



# APLIKASI-APLIKASI AUTHENTIKASI

Muhammad Adri

AMIK - STMIK Jaya Nusa  
Padang

1

## Topik Pembahasan :

- Security Concerns
- Kerberos
- X.509 Authentication Service

2

## Security Concerns

- key concerns are **confidentiality** and **timeliness**
- to provide confidentiality must encrypt identification and session key info
- which requires the use of previously shared private or public keys
- need timeliness to prevent **replay attacks**
- provided by using sequence numbers or timestamps or challenge/response

3

## KERBEROS



In Greek mythology, a many headed dog, the guardian of the entrance of Hades

4

## KERBEROS

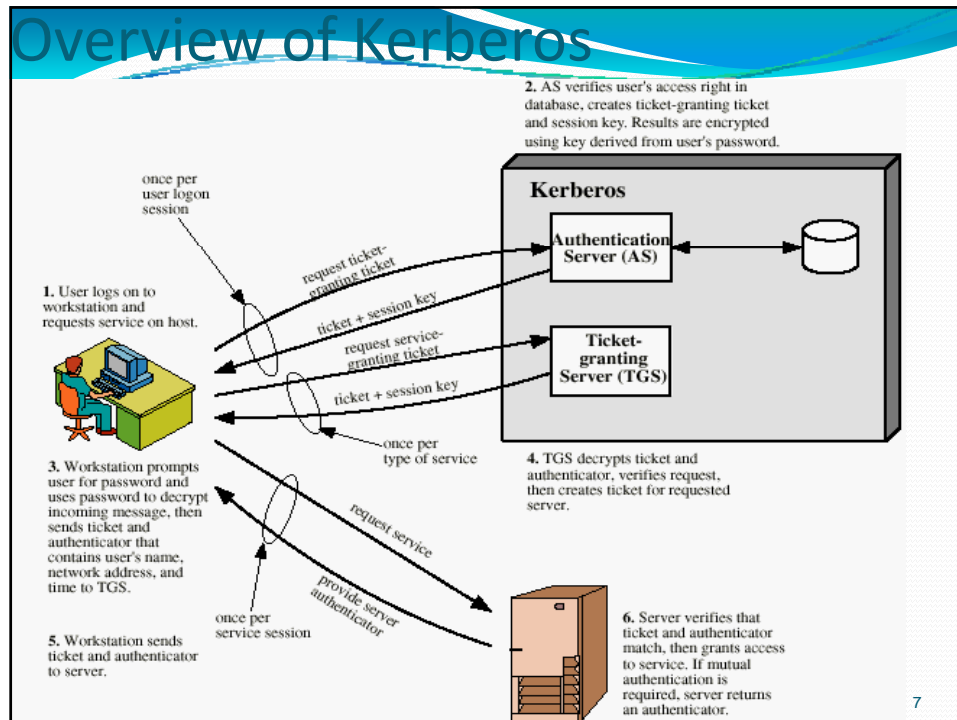
- Users wish to access services on servers.
- Three threats exist:
  - User pretend to be another user.
  - User alter the network address of a workstation.
  - User eavesdrop on exchanges and use a replay attack.

5

## KERBEROS

- Provides a centralized authentication server to authenticate users to servers and servers to users.
- Relies on conventional encryption, making no use of public-key encryption
- Two versions: version 4 and 5
- Version 4 makes use of DES

