Network Security and Public Key Infrastructure

Unit -6 [6Hours]

Overview of Network Security

- Network security entails protecting the usability, reliability, integrity, and safety of network and data.
- Effective network security defeats a variety of threats from entering or spreading on a network.
- The primary goal of network security are Confidentiality, Integrity, and Availability.
  - It includes both hardware and software technologies.
  - it targets a variety of threats.
  - It stops them from entering or spreading on your network.
  - Effective network security manages access to the network.
- Network security combines multiple layers of defenses at the edge and in the network.
- Each network security layer implements policies and controls.
- Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

Network Security Model

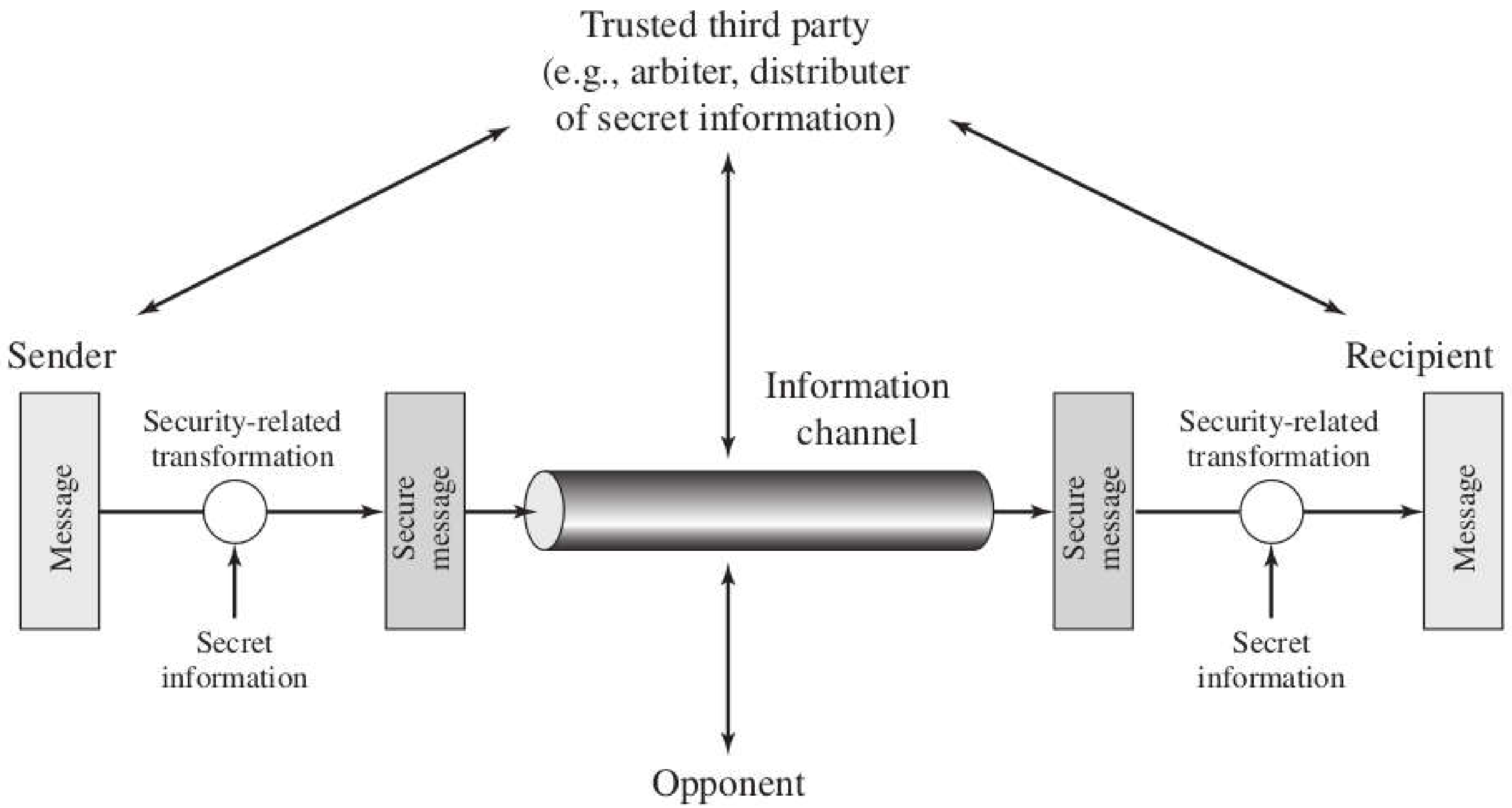


Figure: Model for Network Security

Network Security

The major types of network security include:

- Access Control
- Antivirus and Antimalware Software
- Application Security
- Behavioral analytics to detect abnormal network behavior
- Email Security, Web Security
- Data loss prevention
- Firewalls
- Intrusion prevention and detection system
- Virtual Private Networks (VPN)

- To sum up, Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

Digital Certificates

- Also called ***public-key certificate*** or ***identity certificate***.
- IT is an electronic file that typically contains identification information about the holder, including the person's public key (used for encrypting and decrypting messages), along with the authority's digital signature (trusted third party), so that the recipient can verify with the authority that the certificate is authentic.
- It is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the ***public key infrastructure***. (PKI).
- A digital certificate is issued by a ***certification authority*** (CA) (i.e. trusted third party).

Digital Certificates

- A user can present his or her public key to the authority in a secure manner and obtain a certificate.
- The user can then publish the certificate.
- Anyone needing this user’s public key can obtain the certificate and verify that it is valid by way of the attached trusted signature.
- A participant can also convey its key information to another by transmitting its certificate.
- Other participants can verify that the certificate was created by the authority.

Requirements for Digital Certificates:

- Any participant can read a certificate to determine the name and public key of the certificate's owner.
- Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
- Only the certificate authority can create and update certificates.
- Any participant can verify the time validity of the certificate.

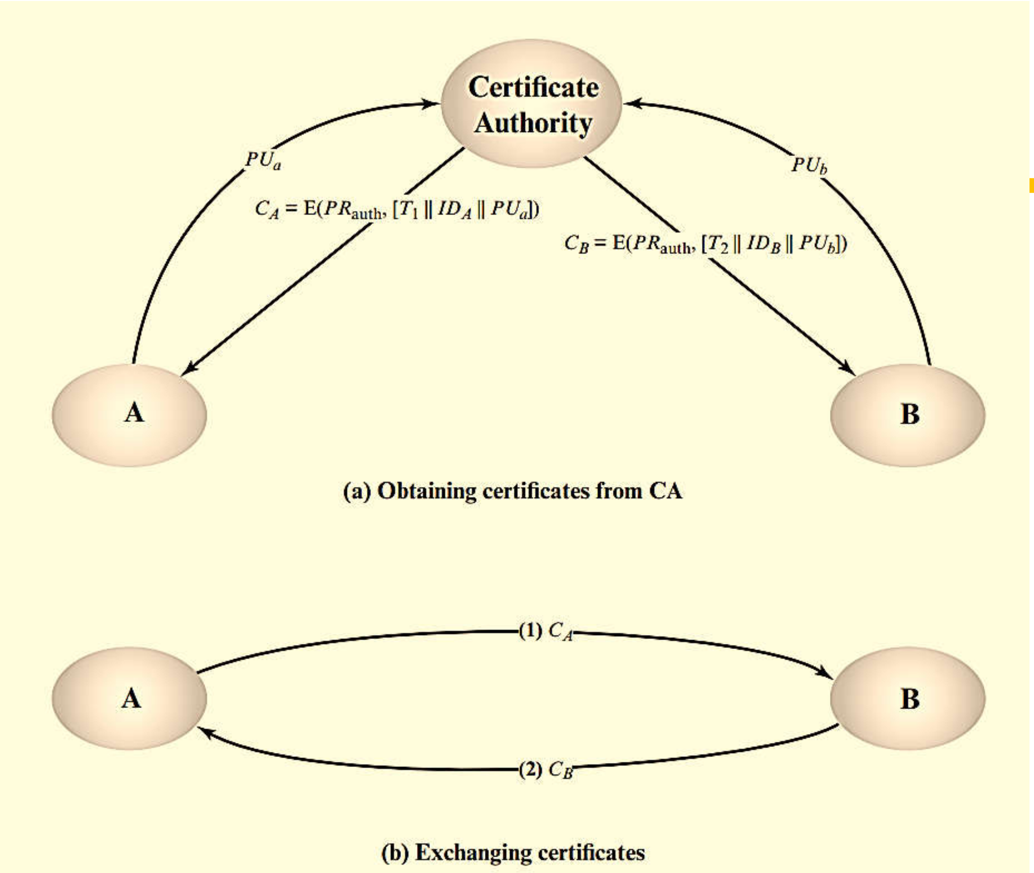

Certificate Authority
PU_a
PU_b
$C_A = E(PR_{auth}, [T_1 \| ID_A \| PU_a])$
$C_B = E(PR_{auth}, [T_2 \| ID_B \| PU_b])$
A
B
(a) Obtaining certificates from CA
A
B
(1) C_A
(2) C_B
(b) Exchanging certificates

