X.509

Mridul Sankar Barik

Dept. of Comp. sc. & Engg.

Jadavpur University

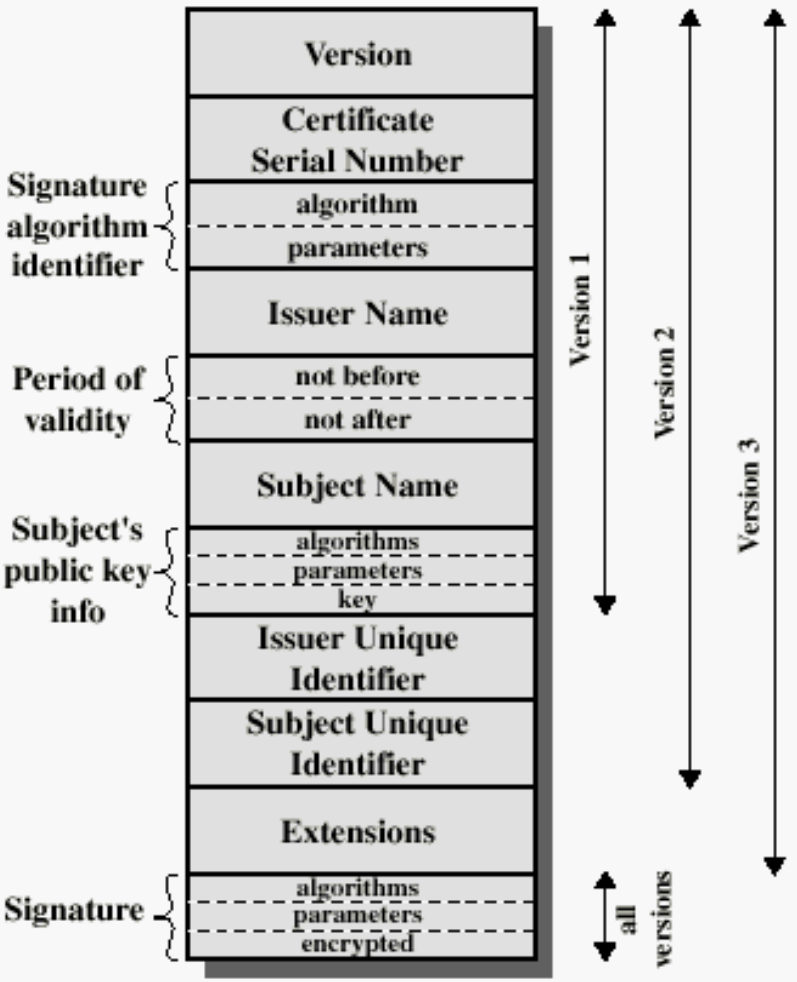
X.509 Authentication Service

- ITU-T recommendation X.509 is part of X.500 series recommendations that defines a directory service
- A directory is a single or distributed set of servers that maintain database of information about users
- X.509 is a framework for the provision of authentication services
- Used by other protocols such as S/MIME, IPSec, SSL/TLS, SET etc.

Digital Certificates

- Created by some trusted certification authority (CA) and placed in the directory by the user or CA
- Notation
  - Y<<X>>
    - Certificate of user X is issued by certification authority Y

X.509 Format



(a) X.509 Certificate

Version: Can be either version 1 or 2 or 3

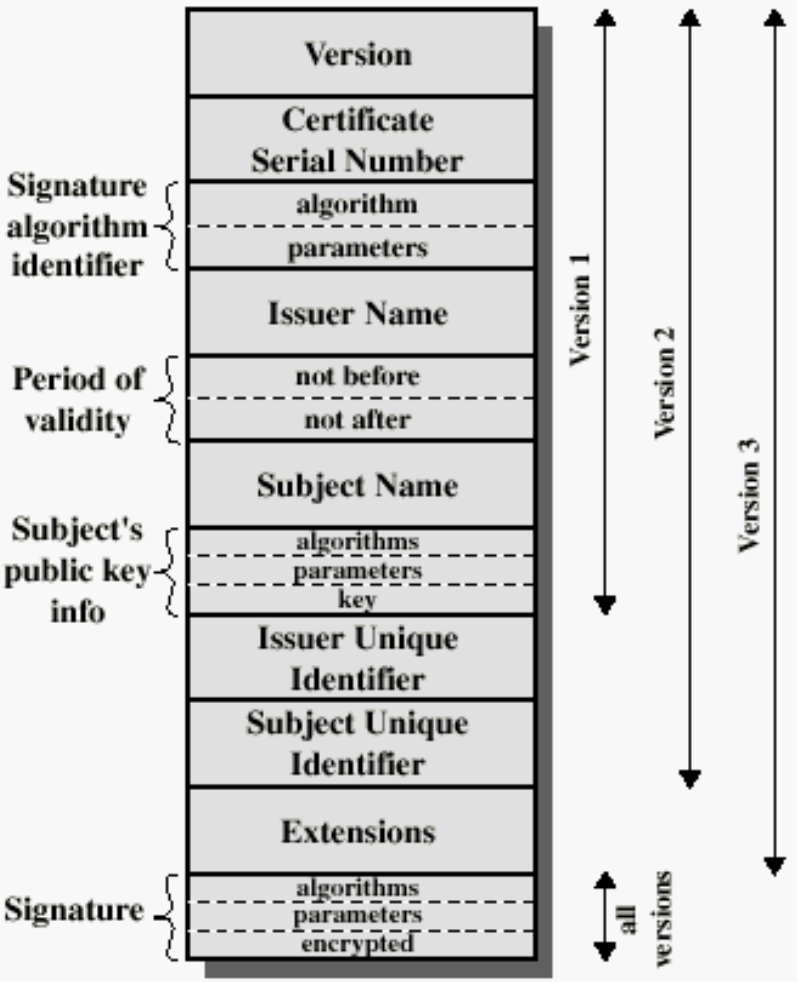
Serial number: An integer value unique within the issuing CA

