Cryptography and Network Security

X.509 Certificate

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	1 August 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

X.509 Authentication Service

- part of CCITT X.500 directory service standards
  - distributed servers maintaining some info database
- defines framework for authentication services
  - directory may store public-key certificates
  - with public key of user
  - signed by certification authority
- also defines authentication protocols
- uses public-key crypto & digital signatures
  - algorithms not standardised, but RSA recommended

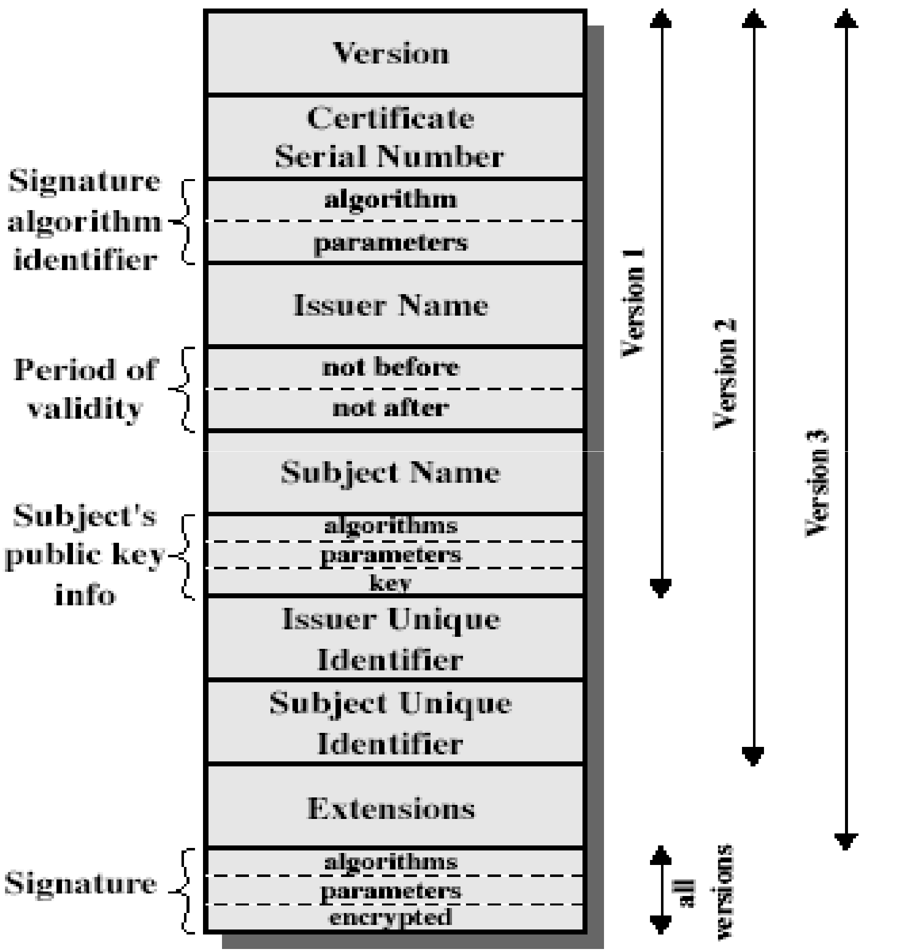
Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

