Information security

Eng. Taghreed Harfoush

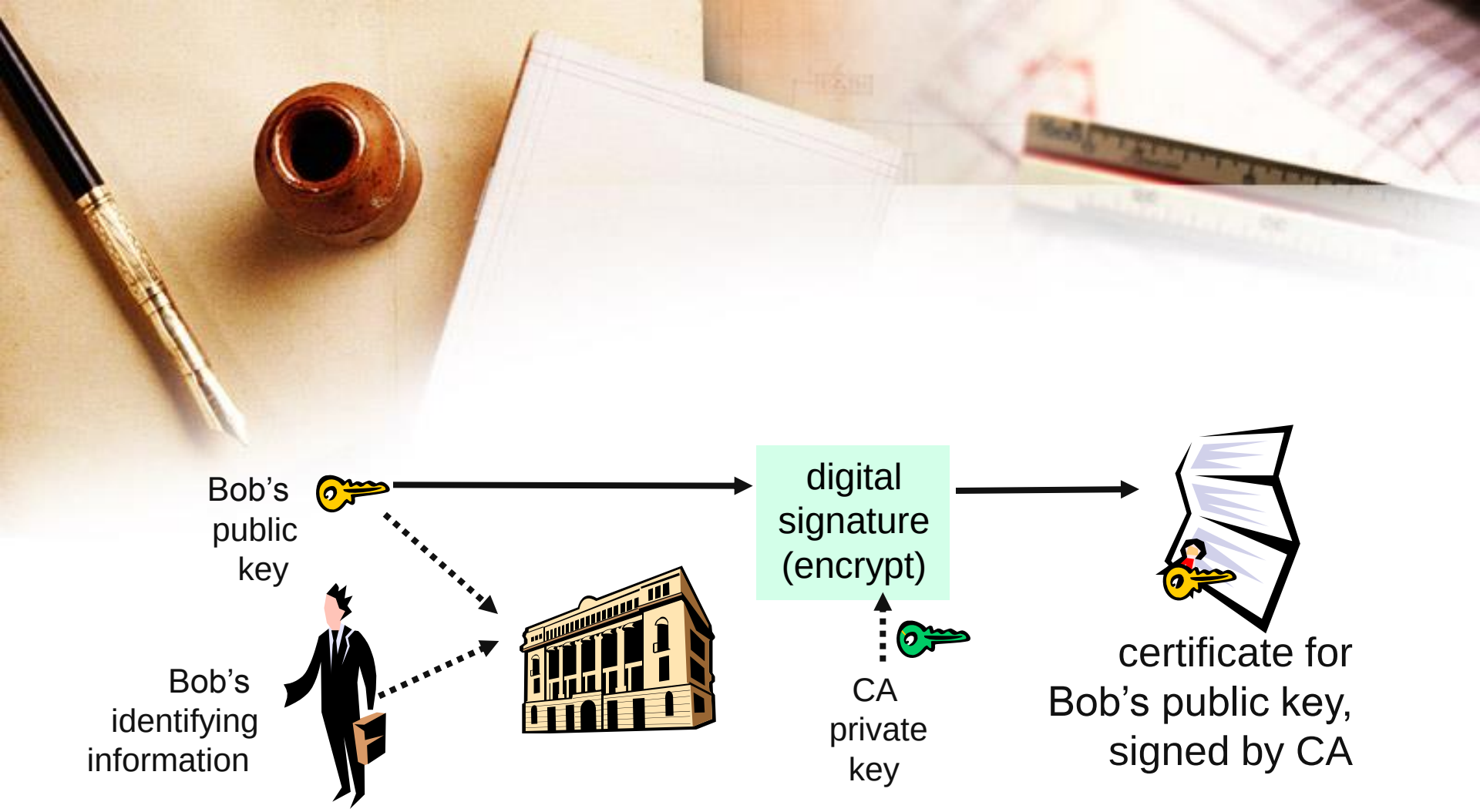
Lecture-7

Certification Authorities

- Certificates allow key exchange without real-time access to public-key authority
- Certification authority (CA): binds public key to particular entity, E.

