3. Digital Signatures, Digital Certificates, Key Management and Distribution

Digital Signatures

Digital Signatures: An Introduction

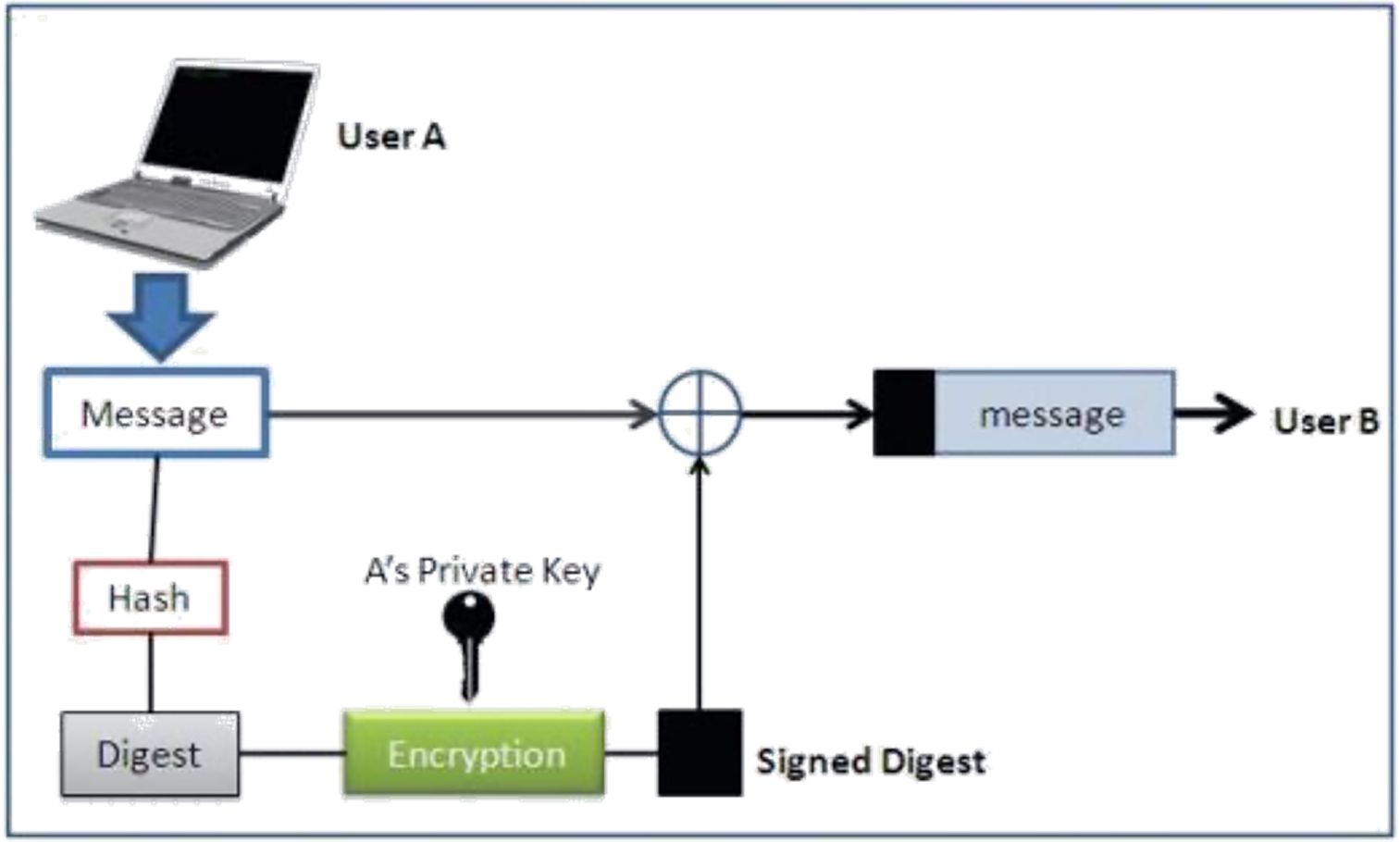
- The authenticity of many legal, financial, and other documents is determined by the presence or absence of an authorized handwritten signature.

- Various methods have been devised to digitally solve this problem, but the use of 'digital signature' is the best solution amongst them.

- A digital signature is nothing but an attachment to any piece of electronic information, which represents:

1. the content of the document and
2. the identity of the originator of that document uniquely.

What is a digital signature?



What is a digital signature

- Hash value of a message when encrypted with the private key of a person represents his digital signature on that e-Document.
- Digital Signature of a person therefore varies from document to document thus ensuring authenticity of each word of that document.
- As the public key of the signer is known, anybody can verify the message and the digital signature.

Why Digital Signatures?

- To provide:
  - Authenticity,
  - Integrity and
  - Non-repudiation to electronic documents

- To use the Internet as a safe and secure medium for Banking, e-Commerce and e-Governance with Security of Servers

Authenticity

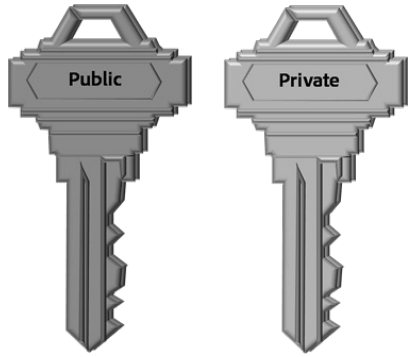
- Digital signatures can be used to authenticate the source of messages.
- When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.
- The importance of high confidence in sender authenticity is especially obvious in a financial context.

Integrity

- If a message is digitally signed, any change in the message will invalidate the signature.

- Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

BASIC REQUIREMENTS….



