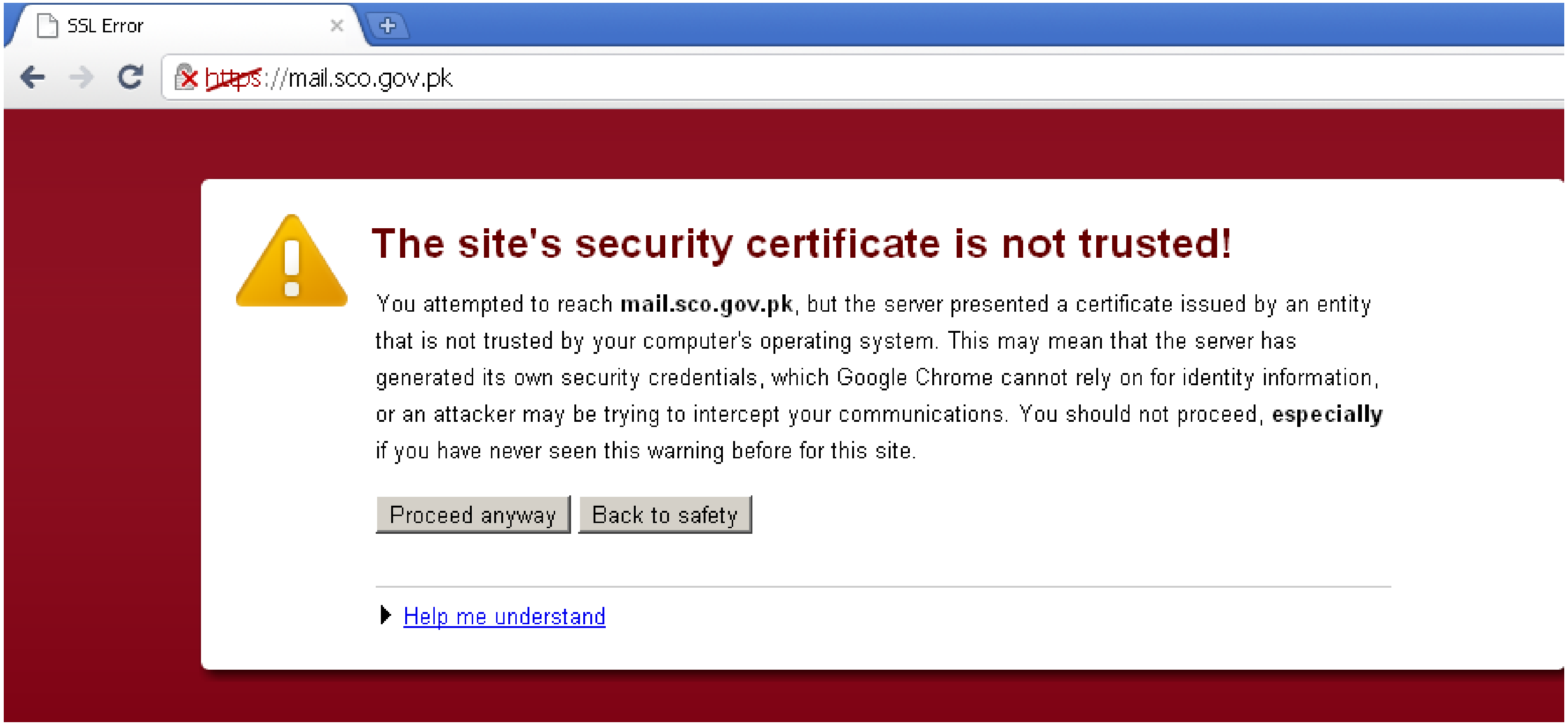
Network Security

Asim Rasheed

Where we are …

- Introduction to network security
- Vulnerabilities in IP
- I. CRYPTOGRAPHY
  - Symmetric Encryption and Message Confidentiality
  - Public-Key Cryptography and Message Authentication
- II. NETWORK SECURITY APPLICATIONS
  - Authentication Applications (Kerberos, X.509)
  - Electronic Mail Security (PGP, S/MIME)
  - IP Security (IPSec, AH, ESP, IKE)
  - Web Security (SSL, TLS, SET)
- III. SYSTEM SECURITY
  - Intruders and intrusion detection
  - Malicious Software (viruses)
  - Firewalls and trusted systems

Certificate Error



The site's security certificate is not trusted!

