CHAPTER 7

Unit II

Authentication Applications

Syllabus

Authentication Applications: Kerberos, X.509 Authentication, Public-Key Infrastructure.

Syllabus Topic : Kerberos

7.1 Kerberos

- It is Network Authentication Protocol.
- It ensures strong authentication for all client server applications.
- To provide strong authentication, it uses secret key cryptography.
- It is an authentication service.
- It Provides very high security for physically insecure network.
- It also provids centralised authenticated server which authenticates users to servers and servers to users.
- Rather than using public key encryption, it depends on conventional encryption.

7.1.1 Requirements for Kerberos

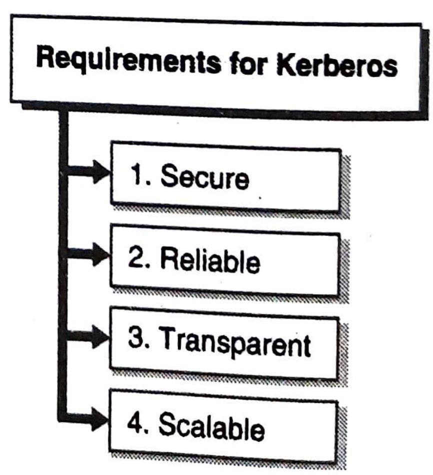

Fig. 7.1.1

1. **Secure** : The essential information about the user should be gained by a network listener. Kerberos should be so strong that potential attacker should not find it as a weak link.
2. **Reliable** : The access control services are dependent on Kerberos. So it should be reliable and configured as distributed server architecture where systems are interrelated so that they can take back up of one another.

3. **Transparent** : An user should be aware of authentication process.
4. **Scalable** : The system should be scalable enough to support multiple clients and servers. It provides distributed, integrated and flexible architecture.

7.1.2 Working of Kerberos

Four parties are involved in the process of Kerberos protocol :

- **Alice** : The client workstation
- **Authentication Server (AS)** : Verifies user during login
- **Ticket Granting Server (TGS)** : Tickets Issuer to provide identity proof.
- **Bob** : The server offering various services like application program, network printing or file sharing.

Step 1 : Login

- Alice enters her name into workstation.
- The name as a plain text is sent to AS by workstation.
- AS produces a package of Alice and randomly generates a session key (KS).
- The encryption of this package and symmetric key takes place which send to Ticket Granting Server (TGS) by AS.
- The output of the above step is called Ticket Granting Ticket (TGT).
- TGT is combined with KS and then encrypted by symmetric key generated from Alice password (KA).

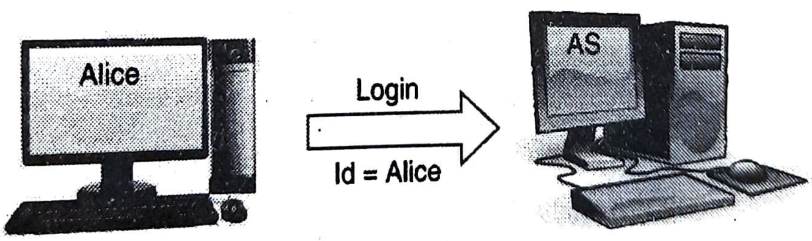

Fig. 7.1.2 : Alice sends a login request to AS

- After receiving this message, Alice's workstation will ask her to her password.
- After entering the password Alice Key KA is generated by the workstation and uses the same to obtain TGT and KS.
- The password is deleted from the workstation's memory for protection purpose.