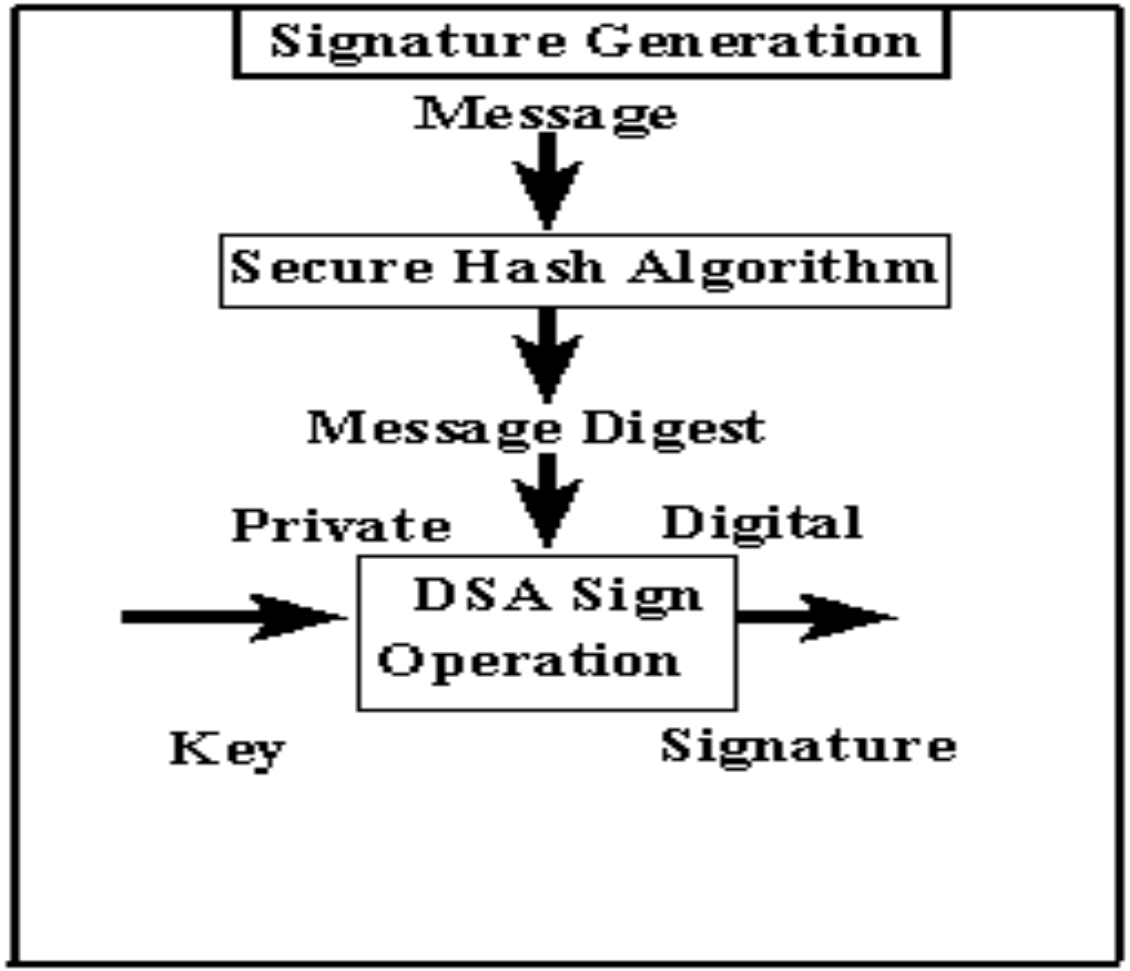
- Private Key
  - The private key is one which is accessible only to the signer. It is used to generate the digital signature which is then attached to the message.
- Public Key
  - The public key is made available to all those who receive the signed messages from the sender. It is used for verification of the received message.
- Digital Signature Certificate
  - A subscriber of the private key and public key pair makes the public key available to all those who are intended to receive the signed messages from the subscriber.

How it works?

- The use of digital signatures usually involves two processes performed by the:
- The signer of the message: signature creation
- The receiver of the signed message: validation

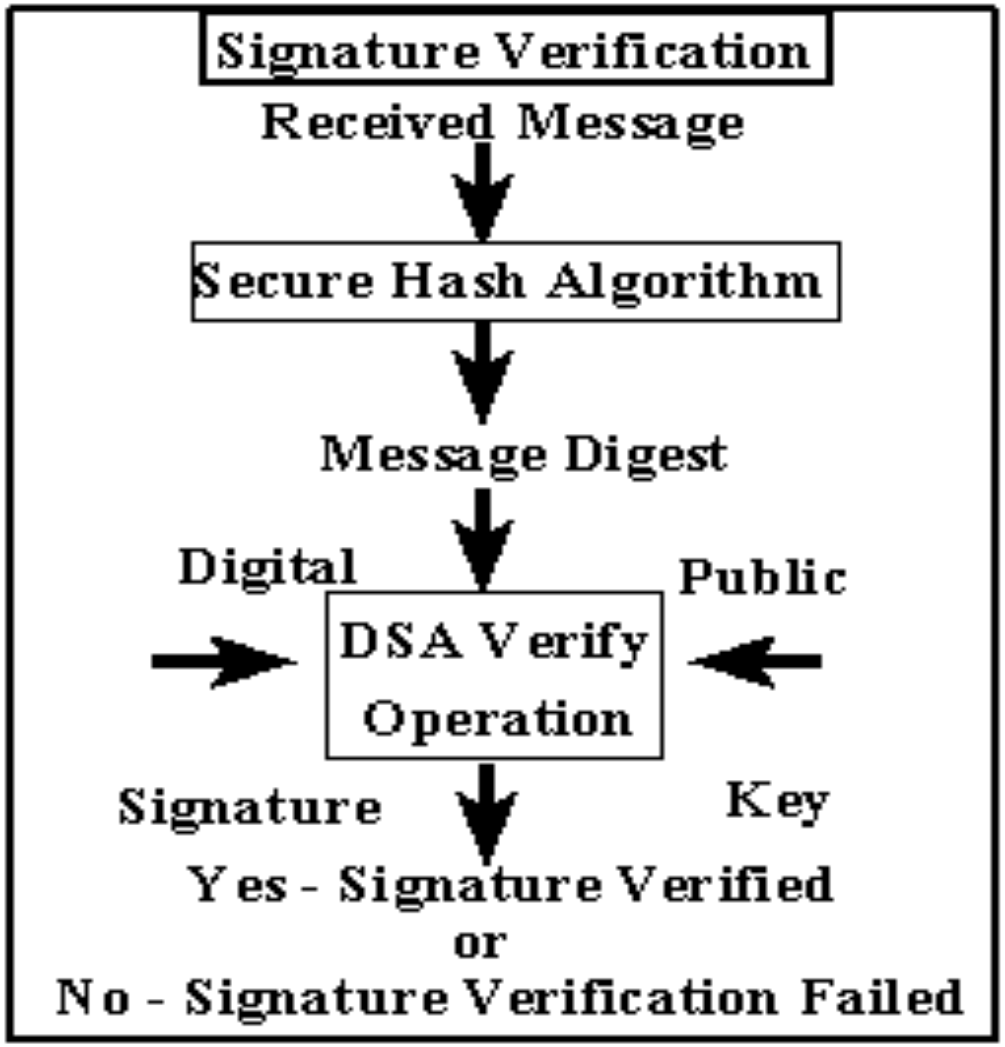
Digital signature creation algorithm

- Digital Signature Generation via Digital Signature Algorithm



Digital signature verification algorithm

- Digital Signature Verification



Challenges and Opportunities

- Institutional overhead:
  - The cost of establishing and utilizing certification authorities, repositories, and other important services,
  - Assuring quality in the performance of their functions.