Figure: Exchange of Public Key Certificates

$$D(PU_{auth}, C_A) = D(PU_{auth}, E(PR_{auth}, [T \| ID_A \| PU_a])) = (T \| ID_A \| PU_a)$$

X. 509 Certificates

- X.509 is an **International Telecommunication Union (ITU) standard** defining the format of public key certificates (digital certificate).
- An X.509 certificate binds an identity to a public key using a digital signature.
- A certificate contains an identity (a hostname, or an organization, or an individual) and a public key (RSA, DSA, ECDSA, ed25519, etc.).
- It is either signed by a certificate authority or is self-signed.
- X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web.
- **X.509 is part of the X.500 series of recommendations that define a directory service**. The directory is, in effect, a server or distributed set of servers that maintains a database of information about users. The information includes a mapping from user name to network address, as well as other attributes and information about the users

X. 509 Certificates

- The heart of the X.509 scheme is the public-key certificate associated with each user.
- These user certificates are assumed to be created by some trusted certification authority (CA) and placed in the directory by the CA or by the user.
- The directory server itself is not responsible for the creation of public keys or for the certification function; it merely provides an easily accessible location for users to obtain certificates

X. 509 Certificates

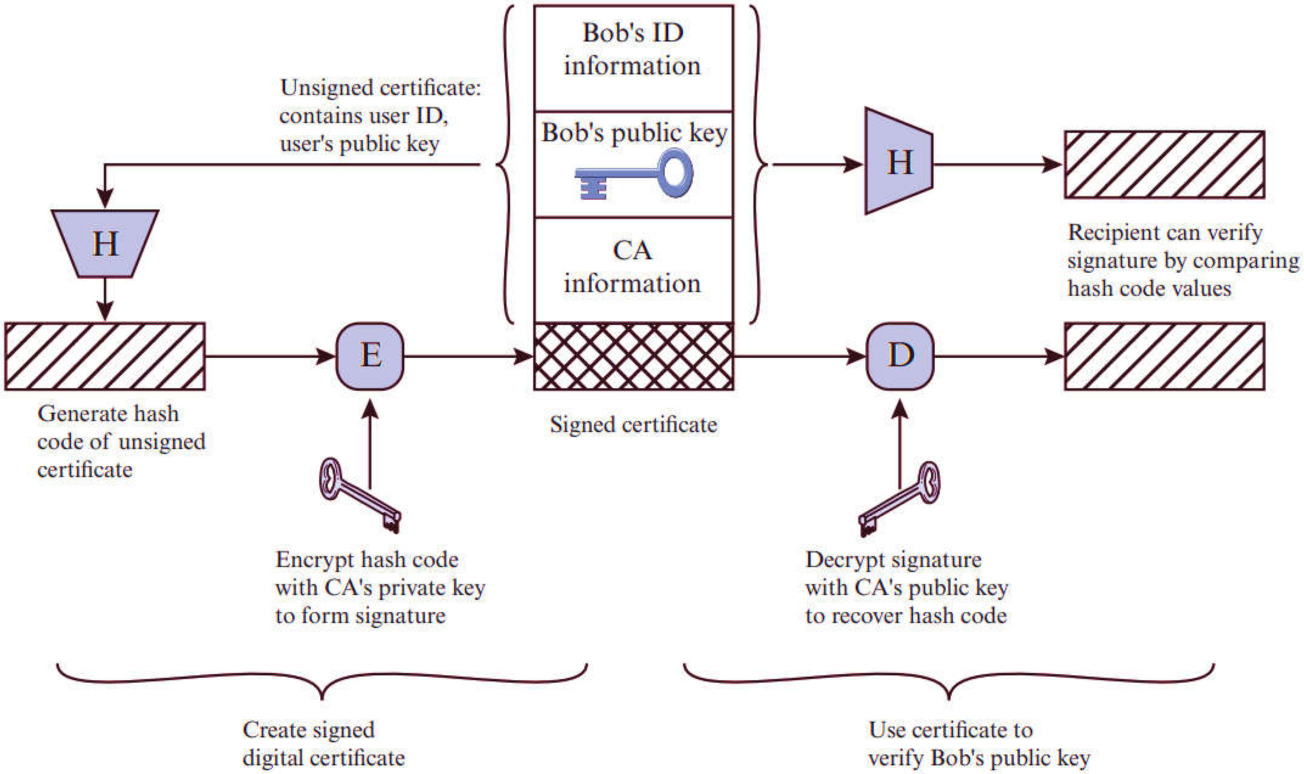
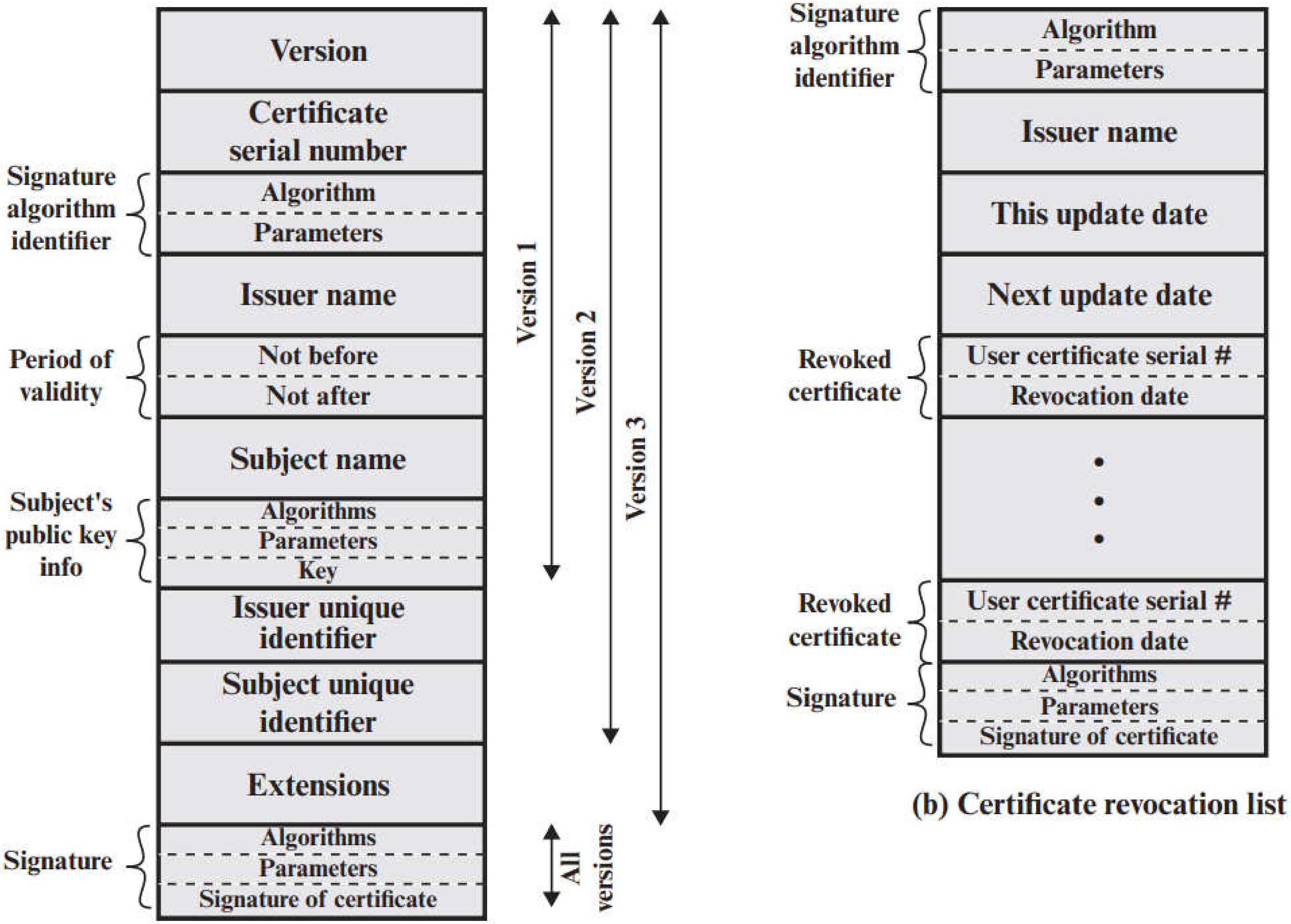

Bob's ID information
Bob's public key
CA information
Unsigned certificate: contains user ID, user's public key
H
E
Generate hash code of unsigned certificate
Encrypt hash code with CA's private key to form signature
Signed certificate
H
D
Recipient can verify signature by comparing hash code values
Decrypt signature with CA's public key to recover hash code
Create signed digital certificate
Use certificate to verify Bob's public key

Figure: X.509 Public-Key Certificate Use

- The certificate for Bob's public key includes unique identifying information for Bob, Bob's public key, and identifying information about the CA, plus other information.
- This information is then signed by computing a hash value of the information and generating a digital signature using the hash value and the CA's private key.
- X.509 indicates that the signature is formed by encrypting the hash value.