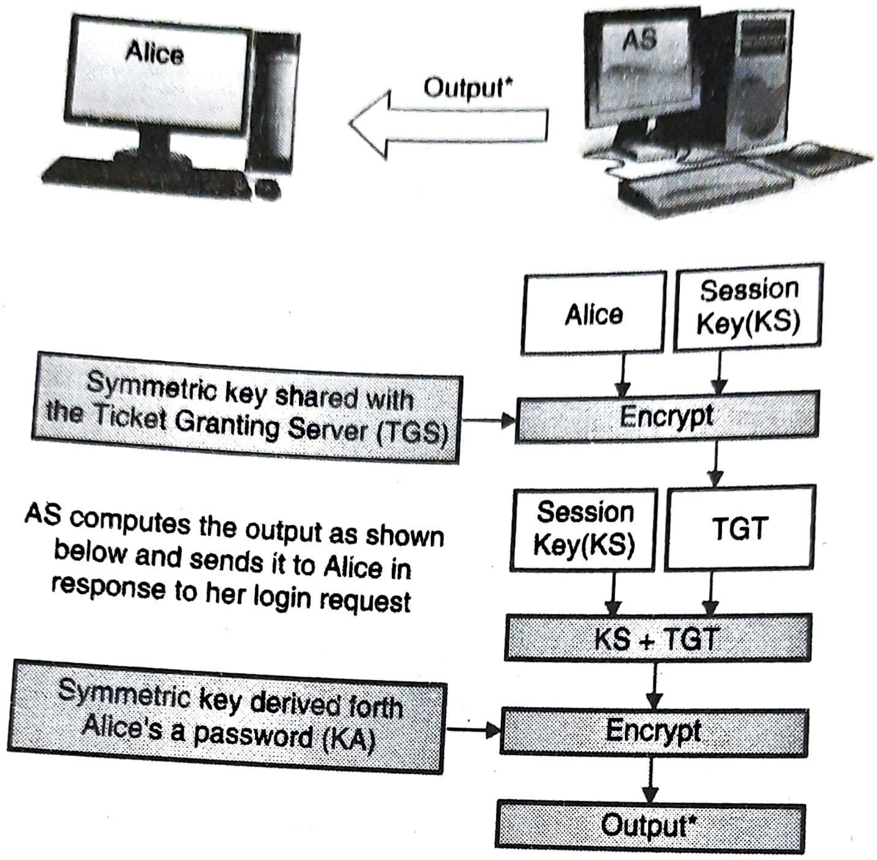

Fig. 7.1.3 : AS sends back encrypted session key and TGT to Alice

Step 2 : Obtaining Service Granting Ticket (SGT)

- Alice's workstation produces message meant for TGS which comprises :-
  - TGT as computed in step 1
  - Bob's id whose services Alice is interested for
  - Current timestamp, encrypted with KS
- When TGS satisfies authorizations of Alice, it produces session key KAB.
- Key is sent twice to Alice by TGS. First time, it is combined with Bob's id and encrypted with KS and next time, it is combine with Alice's id and encrypted with Bob key KB.

