Cryptography and Network Security II

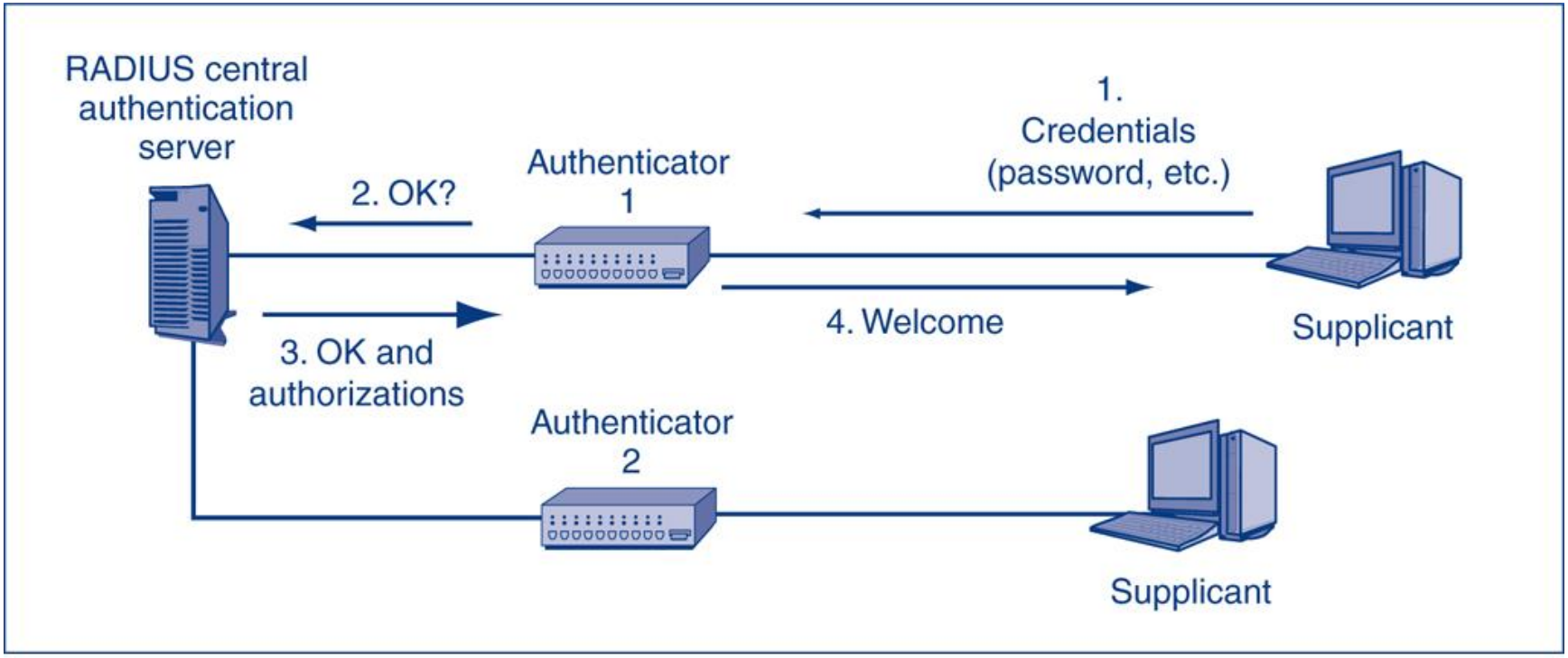
Second Course

Lecture 8: Internet Authentication Applications

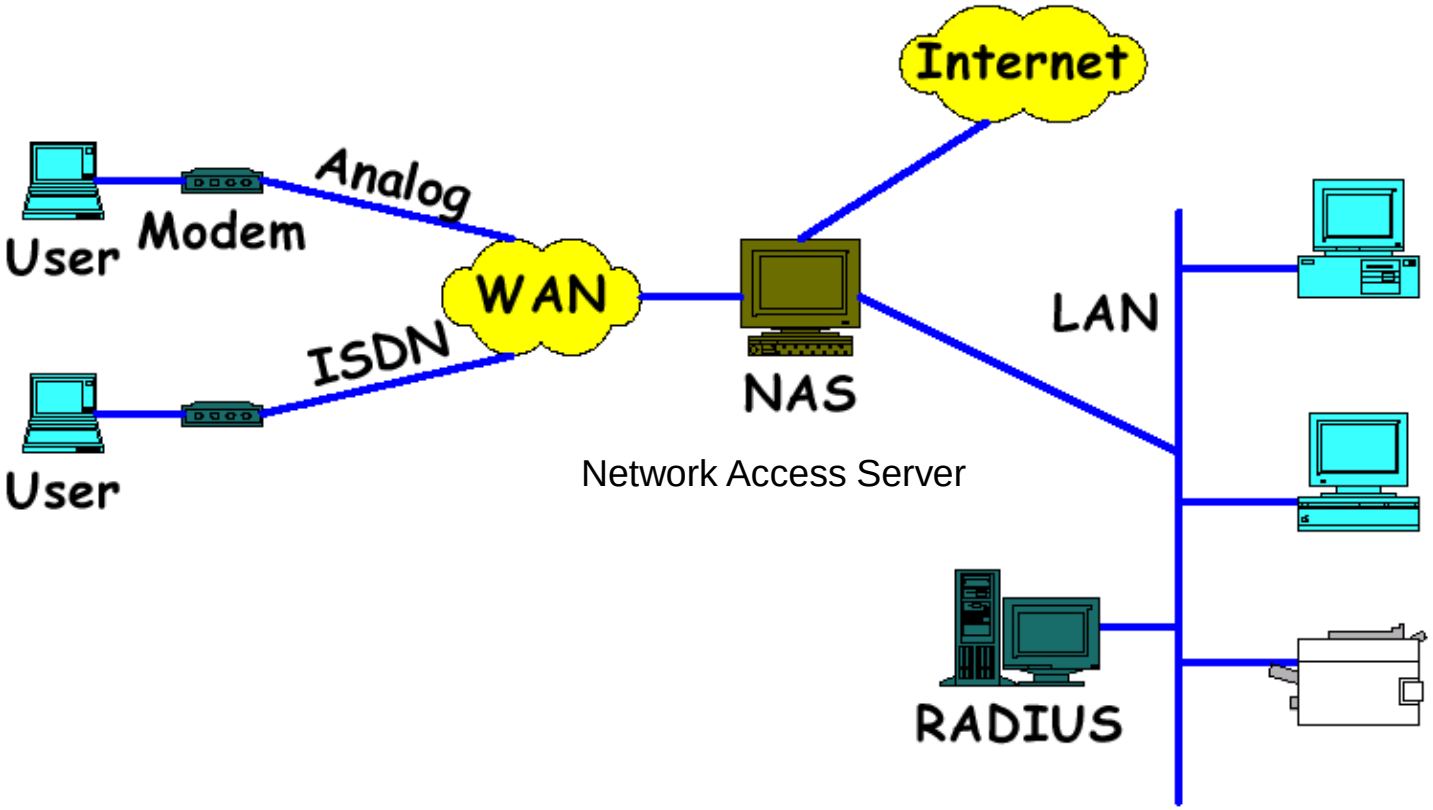
Internet Authentication Applications

- Internet authentication functions: Developed to support application-level authentication & digital signatures
- Will consider
  - RADIUS
  - Kerberos private-key authentication service
  - X.509 public-key directory authentication
  - Public-key infrastructure (PKI)
  - Federated identity management

