

**INFS 766**  
**Internet Security Protocols**

**Lecture 6**  
**Digital Certificates**

**Prof. Ravi Sandhu**

**X.509 CERTIFICATE**

VERSION
SERIAL NUMBER
SIGNATURE ALGORITHM
ISSUER
VALIDITY
SUBJECT
SUBJECT PUBLIC KEY INFO
SIGNATURE

© Ravi Sandhu 2002

4

**PUBLIC-KEY CERTIFICATES**

- ❖ **reliable distribution of public-keys**
- ❖ **public-key encryption**
  - > sender needs public key of receiver
- ❖ **public-key digital signatures**
  - > receiver needs public key of sender
- ❖ **public-key key agreement**
  - > both need each other's public keys

© Ravi Sandhu 2002

2

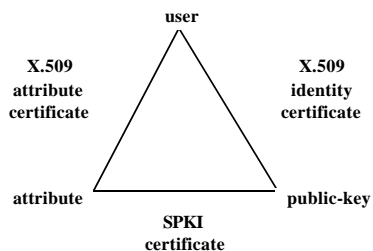
**X.509 CERTIFICATE**

0
1234567891011121314
RSA+MD5, 512
C=US, S=VA, O=GMU, OU=ISE
9/9/99-1/1/1
C=US, S=VA, O=GMU, OU=ISSE, CN=Ravi Sandhu
RSA, 1024, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
SIGNATURE

© Ravi Sandhu 2002

5

**THE CERTIFICATE TRIANGLE**



© Ravi Sandhu 2002

3

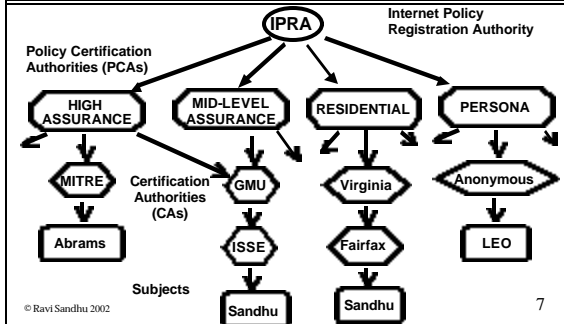
**CERTIFICATE TRUST**

- ❖ **how to acquire public key of the issuer to verify signature**
- ❖ **whether or not to trust certificates signed by the issuer for this subject**

© Ravi Sandhu 2002

6

## PEM CERTIFICATION GRAPH



© Ravi Sandhu 2002

7

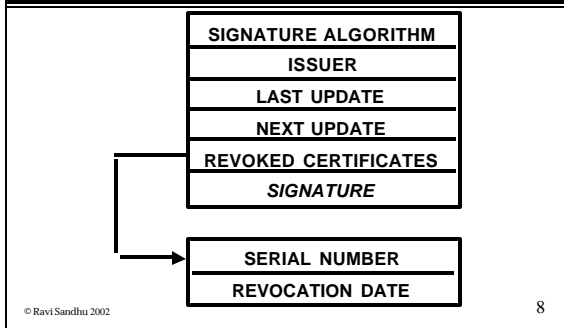
## X.509 CERTIFICATES

- ❖ X.509v1
  - very basic
- ❖ X.509v2
  - adds unique identifiers to prevent against reuse of X.500 names
- ❖ X.509v3
  - adds many extensions
  - can be further extended

© Ravi Sandhu 2002

10

## CRL FORMAT



© Ravi Sandhu 2002

8

## SEPARATE KEYS FOR SEPARATE PURPOSES

- ❖ RSA is the only known public-key cryptosystem in which the same public-private key pair can be used for
  - digital signatures
  - encryption
- ❖ perceived as a major advantage

© Ravi Sandhu 2002

11

## PGP BOTTOM UP TRUST MODEL

- ❖ How does Alice get Bob's public key
  - directly from Bob through some secure channel (e.g., post, phone, floppy)
  - from Chuck, who is known to both Alice and Bob and introduces Bob to Alice
  - from a trusted certifying authority
- ❖ PGP has mechanisms to support these, and related, alternatives

