Authentication Application

X.509

Authentication Applications

- Developed to support application-level authentication and digital signatures
- Most widely used services:
  - Kerberos
  - X.509
- Kerberos – a private-key authentication service
- X.509 – a public-key directory authentication service

X.509 Authentication Service

- **ITU came up with this standard in 1988**
- **part of X.500 directory service standards**
- Distributed set of servers that maintains a database about users & other Attributes.
- 1993 V1,1995 V2,1999 V3 by Internet Engg Task Force.
- **defines framework for authentication services**
- Each certificate contains the public key of a user and is signed with the private key of a CA.
- **Is used in** S/MIME, IP Security, SSL/TLS **and** SET.
- **also defines authentication protocols**

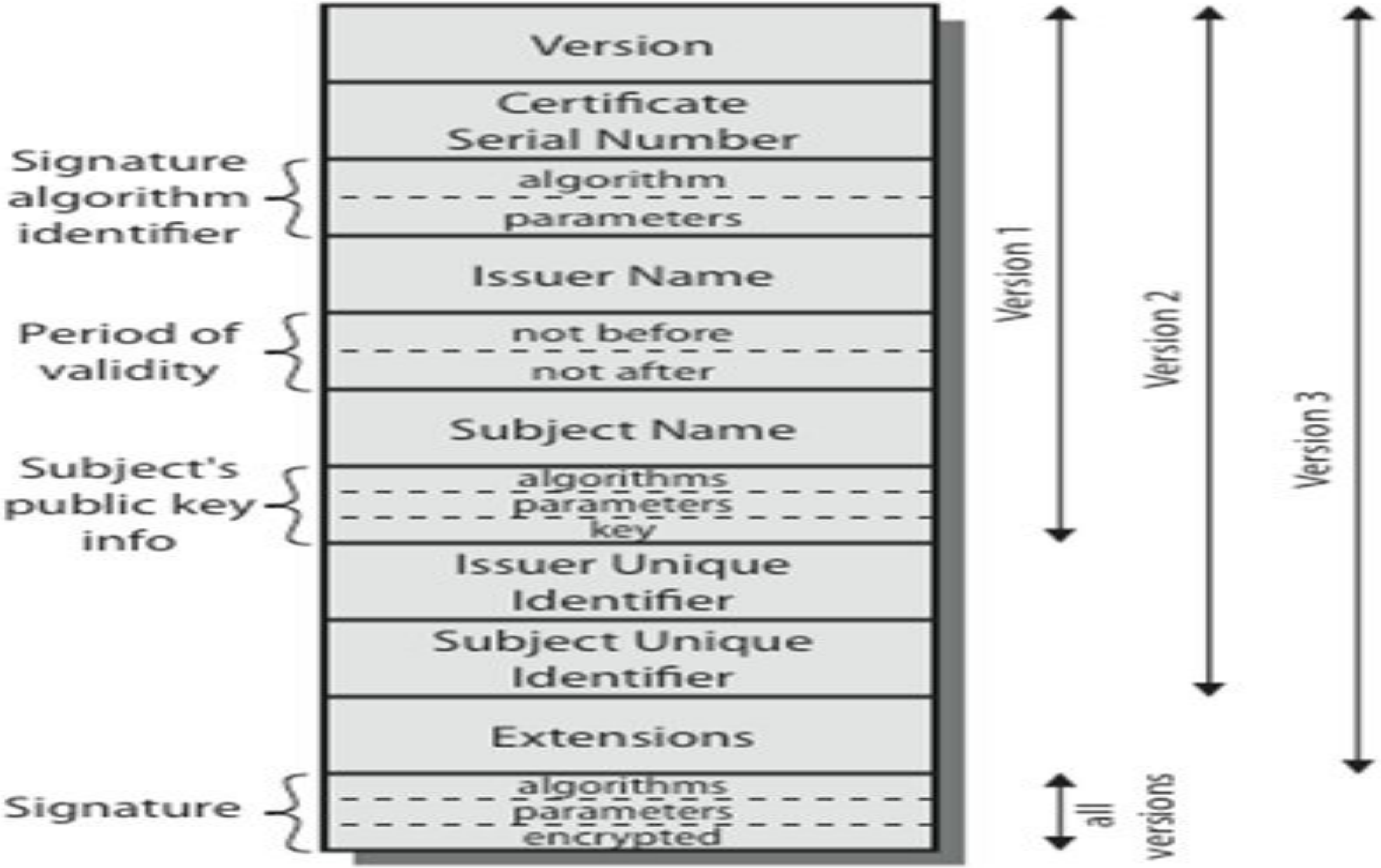
X.509

- **uses public-key cryptology & digital signatures**
  - *algorithms not standardised, but RSA recommended*
- **X.509 certificates are widely used**
- **Public key certificate associated with each user**
  - *Generated by some trusted CA*
- **Certification Authority (CA) issues certificates**
- **The notation `CA<<A>>` represents a certificate for a client A signed by CA**

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)

X.509 Certificates



Version

Certificate Serial Number

Signature algorithm identifier: algorithm, parameters

Issuer Name

Period of validity: not before, not after

Subject Name

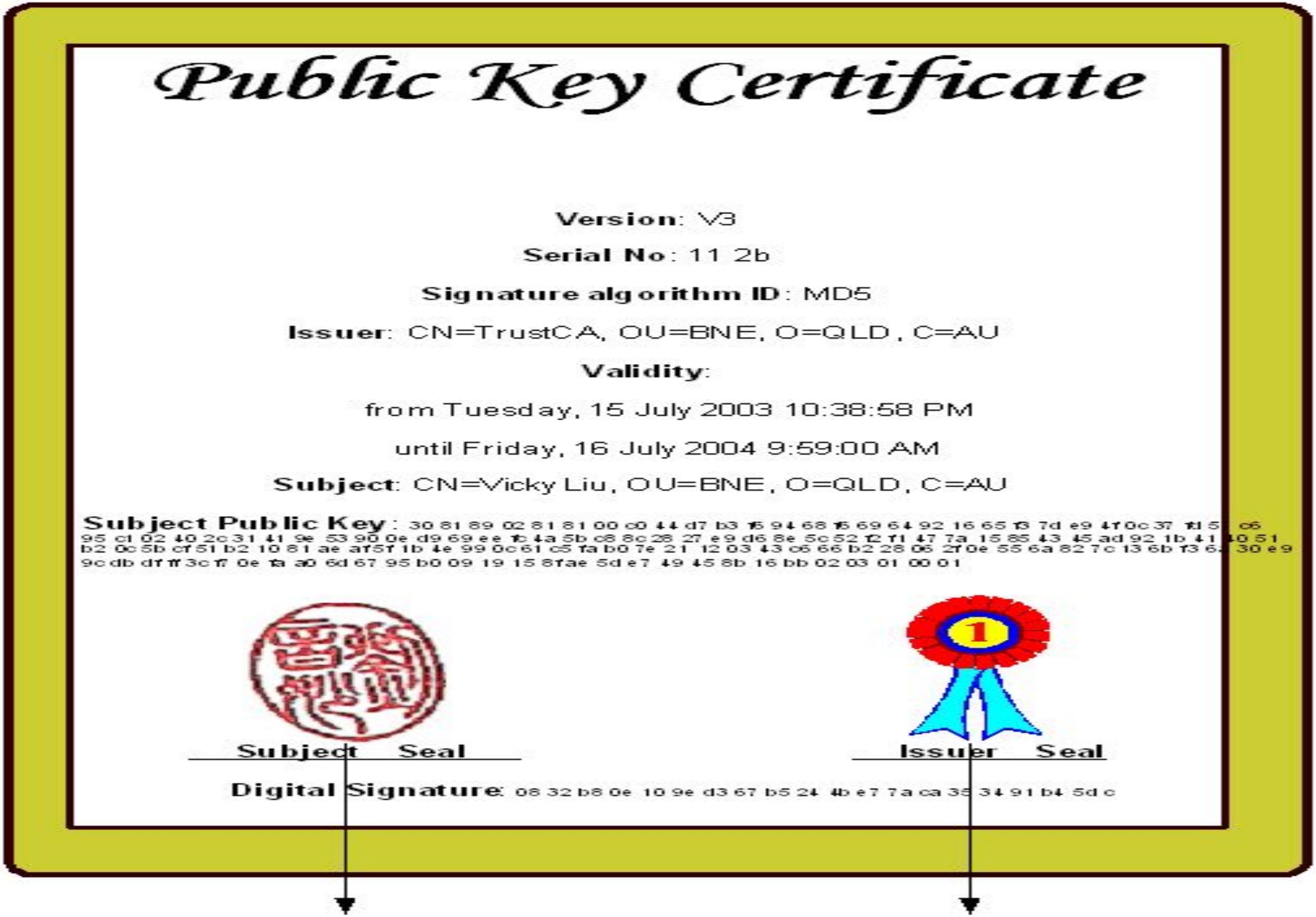
Subject's public key info: algorithms, parameters, key