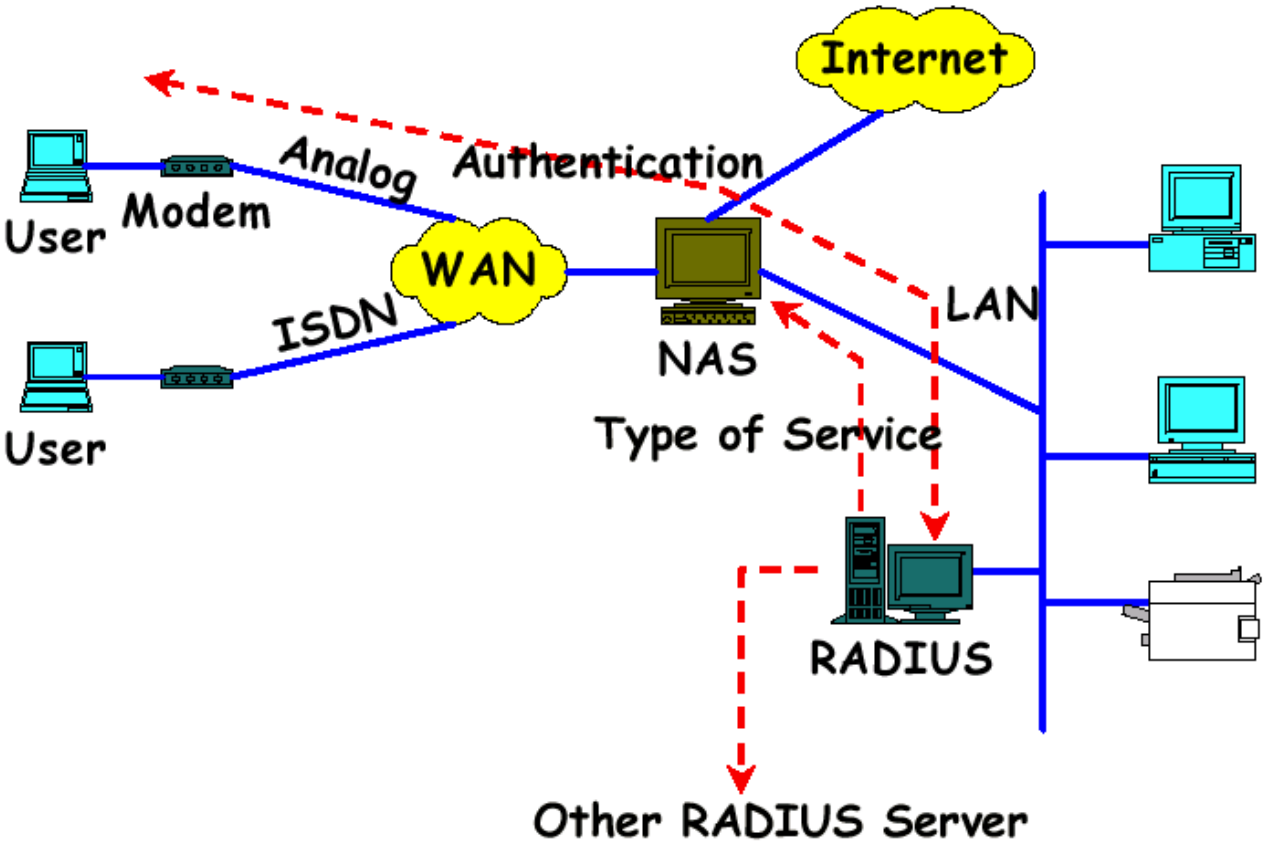
RADIUS Architecture



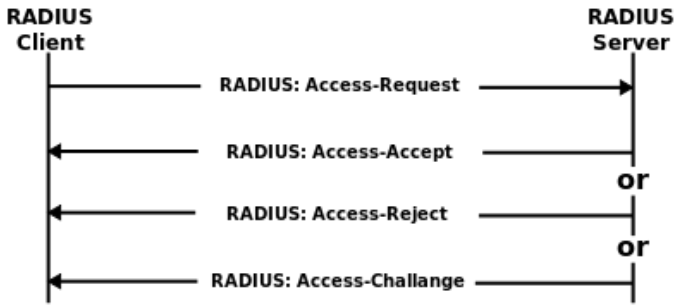
RADIUS Components

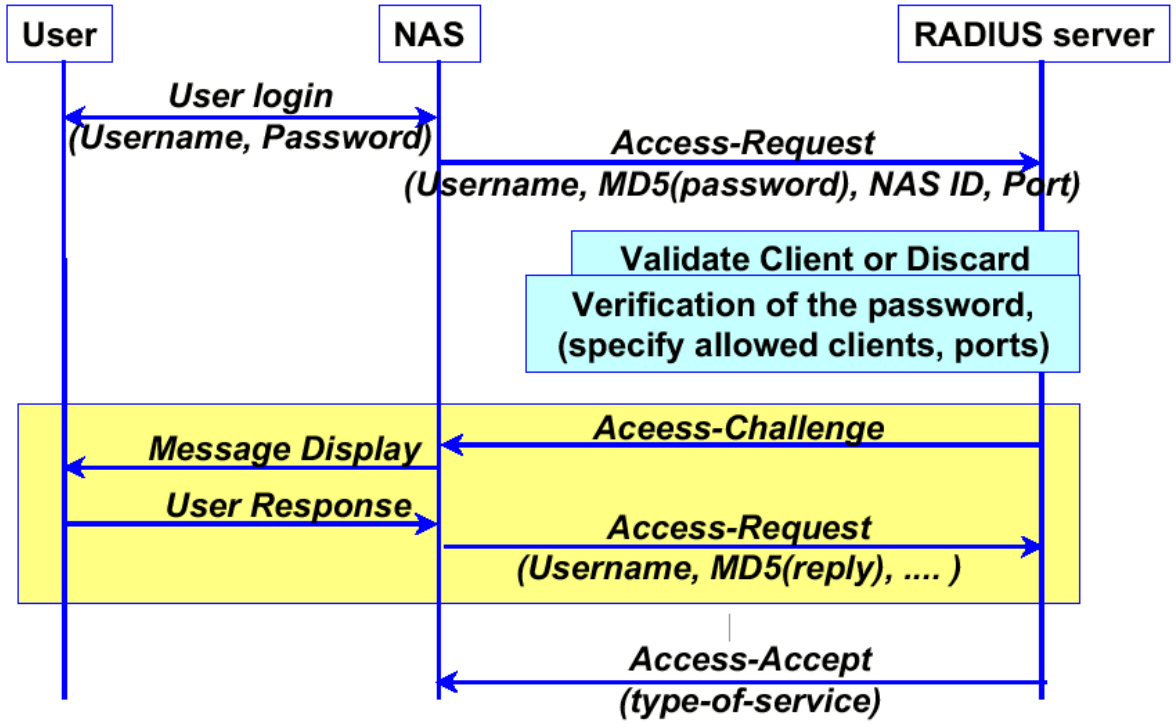


RADIUS Architecture



Authentication Flow





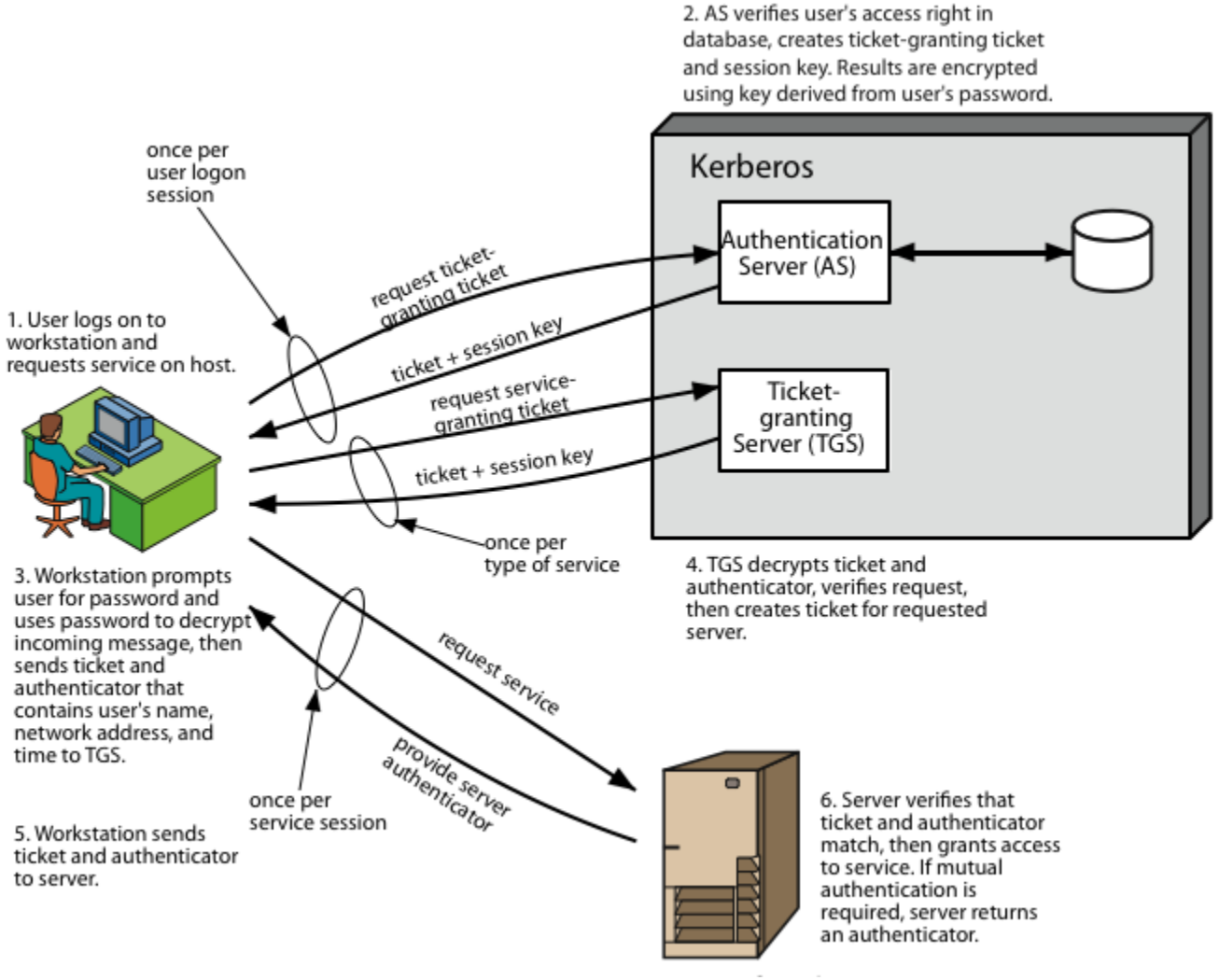
Kerberos

- Trusted key server system from MIT
- Provides centralised private-key third-party authentication in a distributed network
  - Allows users access to services distributed through network
  - Without needing to trust all workstations
  - Rather all trust a central authentication server
- Two versions in use: 4 & 5

Kerberos Overview

- A basic third-party authentication scheme
- Have an Authentication Server (AS)
  - Users initially negotiate with AS to identify self
  - AS provides a non-corruptible authentication credential (ticket granting ticket TGT)
- Have a Ticket Granting server (TGS)
  - Users subsequently request access to other services from TGS on basis of users TGT