You attempted to reach **mail.sco.gov.pk**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

X.509

X.509 Authentication Service

- Part of X.500 directory service standards
  - Distributed servers maintaining some info database
- Defines framework for authentication services
  - Directory may store public-key certificates
- Certificate contains public key of user
  - Signed by private key of certification authority
- Also defines authentication protocols
- Uses public-key cryptography & digital signatures
  - No algorithm standardized, but RSA is recommended

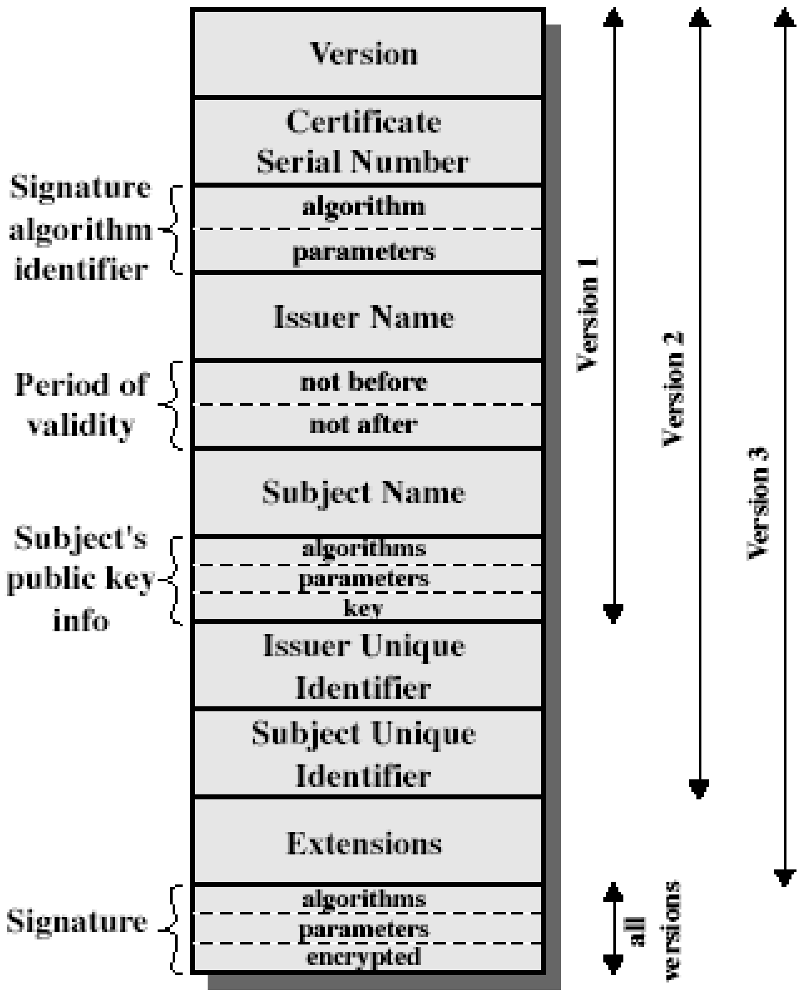
X.509 Certificates

- Public key certificates are associated with each user
- Created by some trusted Certification Authority (CA) and placed in a directory
- X.509 Certificates contain:
  - Version: Three versions are available
  - Serial number: An integer value unique within CA, identifying certificate
  - Signature algorithm identifier: specifies the algorithm used to compute the signature
  - Issuer: X.500 name of issuing CA

