

Information security

Eng. Taghreed Harfoush

Lecture-7

1

A background image showing a desk with a fountain pen, an inkwell, and a ruler.

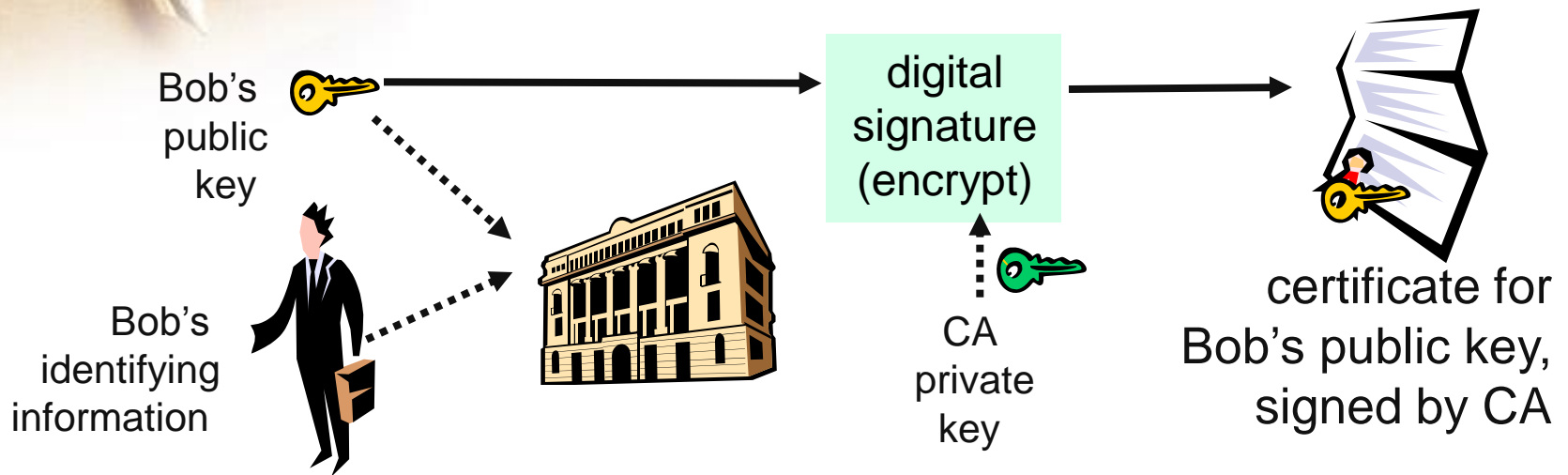
Certification Authorities

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

A close-up photograph of a desk setup. On the left, a fountain pen with a black barrel and gold-colored accents lies diagonally. Next to it is a small, round, brown inkwell. In the background, a white ruler is visible, and a piece of lined paper is partially seen. The overall lighting is warm and soft.

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”