- Subscriber and Relying Party Costs
  - A digital signer will require software, and will probably have to pay a certification authority some price to issue a certificate.
  - Hardware to secure the subscriber's private key may also be advisable.

APPLICATIONs

- E-Mail
- Data storage
- Electronic funds transfer
- Software Distribution
- eGovernance Applications

DRAWBACKS

- The private key must be kept in a secured manner
- The process of generation and verification of digital signature requires a considerable amount of time.
- For using the digital signature,
  - the user has to obtain private and public key,
  - the receiver has to obtain the digital signature certificate also.

Digital Certificate

Public-Key Infrastructure

- PKI is an integrated system of:
  - Software
  - Encryption methodologies
  - Protocols
  - Legal agreements
  - Third-party services
- PKI enables users to communicate securely
- PKI is based on public-key cryptosystems
  - Include digital certificates and certificate authorities (CAs)

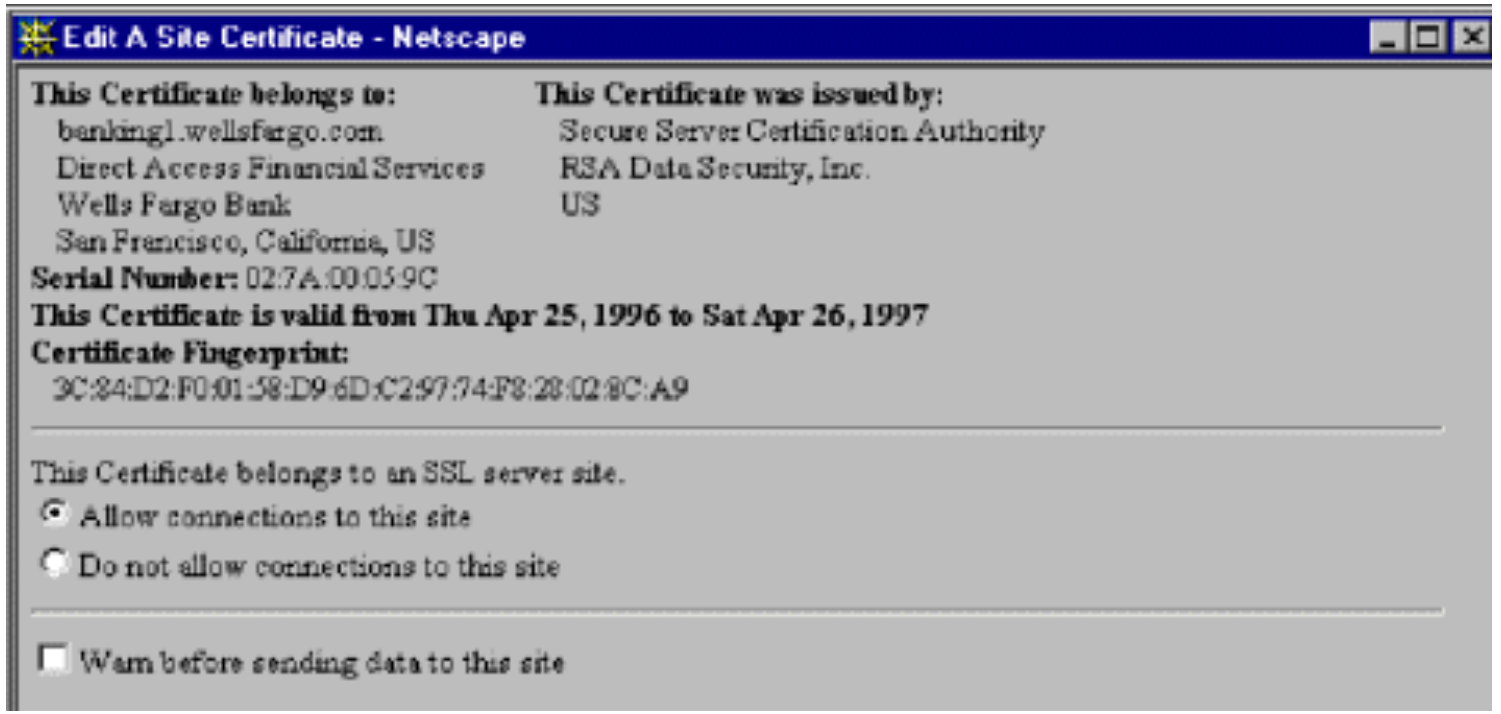
Certificate Authority

- Issues, manages, authenticates, signs, and revokes users' digital certificates
- Digital certificates typically contain the user name, public key, and other identifying information
- Unlike digital signatures, which help authenticate the origin of a message, digital certificates authenticate the cryptographic key that is embedded in the certificate

