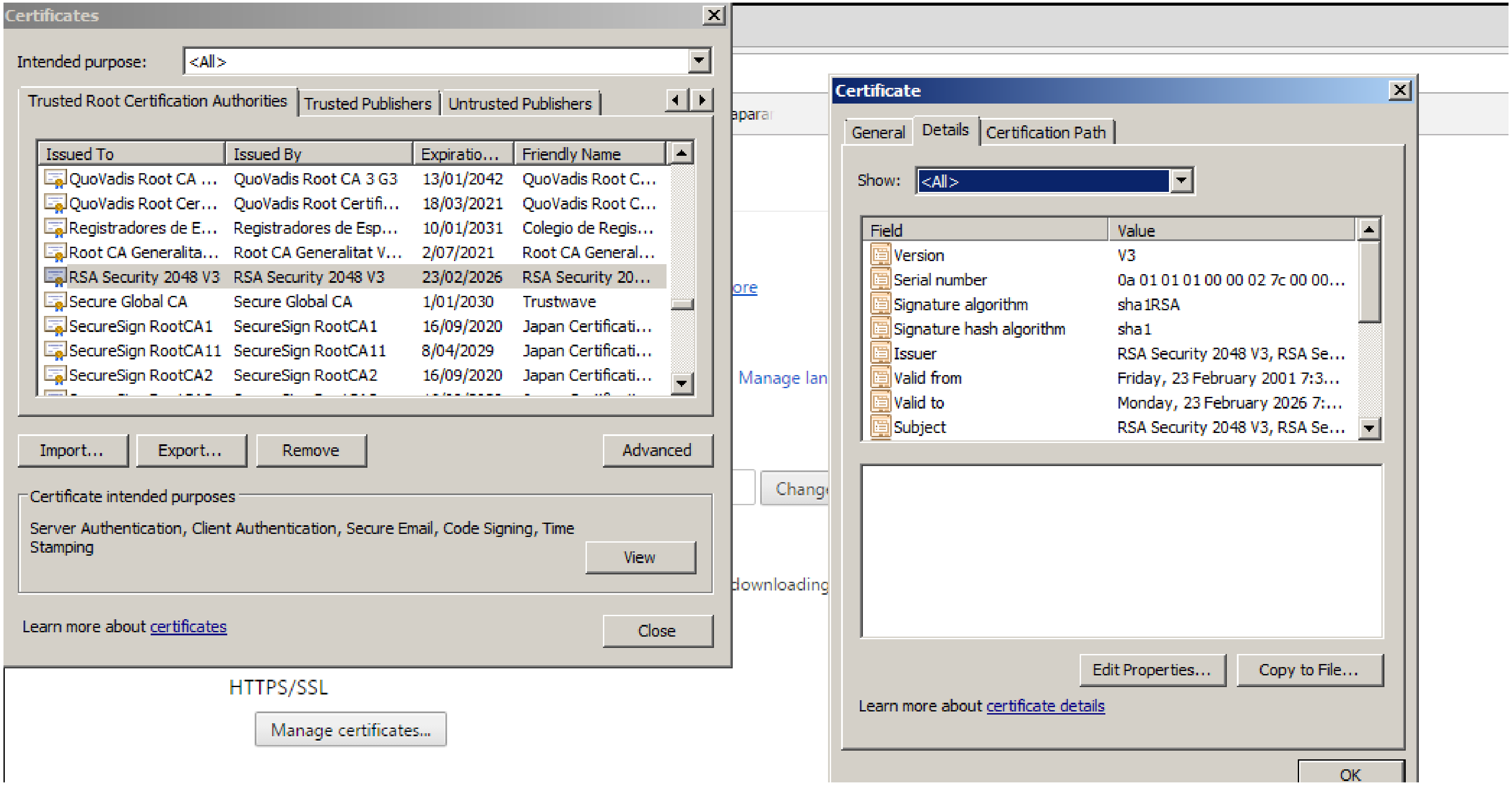
Plan of Talk

- **Certificates Revision**
- **User Authentication**
- **Replay Attacks**
- Needham-Schroeder Protocol
- Remote User-Authentication
- **Example**
  - **Kerberos**

Public Key Certificates

- What are certificates?
  - Example X.509 certificate
- Who creates them?
- What are the main requirements for the use of a certificate scheme?
- How certificates help in User Authentication?