Kerberos Overview



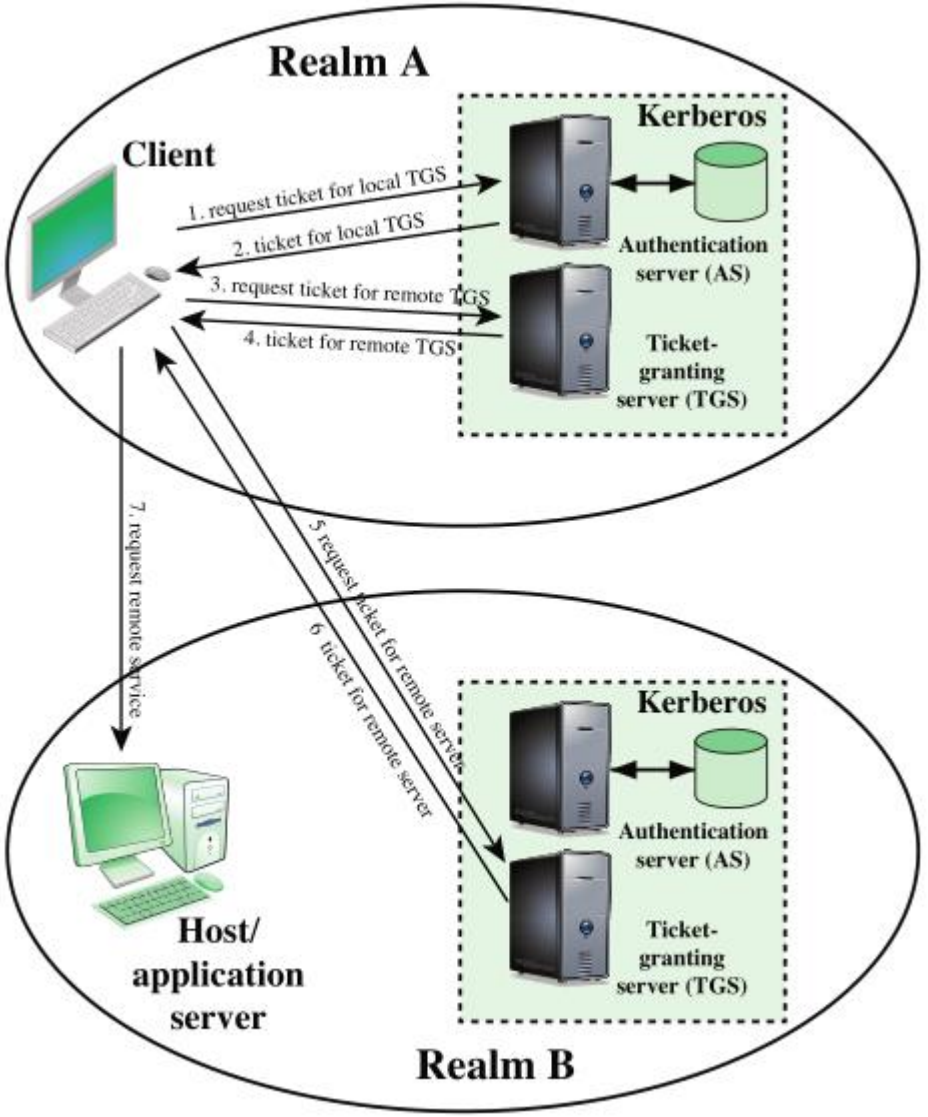
Kerberos Realms

- A Kerberos environment consists of:
  - A Kerberos server
  - A number of clients, all registered with server
  - Application servers, sharing keys with server
- This is termed a realm
  - Typically a single administrative domain
- If multiple realms, their Kerberos servers must share keys and trust

Kerberos Realms (Service Areas)

Kerberos servers in each realm may share a secret key with the server in other realm; the two Kerberos are registered with each other

Server in one realm must trust the Kerberos in the other realm



Kerberos Version 5

- Kerberos v4 is most widely used version
- Also have v5, developed in mid 1990's
  - Specified as Internet standard RFC 1510
- Provides improvements over v4
  - Addresses environmental shortcomings
    - Encryption alg, network protocol, byte order, ticket lifetime, authentication forwarding, inter-realm auth
  - And technical deficiencies
    - Double encryption, non-std mode of use, session keys, password attacks

Certificate Authorities

- Certificate consists of:
  - A public key plus a User ID of the key owner
  - Signed by a third party trusted by community
  - Often govt/bank **certificate authority** (CA)
- Users obtain certificates from CA
  - Create keys & unsigned cert, gives to CA, CA signs cert & attaches sig, returns to user
- Other users can verify cert
  - Checking sig on cert using CA's public key