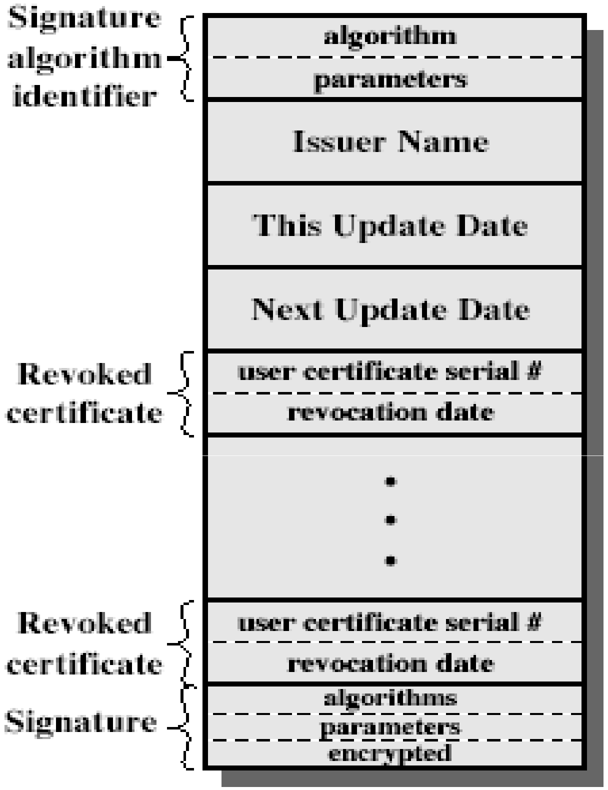
X.509 Certificates

- issued by a Certification Authority (CA), containing:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (from - to dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (of hash of all fields in certificate)
- notation CA<<A>> denotes certificate for A signed by CA

X.509 Certificates



(a) X.509 Certificate



(b) Certificate Revocation List

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

Obtaining a Certificate

- any user with access to CA can get any certificate from it
- only the CA can modify a certificate
- because cannot be forged, certificates can be placed in a public directory

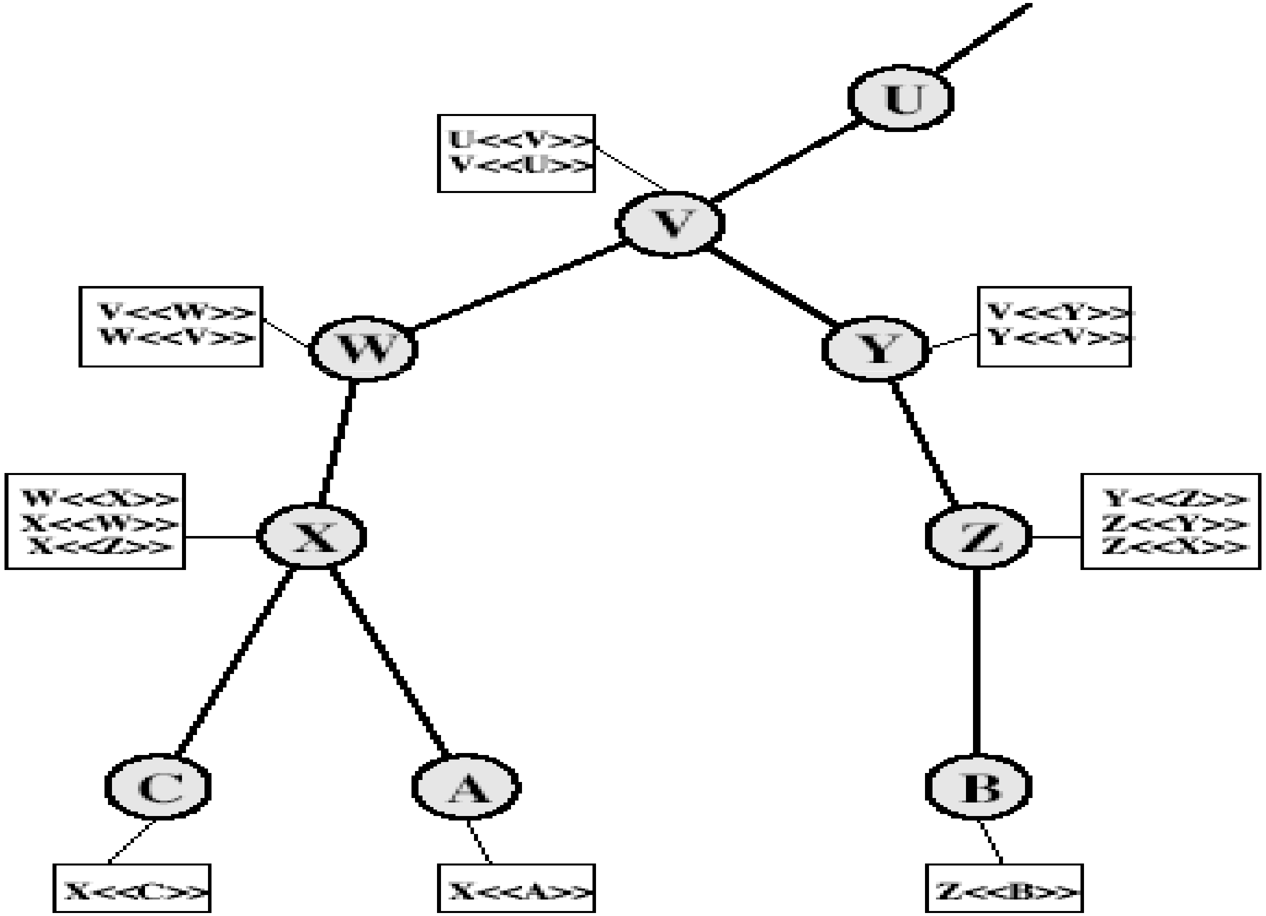
Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