X.509 Format

- Validity: contains two subfields, time the certificate becomes valid and the time till it is valid
- Subject: X.500 name of entity whose key is being certified
- Subject public-key info: algorithm identifier and the subject’s public key
- Issuer unique identifier: Optional, identifies the issuer of this certificate
- Subject unique identifier: Optional, identifies the subject of this certificate
- Extension fields
- Signature: hash of all fields in certificate

X.509 Formats



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

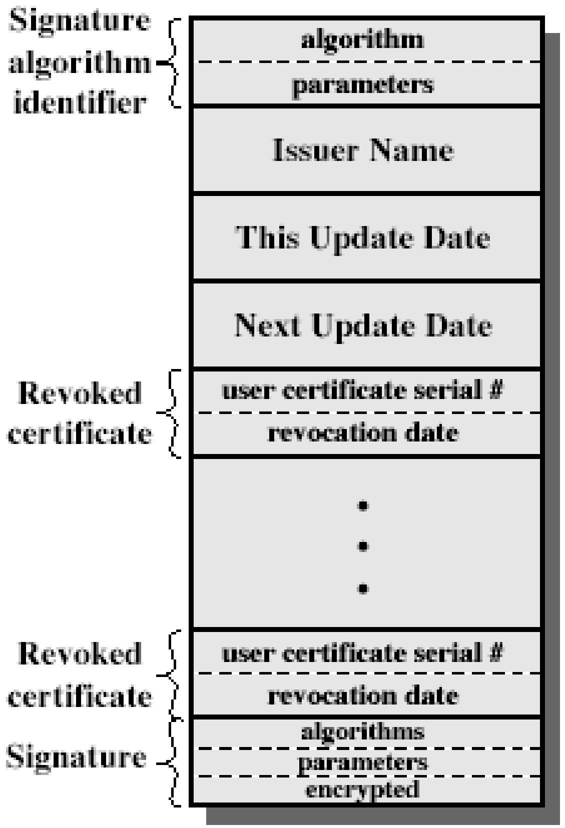
Version 1

Version 2

Version 3

all versions

(a) X.509 Certificate



Signature algorithm identifier: algorithm, parameters

Issuer Name

This Update Date

Next Update Date

Revoked certificate: user certificate serial #, revocation date

•
•
•

Revoked certificate: user certificate serial #, revocation date

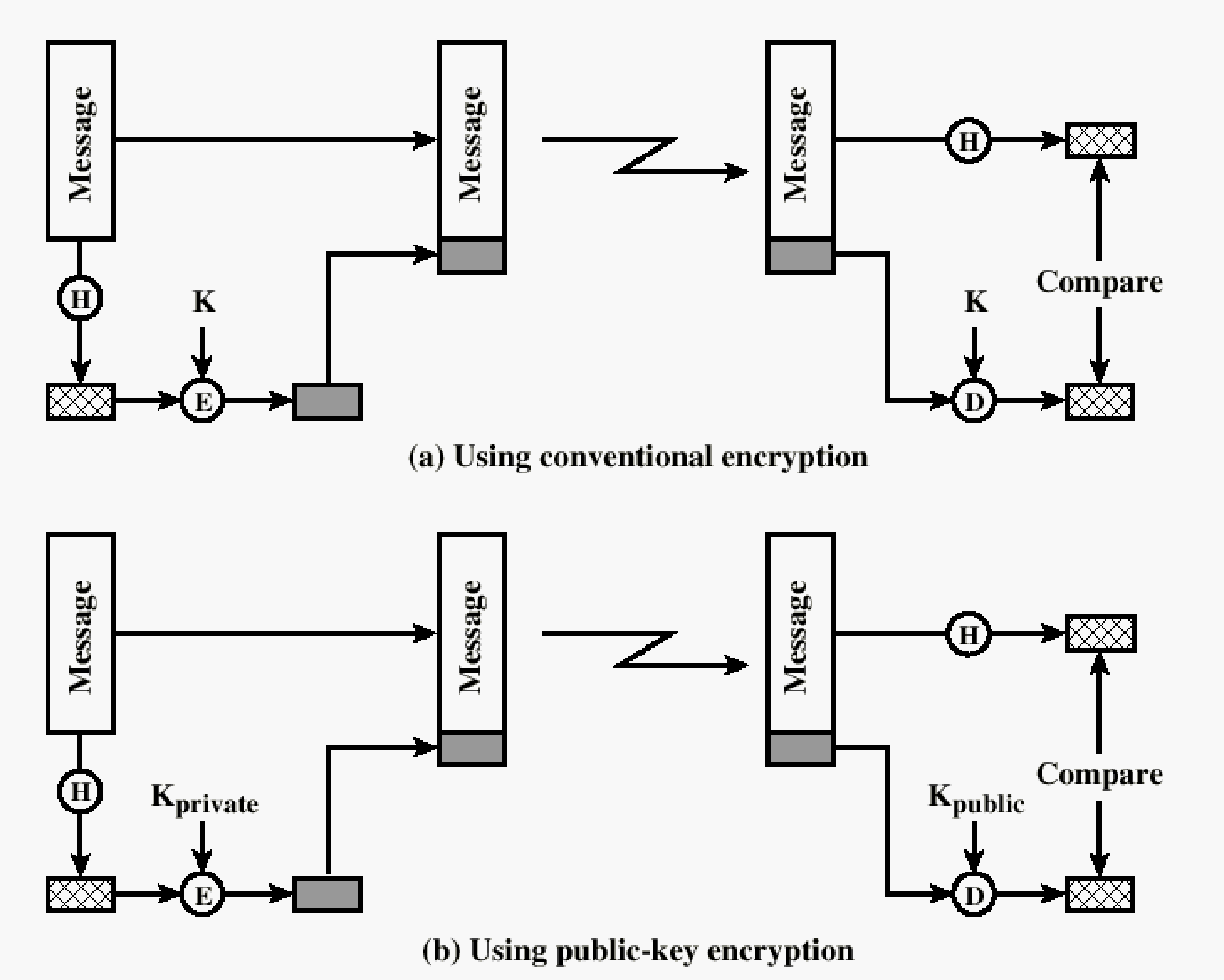
Signature: algorithms, parameters, encrypted

(b) Certificate Revocation List

X.509 Notation

- CA<<A>>
  - Denotes certificate for A signed by CA
- CA signs the certificate with its private key

