestamping, Privilege Management, Automated Registration Authorities, etc…

Because of their central role in a Public Key Infrastructure, regardless of the environment, these components must interact and interoperate. These operations can be summarized as follows:

- Certificate Generation. This includes the generation of public key digital certificates and Certificate Revocation Lists with a defined format and syntax to enable interoperability with other client applications and other PKIs. Also included is the generation of cross-certificates used to interoperate between Certification Authorities.
- Certificate Distribution. In order to conduct public key operations, one user must access another's certificates as well as associated CRLs. Accordingly, there must be a common protocol to allow for access to other user's certificates and associated revocation information.
- Certificate Management. Managing keys and certificates represent the most common PKI operations. Protocols for requesting, renewing, backing-up,

restoring and revoking keys and certificates require interoperability between client applications and the Certification Authority.