Signature Algorithm Identifier: Algorithm used to sign the certificate together with any associated parameters

Issuer Name: X.500 name of the issuer

Period of Validity: First and last date on which the certificate is valid

X.509 Format



(a) X.509 Certificate

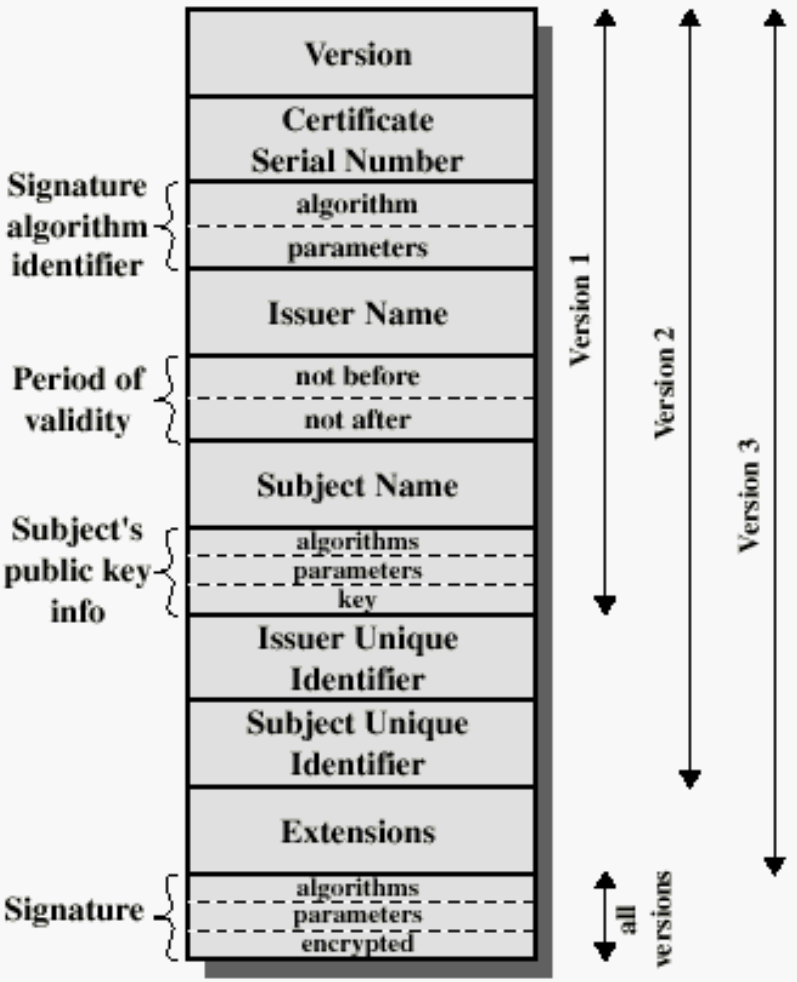
Subject Name: X.500 name of the user to whom this certificate refers

Subject's Public Key Information: Public key of the subject together with an identifier of the algorithm and any associated parameters

Issuer Unique Identifier: An optional bit string used to identify issuing CA

Subject Unique Identifier: An optional bit string used to identify subject

X.509 Format



(a) X.509 Certificate

Extensions: One or more extension fields added in version 3

Signature: Hash code of all other field encrypted with CA's private key

Certificate Characteristics

- Any user with access to public key of CA can recover the user public key that was certified
- No party other than CA can modify the certificate without being detected

Obtaining a User's Certificate

- If all users subscribe to the same CA then there is a common trust of that CA
- With many users it may be more practical to have number of CAs

Certificate Types/Classes

- Personal Certificates
  - These certificates identify individuals
  - They may be used to authenticate users with a server, or to enable secure e-mail using S/MIME
- Server Certificates
  - Identify servers that participate in secure communications with other computers using communication protocols such as SSL
- Software Publisher Certificates
  - These certificates are used to sign software to be distributed over the Internet
- Certificate Authority Certificates
  - Root Certification Authorities
    - Have the ability to assign certificates for Intermediate Certification Authorities
    - Root certificates are self-signed
  - Intermediate Certification Authorities
    - Can issue server certificates, personal certificates, publisher certificates, or certificates for other Intermediate Certification Authorities

Revocation of Certificates

- Reasons
  - Users secret key is assumed to be compromised
  - User is no longer certified by this CA
  - The CAs certificate is assumed to be compromised
- Each CA must maintain a list consisting of all revoked but not expired certificates issued by that CA
- When a user receives a message it must determine whether it has been revoked