

# Public Key Infrastructures (PKI)

Raj Jain  
Washington University in Saint Louis  
Saint Louis, MO 63130  
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:  
<http://www.cse.wustl.edu/~jain/cse571-09/>



- ❑ PKI, X.509 and PKIX
- ❑ PKI Trust Models
- ❑ Object ID and X.509 Policies
- ❑ X.500
- ❑ X.509 Certificate Fields and Extensions
- ❑ Authorizations, Anonymous groups, Blind Signatures

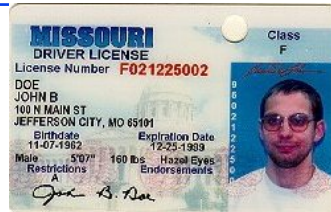
## What is PKI?

- ❑ Infrastructure to find public keys
- ❑ S/MIME, PGP, SSL use asymmetric cryptography and make use of PKI
- ❑ Certificate authorities
- ❑ Standards for certificates

## X.509 and PKIX

- ❑ X.509 is the ISO standard for Certificate formats
- ❑ PKIX is the IETF group on PKI
- ❑ PKIX adopted X.509 and a subset of its options
- ❑ PKIX is a "Profile" of X.509
- ❑ TLS, IPSec, SSH, HTTPS, Smartcard, EAP, CableLabs, use X.509

## Concepts



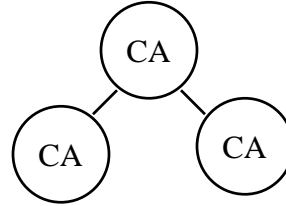
- ❑ **Subject:** Whose certificate is it?
- ❑ **Target:** Whose certificate do we want?
- ❑ **Relying Party:** Who wants to check the certificate
- ❑ **Verifier:** Relying Party
- ❑ **Issuer:** Who issued the certificate?
- ❑ **Certification Authority:** Issuer
- ❑ **Trust Anchor:** The CA that we trust
- ❑ **Root CA:** Issuer = Self
- ❑ **Principal:** Subject, Verifier, Issuer

## PKI Trust Models

- ❑ How Many CAs?
  - Monopoly = One
  - Oligarchy = Many
  - Anarchy = Any
- ❑ How is the name space divided among CAs?
  - Top-Down
  - Bottom-Up

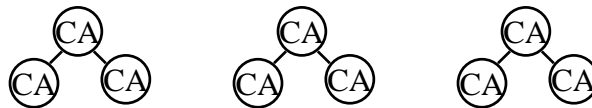
## Monopoly Model: Single Root CA

- ❑ Registrars to check identity
- ❑ Delegated CAs



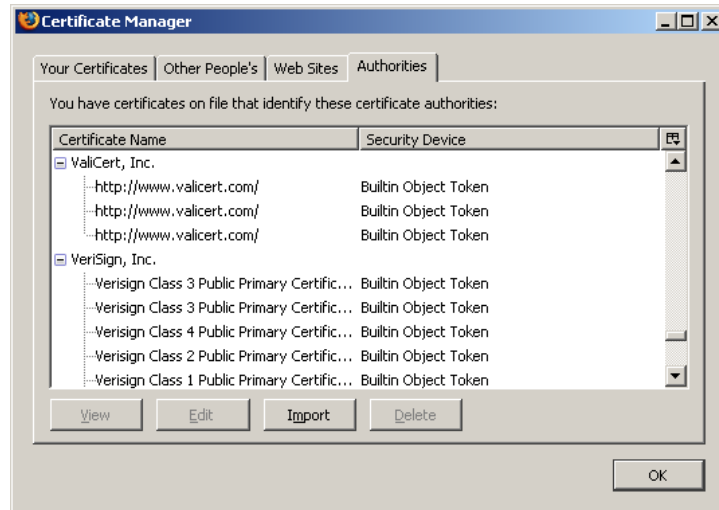
- ❑ Issues:
  - Single point of failure
  - Whole world cannot trust just one organization
  - You may not want internal principals to be certified by external CA

## Oligarchy

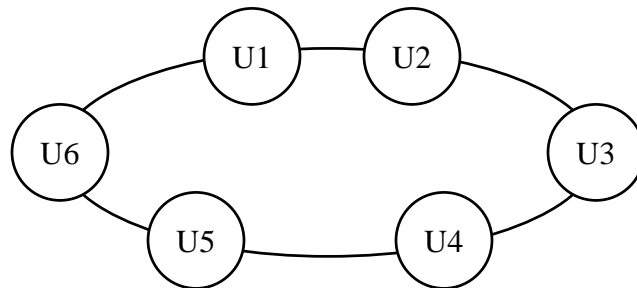


- ❑ Multiple Root CA's
- ❑ Used in browsers
- ❑ Can select which root CA's to trust
- ❑ No Monopoly  $\Rightarrow$  Price efficient

## Oligarchy Example



## Anarchy Model



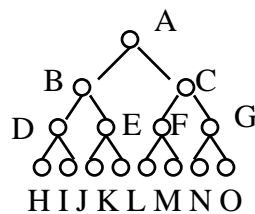
- User driven
- Used in PGP
- Trust Ring, Web of Trust
- Volunteer Databases