6



## Kerberos - in practice

### To use Kerberos:

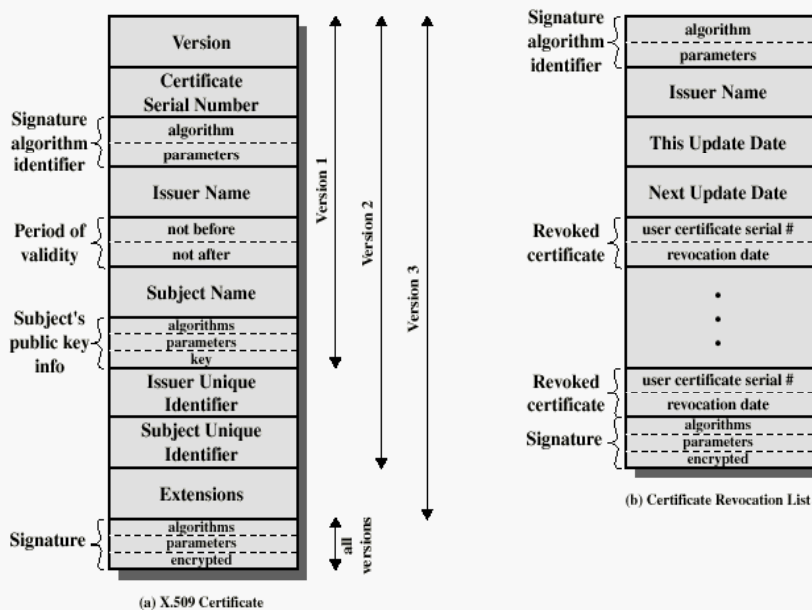
- need to have a KDC on your network
- need to have Kerberised applications running on all participating systems
- major problem - US export restrictions
- Kerberos cannot be directly distributed outside the US in source format (& binary versions must obscure crypto routine entry points and have no encryption)
- else crypto libraries must be reimplemented locally

## X.509 Authentication Service

- Distributed set of servers that maintains a database about users.
- 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.
- RSA is recommended to use.

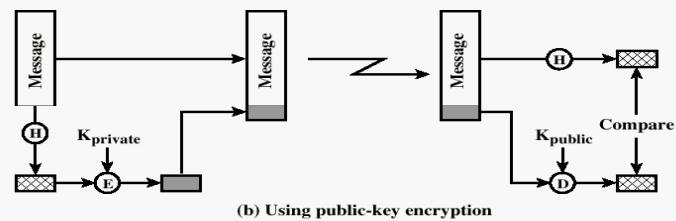
9

## X.509 Formats



10

## Typical Digital Signature Approach

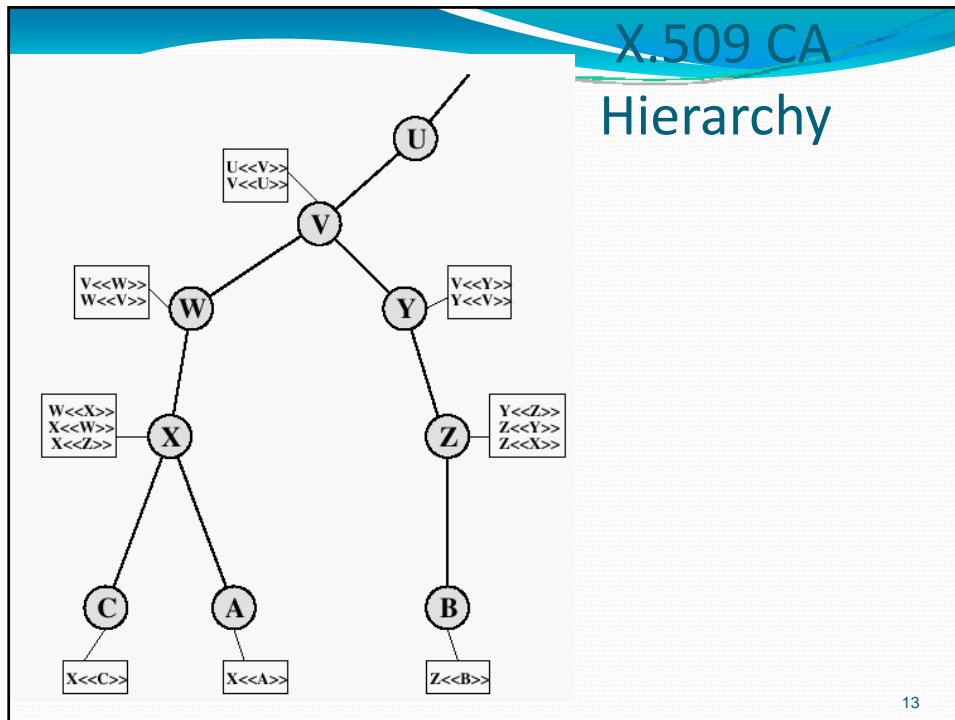


11

## Obtaining a User's Certificate

- Characteristics of certificates generated by CA:
  - Any user with access to the public key of the CA can recover the user public key that was certified.
  - No part other than the CA can modify the certificate without this being detected.

12



## Revocation of Certificates

- Reasons for revocation:
  - The user's secret key is assumed to be compromised.
  - The user is no longer certified by this CA.
  - The CA's certificate is assumed to be compromised.