Typical Digital Signature Approach



(a) Using conventional encryption

(b) Using public-key encryption

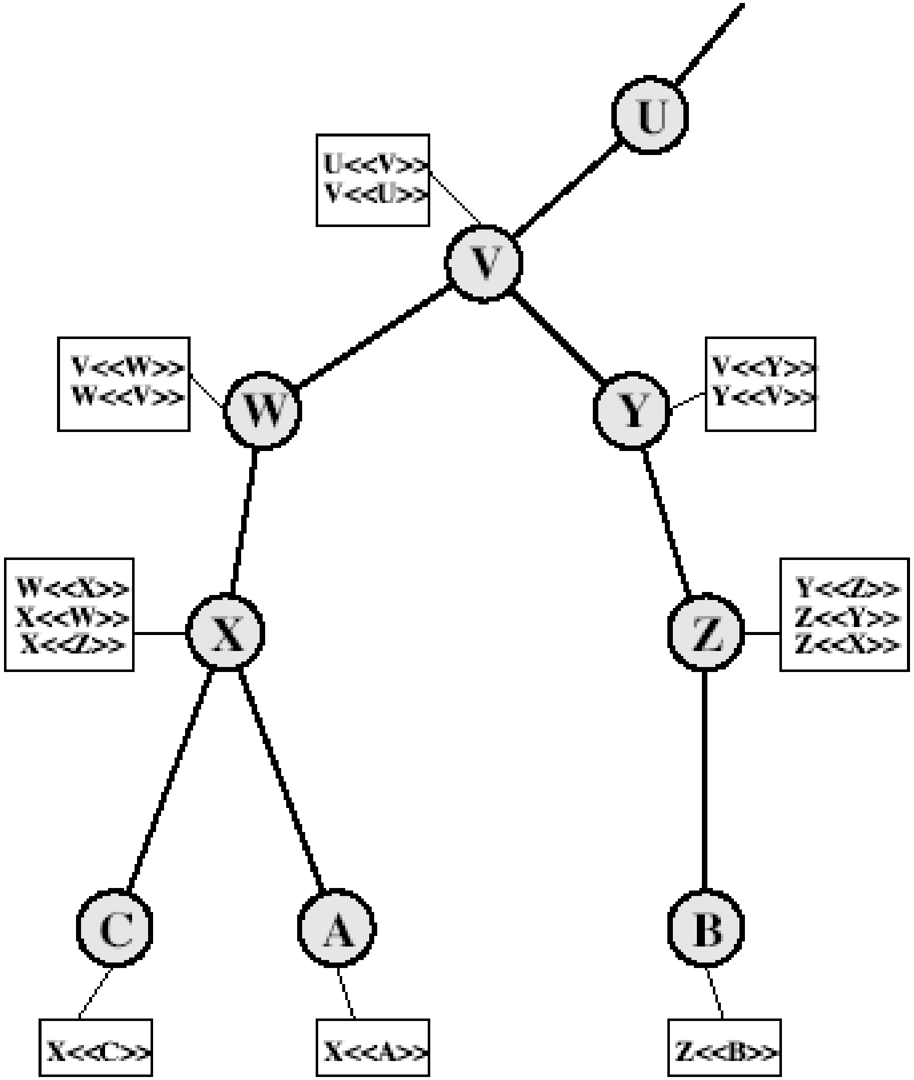
Obtaining a Certificate

- Any user with access to public key of CA can verify user public key
- Only the CA can modify a certificate
- Certificates cannot be forged, therefore, certificates can be placed in a public directory
- All users subscribed to same CA and hence have a common trust
- B having certificate of A, has confidence that message can neither be eavesdropped nor forged

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



CA Hierarchy Use

- User A can acquire certificate for B:

X<<W>> W<<V>> V<<Y>> Y<<Z>>Z<<B>>

- After obtaining these certificates it can get B’s public key
- Each client trusts parent’s certificates
- Enable verification of any certificate from one CA by users of all other CAs in hierarchy

Certificate Revocation

- Certificates have a period of validity
- May need to revoke before expiry, because:
  - user's private key is compromised
  - user is no longer certified by this CA
  - CA's certificate is compromised
- CA’s maintain list of revoked certificates
  - The Certificate Revocation List (CRL)
- Users should check certificates with CA’s CRL