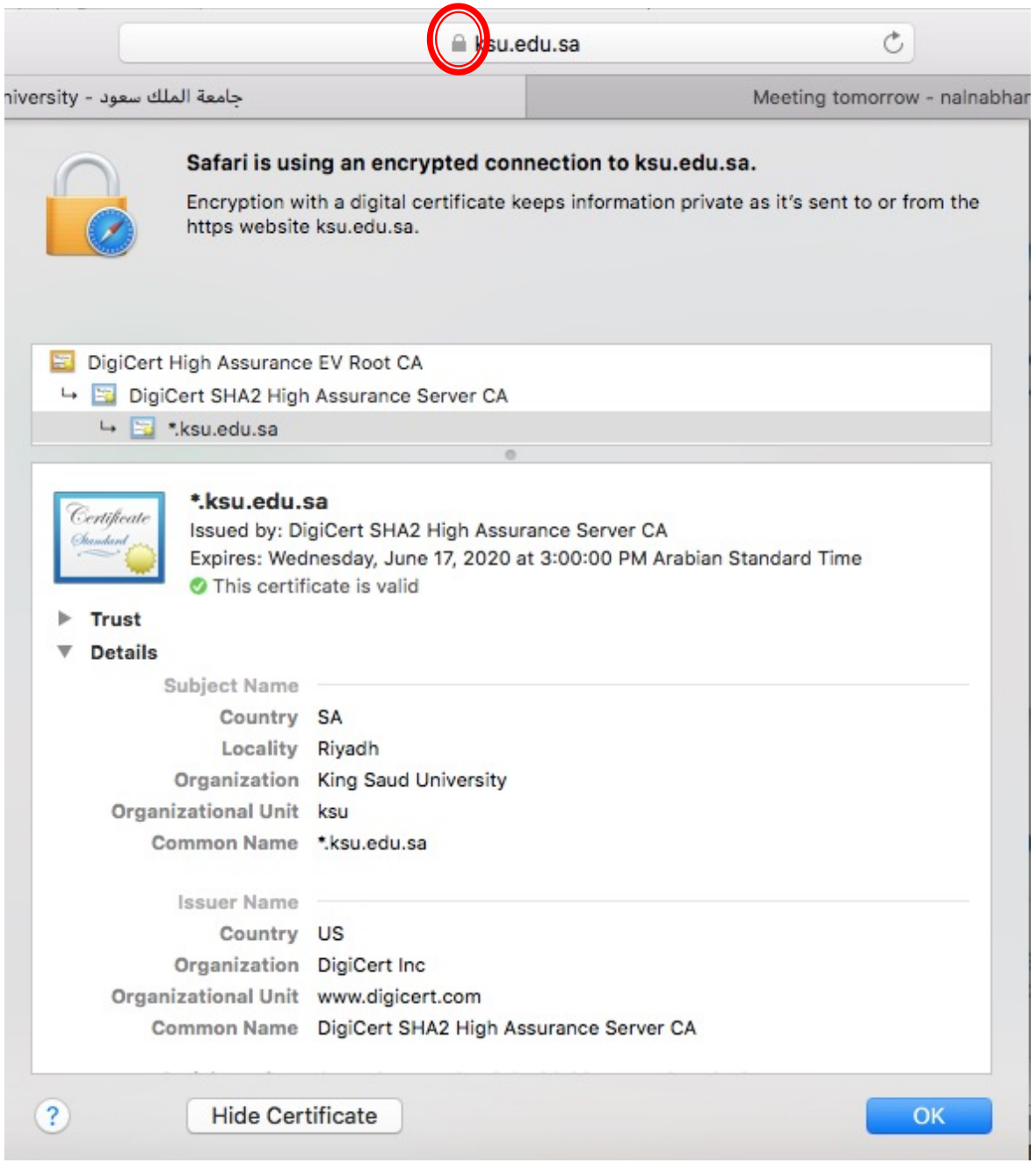
Digital Certificates

- Digital Certificates are the framework for identification information, and binding identities with their public keys.
- They provide a foundation for
  - identification
  - authentication
  - non-repudiation
- Types of Digital Certificates
  - Private: E-mail and for Website access
  - Server: By big e-commerce sites to protect their web servers and for communication purposes.
  - Developer: For code signing purposes

Sample View of a Certificate



Sample :

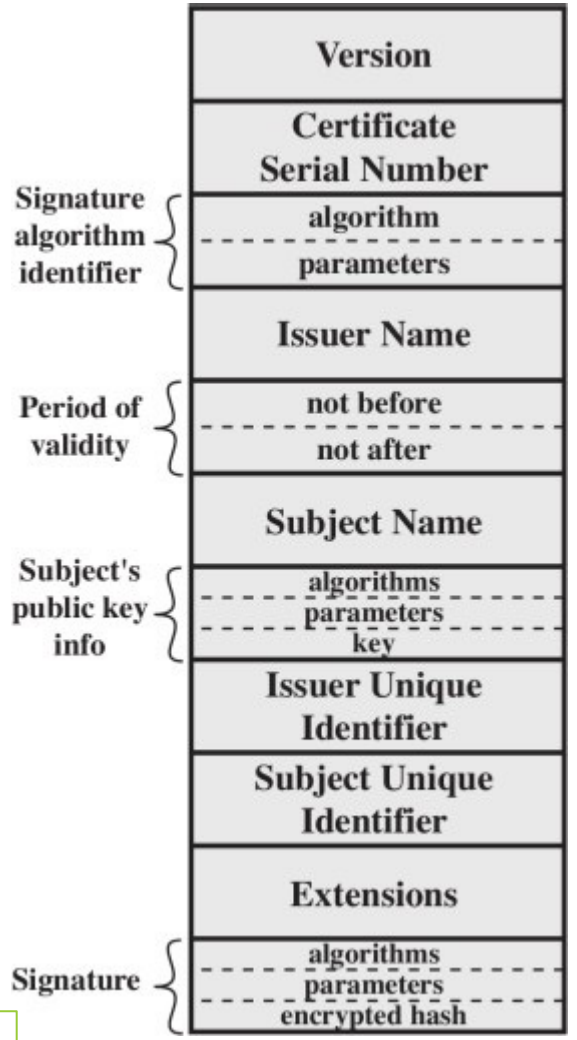

ksu.edu.sa
جامعة الملك سعود - iversity
Meeting tomorrow - nalnabhar
Safari is using an encrypted connection to ksu.edu.sa.
Encryption with a digital certificate keeps information private as it's sent to or from the https website ksu.edu.sa.
DigiCert High Assurance EV Root CA
DigiCert SHA2 High Assurance Server CA
*.ksu.edu.sa
*.ksu.edu.sa
Issued by: DigiCert SHA2 High Assurance Server CA
Expires: Wednesday, June 17, 2020 at 3:00:00 PM Arabian Standard Time
This certificate is valid
Trust
Details
Subject Name
Country SA
Locality Riyadh
Organization King Saud University
Organizational Unit ksu
Common Name *.ksu.edu.sa
Issuer Name
Country US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert SHA2 High Assurance Server CA
Hide Certificate
OK