Issuer Unique Identifier

Subject Unique Identifier

Extensions

Signature: algorithms, parameters, encrypted



Public Key Certificate

Version: V3

Serial No: 11 2b

Signature algorithm ID: MD5

Issuer: CN=TrustCA, OU=BNE, O=QLD, C=AU

Validity:

from Tuesday, 15 July 2003 10:38:58 PM

until Friday, 16 July 2004 9:59:00 AM

Subject: CN=Vicky Liu, OU=BNE, O=QLD, C=AU

Subject Public Key: 30 81 89 02 81 81 00 c0 44 d7 b3 f5 94 68 f5 69 64 92 16 65 f3 7d e9 4f 0c 37 fd 5 c6
95 c1 02 40 2c 31 41 9e 53 90 0e d9 69 ee fc 4a 5b c8 8c 28 27 e9 d6 8e 5c 52 f2 f1 47 7a 15 85 43 45 ad 92 1b 41 40 51
b2 0c 5b cf 51 b2 10 81 ae af 5f 1b 4e 99 0c 61 c5 fa b0 7e 21 12 03 43 c6 66 b2 28 06 2f 0e 55 6a 82 7c 13 6b f3 64 30 e9
9c db df ff 3c f7 0e fa a0 6d 67 95 b0 09 19 15 8f ae 5d e7 49 45 8b 16 bb 02 03 01 00 01

Subject Seal

Issuer Seal

Digital Signature: 08 32 b8 0e 10 9e d3 67 b5 24 4b e7 7a ca 35 34 91 b4 5d c

Signer's seal

Issuer seal

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

Certificate Extensions

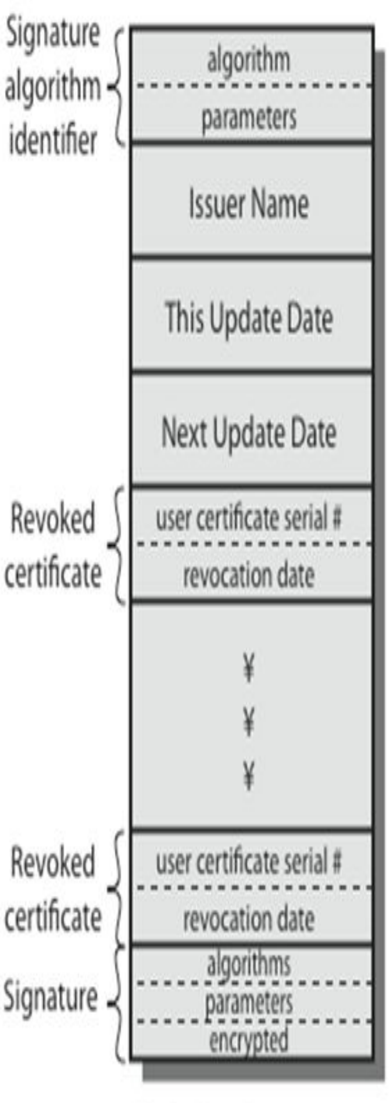
- key and policy information
  - convey info about subject & issuer keys, plus indicators of certificate policy
- certificate subject and issuer attributes
  - support alternative names, in alternative formats for certificate subject and/or issuer
- certificate path constraints
  - allow constraints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