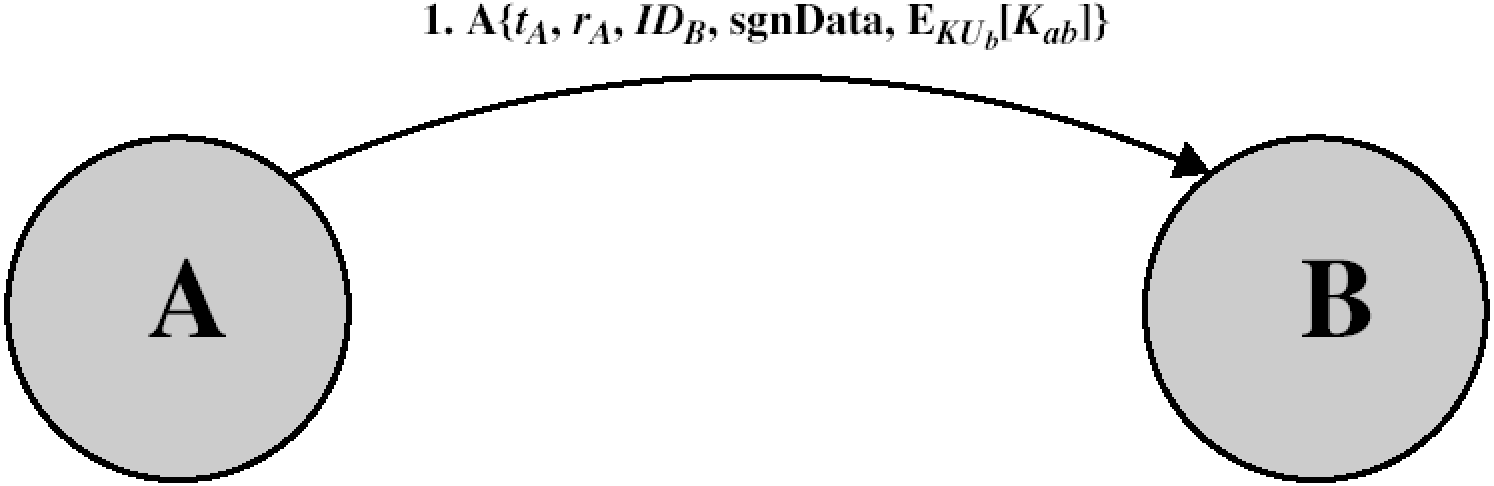
Authentication Procedures

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

One-Way Authentication

- One 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
- May include additional info for B
  - E.g session key

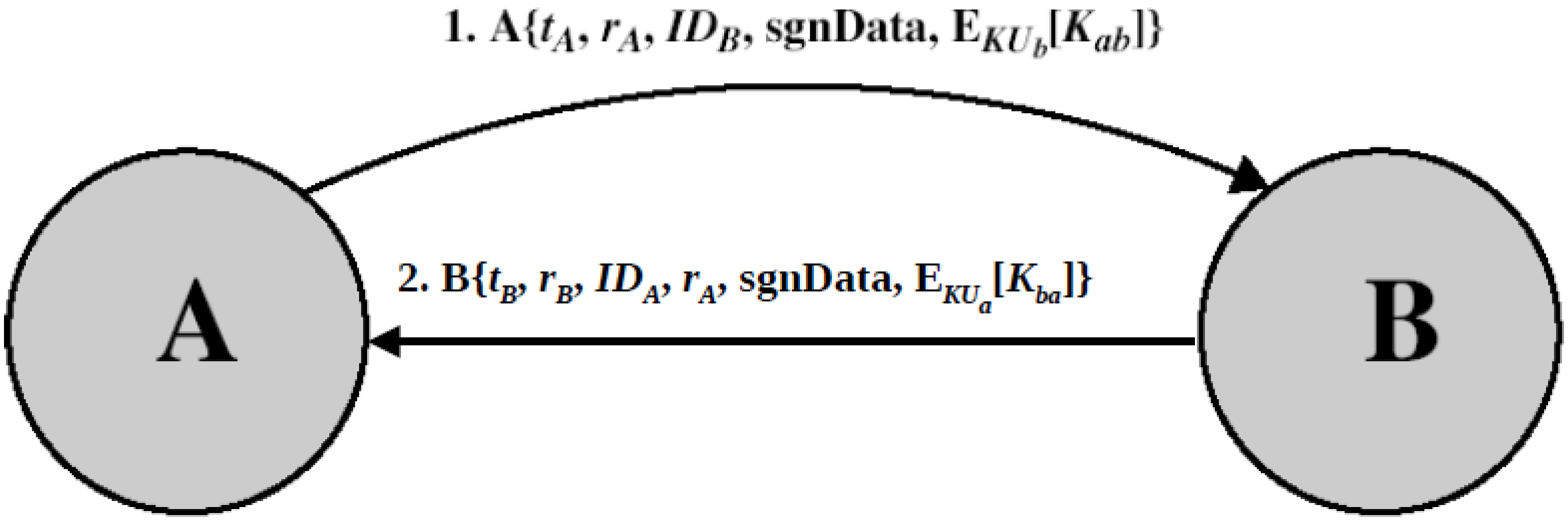
One-Way Authentication



Two-Way Authentication

- Two messages (A->B, B->A), which additionally establishes:
  - 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 and timestamp and nonce from B
- May include additional info for A