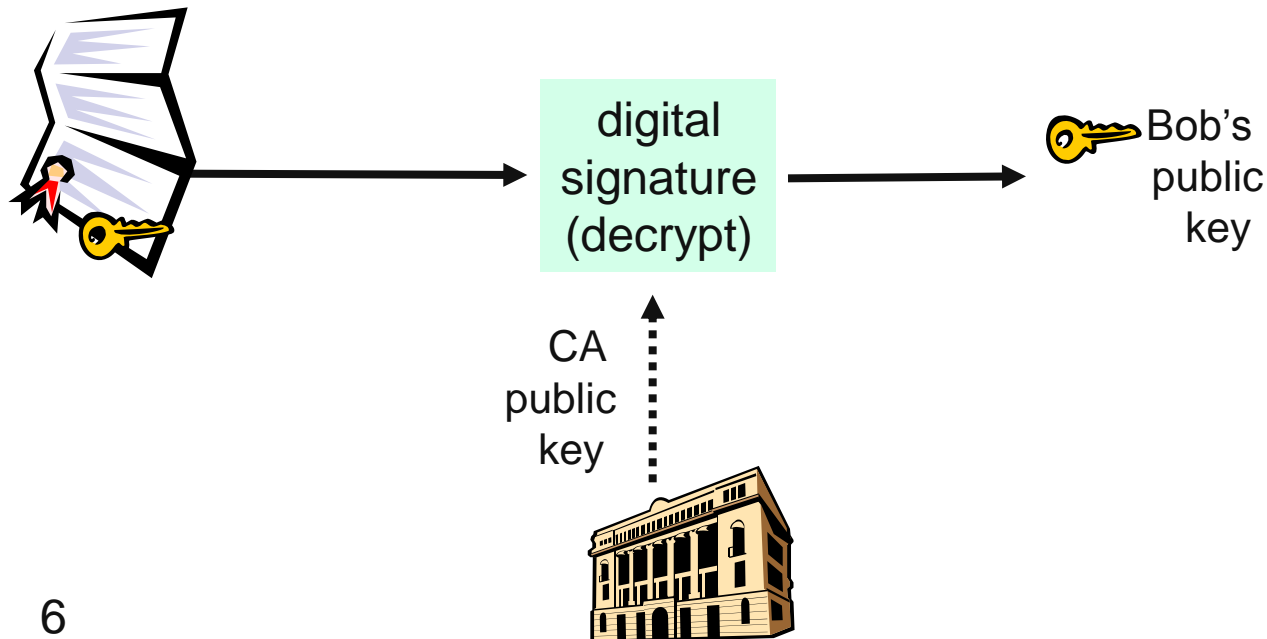
A close-up photograph of a desk setup. On the left, a fountain pen with a black barrel and gold-colored accents lies diagonally. Next to it is a small, round, dark brown inkwell. In the background, a white notepad with a red cover is visible, along with a wooden ruler and a stack of papers.

Requirement on Certificates:

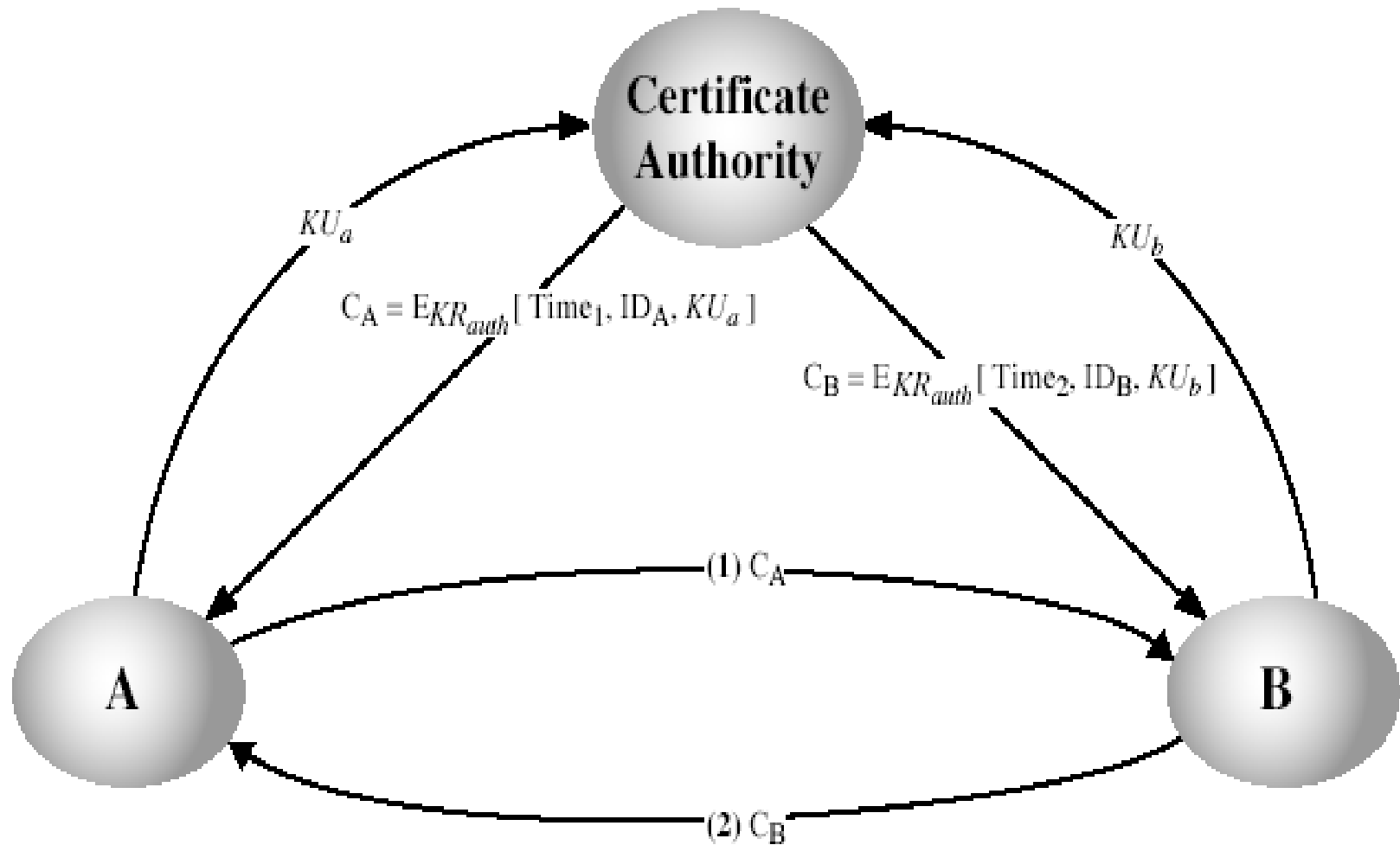
1. Any participant can read a certificate to determine the name and public key of the certificates owner
2. Any participant can verify that the certificate originated from the authority
3. Only the certificate authority can create and update certificate