CA Hierarchy

- if both users share a common CA then they are assumed to know its public key
- otherwise CA's must form a hierarchy
- use certificates linking members of hierarchy to validate other CA's
  - each CA has certificates for clients (forward) and parent (backward)
- each client trusts parents certificates
- enable verification of any certificate from one CA by users of all other CAs in hierarchy

CA Hierarchy Use



Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

Certificate Revocation

- certificates have a period of validity
- may need to revoke before expiry, eg:
  1. user's private key is compromised
  2. user is no longer certified by this CA
  3. CA's certificate is compromised
- CA’s maintain list of revoked certificates
  - the Certificate Revocation List (CRL)
- users should check certs with CA’s CRL

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

Authentication Procedures

- X.509 includes three alternative authentication procedures:
- One-Way Authentication
- Two-Way Authentication
- Three-Way Authentication
- all use public-key signatures

One-Way Authentication

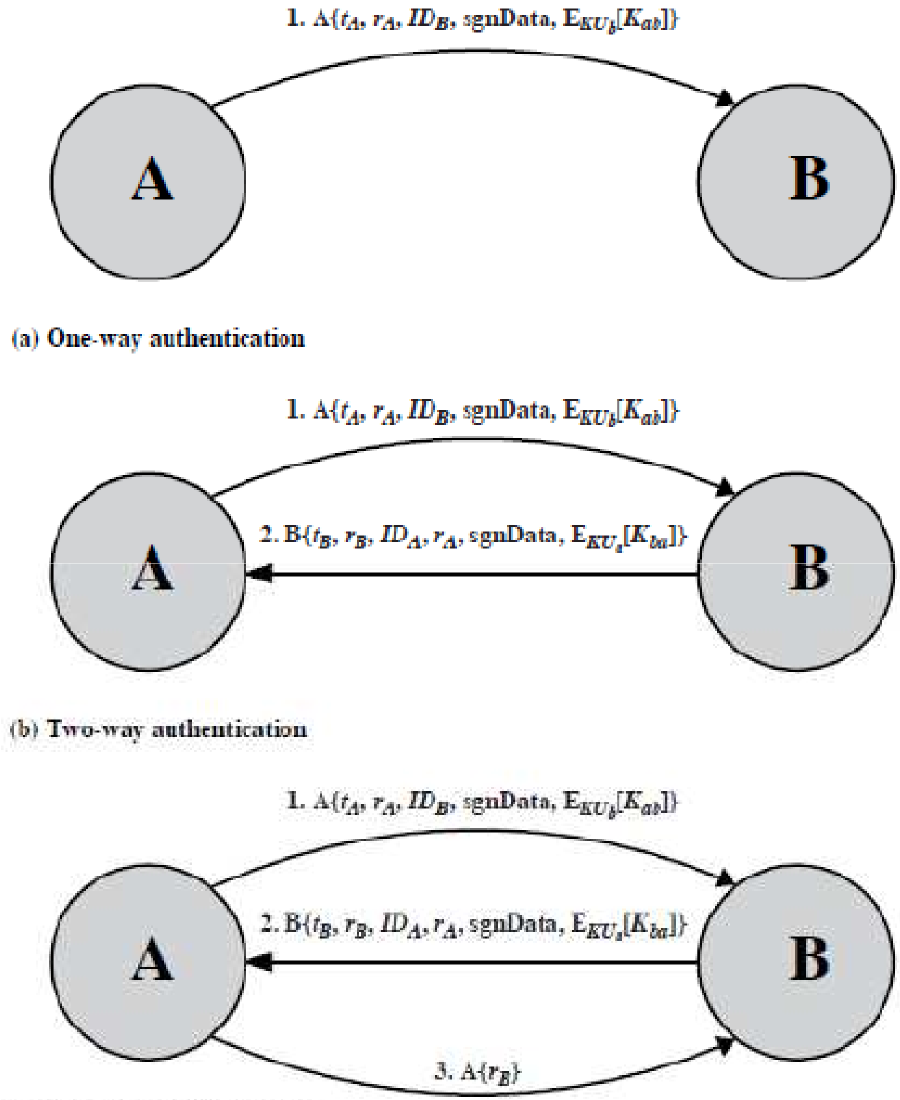
- 1 message (A->B) used to establish
  - the identity of A and that message is from A
  - message was intended for B
  - integrity & originality of message
- message must include timestamp, nonce, B's identity and is signed by A