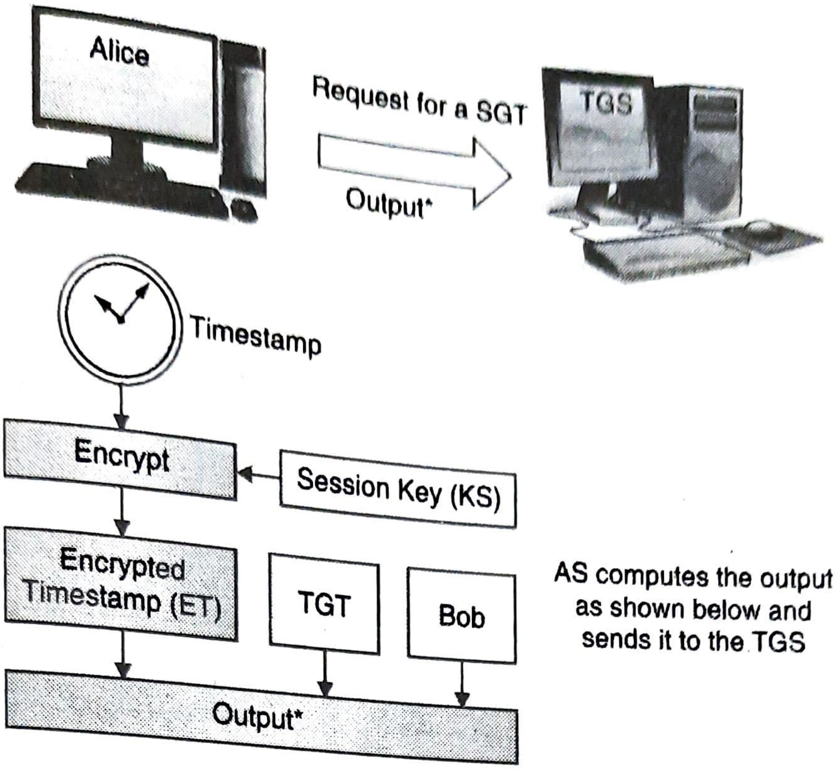

Fig. 7.1.4 : Alice sends a request for a SGT to the TGS

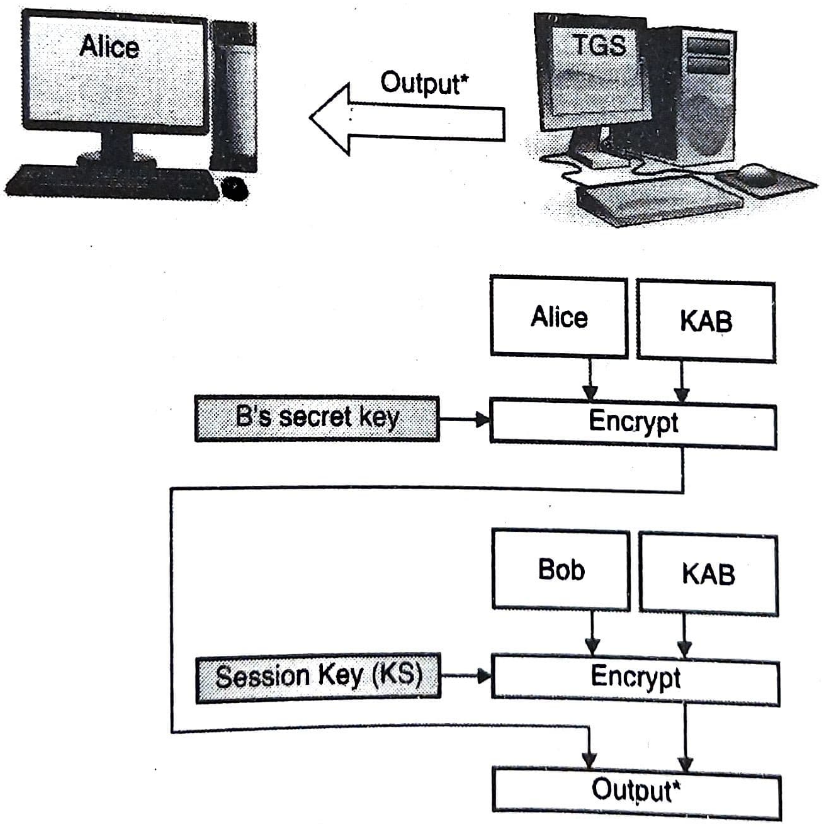

Fig. 7.1.5 : TGS sends Response back to Alice

Step 3 : User communicates with Bob for accessing server

- Alice transmits KAB encrypted with Bob's secret key as well as timestamp to Bob.
- Bob appends 1 to timestamp then with KAB it encrypts the result and sends it Alice again.