E registers its public key with CA:

- E provides “proof of identity” to CA.
- CA creates certificate binding E to its public key.
- Certificate containing E’s public key digitally signed by CA
- CA says “this is E’s public key”

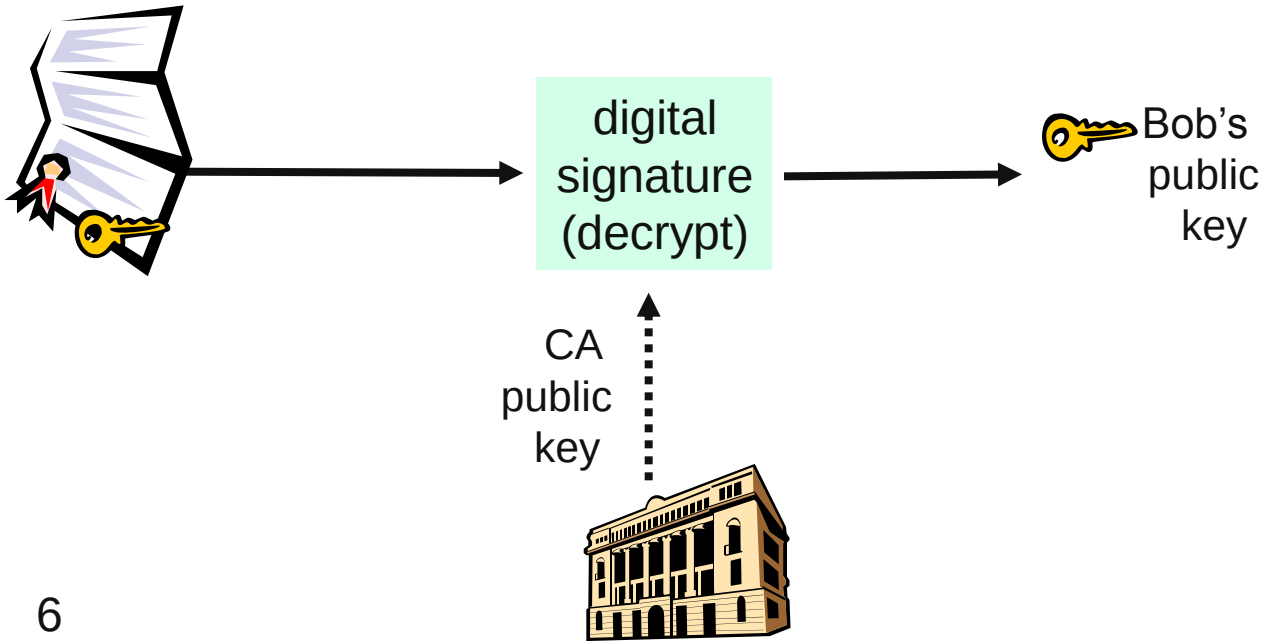


Requirement on Certificates:

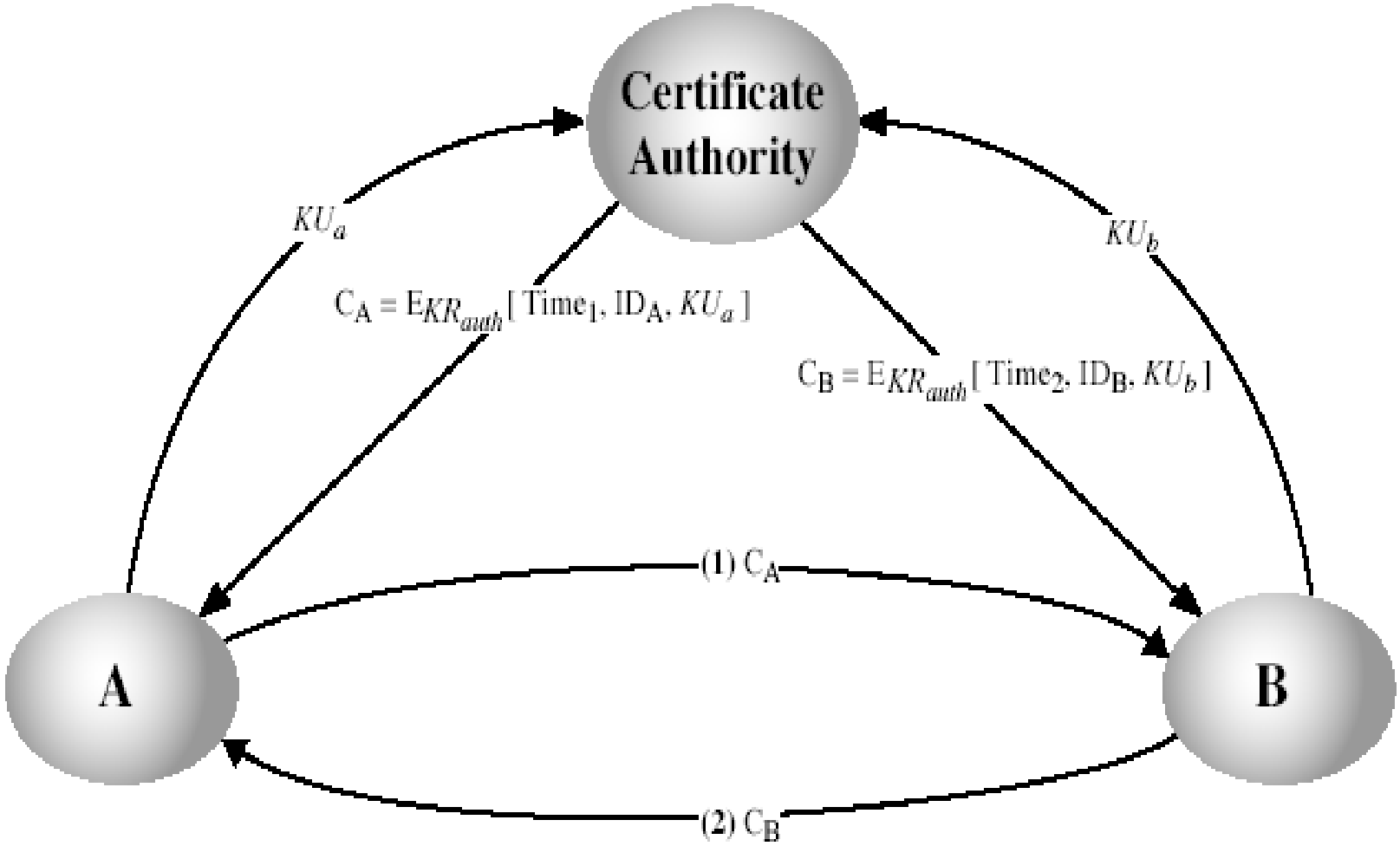
1. Any participant can read a certificate to determine the name and public key of the certificates owner
2. Any participant can verify that the certificate originated from the authority
3. Only the certificate authority can create and update certificate