## Name Constraints



- ❑ Which part of name space?
- ❑ 1. Top Down:
- ❑ 2. Bottom-Up:
  - Two-way certification:  
Parent → Child, Child → Parent
  - Cross links

## Relative Names



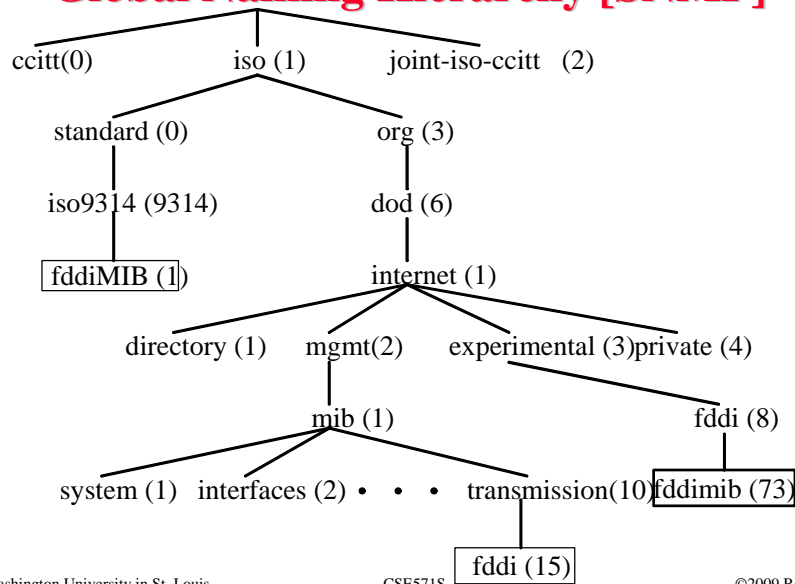
H to J:

- ❑ Absolute: D/B/E/J or A/B/E/J
- ❑ Relative: .././E/J
  - ⇒ No changes required if the parents change name

# OID

- ❑ Object Identifier
- ❑ Identify objects by a universally unique sequence of numbers
- ❑ Similar to what is done in SNMP to name objects

## Global Naming Hierarchy [SNMP]



## **X.509 Policies**

- ❑ Policies in X.509 are identified by OID
- ❑ Company X
  - ❑ X.1 = Security Level
    - ❑ X.1.1 = Confidential
    - ❑ X.1.2 = Secret
    - ❑ X.1.3 = Public

## **X.509 Revocations**

- ❑ **Certificate Revocation Lists:**
  - Too much work on the client
  - Too much traffic on the net
    - ⇒ Not used
- ❑ **On-Line Revocation Server (OLRS):**
  - On-line Certificate Status Protocol (OCSP)
  - RFC 2560
  - Provides current information
  - Saves traffic on the net
  - Also allows chaining of OCSP responders

## X.500

- ❑ Series of standards covering directory services
- ❑ Similar to white/yellow pages
- ❑ Directory Access Protocol (**DAP**) designed by ISO
- ❑ Lightweight Directory Access Protocol (**LDAP**) designed by IETF
- ❑ LDAPv3 is RFC4510
- ❑ Each entry has a "Distinguished Name" and a set of attributes
- ❑ Formed by combining Relative distinguished names
- ❑ X.500 Example: C= US, O=WUSTL, OU=CSE, CN=Raj Jain
- ❑ DNS Example: jain@cse.wustl.edu

## X.509 Certificate Fields

- ❑ Version: X.509 Version 1, 2, or 3
- ❑ Serial Number: Certificate Serial #
- ❑ Signature: Signing algorithm
- ❑ Issuer:
- ❑ Validity:
- ❑ Subject: Issued to
- ❑ Subject Public Key Info: Algorithm/parameters, and Public Key
- ❑ Issuer Unique Identifier: OID of the Issuer (not used)
- ❑ Subject Unique Identifier: OID of the subject (not used)
- ❑ Algorithm Identifier: Signature algorithm (again)
- ❑ Encrypted: Signature
- ❑ Extensions: Only in Version 3. Specified by OID

## **X.509 Extensions**

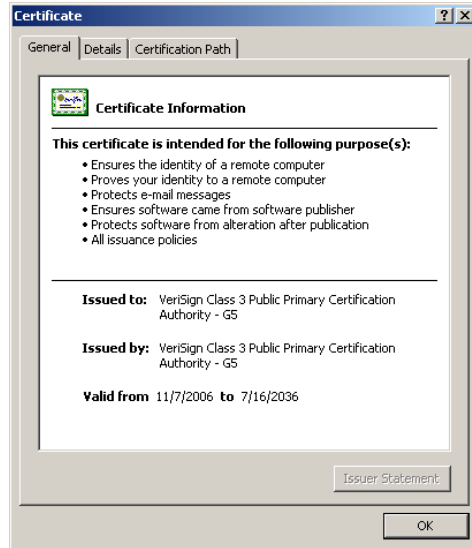
- ❑ Authority Key Identifier: Serial # of CA's key
- ❑ Subject Key Identifier: Uniquely identifies the subjects key. Serial # or hash.
- ❑ Key Usage: Allowed usage - email, business, ...
- ❑ Private Key Usage Period: Timestamps for when key can be used (similar to validity)
- ❑ Certificate Policies
- ❑ Policy Mappings: from Issuer's domain to subject's domain
- ❑ Subject Alt Name: Alternative name. DNS.
- ❑ Subject Directory Attributes: Other attributes