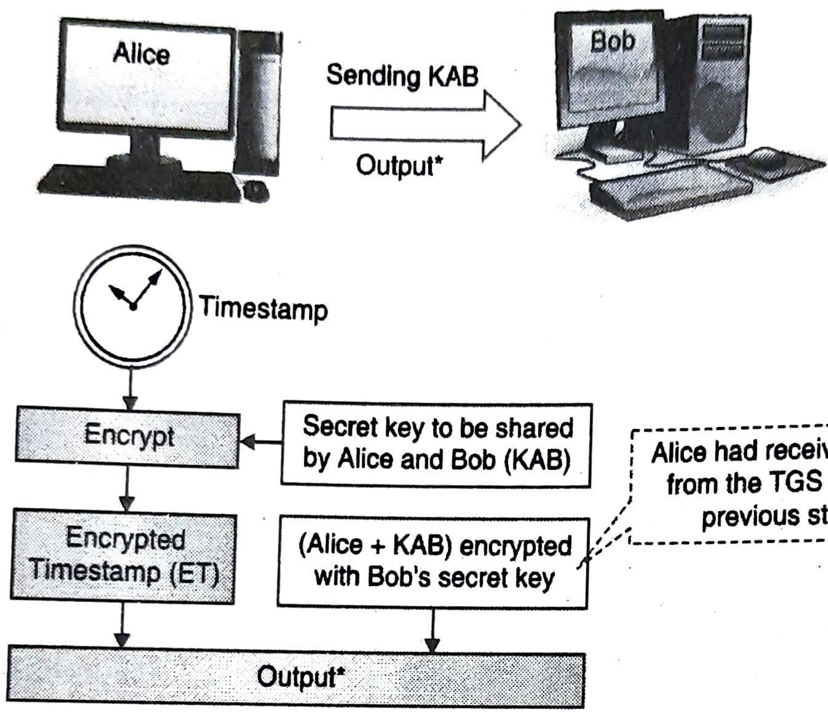

Fig. 7.1.6 : Alice sends KAB securely to Bob

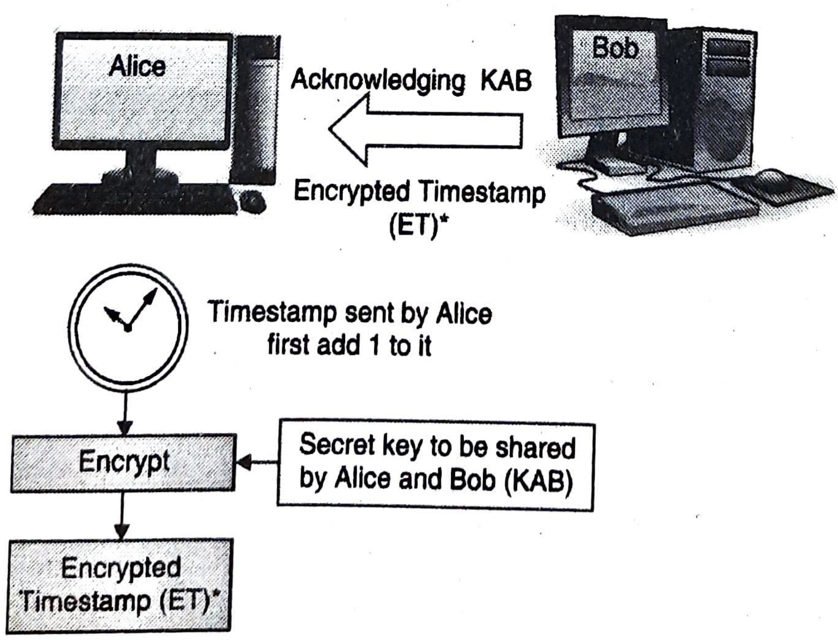

Fig . 7.1.7 : Bob acknowledges the receipt of KAB

7.1.3 Difference between Kerberos v4 and v5

- Kerberos version 4 and version 5 both are updates by the Kerberos software.

	Kerberos Version 4	Kerberos Version 5
History	Released in late 1980's.	Published in 1993
Encoding	'receiver makes right' encoding system is used	ASN.1 encoding system is used.
Support for ticket	Satisfactory	Further enhanced with facilitates like sending, renewing and postdating tickets.
Network addresses	Few IP addresses and other addresses for network protocols types	Multiple IP addresses and other addresses for network protocols types
Authentication support for transitive cross realm	No	Reasonable support
Dependency on encryption system	DES required	Any encryption type can be used.
Ordering of message byte	Choice of the byte ordering by the sender	ASN.1 and BER used to define message structures
Ticket lifespan	Maximum 1280 min.	arbitrary
Authentication forwarding	Does not allow essentials required to issue one client to be send to some other host and used by some other client	Accessing client's file from server using client's credentials are allowed
PCBC (Propagating Cipher Block Chaining) encryption	uses PCBC	uses standard CBC mode
Session keys	No negotiate between client and server for a sub session key	client and server negotiates a sub session key used for that particular connection

7.2 Kerberos Realm

- In a Kerberos realm, the same Kerberos database is shared by a group of managed nodes.
- The Kerberos master computer system stores Kerberos database which needs to be preserved in a physically secure room.
- Though multiple read only copies of the Kerberos database can be store on other Kerberos computer systems, but all the modification to the database needs to be made on the master computer system
- The Kerberos master password is required for accessing or updating the contents of a Kerberos database.
- The principal of Kerberos is a user or a service which is known by the Kerberos system.
- The identification of each Kerberos principal is its name.
- Principal name consists of a user or service name, an instance name and a realm name.

