Authentication in Distributed System

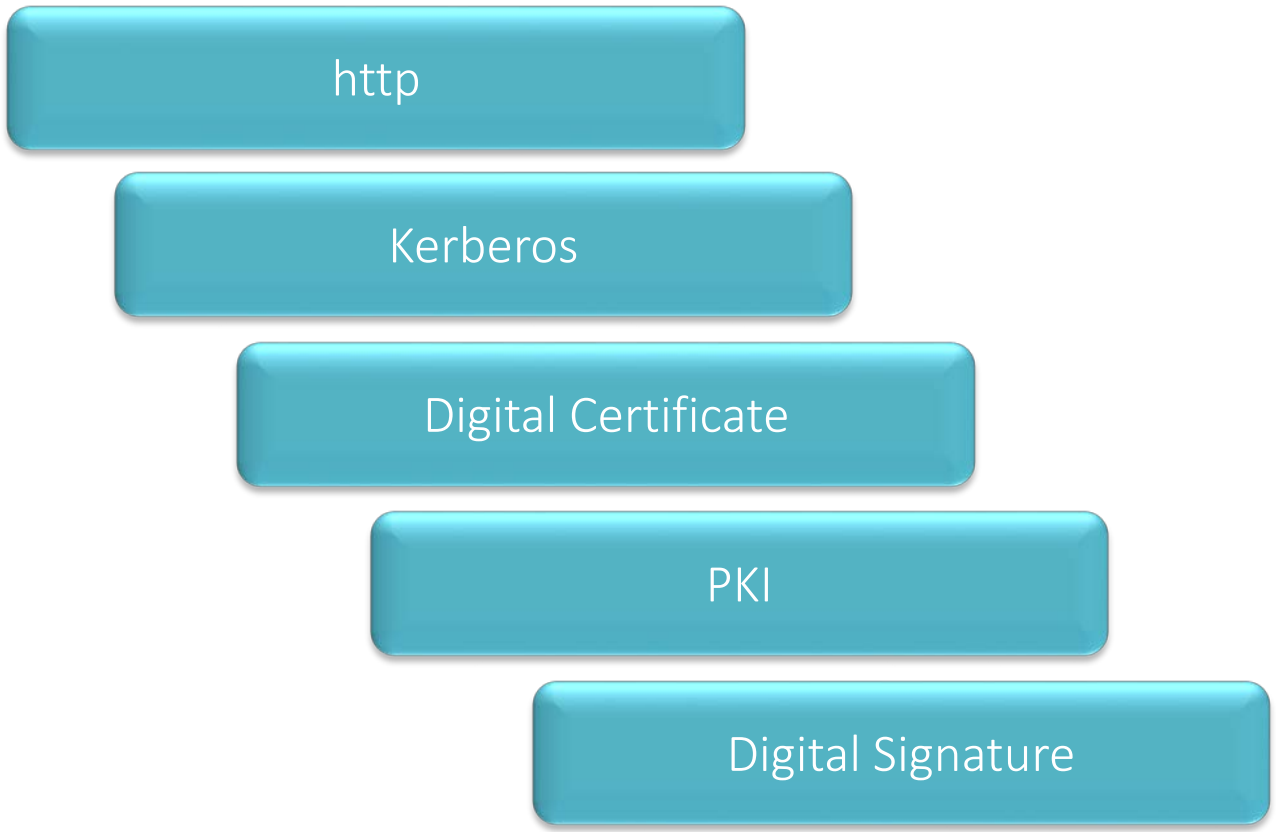
Prof. Dr. Eşref ADALI

www. Adalı.net

Questions

- Are user information belong to real user?
- Are they stolen information?
- The server that we are logging, is the one we want to connect?

ID Authentication Methods



http

User has to be register the system by

- User name
- Password

http provides 2 options:

- Basic Access Authentication
- Digest Access Authentication

Basic Access Authentication

- User name and password are coded by Base64. It is so simple coding and can be solved easily.
- So it can not say, Basic Authentication method is safe.