X.509 Certificates

- An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard
- Each user/developer/server has a certificate, although it is created by the Certificate Authority (CA)
- Certificates are stored in a public directory
- Certificate format includes many fields
- Certificates may be revoked before expiry
  - CA signs a Certificate Revocation List (CRL), which is stored in public directory

X.509 v3 Certificate Format

- **Information on the subject** – "subject" refers to the site represented by the cert.
- **Information about the certificate issuer/certificate authority (CA)**
- **Serial number** – this is the serial number assigned by the issuer to this certificate.
- **Version** – the X.509 version used by a given certificate(version 3)
- **Validity period** – the period over which the cert can still be deemed trustworthy.
- **Signature** – digital signature of the entire digital certificate, generated using the certificate issuer's private key
- **Signature algorithm** – The cryptographic signature algorithm used to generate the digital signature
- **Public key information** – Information about the subject's public key. This includes: the algorithm, the key size (e.g. 256 bits), the key usage (e.g. can encrypt, verify, derive), and the public key itself



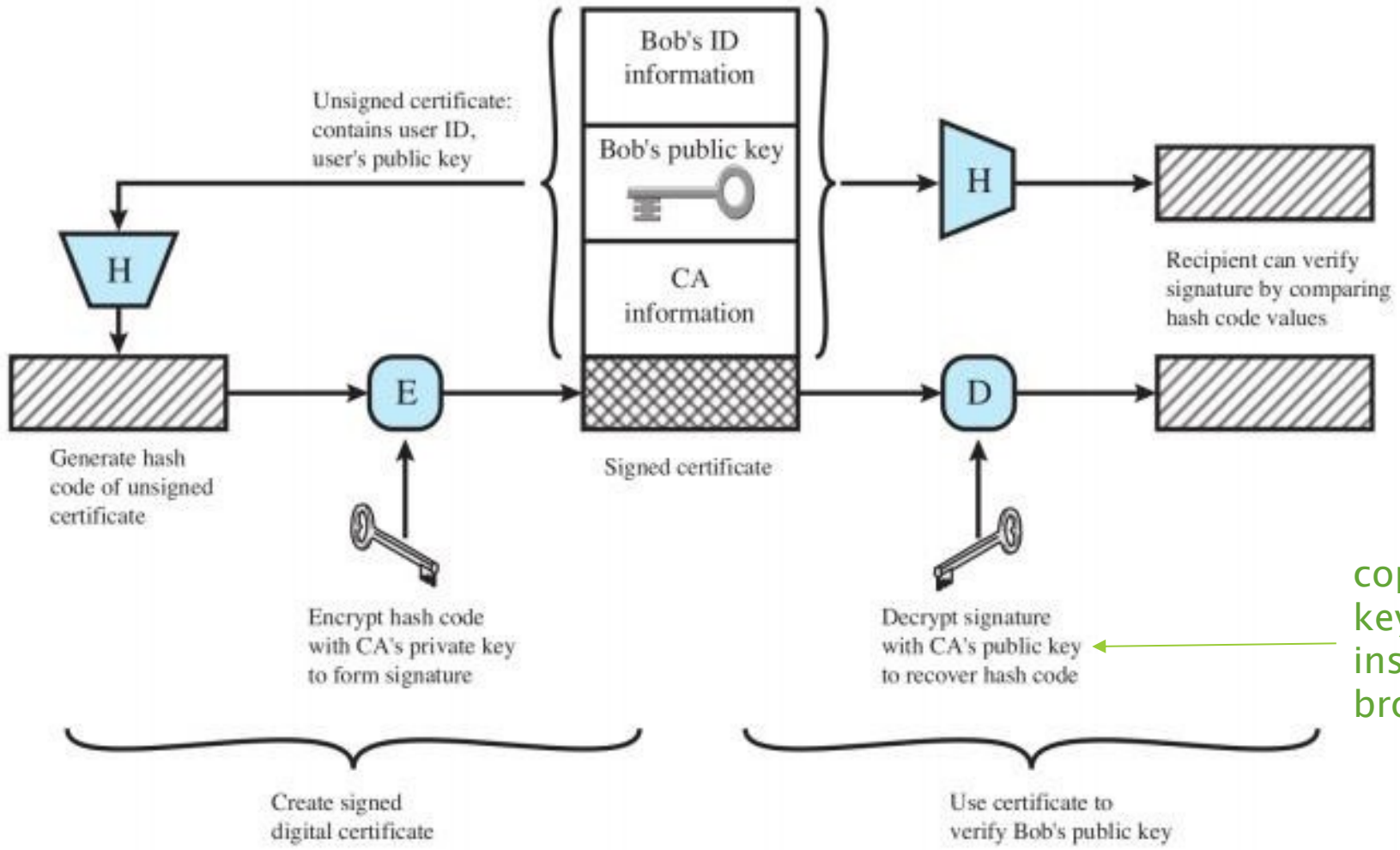
vital component in the encryption of data exchanged between the server and the client

Certificate Sample

Data:
Version: v1 (0x0)
Serial Number: 91 (0x5b)
Signature Algorithm: PKCS #1 MD5 With RSA Encryption
Issuer: CN=Chini Krishnan, OU=Network Systems Division, O=ValiCert Incorporated, C=US
Validity:
Not Before: Tue Oct 28 12:08:20 1997
Not After: Wed Oct 28 12:08:20 1998
Subject: CN=Brian Tretick, OU=ISS, O=Ernst & Young, C=US
Subject Public Key Info:
Algorithm: PKCS #1 RSA Encryption
Public Key:
Modulus:
00:b8:78:74:04:ca:b4:68:83:6d:61:48:1e:22:40:31:5a:c2:
1f:2e:aa:9b:b4:9d:7d:4d:2e:65:77:89:c6:5b:bb:5a:50:69:
e4:36:f0:73:d1:82:24:e4:3d:4e:93:c8:9f:17:eb:0b:2a:2e:
30:2e:30:58:44:49:b5:49:26:de:f1
Public Exponent: 65537 (0x10001)