Revocation Of Certificate

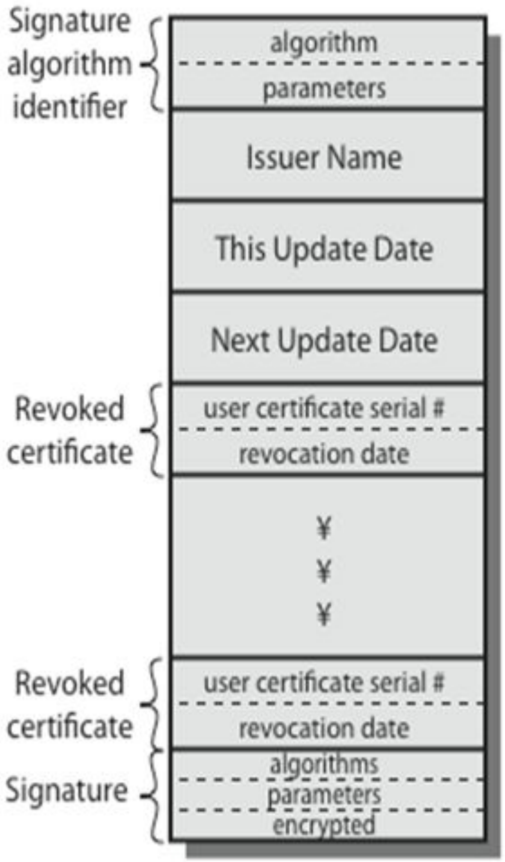
- Revoked before Expiry because of following reasons:

1. User's Private Key Compromised.
2. User is not certified by CA.
3. CA's certificate is compromised.

- If the certificate invalidated due to any reasons.
- certificates have a period of validity
- CA's maintain list of revoked certificates
  - the Certificate Revocation List (CRL)
- users should check certificates with CA's CRL