Steps of Basic Authentication are

1. Client sends a request (GET Request)
2. Server answer with ‘401 Authentication Request’. It contains type of authentication and header of source domain ‘www-Authenticate’
3. Client sends ‘http GET’ with ‘Authentication’ header. This message consists of user name and password for site which is call castell.
4. Server generate a digest of user information. Then compare this with a digest which user sent tor server. If two digest are the same sand ‘200 OK’ if not ‘401 Authorization Required’ messages.

Digest Access Authentication

- Due to the weakness of Basic Authentication method, Digest Access Authentication was developed.
- User password do not send to server. Instead, the Hash value is send. In order to generate the Hash value MD5 is used.
- Server has a list of user name and passwords which are in Hash form.

Steps of Digest Authentication are

1. Client sends a request (GET Request)
2. Server answer with '401 Authentication Request'. It contains type of authentication and header of source domain 'www-Authenticate'
3. Client generates a digest of password + one time number + method of http and URI and sand it to server.

   MD5(MD5(<password>+';' + + ';'+MD5(method> + ';' + uri)
4. Server generate a digest of user information. Then compare this with a digest which user sent tor server. If two digest are the same sand '200 OK' if not '401 Authorization Required' messages.

Kerberos - 1

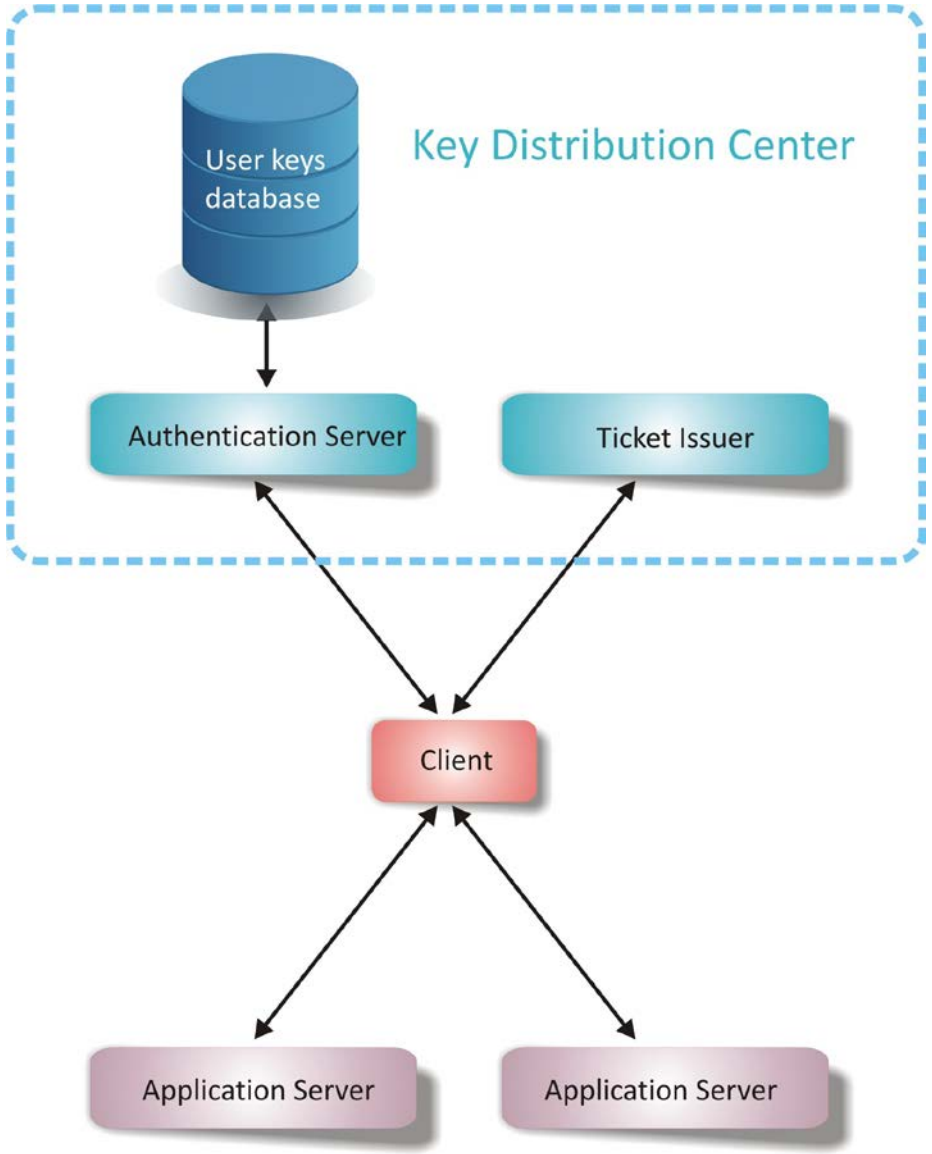
- Kerberos is developed in MIT for student registration system, in 1980. Leather on is extended for administration and accounting application.
- It is become an industry standard as RFC 1510.
- Kerberos use key distribution protocol which is developed by Needham and Schroerder.
- Kerberos uses DES for communication between client and server.

