3/6/07

PKI & X.509

PKI

Components necessary to distribute public keys.

Alice - signs a certificate for Bob's name, public key.
Monopoly Model

Single Certificate Authority
Trust Anchor

Monopoly + Registration Authority (RA)

CA + RA
Security check identities
Delegated CAs

RA  \rightarrow CA_1 \rightarrow RA

Alice  \rightarrow CA_2  \rightarrow CA_3 \rightarrow CA_4  \rightarrow RA  \rightarrow RA  \rightarrow Bob

Oligarchy

Multiple Anchored CAs
Anarchy Model

Any body (with some restrictions) can create certificate & deposit

Name Constraints

CA can be trusted for a subset of certificates

Top-down with name constraints
Bottom-up with name constraints

Relative Names
X.509

Directory - Depository

PK certificates

Standard. (1988)

(2000)

RSA

Certificate - Signature

Hash function

Flexibility - Specify what you are using

versions
Certificate

Bob — Subject
— public key information
period of validity

issuer — CA + RA
Signature of issuer.

Unique identification of
Subject
issuer.

(X.500)

Extensions —
\[ CA \leftarrow A \rightarrow = CA \left( V, SN, AI \right) \]

\[ A \rightarrow B \]

\[ A \rightarrow A \times_1 \times_2 \times_3 \ldots \times_n \rightarrow B \]

Revoked.

\[ CA \rightarrow \text{Revoked list} \]

Date of creation.
List of revoked certificates.