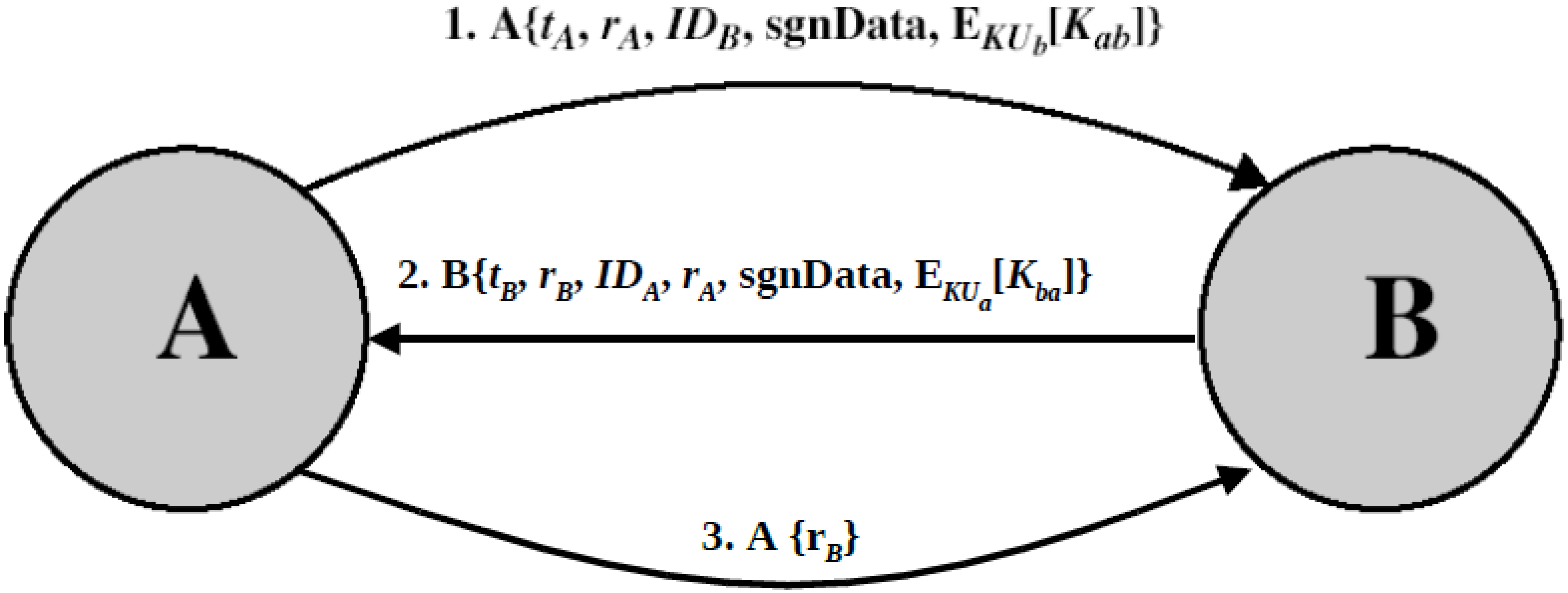
Two-Way Authentication


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

Three-Way Authentication

- Three 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

Three-Way Authentication