  principal_name.instance_name@realm_name
- The user's role for a certain realm is described by the authorization role, like robin.user@realm1 for the user principal.
- Even location of a service on a computer system can also be described by principal name, like ftp.client1@realm2 for a service principal.
- The identification of computer system on which service is available is given by the instance of the principal name.
- Similar services on different computer systems are consider as a different services for principals by Kerberos.
- The Kerberos network authentication service is implemented by the Tivoli Management Framework.
- The process of creating a Kerberos realm :
  - A computer system is selected which is considered to be the master of the realm.
  - Kerberos commands needs to be in your search path.
  - Make a Kerberos configuration file
  - The distribution center key database is initialized and occupied on the master.
  - One or more Tivoli administrators are initiated as Kerberos principals.
  - Some other computer systems are set up in the realm.
  - Tivoli daemon is designed in such a way that it ensure Kerberos authentication.

7.3 Certificate Based Authentication

A certification authority issues a certificate binding a public key to a particular distinguished name in the X.500 tradition, or to an *alternative name* such as an e-mail address or a DNS-entry.

Syllabus Topic : X.509 Authentication

7.3.1 X.509 Authentication Service

- It is a section of CCITT X.500 directory service standards.
- Database maintained by distribution servers.
- Authentication services framework is defined by
  - Public key certificates stored at directory
  - User's public key
  - Certification authority CA's sign
- Even it defined authentication protocols.
- It uses RSA recommended algorithms.

7.3.2 X.509 Certificates

- X.509 is a paradigm which defines the public key cryptography certificate formats in cryptography.
- A framework is defined by X.509 for providing authentication services to users.
- Internet protocols such as TLS / SSL, secure protocol for browsing the web is using X.509 certificates.
- Even offline applications such as electronic signatures are using X.509 certificates.
- A X.509 certificate comprises an identity of an individual or an organization or hostname and a public key.
- It is either self-signed or signed by Certificate Authority (CA).
- When trusted certificate authority signs the certificate or by using any other means it is validated, someone having that certificate can ensures the public key it contains to create protected communication with another party or authenticate documents digitally signed by its private key.
- Certification Authority CA signs the A's certificate is denoted by CA<<A>>.