Common Key Steps

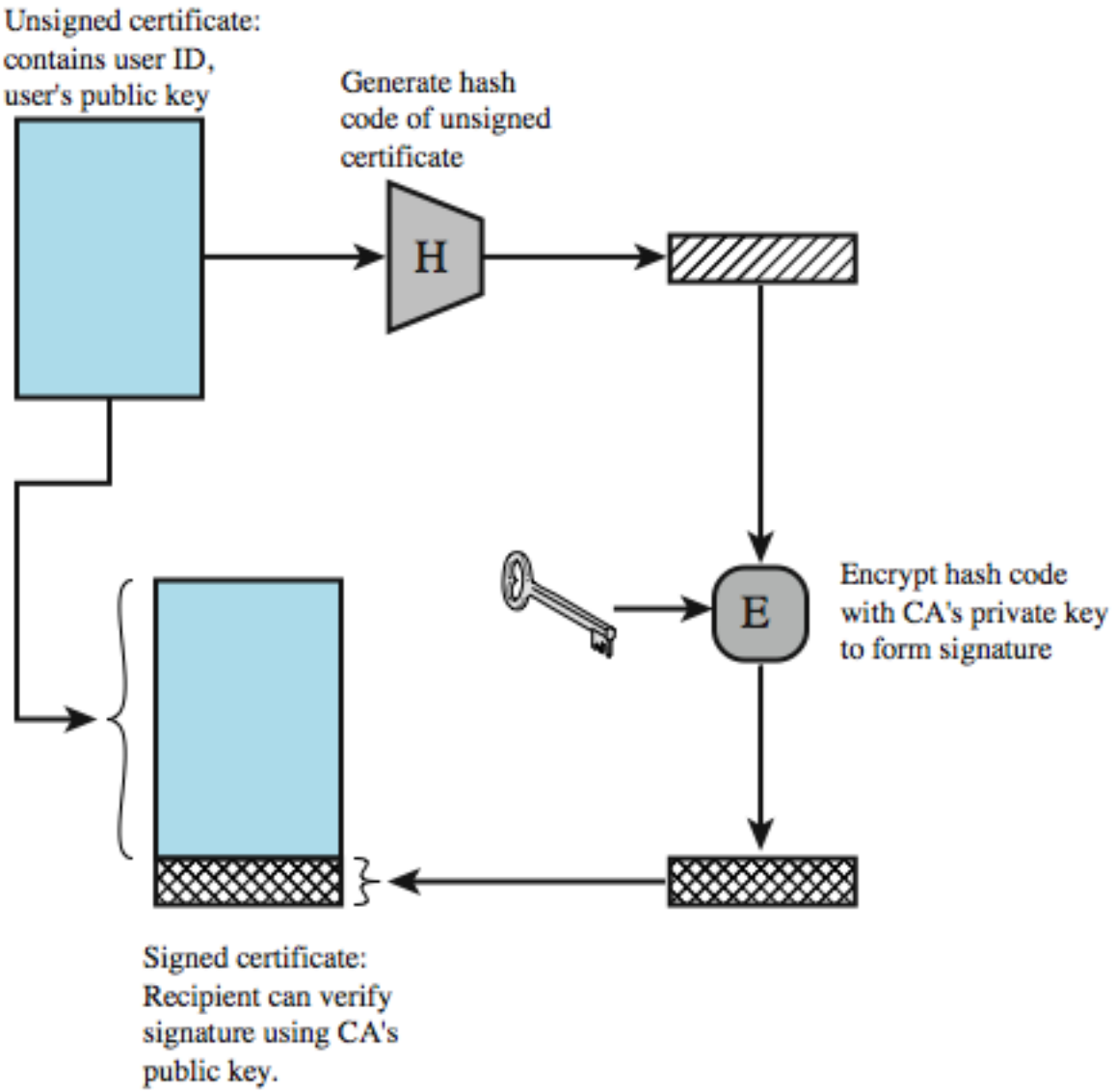
1. User software creates a pair of keys: private and public
2. Clients prepares unsigned certificate that includes user ID and public key
3. User provides unsigned certificate to a CA
4. CA creates a signature:
   i. Creates a hash code of the unsigned certificate
   ii. Encrypts the hash code with the CA's private key
5. CA attaches the signature to unsigned certificate to make signed certificate

Key Steps (continued)

6. CA returns the signed certificate to the client
7. Client may provide signed signature to other users
8. Any user may verify the certificate
   I. Calculate the hash code of certificate (exclude signature)
   II. Decrypt signature using CA's public key
   III. Compare the two