Certificate



Certificates

Intended purpose: <All>

Trusted Root Certification Authorities | Trusted Publishers | Untrusted Publishers

Issued To	Issued By	Expiratio...	Friendly Name
QuoVadis Root CA ...	QuoVadis Root CA 3 G3	13/01/2042	QuoVadis Root C...
QuoVadis Root Cer...	QuoVadis Root Certifi...	18/03/2021	QuoVadis Root C...
Registradores de E...	Registradores de Esp...	10/01/2031	Colegio de Regis...
Root CA Generalita...	Root CA Generalitat V...	2/07/2021	Root CA General...
RSA Security 2048 V3	RSA Security 2048 V3	23/02/2026	RSA Security 20...
Secure Global CA	Secure Global CA	1/01/2030	Trustwave
SecureSign RootCA1	SecureSign RootCA1	16/09/2020	Japan Certificati...
SecureSign RootCA11	SecureSign RootCA11	8/04/2029	Japan Certificati...
SecureSign RootCA2	SecureSign RootCA2	16/09/2020	Japan Certificati...

Certificate intended purposes

Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping

Learn more about certificates

HTTPS/SSL

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	0a 01 01 01 00 00 02 7c 00 00...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	RSA Security 2048 V3, RSA Se...
Valid from	Friday, 23 February 2001 7:3...
Valid to	Monday, 23 February 2026 7:...
Subject	RSA Security 2048 V3, RSA Se...

Learn more about certificate details

X.509 Certificates

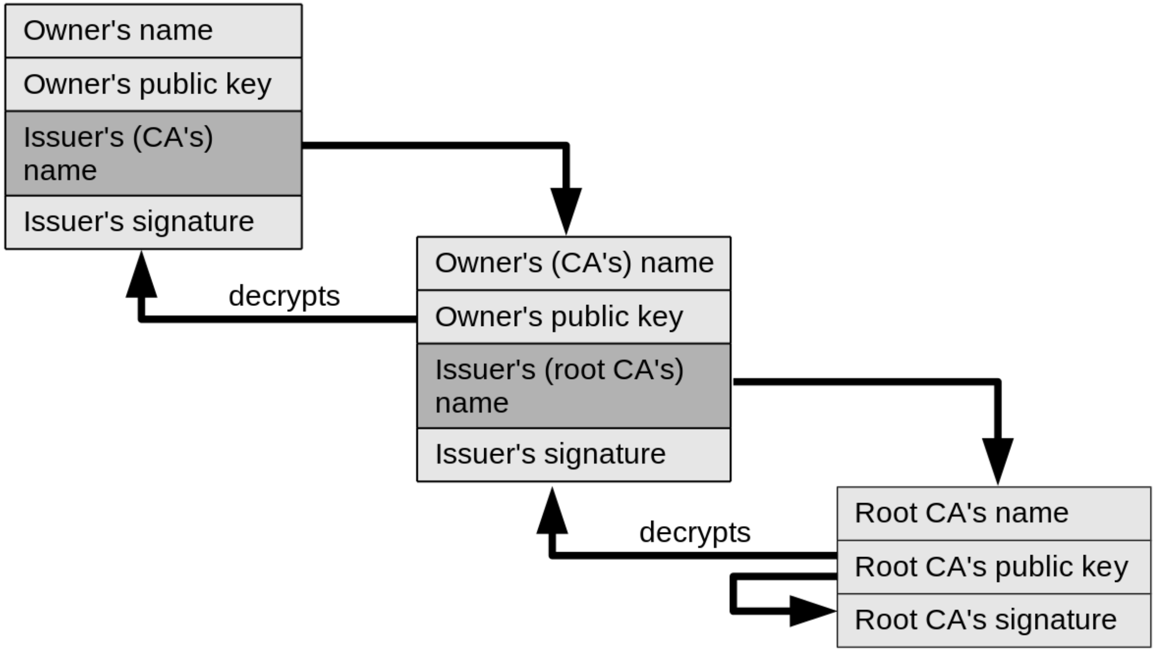
- Created by a trusted Certification Authority (CA) and have the following elements:

- KDC: **PR_{auth} Pu_{auth}**
- Alice's Certificate
- **$C_A = E(PR_{auth}, [ID_A, PU_A, T])$** and Bob's certificate
- **$C_B = E(PR_{auth}, [ID_B, PU_B, T])$**,
- Both trusts KRC, hence they can obtain authenticated public key of each other through verification.

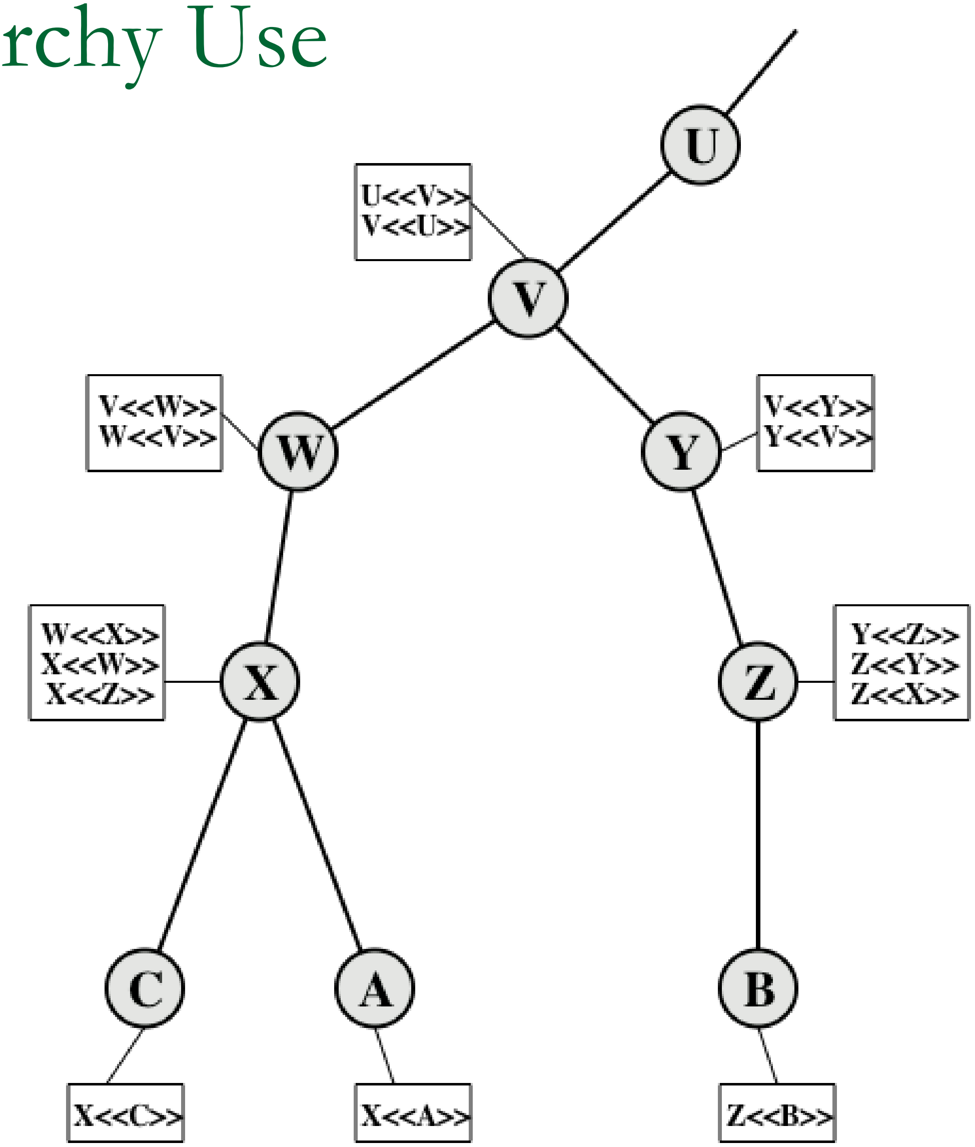
- Version
- Serial number
- Signature algorithm identifier
- Issuer name
- Period of validity
- Subject name
- Subject's public-key information
- Issuer unique identifier
- Subject unique identifier
- Extensions
- Signature