Signature:
Algorithm: PKCS #1 MD5 With RSA Encryption
Signature:
55:c1:30:30:b1:d4:d4:a4:f2:24:10:45:0c:ec:26:66:8a:11:a4:e3:3c:
b0:25:cd:d3:dc:09:a7:36:d5:10:2e:43:90:67:c5:f4:b5:fe:45:69:27:
d7:06:14:cb:84:68:c1:7e:fc:b2:e3:2c:93:95:1b:02:ee:06:3e:4a:50:
46:4f:7f:07:66:12:b6:b0:06:90:28:46:6d:8c:f1:e4:7d:f7:b8:d2:cb:
29:cd:34:8a:d1:00:aa:44:57:49:10:28:2e:04:4a:67:55:92:37:5a:29:
5f:da:d5:b5:d9:8a:26:c0:6a:a5:58:d8:df:65:b3:7f:18:a6:1c:ea:11:
3e:9c

Public-Key Certificate Use



copy of that CA's public key will likely be pre-installed in the user's web browser

Key Distribution and Management

Key Distribution and Management

- Symmetric key cryptography
  - Encryption and decryption is based on a shared secret key
- Asymmetric (public) key cryptography
  - Public and private key pair of keys

Key Distribution and Management

- Symmetric key cryptography:
  - fast implementations,
  - good for encrypting large amounts of data;
  - requires shared secret key

- Asymmetric (public) key cryptography:
  - inefficient for large data,
  - good for authentication;
  - no need to share a secret

- Key distribution issues:

1. How to share symmetric keys?
2. How to distribute public keys?

Key Management

- Challenges
  - How to share a secret key?
  - How to obtain someone else's public key?
  - When to change keys?

- Assumptions and Principles
  - Many users wish to communicate securely across network
  - Attacker can intercept any location in network
  - Manual interactions between users are undesirable (e.g. physical exchange of keys)
  - More times a shared secret key is used, greater chance for attacker to discover the key

Key Agreement – Symmetric Algorithms

- Number of keys to be exchanged: depends on number of entities wishing to communicate
- For a group of N parties, every pair needs to share a different key.
- What is the total number of keys?

- Solution:
  - Need a key distribution protocol.
  - Uses a central authority, a.k.a., Trusted Third Party (TTP)
  - Every party shares a key with a central server.

Needham–Schroeder Protocol

- Parties:
- Users A and B.
- Trusted server T
- Setup:
- A and T share K_{AT},
- B and T share K_{BT}
- Goals:
- Mutual entity authentication between A and B
- key establishment

- Messages:
  - $A \rightarrow T$: A, B, N_A (1)
  - $A \leftarrow T$: $E[K_{AT}]\ (N_A, B, k, E[K_{BT}](k,A))$ (2)
  - $A \rightarrow B$: $E[K_{BT}]\ (k, A)$ (3)
  - $A \leftarrow B$: $E[k]\ (N_B)$ (4)
  - $A \rightarrow B$: $E[k]\ (N_B\text{-}1)$ (5)

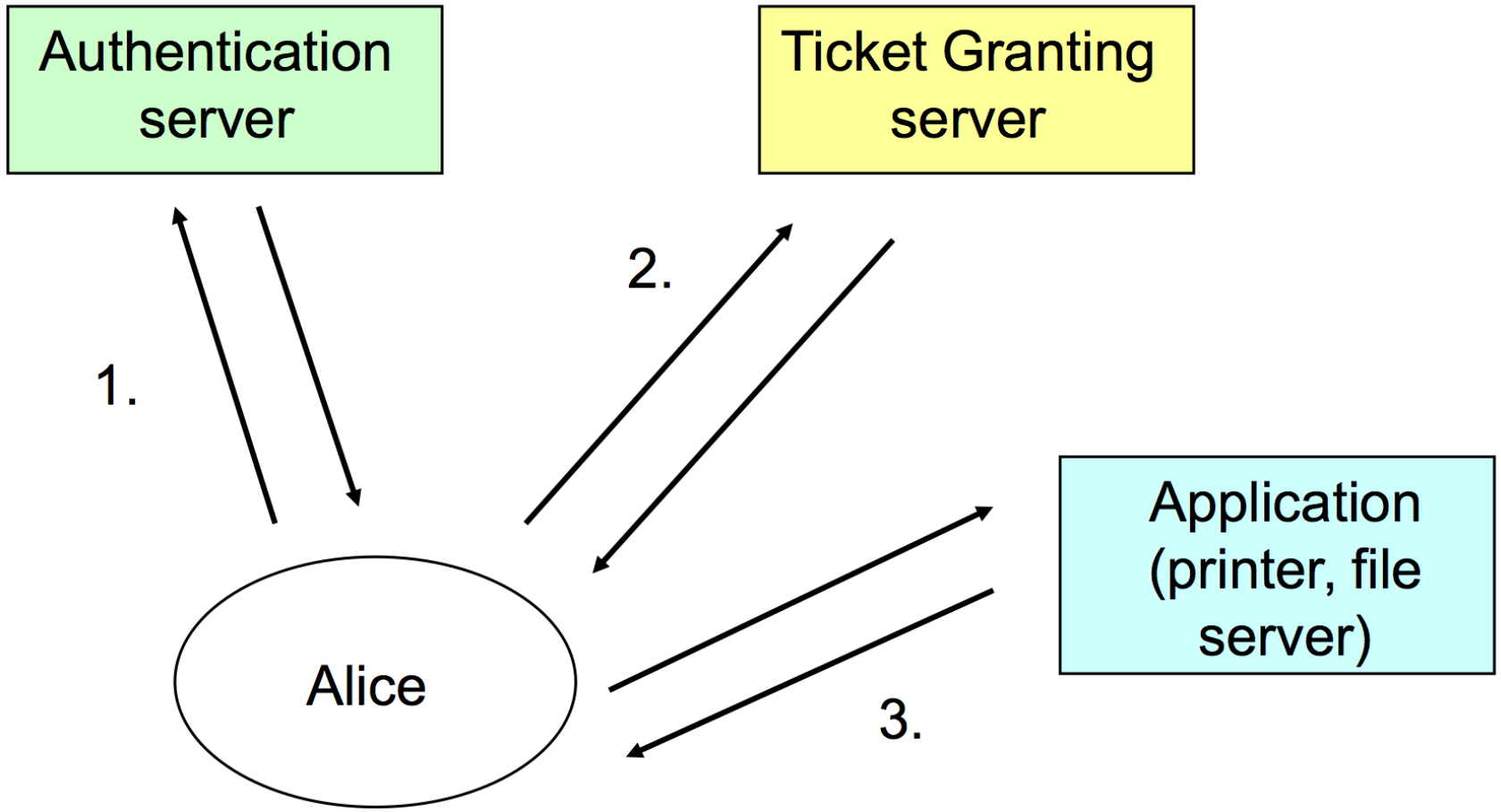
Kerberos

- Implement the idea of Needham-Schroeder protocol.
- Provides authentication and secure communication• Developed at MIT:
- http://web.mit.edu/kerberos/www
- Used in many systems, e.g., Windows 2000 and later as default authentication protocol.