Public Key Certificates

See textbook figure p.63



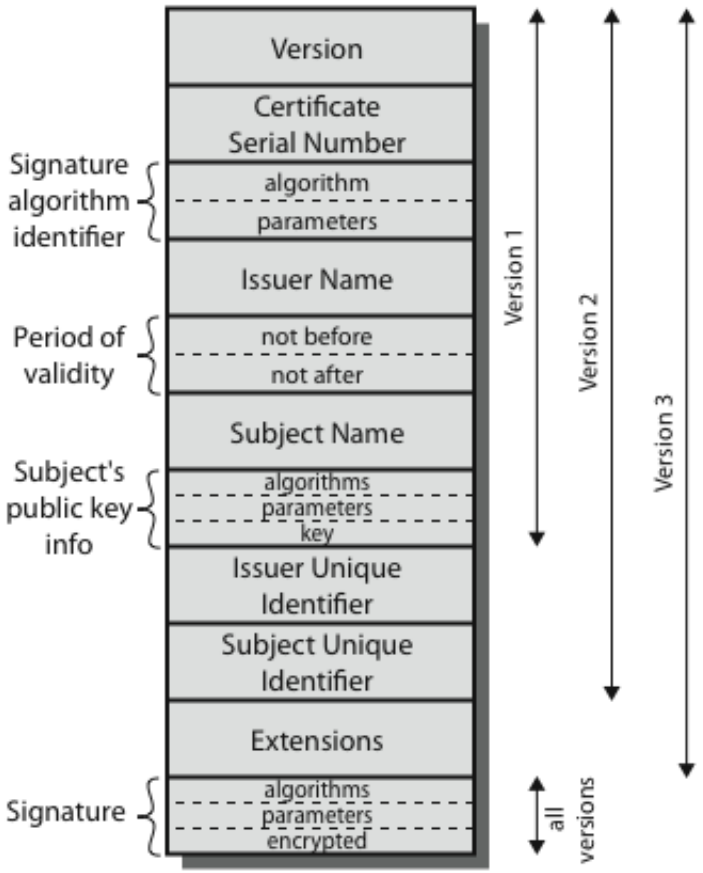
X.509 Authentication Service

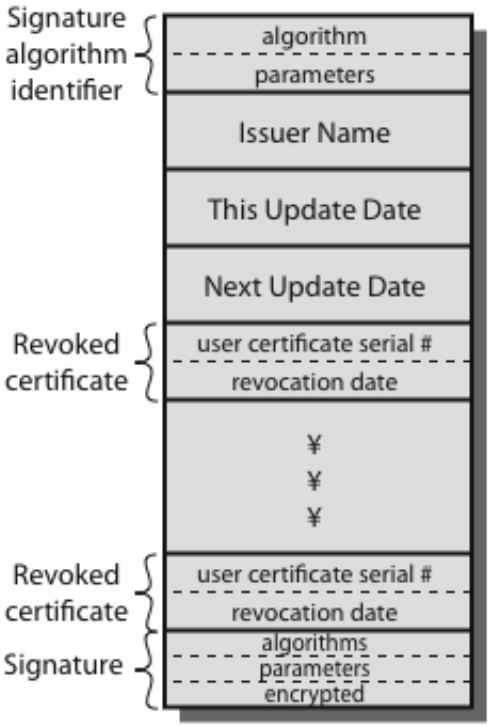
- Universally accepted standard for formatting public-key certificates
  - Widely used in network security applications, including IPSec, SSL, and S/MIME
- Part of CCITT X.500 directory service standards
- Uses public-key crypto & digital signatures
  - Algorithms not standardised, but RSA recommended

Certificate Variations

- Conventional (long-lived) certificates
  - CA and “end user” certificates
  - Typically issued for validity periods of months to years
- Short-lived certificates