## **X.509 Extensions (Cont)**

- ❑ Basic Constraints: Whether CA and length of chain
- ❑ Name Constraints: Permitted and excluded subtrees
- ❑ Policy Constraints: OIDs
- ❑ Extended Key Usage: Additional key usages
- ❑ CRL Distribution Points:
- ❑ Inhibit Any Policy: “Any Policy” is not allowed
- ❑ Freshest CRL: How to obtain incremental CRLs
- ❑ Authority Info Access: How to find info on issuers
- ❑ Subject Info Access: How to find info on subject

## Sample X.509 Certificate

Internet Explorer



## X.509 Sample (Cont)

Field	Value
Version	V3
Serial number	18 da d1 9e 26 7d e8 bb 4a 21...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Public Primary ...
Valid from	Tuesday, November 07, 2006 ...
Valid to	Wednesday, July 16, 2036 6:...
Subject	VeriSign Class 3 Public Primary ...
Public key	RSA (2048 Bits)
version	v3
Serial number	18 da d1 9e 26 7d e8 bb 4a 21...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Public Primary ...
Valid from	Tuesday, November 07, 2006 ...
Valid to	Wednesday, July 16, 2036 6:...
Subject	VeriSign Class 3 Public Primary ...
Public key	RSA (2048 Bits)

## X.509 CRL Fields

- ❑ Signature: Signature Algorithm for this CRL
- ❑ Issuer: X.500 name of issuing CA
- ❑ This Update: Time of this CRL
- ❑ Next Update: Time next CRL will be issued
- ❑ For each revoked Certificate:
  - User Certificate:Serial Number of revoked Certificate
  - Revocation Date:
  - CRL Entry Extensions: Reason code, etc.
- ❑ CRL Extensions: optional information
- ❑ Algorithm Identifier: Repeat of signature
- ❑ Encrypted: Signature

## Entrusted Certificates

Field	Value
Version	V3
Serial number	75 0e 40 ff 97 f0 47 ed f5 56 c...
Signature algorithm	md5RSA
Issuer	VeriSign Commercial Software ...
Valid from	Tuesday, January 30, 2001 7:...
Valid to	Thursday, January 31, 2002 6...
Subject	Microsoft Corporation, Microso...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Key Encipher...
Authority Key Identifier	KeyID=7b 96 e4 d1 43 fd 68 9...
Basic Constraints	Subject Type=End Entity, Pat...
Certificate Policies	[1]Certificate Policy:Policy Ide...
SpcFinancialCriteria	Financial Information=Availabl...
Key Usage Restriction	[1]Cert PolicyId=1.3.6.1.4.1....
SpcSpAgencyInfo	Policy Information:URL=https:...
Thumbprint algorithm	sha1
Thumbprint	7d 7f 44 14 cc ef 16 8a df 6b f...
Friendly name	Fraudulent, NOT Microsoft
Extended Error Information	Revocation Status : The certifi...

## Authorizations

- Access Control Lists: List of users
- Groups: User provides certificate of membership
- Role: User provides credentials

## Anonymous Groups

- User could authenticate to group server
- Certificate  $\Rightarrow$  the owner of the private key is a member of group
- User will need lots of public/private key pairs
- Group servers need not know key/member association
- Group server can do a blind signature

## Blind Signature

- ❑ Client wants server to sign a certificate  $C$
- ❑ Server's public key is  $\langle e, n \rangle$
- ❑ Client picks a random number  $R$  and computes  $C(R^e \bmod n)$
- ❑ Server decrypts it with his private key  $C^d (R^{ed}) \bmod n = C^d R$
- ❑ Client just divides by  $R$  and gets  $C^d = \text{Certificate signed by server}$

## Summary



- ❑ **PKIX** is a profile of the **X.509** PKI standard
- ❑ Browsers have a built-in list of **root CAs**  
⇒ Oligarchy
- ❑ X.509 uses **X.500** names. DNS names in Alternate Name field.
- ❑ X.509 policies are specified using **OIDs**.
- ❑ **OCSP** is used to check revocation
- ❑ Authorization is best done by user, group, **role** level
- ❑ Anonymous group certification is possible.  
**Blind signatures** allow even the group server to not know the public key

## Homework 12

- ❑ Read chapter 15 of the textbook.
- ❑ Study the root certificates in your Internet Explorer  
Find the certificate for “Thawte Premium Server CA”
  - What is the X.500 name of the CA?
  - What version of X.509 does this CA use?
  - What are the two key usage of the certificates issued by this CA?
- ❑ What is the title of RFC810?