Kerberos – Overview

- One issue of Needham-Schroeder
  - Needs the key each time a client talks with a service
- Principle:
  - Alice uses her password to sign on once a day

Kerberos Protocol



Kerberos Protocol – 2

1. Alice gets a “daily key” KA from the authentication server
   - Based on Alice’s long term secret (password)
   - KA is stored on Alice’s machine and deleted at the end of the day
2. Alice uses KA to get application key K from the ticket granting server.
3. Alice establishes a secure link with the application using K.

Kerberos Drawbacks

- Single point of failure:
- requires online Trusted Third Party: Kerberos server.

- Useful primarily inside an organization
- Does it scale to Internet?

Distribution of Public Keys

- By design, public keys are made public
- Issue: how to ensure public key of A actually belongs to A (and not someone pretending to be A)

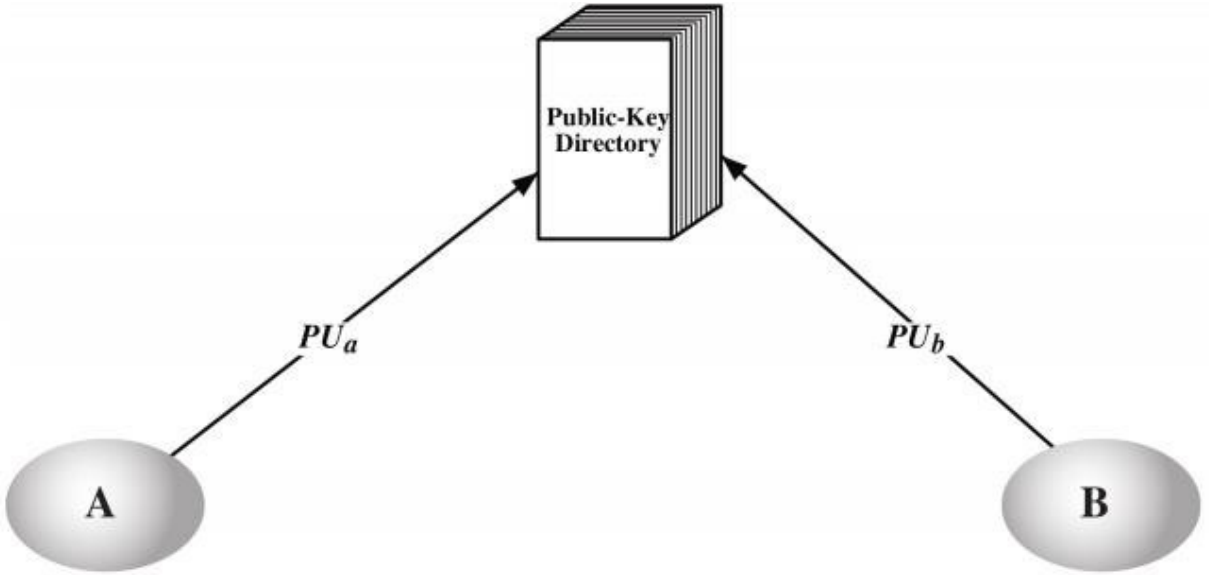
- Four approaches for distributing public keys
  1. Public announcement
  2. Publicly available directory
  3. Public-key authority
  4. Public-key certificates

Public Announcements

- Make public key available in open forum: newspaper, email signature, website, conference, . . .
- Problem: anyone can announce a key pretending to be another user