© Ravi Sandhu 2002

9

## SIGNATURE KEYS

- ❖ private key: must be private for entire life, may never leave smart card
  - needs to be securely destroyed after lifetime
  - no need for backup or archiving (would conflict with above)
  - no need to weaken or escrow due to law
- ❖ public key: must be archive possibly for a long time

© Ravi Sandhu 2002

12

## ENCRYPTION KEY

- ❖ **private key: backup or archive required for recovery**
  - should not be destroyed after lifetime
  - may be weakened/escrowed due to law
- ❖ **public key:**
  - no need to backup RSA or other encryption keys
  - need to backup Diffie-Hellman key agreement keys

© Ravi Sandhu 2002

13

## X.509v3 EXTENSIONS CRITICALITY

- ❖ **non-critical: extension can be ignored by certificate user**
  - alternate name can be non-critical
- ❖ **critical : extension should not be ignored by certificate user**
  - limit on use of signatures for further certification

© Ravi Sandhu 2002

16

## X.509 INNOVATIONS

- ❖ **distinguish various certificates**
  - signature, encryption, key-agreement
- ❖ **identification info in addition to X.500 name**
- ❖ **name other than X.500 name**
  - email address
- ❖ **issuer can state policy and usage**
  - good enough for casual email but not good enough for signing checks
- ❖ **limits on use of signature keys for further certification**

© Ravi Sandhu 2002

14

## X.509v3 EXTENSIONS CRITICALITY

- ❖ **criticality is flagged by certificate issuer**
  - certificate user may consider non-critical extensions more important than critical ones
  - certificate user may refuse to use certificate if some extensions are missing
- ❖ **critical extensions should be few and should be standard**

© Ravi Sandhu 2002

17

## X.509v3 EXTENSIONS

- ❖ **X.509v3 same as X.509v2 but adds extensions**
- ❖ **provides a general extension mechanism**
  - extension type: registered just like an algorithm is registered
  - standard extension types: needed for interoperability

© Ravi Sandhu 2002

15

## X.509v3 NAMES

- ❖ internet email address
- ❖ internet domain name
- ❖ web uri (url's are subset of uri)
- ❖ IP address
- ❖ X.400 email address
- ❖ X.500 directory name
- ❖ registered identifier
- ❖ other name

© Ravi Sandhu 2002

18

## X.509v3 STANDARD EXTENSIONS

- ❖ **Key and policy information**
- ❖ **Subject and issuer attributes**
- ❖ **Certification path constraints**
- ❖ **Extensions related to CRLs**
  - will be discussed with CRLs

© Ravi Sandhu 2002

19

## CERTIFICATION PATH CONSTRAINTS

- ❖ **Basic Constraints**
  - can or cannot act as CA
  - if can act as CA limit on certification path
    - limit=1 means cannot certify other CAs
- ❖ **Name Constraints**
  - limits names of subjects that this CA can issue certificates for
- ❖ **Policy Constraints**
  - concerned with CA policies

© Ravi Sandhu 2002

22

## KEY AND POLICY INFORMATION

- ❖ **key usage**
  - critical: intended only for that purpose, limits liability of CA
  - non-critical: advisory to help find the correct key, no liability implication
- ❖ **private-key usage period**
  - certificate valid for 2 years for verifying signature
  - key valid only for one year for signing
- ❖ **certificate policies**
  - for CAs

© Ravi Sandhu 2002

20

## CERTIFICATE REVOCATION LISTS

- ❖ **CRLs issued periodically as per CA policy**
  - off-cycle CRLs may also be needed
  - blank CRLs can be issued

© Ravi Sandhu 2002

23

## SUBJECT AND ISSUER ATTRIBUTES

- ❖ **Subject alternative names**
- ❖ **Issuer alternative names**
- ❖ **Subject directory attributes**
  - whatever you like
  - position, phone, address etc.