Certification Authorities

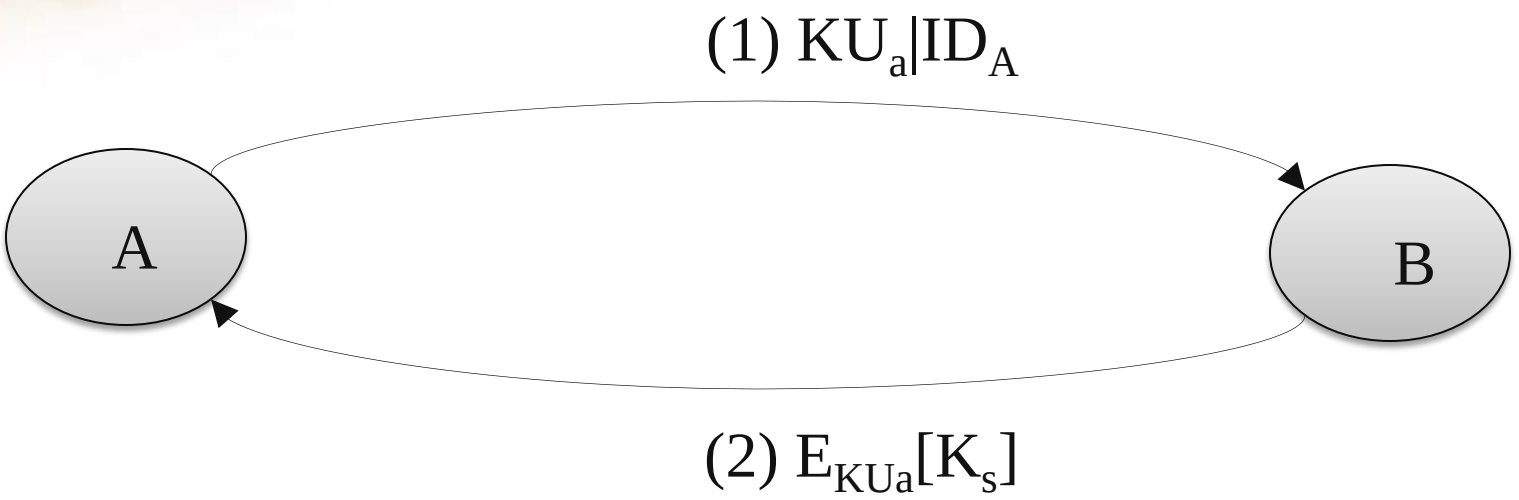
- When Alice wants Bob's public key:
  - Gets Bob's certificate (Bob or elsewhere).
  - Apply CA's public key to Bob's certificate, get Bob's public key