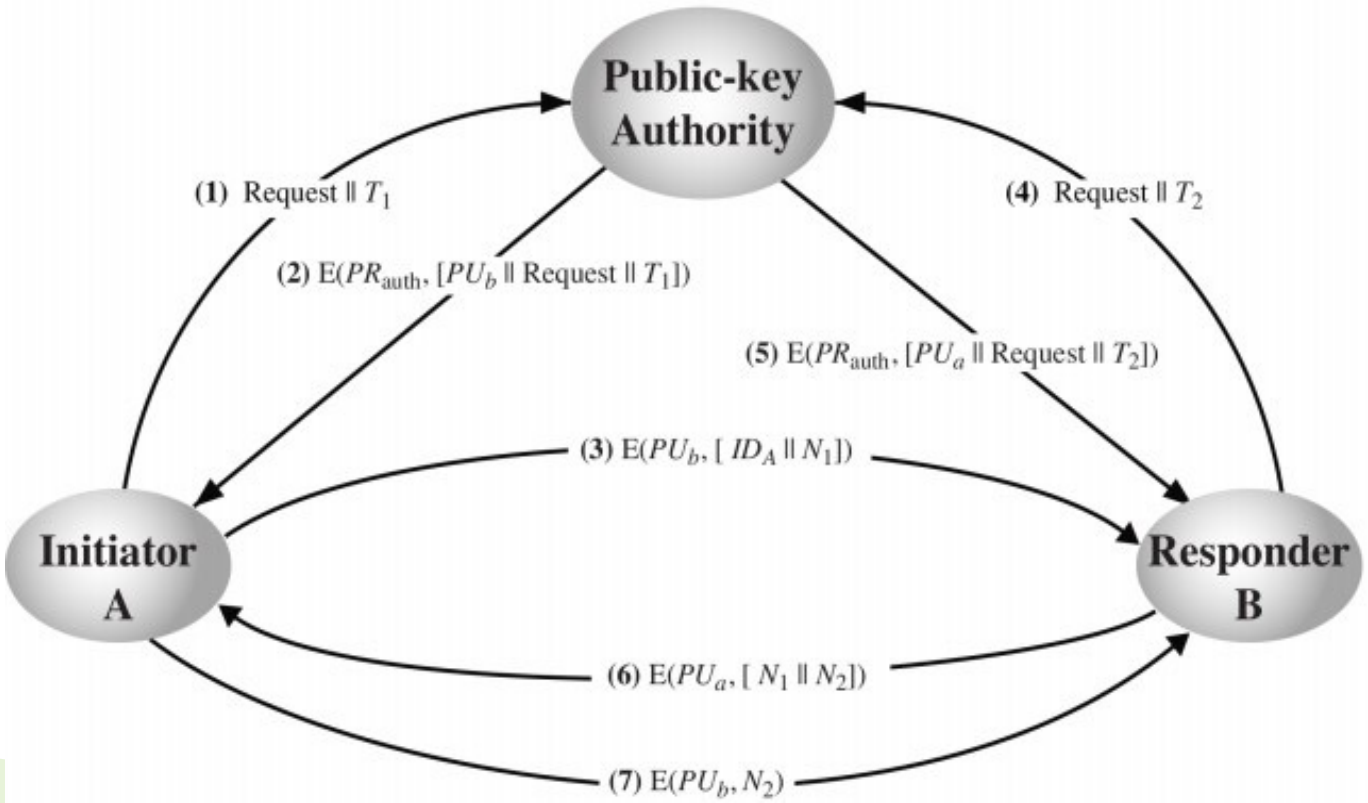
Publicly Available Directory

- All users publish keys in central directory
- Users must provide identification when publishing key
- Users can access directory electronically
- Weakness: directory must be secure



Public-Key Authority

- Specific instance of using publicly available directory
- Assume each user has already security published public-key at authority; each user knows authority's public key

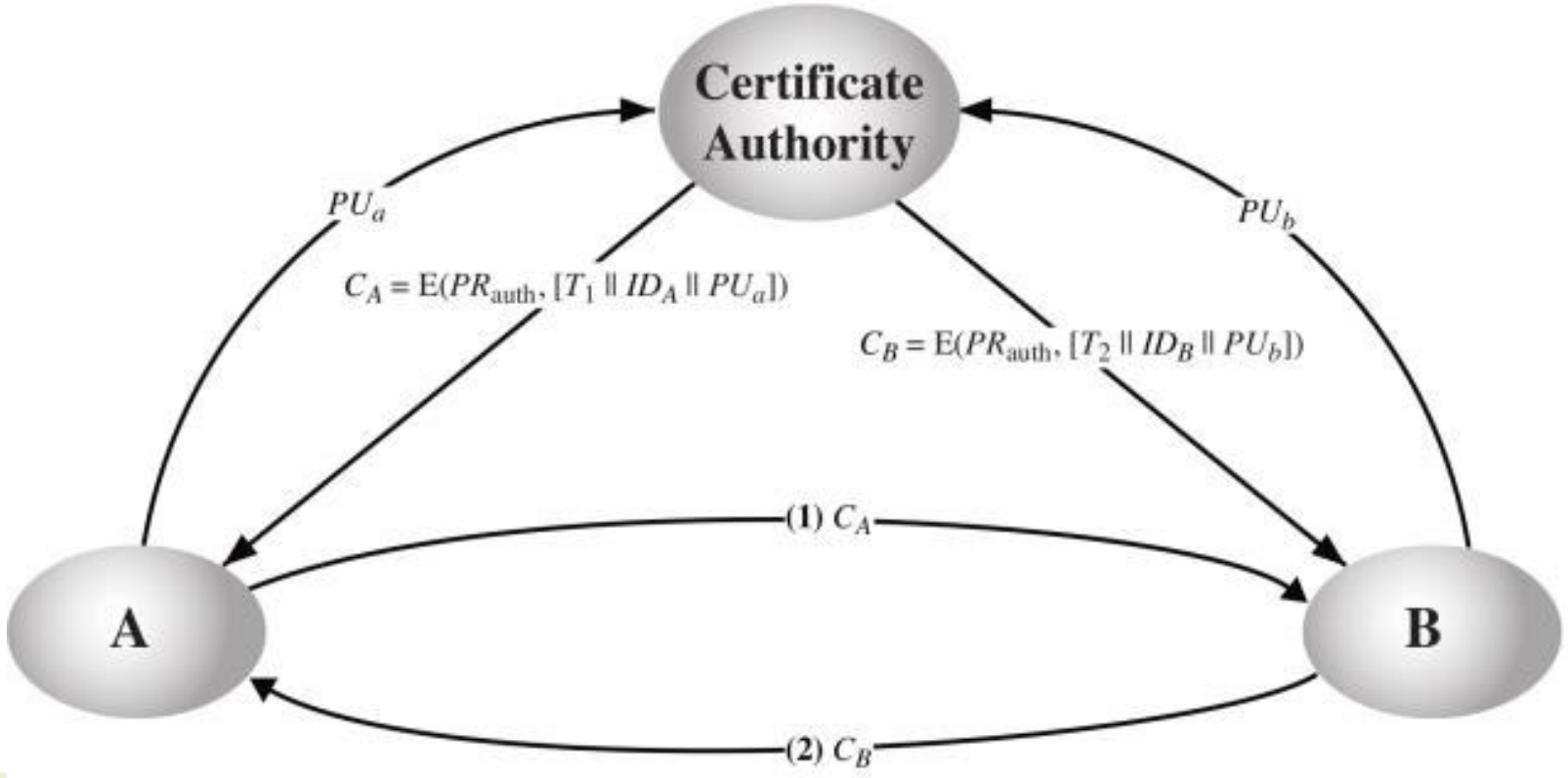


Public-Key Authority

- First 5 messages are for key exchange; last 2 are authentication of users
- Although 7 messages, public keys obtained from authority can be cached
- Problem: authority can be bottleneck
- Alternative: public-key certificates

Public-Key Certificates

- Assume public keys sent to CA can be authenticated by CA;
- Each user has certificate of CA



Public Key Certificates

- A certificate is the ID and public-key of a user signed by CA:

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

- Timestamp T validates currency of certificate (expiration date)
- Common format for certificates is X.509 standard (by ITU)
  - S/MIME (secure email)
  - IP security (network layer security)
  - SSL/TLS (transport layer security)
  - SET (e-commerce)