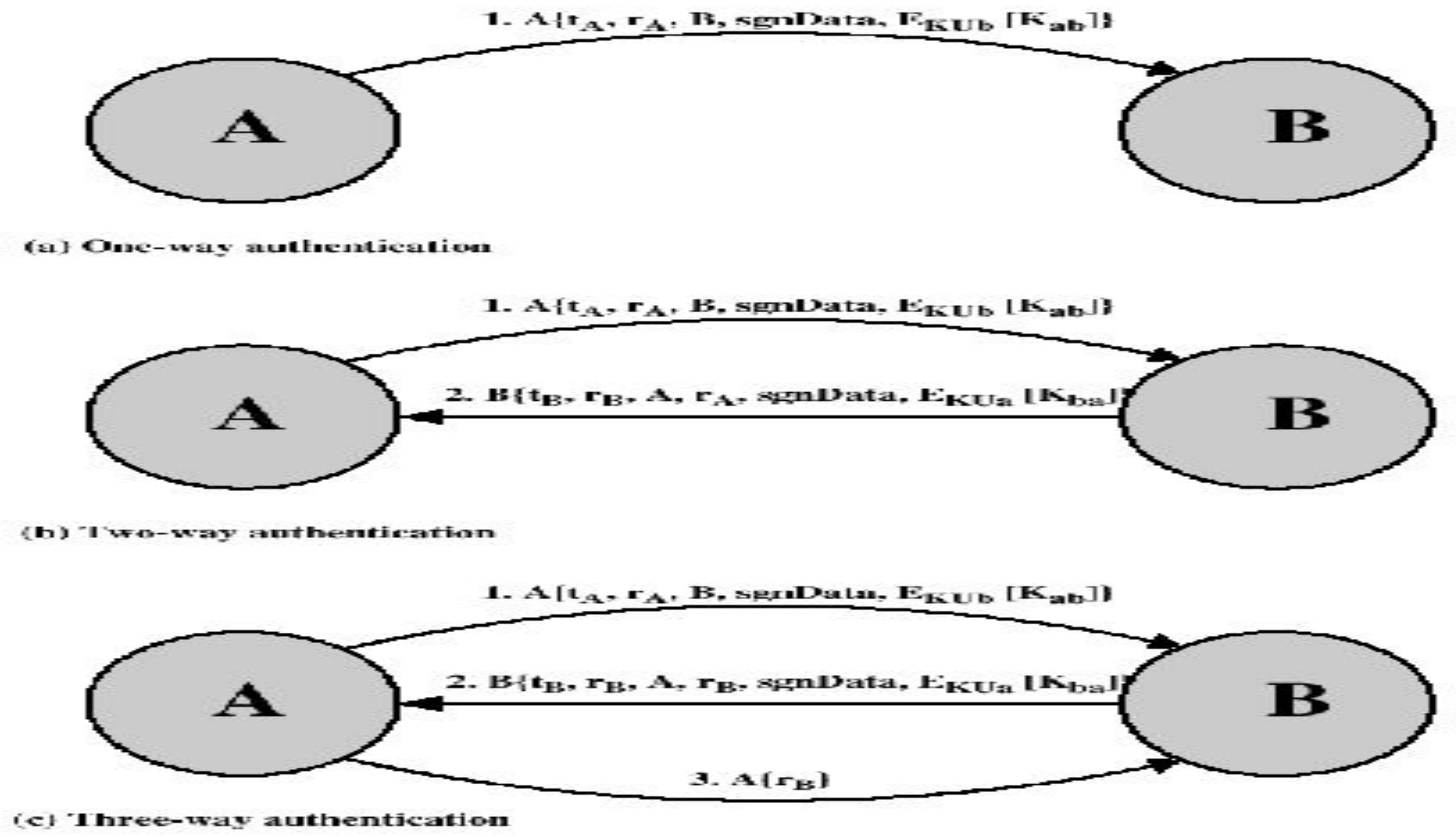


(b) Certificate Revocation List



(b) Certificate Revocation List

Authentication Procedures



1. A{t_A, r_A, B, sgnData, E_{KUb} [K_{ab}]}
A
B
(a) One-way authentication
1. A{t_A, r_A, B, sgnData, E_{KUb} [K_{ab}]}
2. B{t_B, r_B, A, r_A, sgnData, E_{KUa} [K_{ba}]}
A
B
(b) Two-way authentication
1. A{t_A, r_A, B, sgnData, E_{KUb} [K_{ab}]}
2. B{t_B, r_B, A, r_B, sgnData, E_{KUa} [K_{ba}]}
A
B
3. A{r_B}
(c) Three-way authentication

Figure 4.5 X.509 Strong Authentication Procedures

X.509 Service (Continued)

- Authentication procedures
  - One-way
    - Single transfer of information from user to user
  - Two-way
    - Authenticates each to the other
  - Three-way
    - Detects replay attacks using nonces (rather than clock synchronization)
  - In security engineeringIn security engineering, a nonce is an arbitrary number used only once in a cryptographic communication. It is similar in spirit to a nonce wordIn security engineering, a nonce is an arbitrary number used only once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a randomIn security engineering, a nonce is an arbitrary number used only once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-randomIn security engineering, a nonce is an arbitrary number used only once in a cryptographic communication.