Trust Chains

! Browsers come bundled with trusted root certificates.



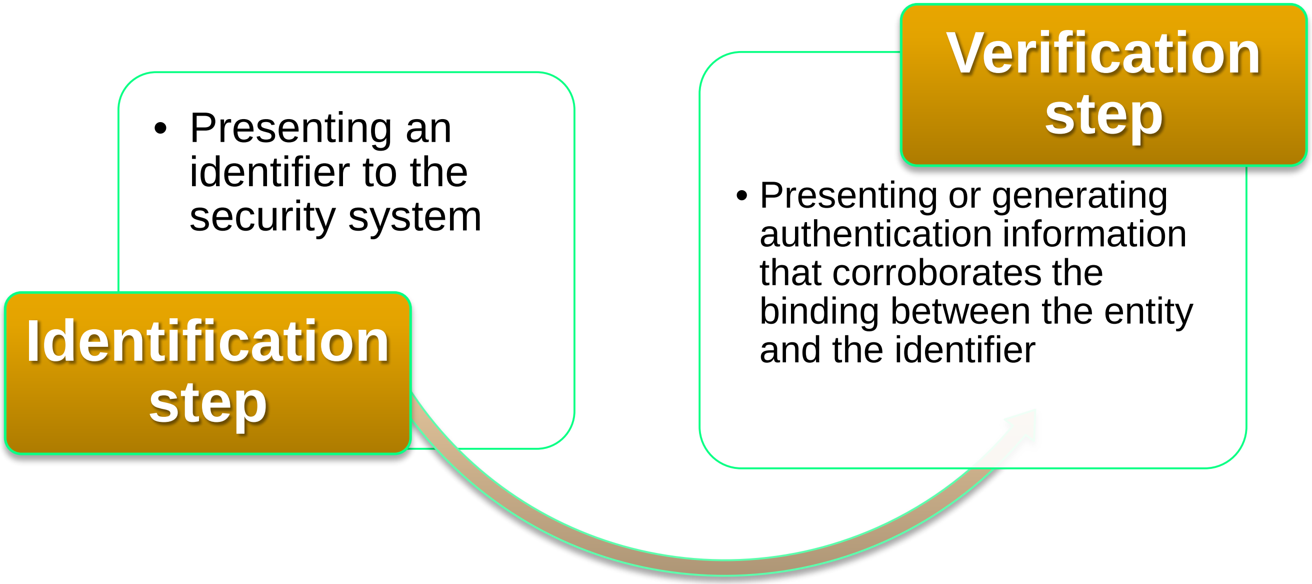
CA Hierarchy Use



Alas part of Certificate Scheme

- What if a certificate is compromised?
- What others reasons you may have for certificates to be revoked?
  - Limited Time validity
  - CA decides to revoke a user
  - Certificate is compromised
- Certificate Revocation List (CRL)is a must.
- We wanted to avoid using directory, but the directory (through CRL) comes back!