Two-Way Authentication

- 2 messages (A->B, B->A) which also establishes in addition:
  - the identity of B and that reply is from B
  - that reply is intended for A
  - integrity & originality of reply
- reply includes original nonce from A, also timestamp and nonce from B

Three-Way Authentication

- 3 messages (A->B, B->A, A->B) which enables above authentication without synchronized clocks
- has reply from A back to B containing signed copy of nonce from B
- means that timestamps need not be checked or relied upon


1. A{t_A, r_A, ID_B, sgnData, $E_{KU_b}[K_{ab}]$}
A
B
1. A{t_A, r_A, ID_B, sgnData, $E_{KU_b}[K_{ab}]$}
2. B{t_B, r_B, ID_A, r_A, sgnData, $E_{KU_a}[K_{ba}]$}
A
B
1. A{t_A, r_A, ID_B, sgnData, $E_{KU_b}[K_{ab}]$}
2. B{t_B, r_B, ID_A, r_A, sgnData, $E_{KU_a}[K_{ba}]$}
A
B
3. A{r_B}

(a) One-way authentication

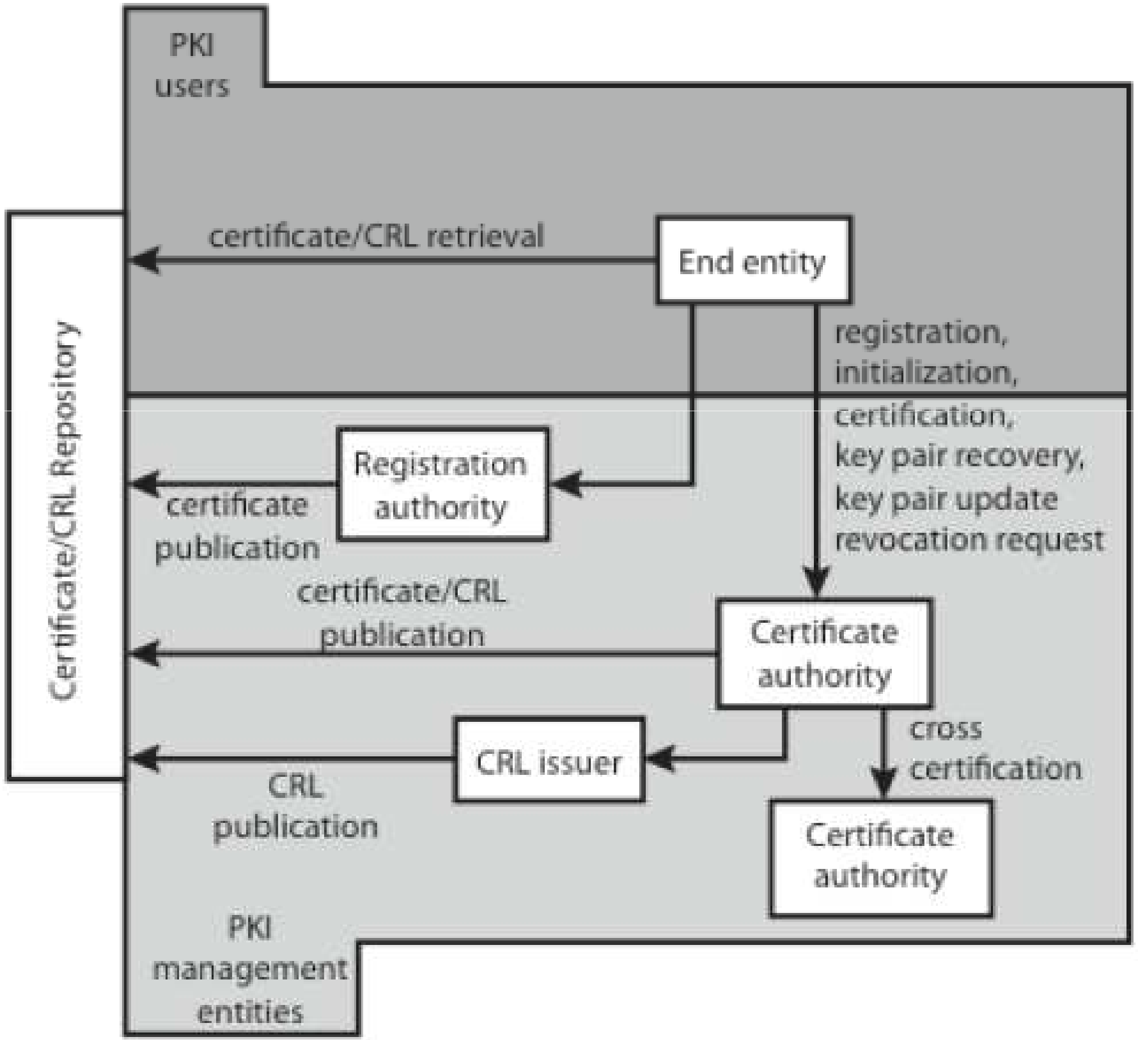
(b) Two-way authentication

(c) Three-way authentication

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

Public Key Infrastructure



PKI users
certificate/CRL retrieval
End entity
registration, initialization, certification, key pair recovery, key pair update revocation request
Certificate/CRL Repository
Registration authority
certificate publication
certificate/CRL publication
Certificate authority
CRL issuer
cross certification
CRL publication
Certificate authority
PKI management entities

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

X.509 Version 3

- has been recognised that additional information is needed in a certificate
  - email/URL, policy details, usage constraints
- rather than explicitly naming new fields defined a general extension method
- extensions consist of:
  - extension identifier
  - criticality indicator
  - extension value

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

Certificate Extensions

- key and policy information
  - convey info about subject & issuer keys, plus indicators of certificate policy
- certificate subject and issuer attributes
  - support alternative names, in alternative formats for certificate subject and/or issuer
- certificate path constraints
  - allow constraints on use of certificates by other CA’s

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

Summary

- have considered:
  - X.509 authentication and certificates

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

Test your understanding

1) What is a public key certificate?
2) What is the purpose of X.509 standard?
3) Why is it sometimes desirable to revoke an X.509 certificate before it expires?

Agenda

- X.509 authentication service
- X.509 certificates
  - Obtaining a certificate
  - CA hierarchy
  - Certificate revocation
  - Authentication procedures
  - Public Key infrastructure
  - X.509 version3
  - Certificate extension
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.