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
- may include additional info for A

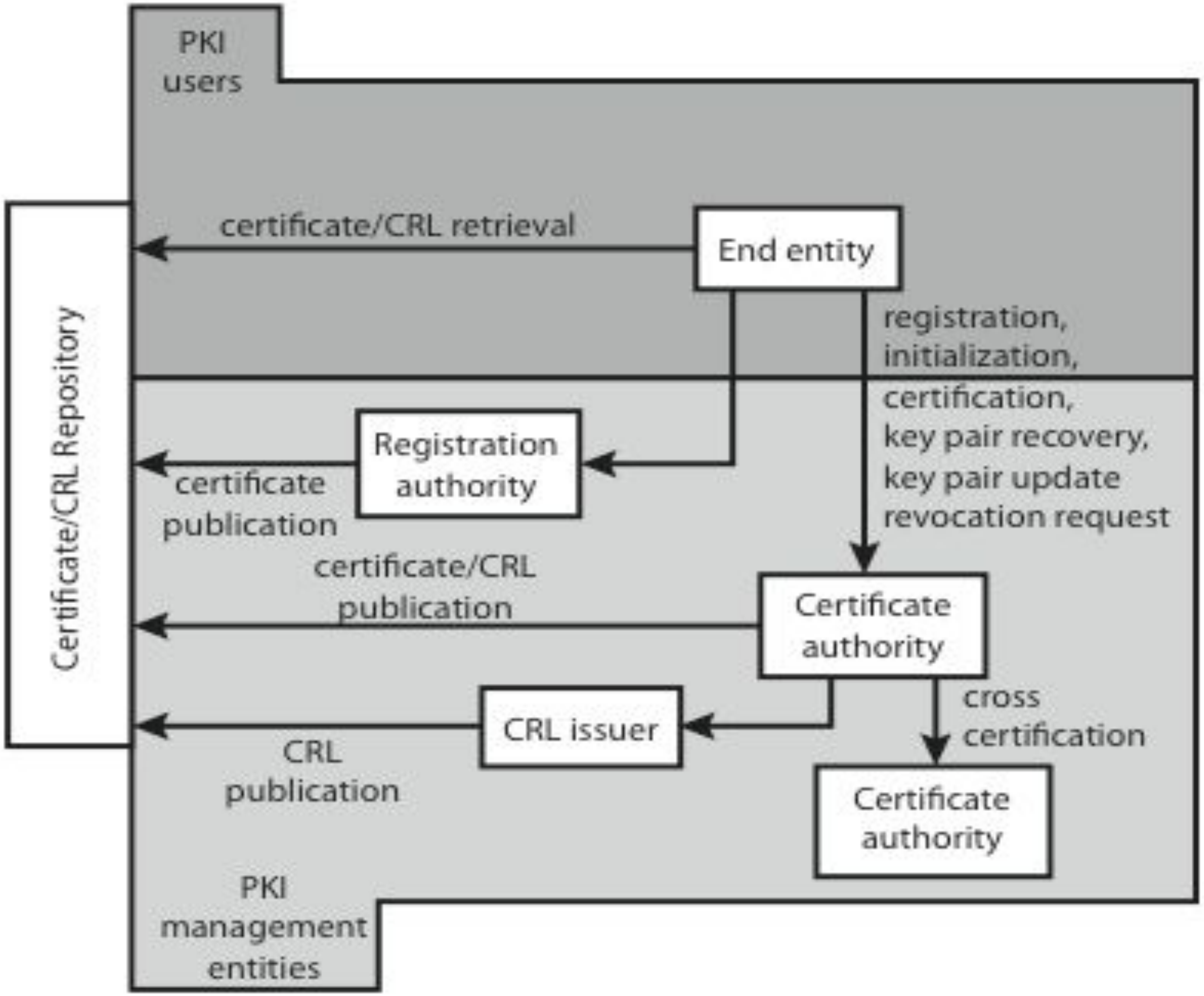
Three-Way Authentication

- 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

Summary

- *Kerberos* trusted key server system
- *X.509* in Digital certificates

Public Key Infrastructure


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