© Ravi Sandhu 2002

21

## CERTIFICATE REVOCATION LISTS

- ❖ **CRL distribution**
  - pull method
  - push method
- ❖ **DMS example**
  - pull method with push for compromised key list (CKL) which is broadcast via secure email, single CKL for entire system

© Ravi Sandhu 2002

24

## CERTIFICATE REVOCATION LISTS

- ❖ **immediate or real-time revocation**
  - needs query to CA on every certificate use
  - maybe ok for small closed communities

© Ravi Sandhu 2002

25

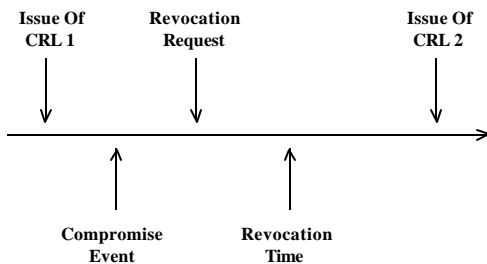
## SHORT-LIVED CERTIFICATES

- ❖ **Authorization certificates can be short lived**
  - minutes, hours, days instead of
  - months, years

© Ravi Sandhu 2002

28

## REVOCATION TIME-LINE



© Ravi Sandhu 2002

26

## X.509 CRL EXTENSIONS

- ❖ **General Extensions**
- ❖ **CRL distribution points**
- ❖ **Delta-CRLs**
- ❖ **Indirect-CRLs**
- ❖ **Certificate Suspension**

© Ravi Sandhu 2002

29

## OCSP ON-LINE CERTIFICATE STATUS PROTOCOL

- ❖ **consult authoritative server**
- ❖ **the server in turn can look up CRLs**

© Ravi Sandhu 2002

27

## GENERAL EXTENSIONS

- ❖ **Reason Code**
  - Key Compromise
  - CA Compromise
  - Affiliation changed
  - Superseded
  - Cessation of operation
  - Remove from CRL: defer till Delta-CRL
  - Certificate hold: defer
- ❖ **Invalidity Date**

© Ravi Sandhu 2002

30

## CRL DISTRIBUTION POINTS

- ❖ **CRLs can get very big**
  - **version 1 CRL (1988, 1993)**
    - each CA has two CRLs: one for end users, one for CAs
    - end user CRL can still be very big
  - **version 2 CRL**
    - can partition certificates, each partition associated with one CRL
    - distribution point
    - also can have different distribution points for different revocation reasons

© Ravi Sandhu 2002

31

## INDIRECT-CRL

- ❖ **CRL can be issued by different CA than issuer of certificate**
  - allows all compromise revocations to be one list
  - allows all CA revocations to be on one list (simplify certificate chasing)

© Ravi Sandhu 2002

34

## CRL DISTRIBUTION POINTS

- ❖ **certificate extension field, says where to look**
- ❖ **CRL extension field**
  - distribution point for this CRL and limits on scope and reason of revocation
  - protects against substitution of a CRL from one distribution point to another

© Ravi Sandhu 2002

32

## CERTIFICATE SUSPENSION

- ❖ **Certificate hold reason code in CRL**
- ❖ **Supporting CRL entry extension**
  - **Instruction code: instructions on what to do with held certificate**
    - call CA, repossess token

© Ravi Sandhu 2002

35

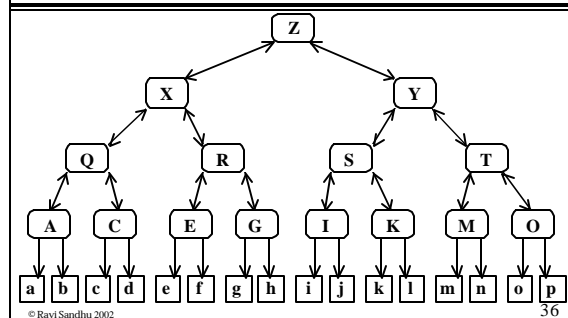
## DELTA-CRLs

- ❖ **Delta CRL indicator**
  - only carries changes from previous CRL
- ❖ **Remove from CRL reason code causes purge from base CRL (stored at certificate user)**
- ❖ **removal due to expiry of validity period or restoration of suspension**

© Ravi Sandhu 2002

33

## GENERAL HIERARCHICAL STRUCTURE



© Ravi Sandhu 2002

36