Public-Key Certificates

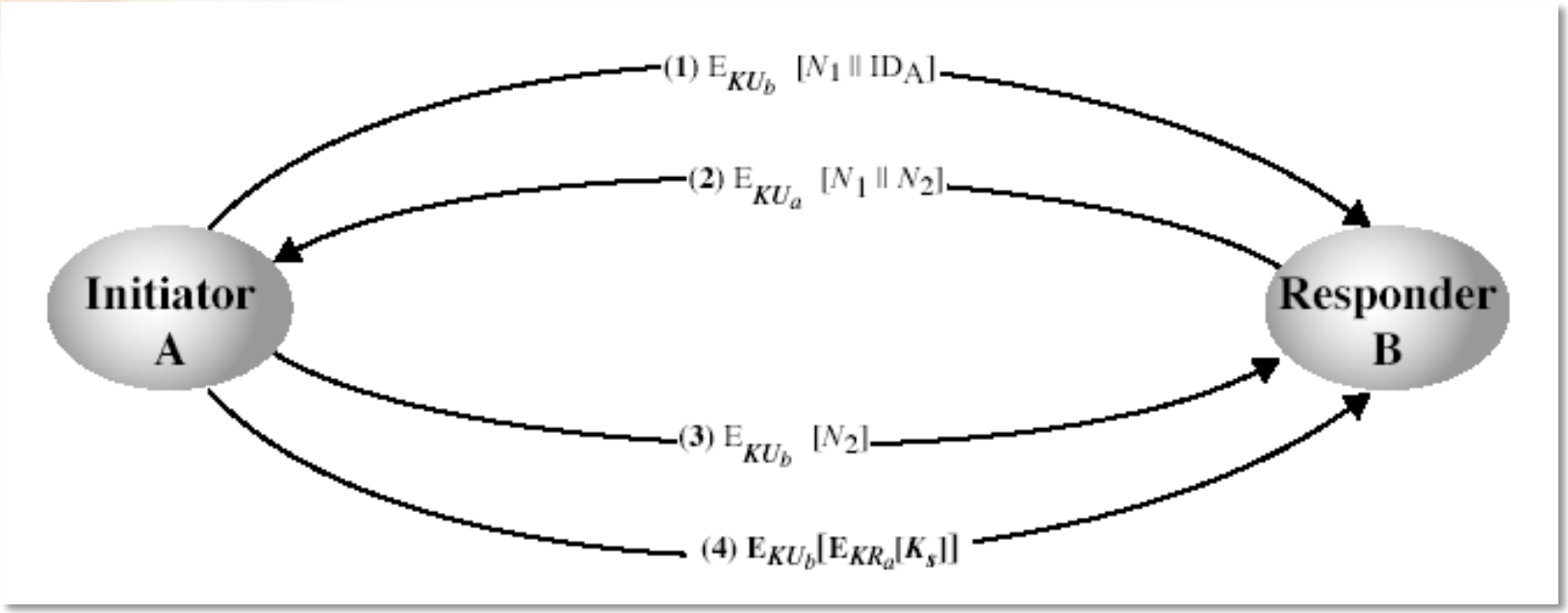


Simple Secret Key Distribution



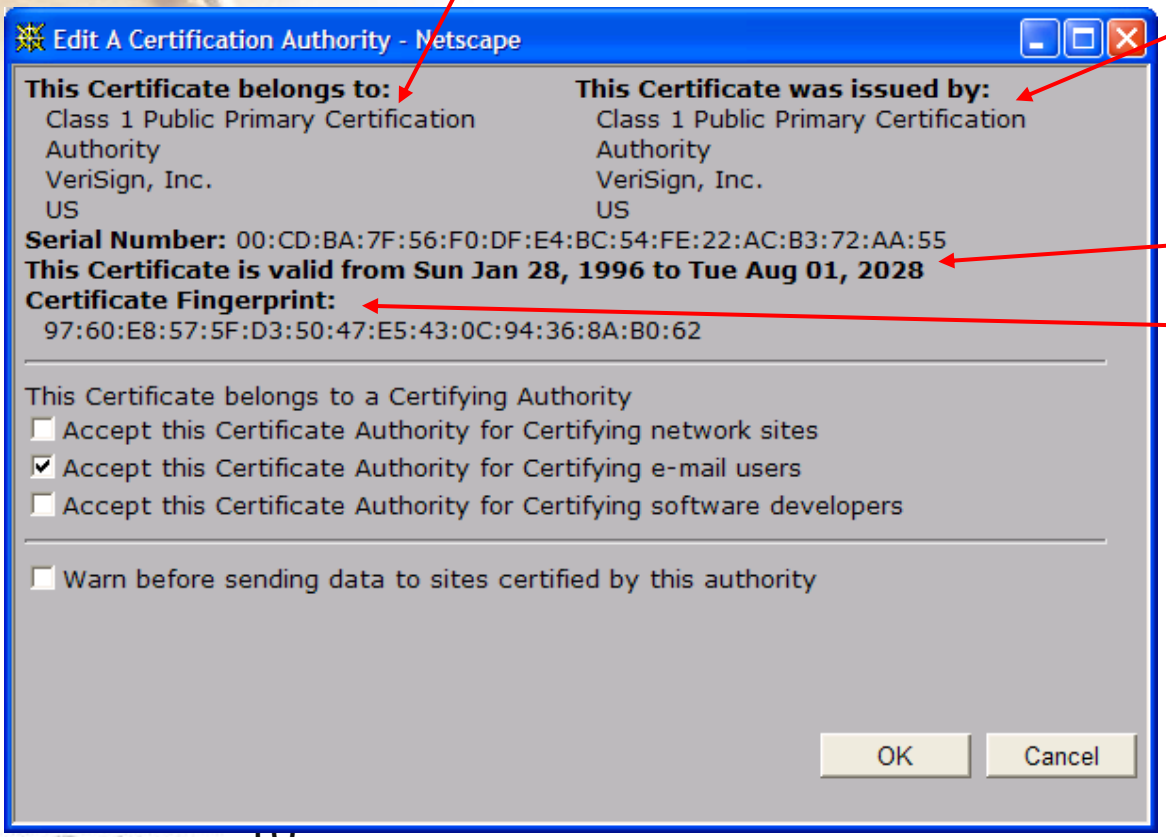
Needham Secret Key Distribution

- if A and B have securely exchanged public-keys:



Certificate Contents

- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)



- Info about certificate issuer
- Valid dates
- Digital signature by issuer

Q&A