User Authentication



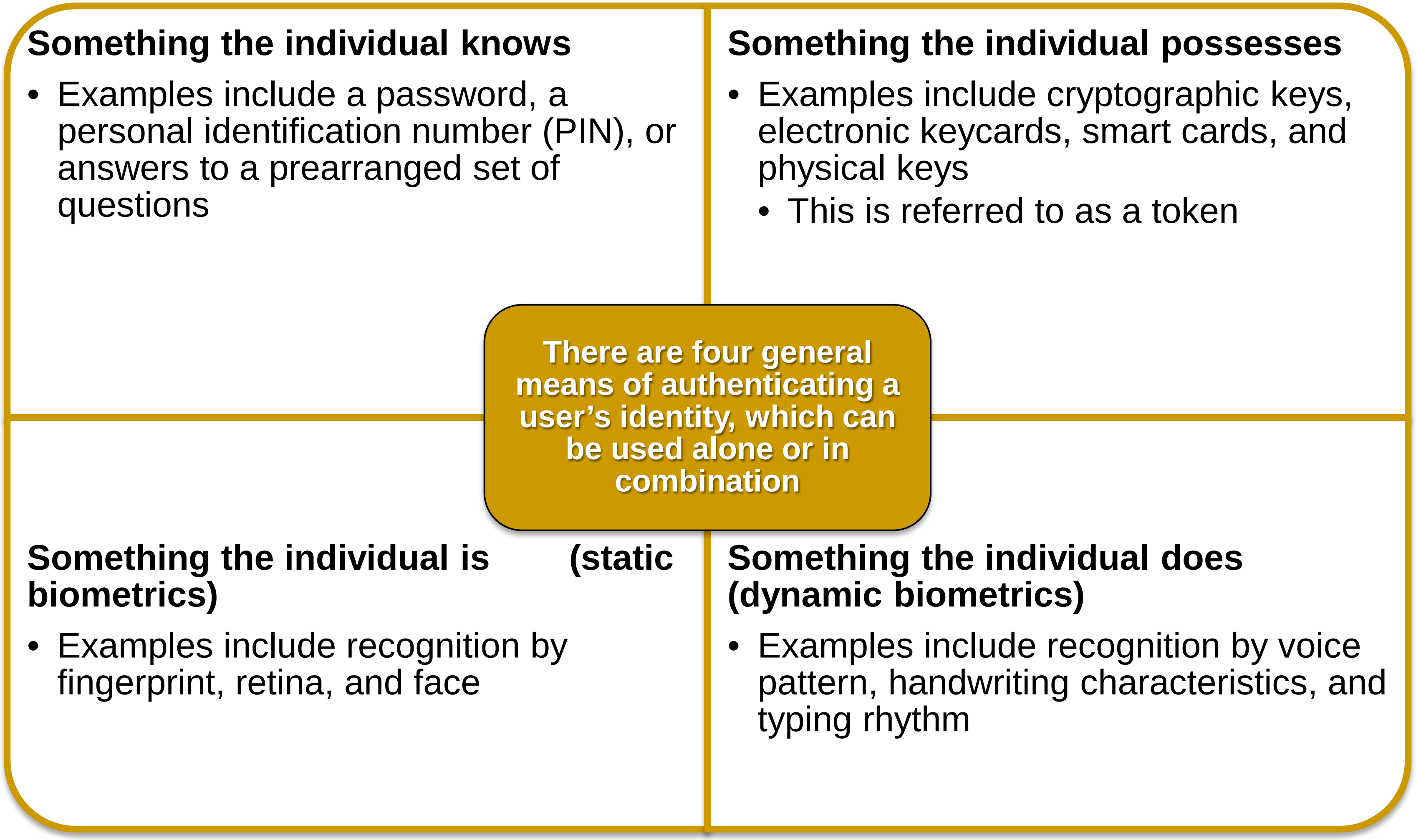
Identification step

- Presenting an identifier to the security system

Verification step

- Presenting or generating authentication information that corroborates the binding between the entity and the identifier

Means of User Authentication



Something the individual knows

- Examples include a password, a personal identification number (PIN), or answers to a prearranged set of questions

Something the individual possesses

- Examples include cryptographic keys, electronic keycards, smart cards, and physical keys
  - This is referred to as a token

There are four general means of authenticating a user's identity, which can be used alone or in combination

Something the individual is (static biometrics)