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, $E_{KU_a}[K_{ba}]$}

3. A {r_B}

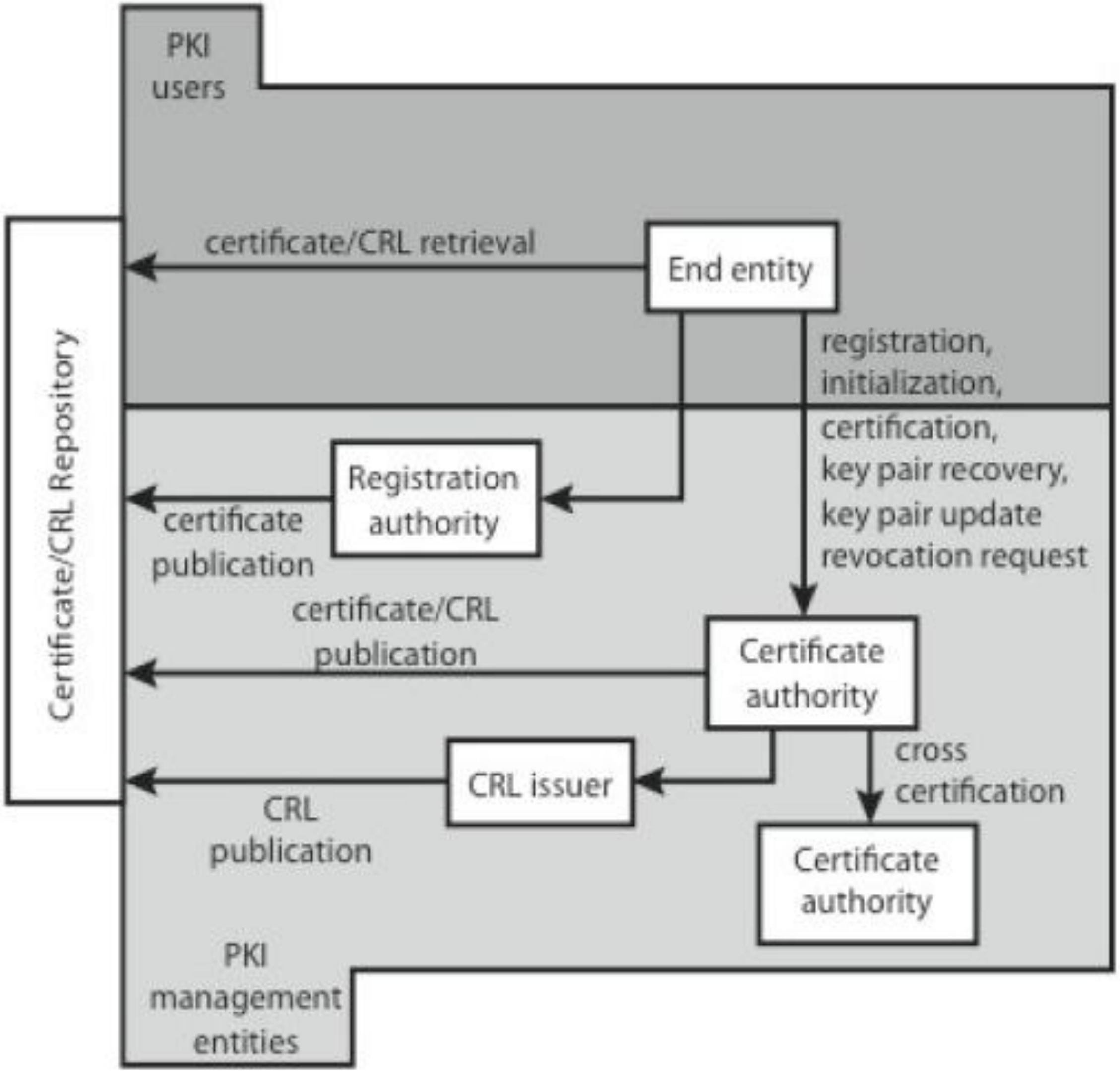
X.509 Version 3

- Has been recognized 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

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

Any question ?