Basic features of Kerberos are

1. Single Sign On : In order to logging all application, only one user name and password is enough.
2. Password Security : The password of user is newer save either in client or server . I t does not transfer over network.
3. Mutual Authentication : Keyberos has secure server and unsecure network topology. Therefore it is necessary to maintain the security of a client while data are transferred between client and server.

Kerberos - 2

- For all servers and clients password are dedicated and they are known by Ticked Issuer (Distribution Center)
- Client askes a ticket to Access an application.
- Ticked is encrypted by password of application server.
- Application server decrypt the ticked and learn the ID of client.
- The content of Keyberos key are:
  - ID of client
  - ID of application server
  - Session cipher key
  - Duration of Ticket



Steps of Kerberos-I

Step-1

Client send its ID to Authentication Server as open text. Authentication server sent Session Key and Ticket Permission Message to client..

Session key encrypted by private key of client. Session key has Hash of client password.

Ticket permission ticket consists of user ID, client IP, duration and session key. All of those are encrypted by the key which provided by Authentication server.

Step-2

Ticket generation step :Client send these 2 message to Ticket Issuer:

Application Server : Ticket permission message and the name of application server.

Authentication : Usr ID, Time stamp of client, encrypted client/Ticked Issuer session key.

Ticket Issuer send client/server ticket and client/server session key.

Step-3

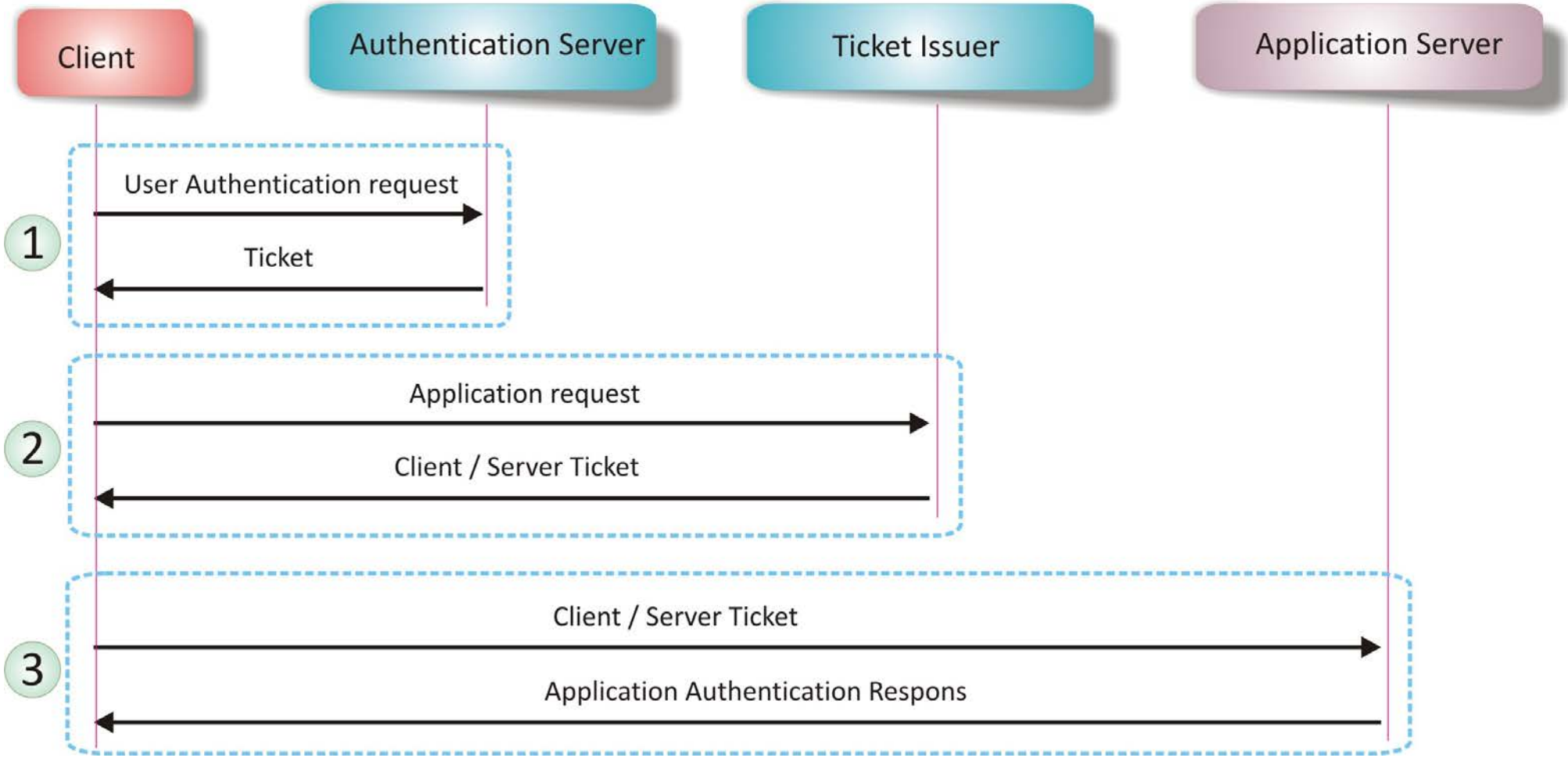
Connection of client to application server :

