3/6/07

PKI & X.509

PKI

Components necessary to distribute public keys.

Alice – signs a certificate for Bob
name, public key.

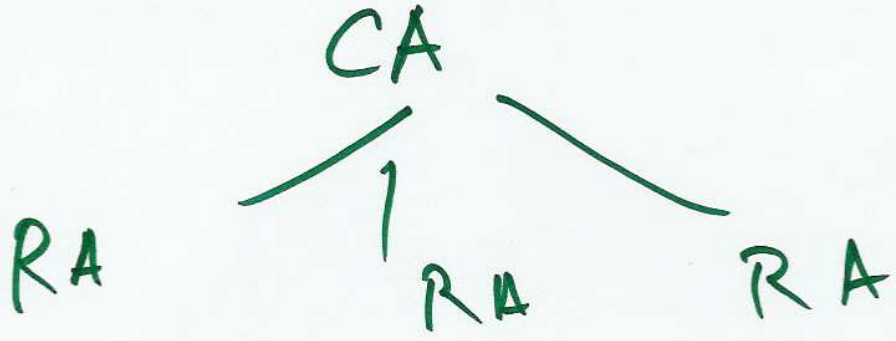
Monopoly Model

Single Certificate Authority
trust Anchor.

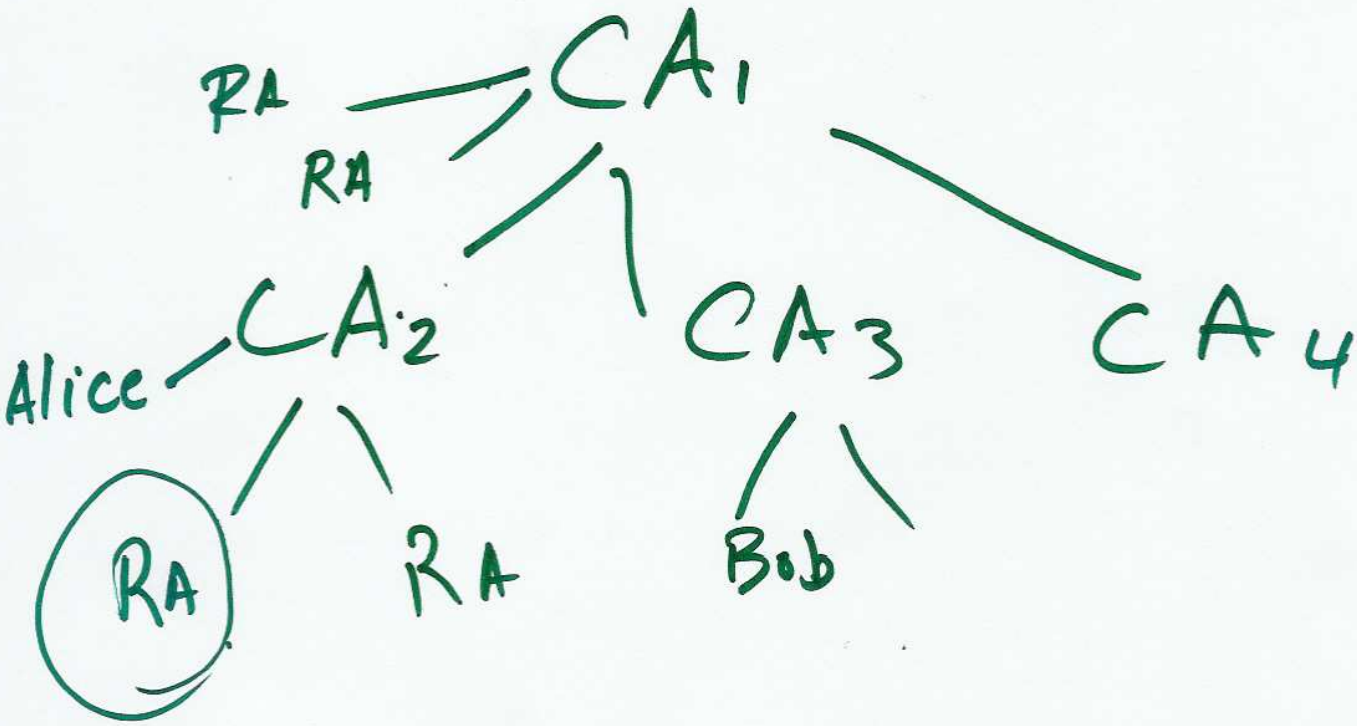
Monopoly + Registration Authority (RA)

CA + RA

security check identities



Delegated CAs



Oligarchy

Multiple Anchored CA's

Anarchy Model

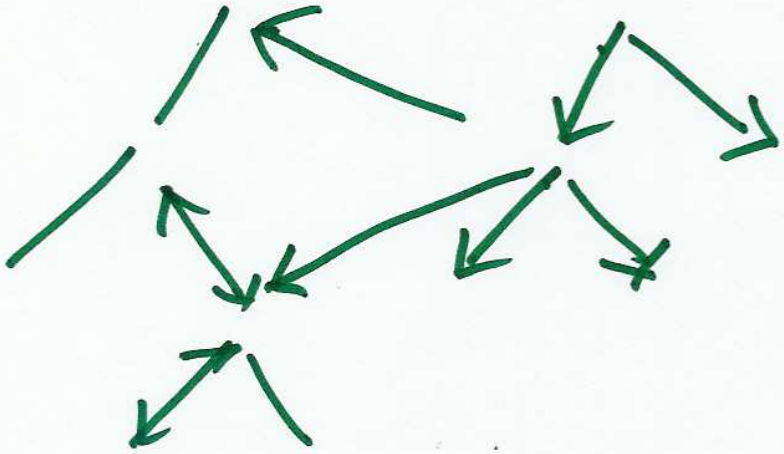
Any body (with some restrictions) can create certificates & deposit

Name Constraints

CA can be trusted for a subset of certificates

Top-down with name contraints.

Bottom-up with name contraints



Relative Names

X.509

Depository -- Directory

PK certificates.

Standard. (1988)
(2000)

RSA.

Certificate - Signature
Hash function.

Flexibility - Specify
what you are using.

Version's

Certificate

Bob — subject
- public key information
period of validity

issuer - CA + RA
signature of issuer.

unique identification of
Subject
issuer.

(X.500)

Extensions —

$CA\ll A\gg = CA(V, SN, AI)$

$A \quad — \quad B$

$A \rightarrow \ll X_1 \gg X_2 \ll X_3 \gg \ldots$

$\ldots \ll X_n \gg B$

Revoked.

CA → Revoked list

Date of creation.

List of revoked ~~tit~~ certificates