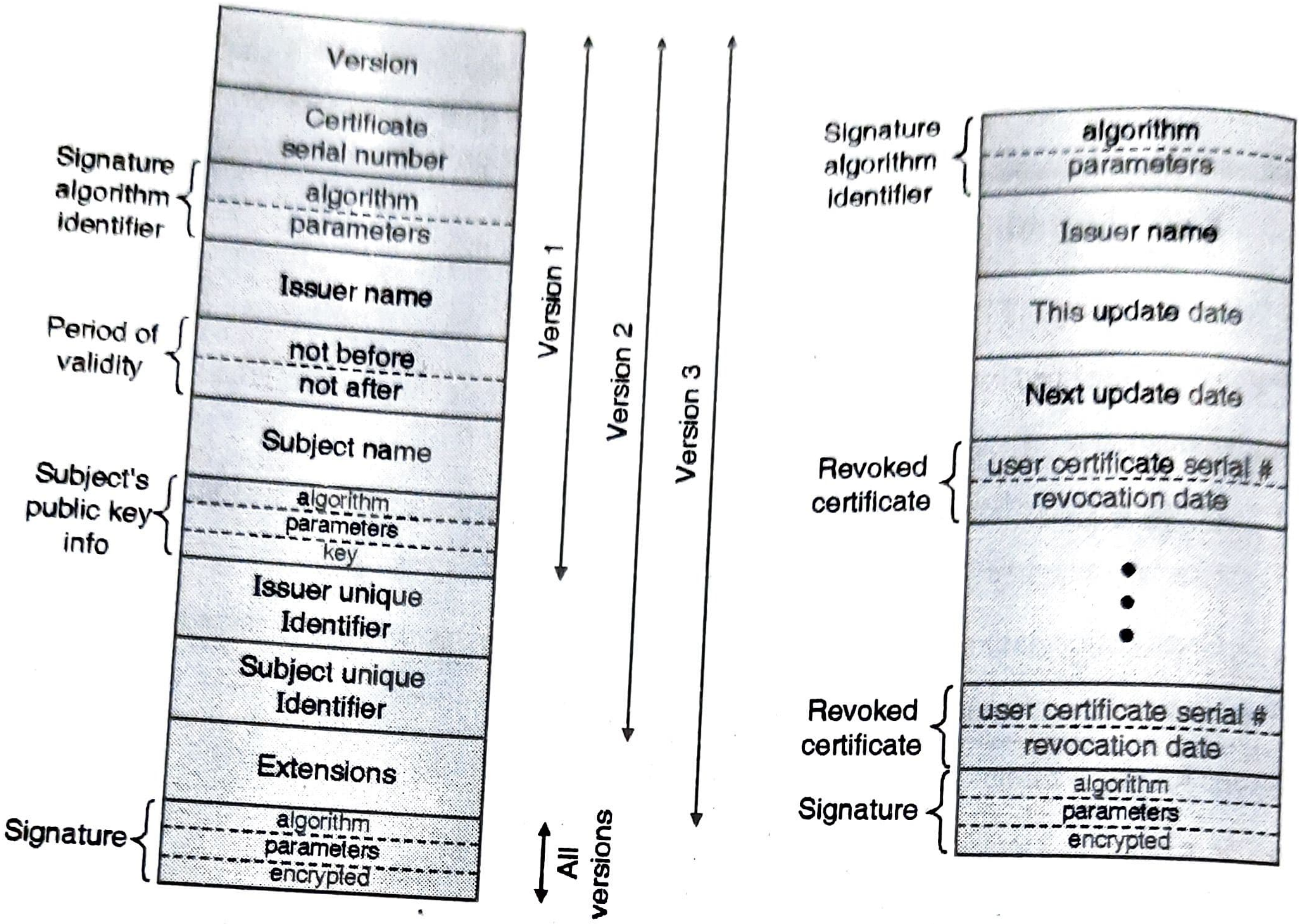

Fig. 7.3.1

Various fields of digital certificate are

- **Version** : Identifies a particular version of the X.509 protocol.
- **Certificate Serial Number** : Contains a unique integer number, which is generated by CA
- **Signature Algorithm Identifier** : Identifies the algorithm used by CA to sign this certificate
- **Issuer Name** : Identifies the Distinguished Name (DN) of CA that created and signed this certificate.
- **Validity (not before / not after)** : Contains two date-time values, which specify the timeframe within which the certificate should be considered as valid.
- **Subject Name** : Identifies the Distinguished Name (DN) of the end entity to whom this certificate refers.
- **Subject Public Key Information** : Contains the subject's public key and algorithms related to that key.

- **Issuer Unique identifier** : Helps identify CA uniquely if two or more CAs have used the same issuer name over time
- **Subject unique identifier** : Helps identify a subject uniquely if two or more subjects have used same subject name over time
- **Authority key identifier** : It defined which of the private-public key pairs is used to sign this certificate
- **Extensions :** A set of one or more extension fields
- **Signature** : Contains all other fields of the certificate

Creation of Digital certificate

The parties involved in creating a digital certificates are :

- The subject (end user),
- The issuer (CA)
- Registration Authority (RA).

7.3.3 Steps of Creation of Digital Certificate

1. Key Generation

Key can be generated in two ways :

(i) The subject can create a private key and public key pair using some software. The private key is kept secret, whereas the public key is sent to the RA along with other information.

(ii) In case if user does not know about creating key pair then on behalf of subject, RA can generate a key pair.

2. Registration

- Registration is done by RA if key is generated by RA.
- If user generates the key, she sends the public key, its associated registration information and also all facts about her to RA.

3. Verification

- After completing the registration process, RA has to verify the user's credentials.
- The second check is to ensure that the user who is requesting for the certificate does indeed possess the private key corresponding to the public key.
- RA can perform Proof of Possession by any of the following methods:

- RA can demand that the user must digitally sign the Certificate Signing Request (CSR) with his/her own private key.
- RA can create random number challenge, encrypt it with user's public key and ask the user to decrypt it using his/her private key.
- RA can create a dummy certificate for the user, encrypt it and sends it to user. The user can decrypt it only if he/she has valid Private Key.

4. Certificate Creation

- If all the above steps are successfully completed, the RA forwards all the details of the user to CA.
- The CA does its own verification and creates a digital certificate for the user.
- The CA sends the certificate to the user and saves one copy of it for its own records. The CA then sends the certificate to the user.