Solving of Client/Server ticket

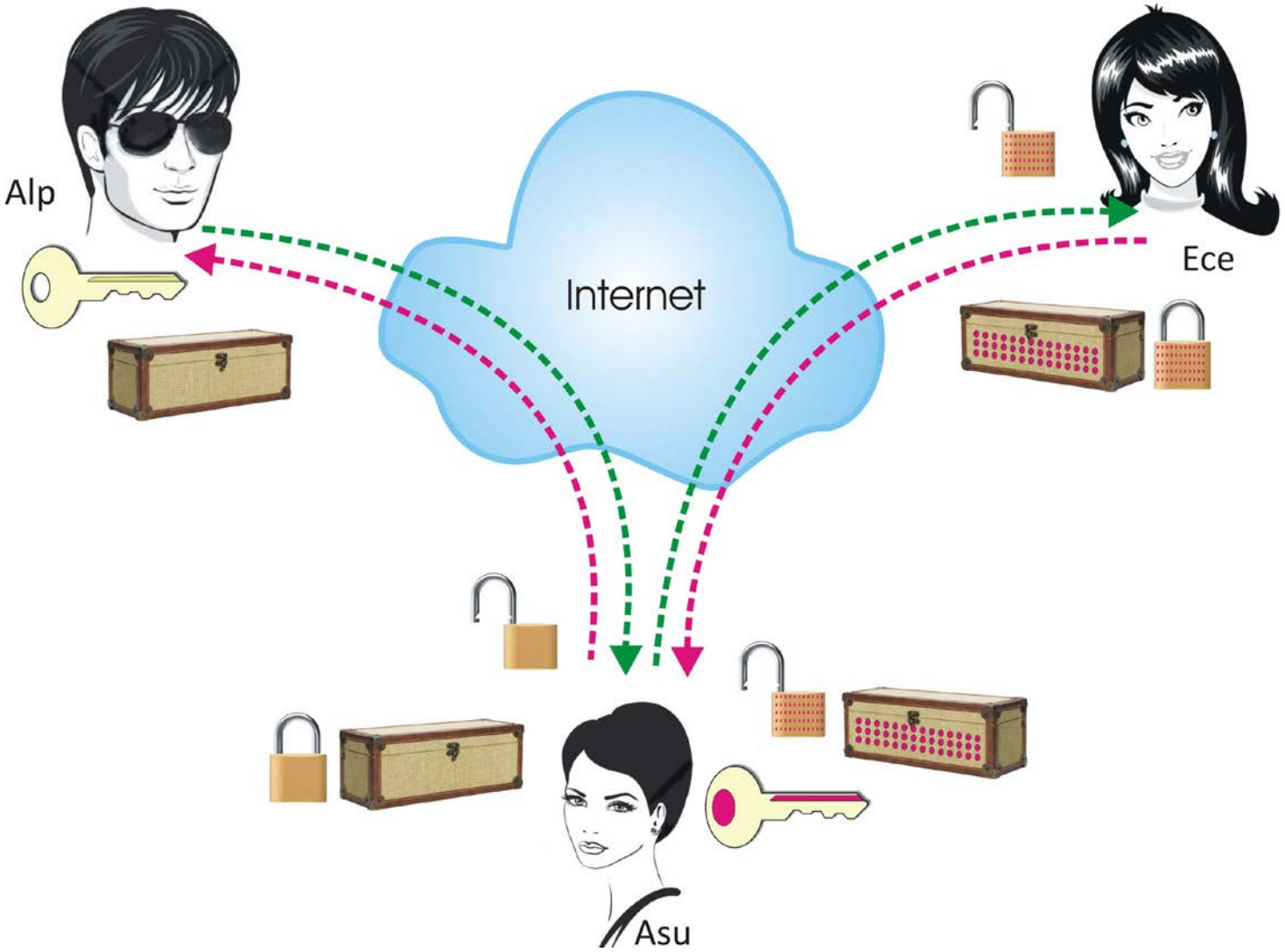
Authentication of application server

Time stamp

Steps of Kerberos - II