  - Used to provide authentication for applications such as grid computing, while avoiding some of the overheads and limitations of conventional certificates
  - They have validity periods of hours to days, which limits the period of misuse if compromised
- Proxy certificates
  - Also used in applications such as grid computing
  - Allow a user to easily create a credential to access resources in some environment, without needing to provide their full certificate and right

X.509 Certificates





(b) Certificate Revocation List

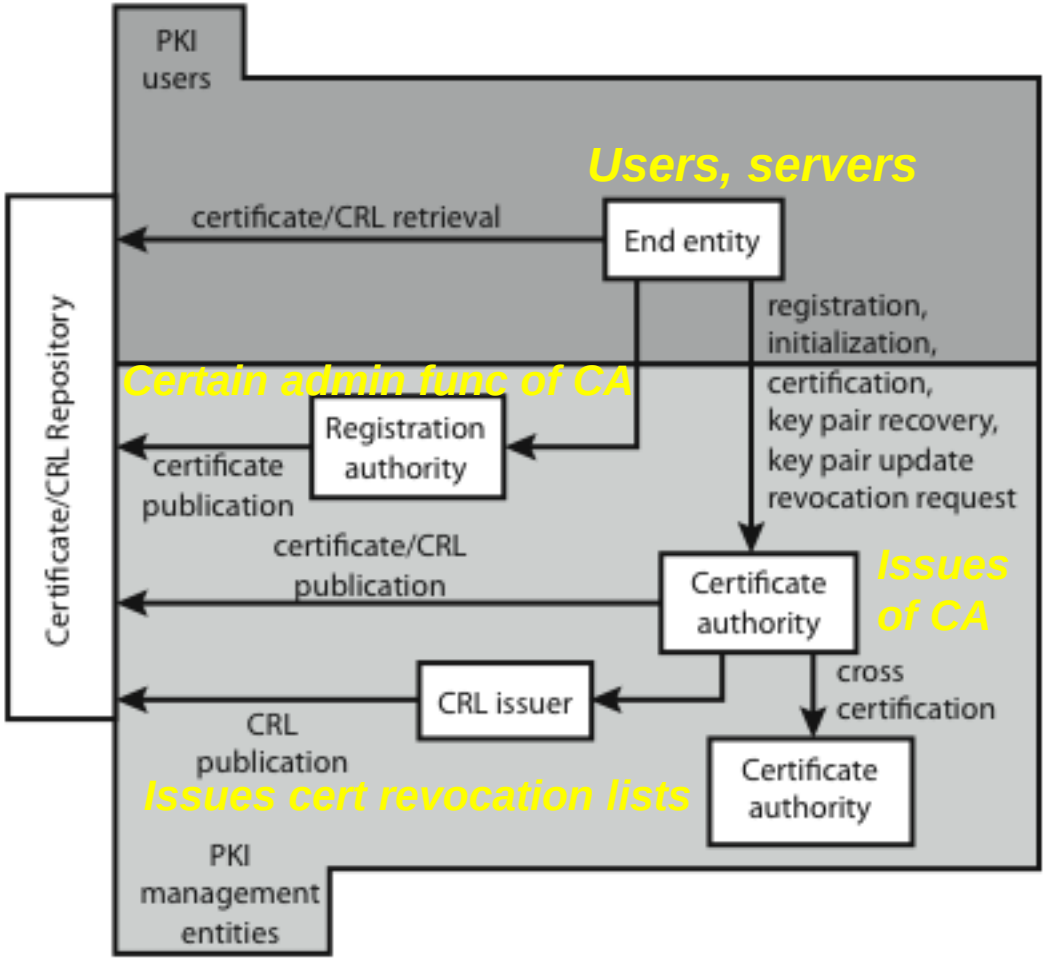
To revoke before expiration (in case the key has been compromised)