(b) Certificate revocation list

(a) X.509 certificate

Figure: X.509 Formats

Digital Certificate Life-Cycle Management

- As described earlier, digital certificates have a lifetime during which they are considered valid.
- When this lifetime expires, the certificate can no longer be used for authentication and must be updated to restore its validity.
- A certificate can also become invalid from being revoked by a CA.
- Common reasons for which a CA might revoke a digital certificate include a change in job status or suspicion of a compromised private key.
- The life cycle of a certificate can be broken into distinct stages, as discussed in the following sections:
  - Certificate Enrollment
  - Certificate Validation
  - Certificate Revocation
  - Certificate Renewal
  - Certificate Destruction
  - Certificate Auditing

Digital Certificate Life-Cycle Management

Certificate Enrollment

- Certificate enrollment is initiated by a user request to the appropriate CA. This is a cooperative process between a user (or a user's PKI software, such as an e-mail or Web browser application) and the CA. The enrollment request contains the public key and enrollment information. Once a user requests a certificate, the CA verifies information based on its established policy rules, creates the certificate, posts the certificate, and then sends an identifying certificate to the user. During the certificate distribution the CA sets policies that affect the use of the certificate.

Certificate Validation

- When a certificate is used, the certificate status is checked to verify that the certificate is still operationally valid. During the validation process, the CA checks the status of the certificate and verifies that the certificate is not its **Certificate Revocation List** (CRL).

Digital Certificate Life-Cycle Management

Certificate Revocation

- A certificate issued by a CA includes an expiration date that defines how long the certificate is valid. If a certificate needs to be revoked before that date, the CA can be instructed to add the certificate to its CRL. Reasons a certificate might need to be revoked include the certificate being lost or compromised, or the person the certificate was issued to leaving the company.

Certificate Renewal

- When a certificate reaches its expiration date, and if the certificate policy allows it, it is renewed either automatically, or by user intervention. When renewing a certificate, you must choose whether or not to generate new public and private keys.

Digital Certificate Life-Cycle Management

Certificate Destruction

- When a certificate is no longer in use, the certificate and any backup copies or archived copies of the certificate should be destroyed, along with the private key associated with the certificate. This helps ensure that the certificate is not compromised and used.

Certificate Auditing

- Certificate auditing involves tracking the creation, expiration, and revocation of certificates. In certain instances, it can also track each successful use of a certificate

PKI Trust Models

- A trust model **is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate**.
- Architecture of a PKI is **composed of operations and security policies, security services and protocols** that support interoperability using public key encryption and key management certificates.
- In PKI a digital certificate issued by CA and applications are usually processed by the **Registration Authorities (RA)**.
- The responsibility of an RA is to analyze individual user who examines each application and notifies the CA, which is closer to the level of confidence of the applicant by checking the level of confidence, CA issue the certificate.
- The architecture of a PKI system describes the organization of its CAs and the trust relationship among them

PKI Trust Models

- Peer to Peer Trust Model
- Bridge Trust Model
- Hierarchical Trust Model
- Hybrid Trust Model
- Web-of-Trust Model

PKIX Architecture Model

- Public-key infrastructure (PKI) is defined as *the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography*.
- The principal objective for developing a PKI is *to enable secure, convenient, and efficient acquisition of public keys*.
- **The Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX)** working group has been the driving force behind setting up a formal (and generic) model based on X.509 that is suitable for deploying a certificate-based architecture on the Internet