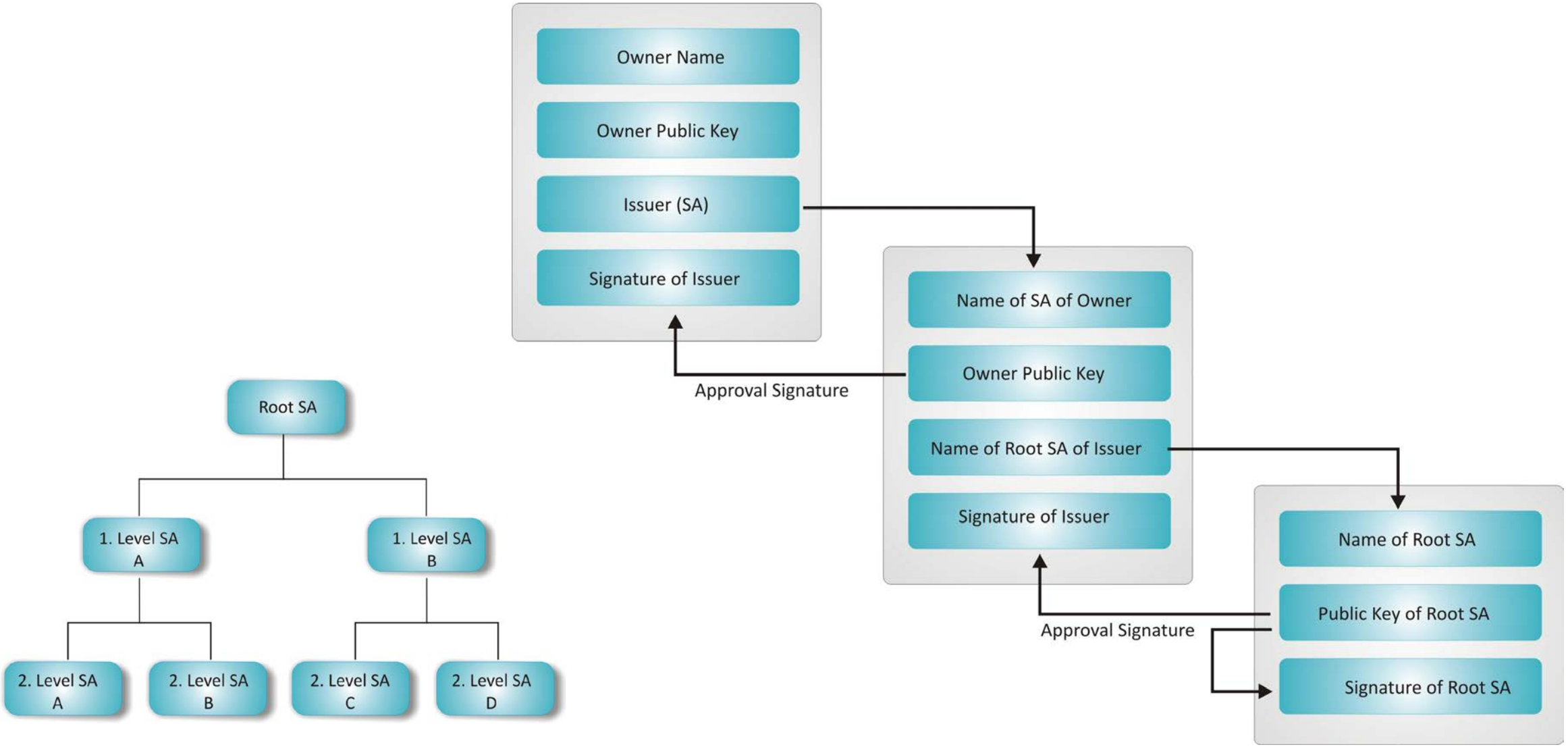
Digital Certificate -I



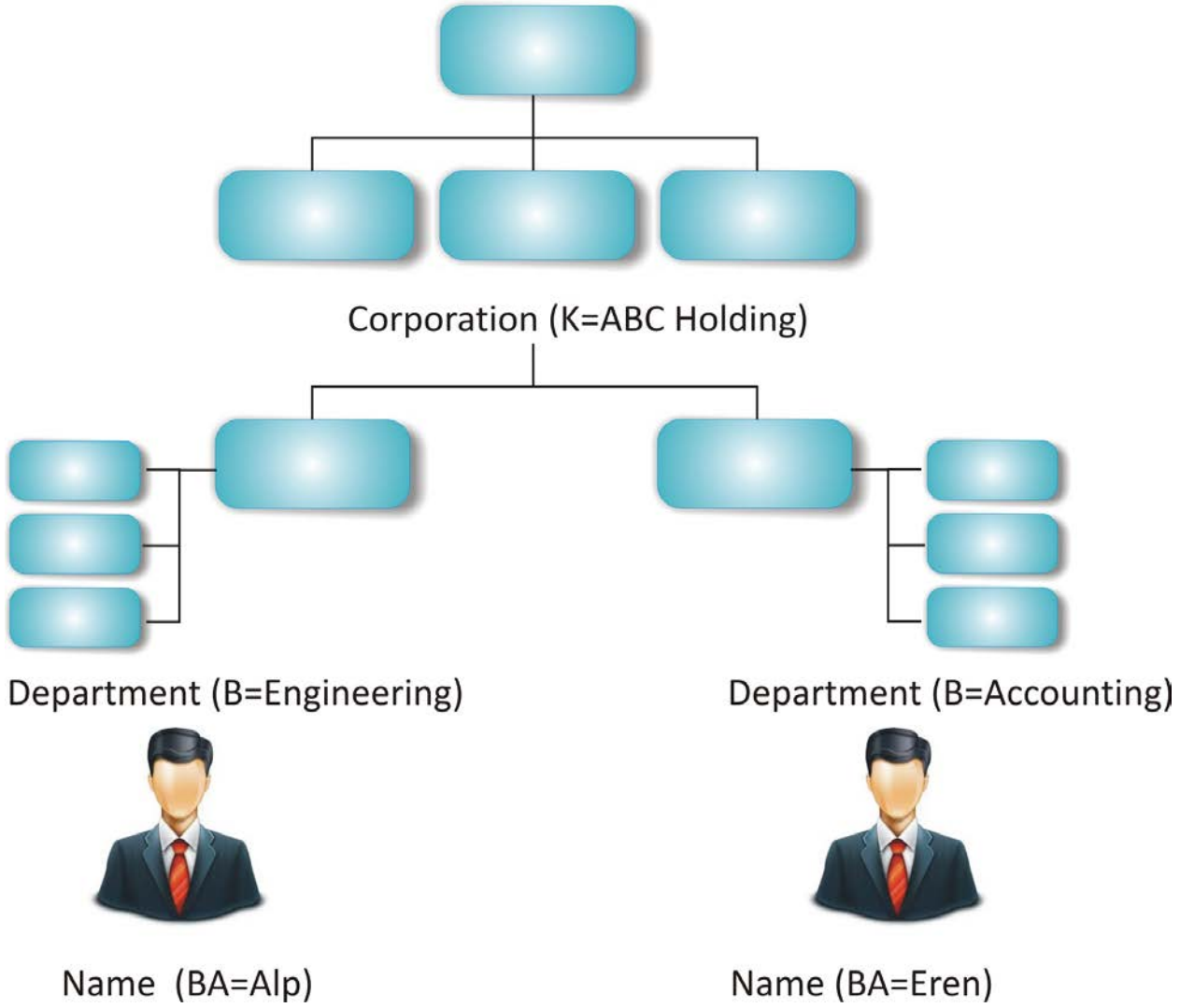
Version
Serial Number
Algorithm of Signature
Name of Issuer
Validation period
* Not valid before
* Not valid after
Owner Name
Owner Public Key
* Algorithm
* Public Key
Supplements
Signature