7.4 Certificate Revocation

- Digital Certificates can be revoked/recalled.
- Reasons to recall the Digital Certificate are:
  - The holder reports that the public or private key is compromised.
  - CA may have made mistake during the issuance of certificate.
  - The certificate holder leaves the job and the certificate was intended for that user only.
- Before invoking any digital certificate, the CA must have Certificate Revocation Request (CRR).
- After verifying CRR, the CA revokes the certificate.
- But before relying any certificate, the user wants to know:
  - Does this certificate belongs to a valid user?
  - Is this certificate valid or is it revoked?
- The user can find out the answer for first question by just checking certificate chain.
- For getting second question's answer, the CA provides digital certificate revocation checks.
- Digital certificate revocation checks are done by following two ways:
  - Offline Certificate Revocation Status Check
  - Online Certificate Revocation Status Check

Syllabus Topic : Public Key Infrastructure

7.5 Public Key Infrastructure (PKI)

- A group of software, hardware, people, procedures and policies are known as Public Key Infrastructure.
- PKI is required to initiate, use, revoke, manage, store, and distribute digital certificates.
- PKI is an arrangement in cryptography which binds public keys with its user identities by means of a CA, Certificate Authority
- Uniqueness of user identity must be maintained with each CA domain.
- The registration and dissemination process is established by the binding, which is dependent on the binding assurance level performed by the software at CA, or under any supervision.
- The role of PKI which ensures the above type of binding is called as Registration Authority RA.
- RA guarantees that the individual who ensures non repudiation is bind to the public key
- Public key cryptography is a cryptographic method which allows users to communicate securely on an unprotected public network, and digital signature verifies whether the user is authenticated.