- Examples include recognition by fingerprint, retina, and face

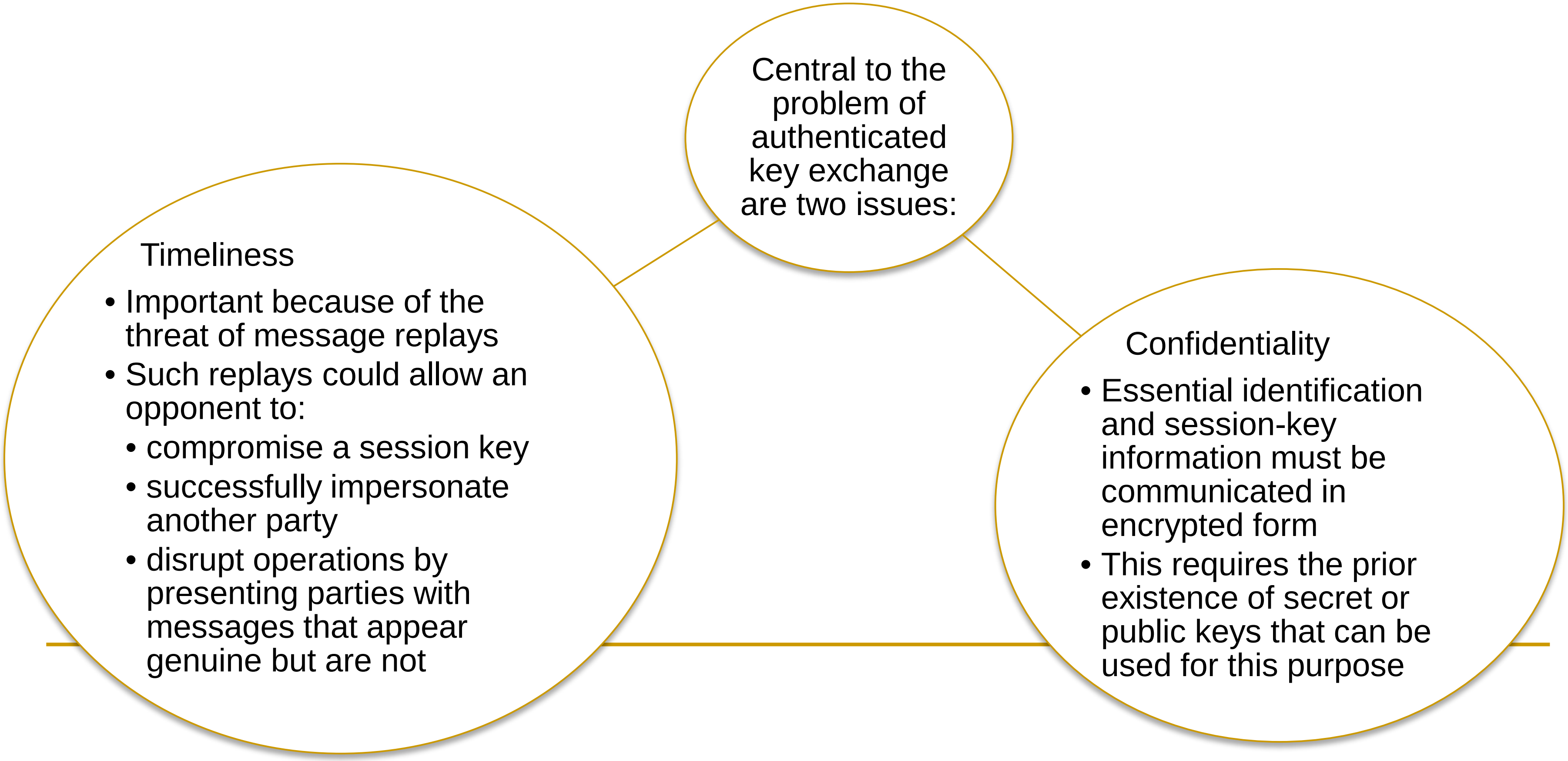
Something the individual does (dynamic biometrics)

- Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm

- For network-based user authentication, the most important methods involve cryptographic keys and something the individual knows, such as a password

Mutual Authentication

- Protocols which enable communicating parties to satisfy themselves mutually about each other’s identity and to exchange session keys



Central to the problem of authenticated key exchange are two issues:

Timeliness

- Important because of the threat of message replays
- Such replays could allow an opponent to:
  - compromise a session key
  - successfully impersonate another party
  - disrupt operations by presenting parties with messages that appear genuine but are not

Confidentiality

- Essential identification and session-key information must be communicated in encrypted form
- This requires the prior existence of secret or public keys that can be used for this purpose

Replay Attacks

1. The simplest replay attack is one in which the opponent simply copies a message and replays it later
2. An opponent can replay a timestamped message within the valid time window
3. An opponent can replay a timestamped message within the valid time window, but in addition, the opponent suppresses the original message; thus, the repetition cannot be detected
4. Another attack involves a backward replay without modification and is possible if symmetric encryption is used and the sender cannot easily recognize the difference between messages sent and messages received on the basis of content

Approaches to Coping With Replay Attacks

- Attach a sequence number to each message used in an authentication exchange
  - A new message is accepted only if its sequence number is in the proper order
  - Difficulty with this approach is that it requires each party to keep track of the last sequence number for each claimant it has dealt with
  - Generally not used for authentication and key exchange because of overhead

- Timestamps
  - Requires that clocks among the various participants be synchronized
  - Party A accepts a message as fresh only if the message contains a timestamp that, in A’s judgment, is close enough to A’s knowledge of current time

- Challenge/response
  - Party A, expecting a fresh message from B, first sends B a nonce (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value

One-Way Authentication

One application for which encryption is growing in popularity is electronic mail (e-mail)

- Header of the e-mail message must be in the clear so that the message can be handled by the store-and-forward e-mail protocol, such as SMTP or X.400
- The e-mail message should be encrypted such that the mail-handling system is not in possession of the decryption key

A second requirement is that of authentication

- The recipient wants some assurance that the message is from the alleged sender

Remote User-Authentication Using Symmetric Encryption

A two-level hierarchy of symmetric keys can be used to provide confidentiality for communication in a distributed environment

- Strategy involves the use of a trusted key distribution center (KDC)
- Each party shares a secret key, known as a master key, with the KDC
- KDC is responsible for generating keys to be used for a short time over a connection between two parties and for distributing those keys using the master keys to protect the distribution

Needham-Schroeder Protocol

- Original third-party key distribution protocol for session between A B mediated by KDC
- Protocol overview is:

1. A->KDC: $ID_A \| ID_B \| N_1$

2. KDC -> A: $E(K_a,[K_s\|ID_B\|N_1\| E(K_b,[K_s\|ID_A]))])$

3. A -> B: $E(K_b, [K_s\|ID_A])$

4. B -> A: $E(K_s, [N_2])$

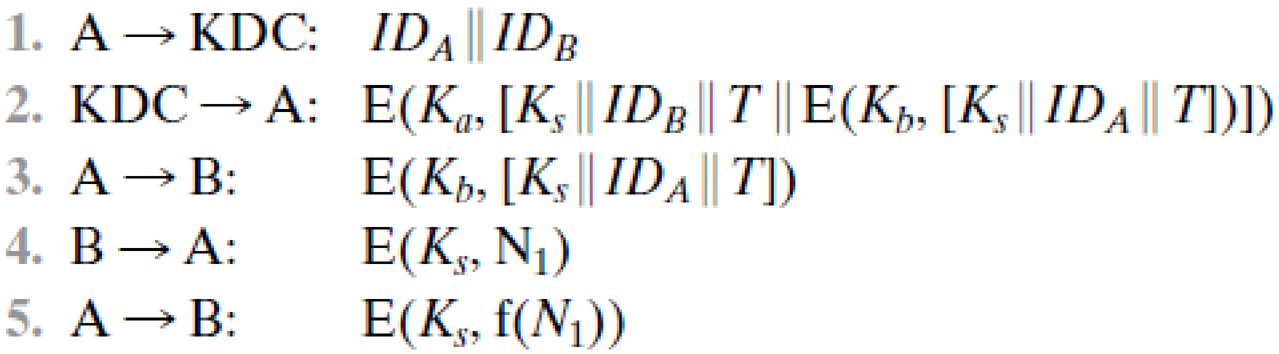
5. A -> B: $E(K_s, [f(N_2)])$

Needham-Schroeder Protocol

- Used to securely distribute a new session key for communications between A & B
- But is vulnerable to a replay attack if an old session key has been compromised
  - then message 3 can be resent convincing B that is communicating with A
- Modifications to address this require:
  - timestamps in steps 2 & 3 (Denning 81)(See also questions in the workshop)
  - using an extra nonce (Neuman 93)

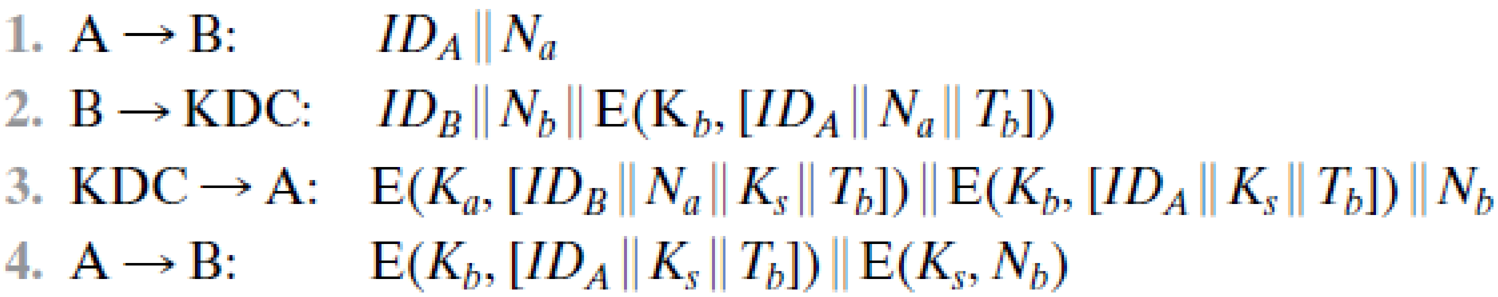
Needham-Schroeder Protocol

- Denning 81 Modification



1. A → KDC: $ID_A \| ID_B$
2. KDC → A: $E(K_a, [K_s \| ID_B \| T \| E(K_b, [K_s \| ID_A \| T])])$
3. A → B: $E(K_b, [K_s \| ID_A \| T])$
4. B → A: $E(K_s, N_1)$
5. A → B: $E(K_s, f(N_1))$

- Neuman 93 Modification



1. A → B: $ID_A \| N_a$
2. B → KDC: $ID_B \| N_b \| E(K_b, [ID_A \| N_a \| T_b])$
3. KDC → A: $E(K_a, [ID_B \| N_a \| K_s \| T_b]) \| E(K_b, [ID_A \| K_s \| T_b]) \| N_b$
4. A → B: $E(K_b, [ID_A \| K_s \| T_b]) \| E(K_s, N_b)$

Suppress-Replay Attacks

- The Denning protocol requires reliance on clocks that are synchronized throughout the network
- A risk involved is based on the fact that the distributed clocks can become unsynchronized as a result of sabotage on or faults in the clocks or the synchronization mechanism
- The problem occurs when a sender's clock is ahead of the intended recipient's clock
  - An opponent can intercept a message from the sender and replay it later when the timestamp in the message becomes current at the recipient's site
  - Such attacks are referred to as *suppress-replay attacks*

Main Application

- Kerberos: See next set of notes.

Authentication using Public Key Approach

- Many varieties of protocols exist.
- We saw before a scheme based on public key encryption.
- Important issue is each party should have correct public key of the other
- A method using Authentication Server is a possibility.
- Various protocols exist making use of time stamps and nonces.