Digital Certificate

Digital Certificate -II



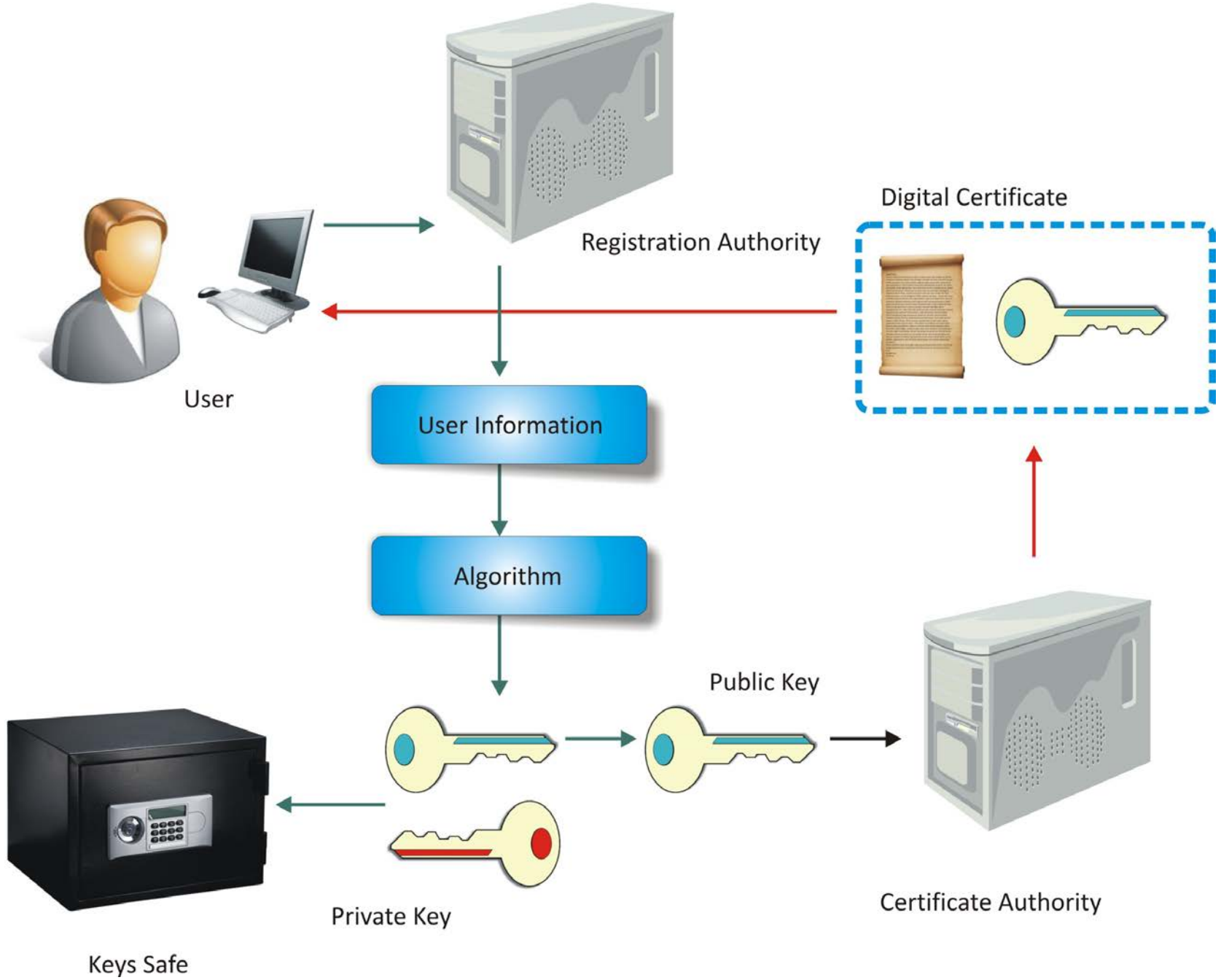
Digital Certificate -III



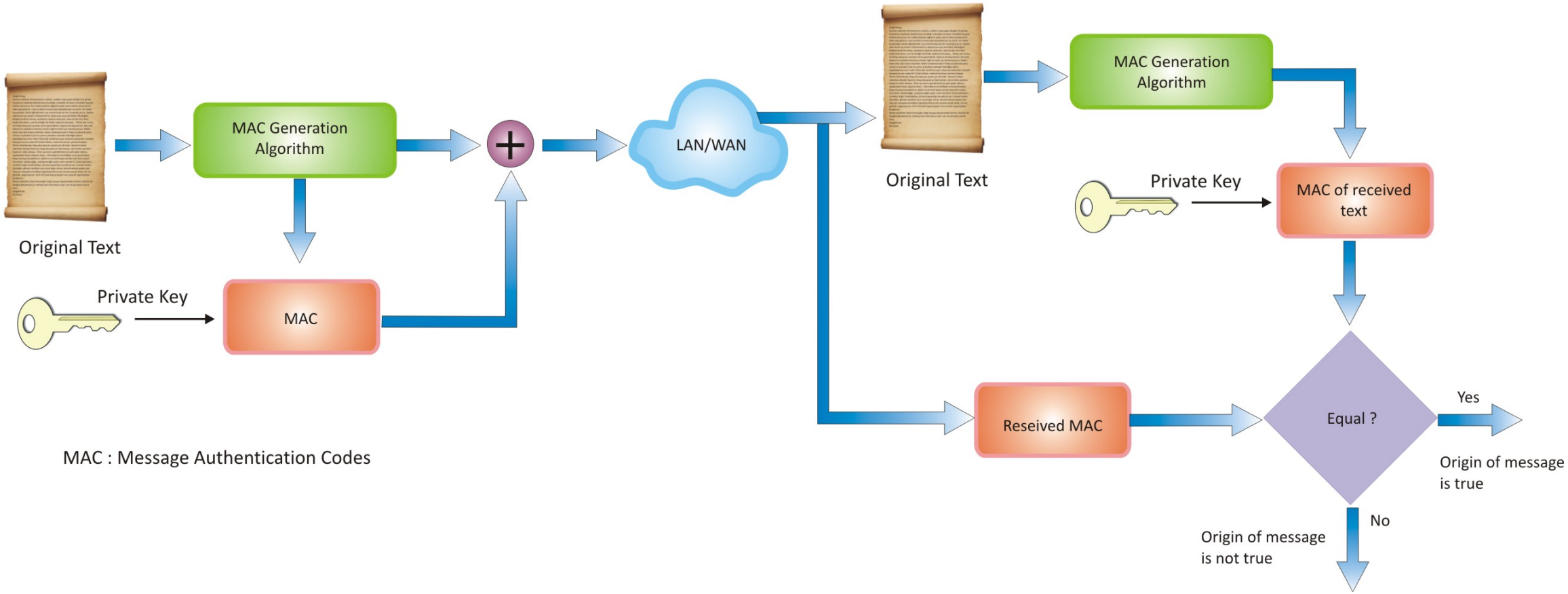
PKI

Certificate Authority : It provide an ID for user and user can use it to prove their ID.

Registration Authority : Requirement of a certificate is evaluate by Registration Authority.



Justifying of Message



MAC : Message Authentication Codes

Digital Signature