PKIX Architecture Model

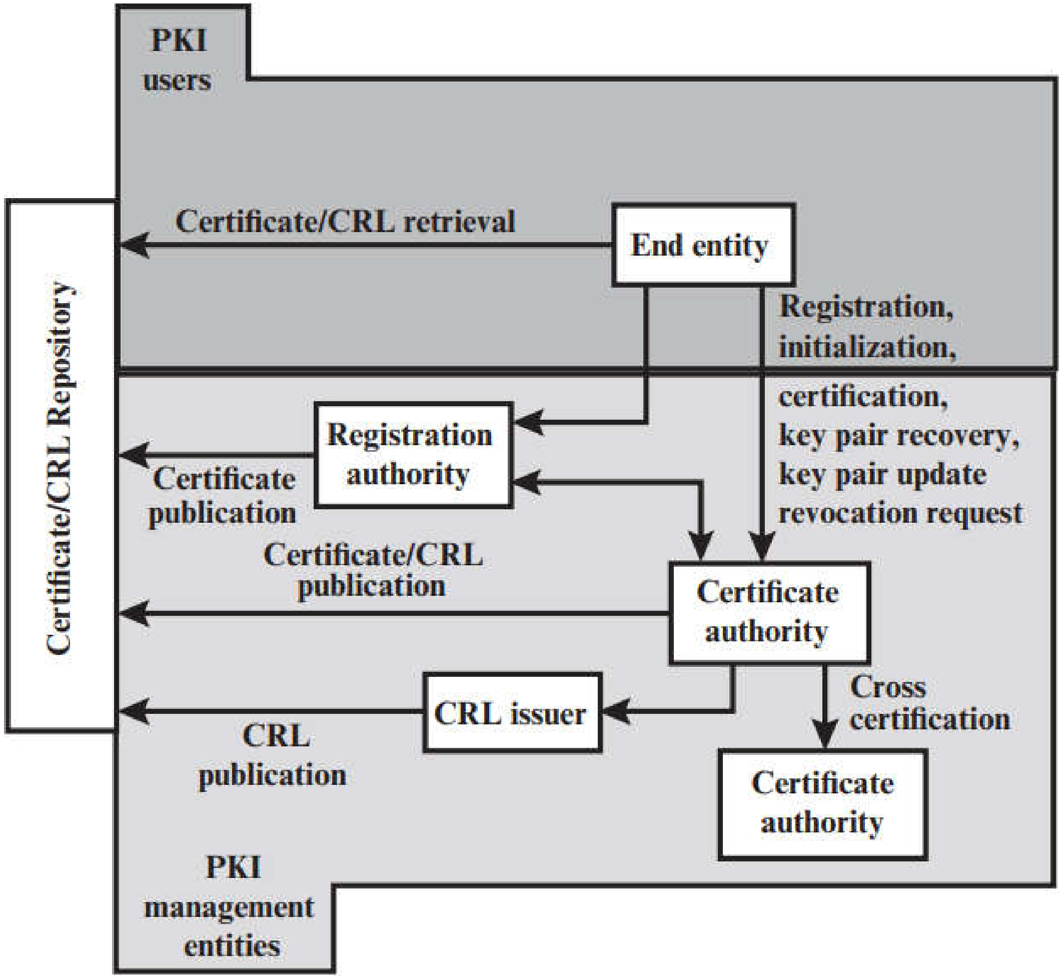

PKI users
Certificate/CRL Repository
Certificate/CRL retrieval
End entity
Registration, initialization,
certification, key pair recovery, key pair update revocation request
Registration authority
Certificate publication
Certificate/CRL publication
Certificate authority
CRL issuer
Cross certification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

Figure: PKIX Architecture Model

PKIX Architecture Model

- **End entity**: A generic term used to denote end users, devices (e.g., servers, routers), or any other entity that can be identified in the subject field of a public-key certificate. End entities typically consume and/or support PKI related services.

- **Certification authority (CA):** The issuer of certificates and (usually) certificate revocation lists (CRLs). It may also support a variety of administrative functions, although these are often delegated to one or more Registration Authorities.

- **Registration authority (RA):** An optional component that can assume a number of administrative functions from the CA. The RA is often associated with the end entity registration process but can assist in a number of other areas as well.

- **CRL issuer**: An optional component that a CA can delegate to publish CRLs.

- **Repository**: A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by end entities.

PKIX Management Functions

- PKIX identifies a number of management functions that potentially need to be supported by management protocols.
  - Registration
  - Initialization
  - Certification
  - Key pair recovery
  - Key pair update
  - Revocation request
  - Cross certification

Self Study Topics

- Email security: PGP
- Secure Socket Layer (SSL) Protocol
- Transport Layer Security (TLS) Protocol
- IP Security (IPSec) Protocol
- Firewall and its different types of firewalls