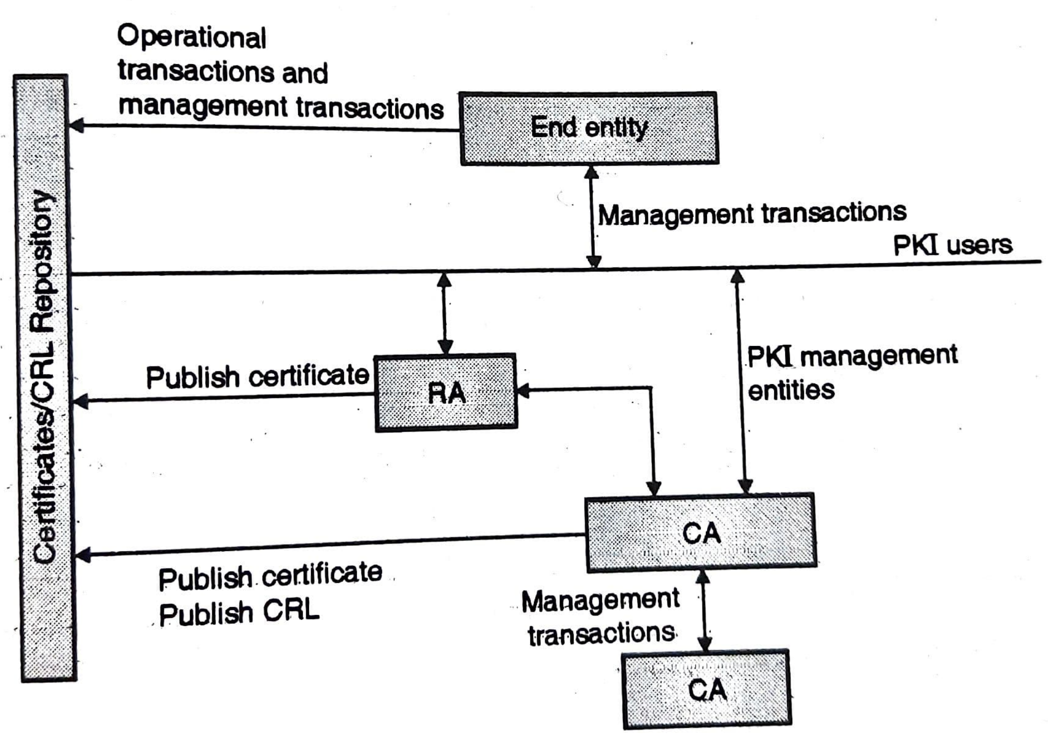

Fig. 7.5.1 : PKIX Architecture Model

7.5.1 PKI Components

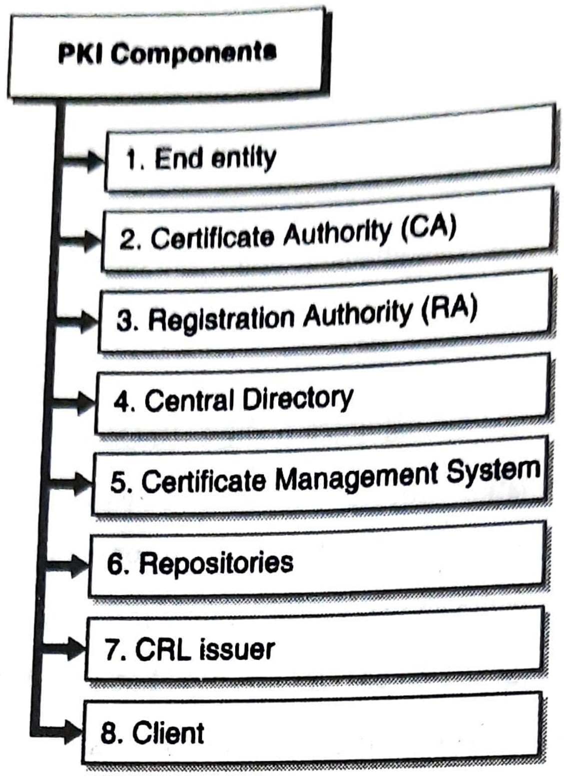

Fig. 7.5.2

1. **End entity**

   Consumes and supports PKI services. End entity indicates users, resources or any entity specified in subject of digital certificate

2. **Certificate Authority (CA)**

   Issues and verifies the digital certificates. Supports various administrative functions.

3. **Registration Authority (RA)**

   Verifies the identity of users requesting information from the CA

4. **Central Directory**

   A secure location to store and index keys.

5. **Certificate Management System**

   Sign and encrypts digital documents.

6. **Repositories**

   Store and make available certificates and Certificate Revocation Lists (CRLs)CRLs.

7. **CRL issuer**

   An optional component that a CA can delegate to publish

8. **Client**

Validates the digital signatures and their certification path from a known public key of a trusted CA.

7.5.2 PKIX Management Function

1. **Registration**

Process of enrollment in PKI.

User introduces itself to CA.

Involves some offline or online processes for authentication

2. **Initialization**

Initialize key resources which is in relationship with keys kept in infrastructure

3. **Certification**

CA issues certificate for user and send to user's client system and also keep one of it in repository.

4. **Key pair recovery**

Allows end entities to restore encryption or decryption key pair from backup repositories.

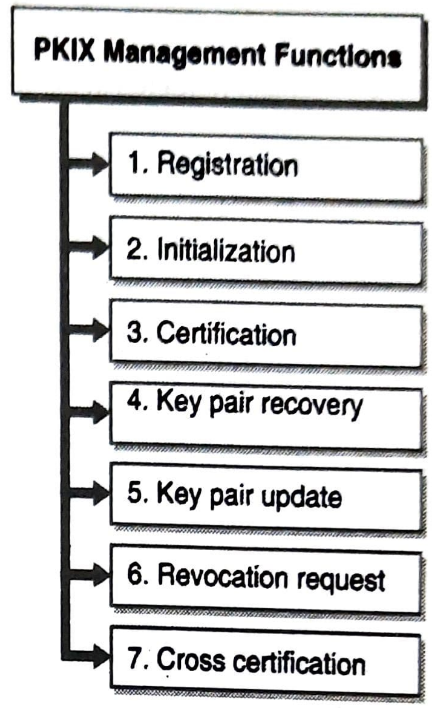

Fig. 7.5.3

5. **Key pair update**

- Key pairs and new issued certificates updating on regular basis is necessary.
- In case of certificate revocation, when lifetime of the certificate gets expired, updating the repositories are required.

6. **Revocation request**

Certificate revocation request made by authorized user in an abnormal situation.

7. **Cross certification**

- Multiple CA's exchange information provided in establishing a cross certificate.
- Cross-certification allows CAs and end users from different PKI domains to interact.