PKI X.509 (PKIX) Management

- Functions:
  - Registration
  - Certification: process to issue CA
  - Key pair recovery: forgotten passwords, corrupted HDs; restore key pairs from authorized backup
  - Key pair update: update with new keys
  - Revocation request: a users CA advises to revoke
  - Cross certification: two CAs exchange info

PKIX Architecture Model

PKI: HW, SW, people, policies, and procedures to create, manage, distribute, and revoke DCs based on asymmetric cryptography



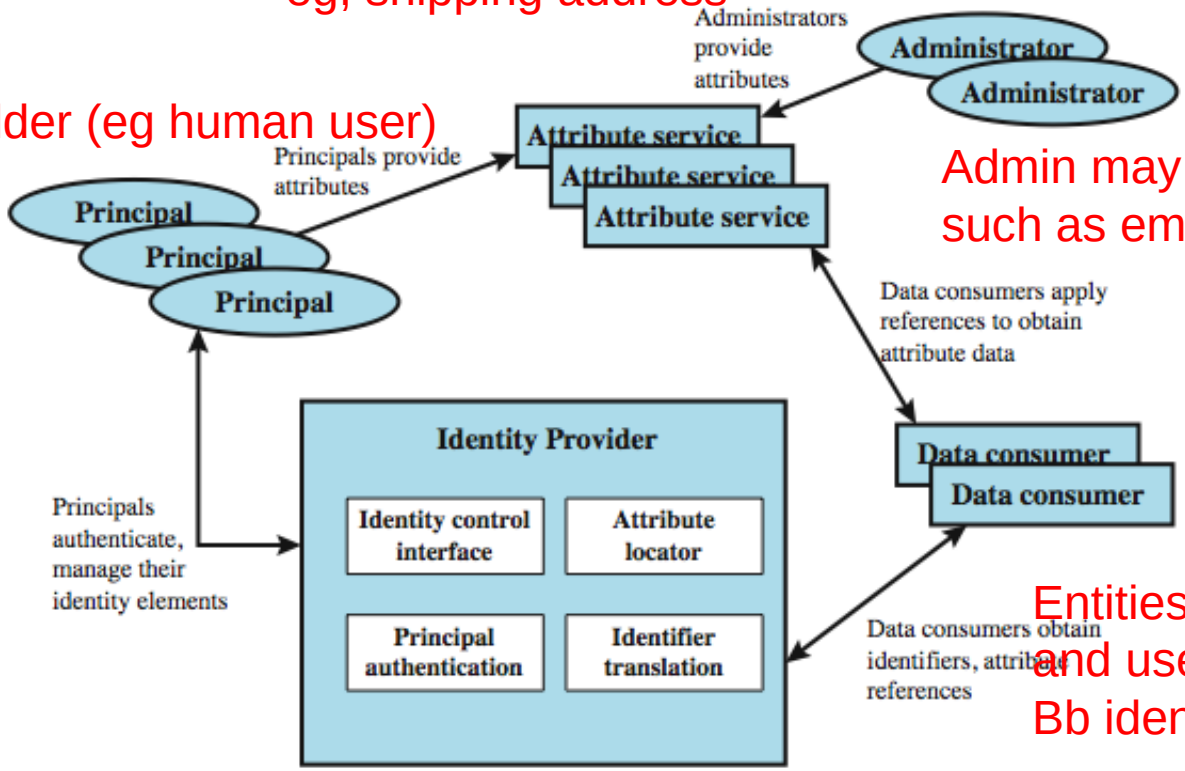
Federated Identity Management

- use of common identity management scheme
  - *across multiple enterprises & numerous applications*
  - supporting many thousands, even millions of users
- principal elements are:
  - authentication, authorization, accounting, provisioning, workflow automation, delegated administration, password synchronization, self-service password reset, federation
- Kerberos contains many of these elements

Generic Identity Management Arch

Attr other than identity
eg, shipping address

Identity holder (eg human user)



Admin may add other attr such as employee info

Entities that obtain and use data maintained Bb identity provider

Principals authenticate to identify provider

Standards Used

- Extensible Markup Language (XML)
  - characterizes text elements in a document on appearance, function, meaning, or context
- Simple Object Access Protocol (SOAP)
  - for invoking code using XML over HTTP
- WS-Security
  - set of SOAP extensions for implementing message integrity and confidentiality in Web services
- Security Assertion Markup Language (SAML)
  - XML-based language for the exchange of security information between online business partners

Summary

- reviewed network authentication using:
  - Kerberos private-key authentication service
  - X.509 public-key directory authentication
  - public-key infrastructure (PKI)
  - federated identity management