Certification Authorities

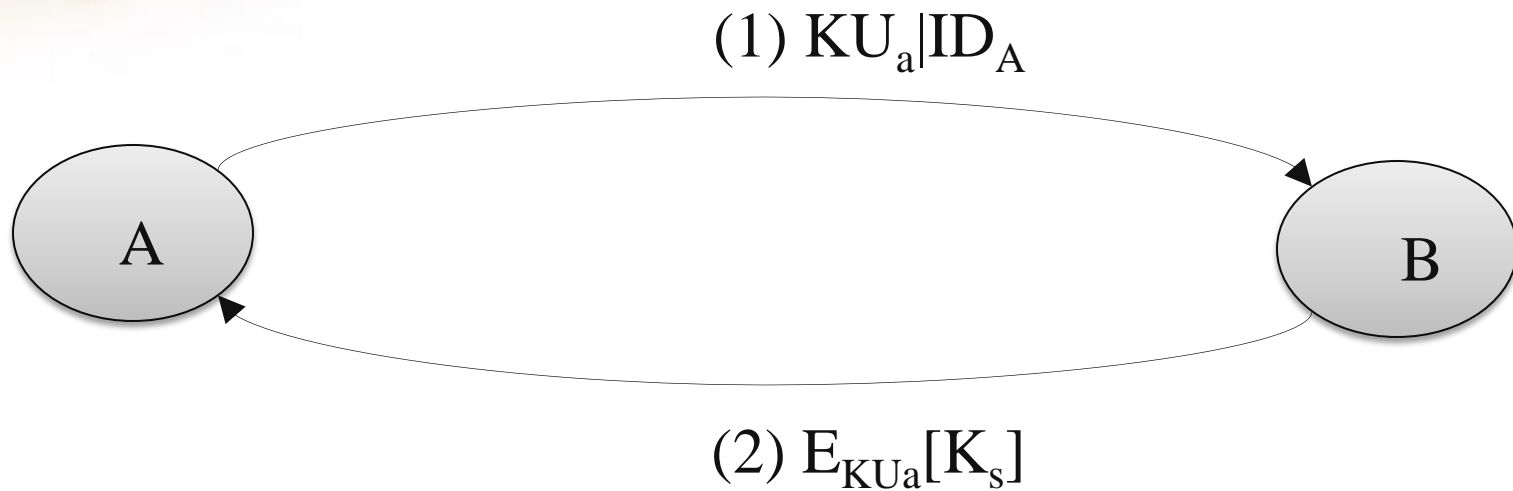
- When Alice wants Bob's public key:
 - Gets Bob's certificate (Bob or elsewhere).
 - Apply CA's public key to Bob's certificate, get Bob's public key



Public-Key Certificates

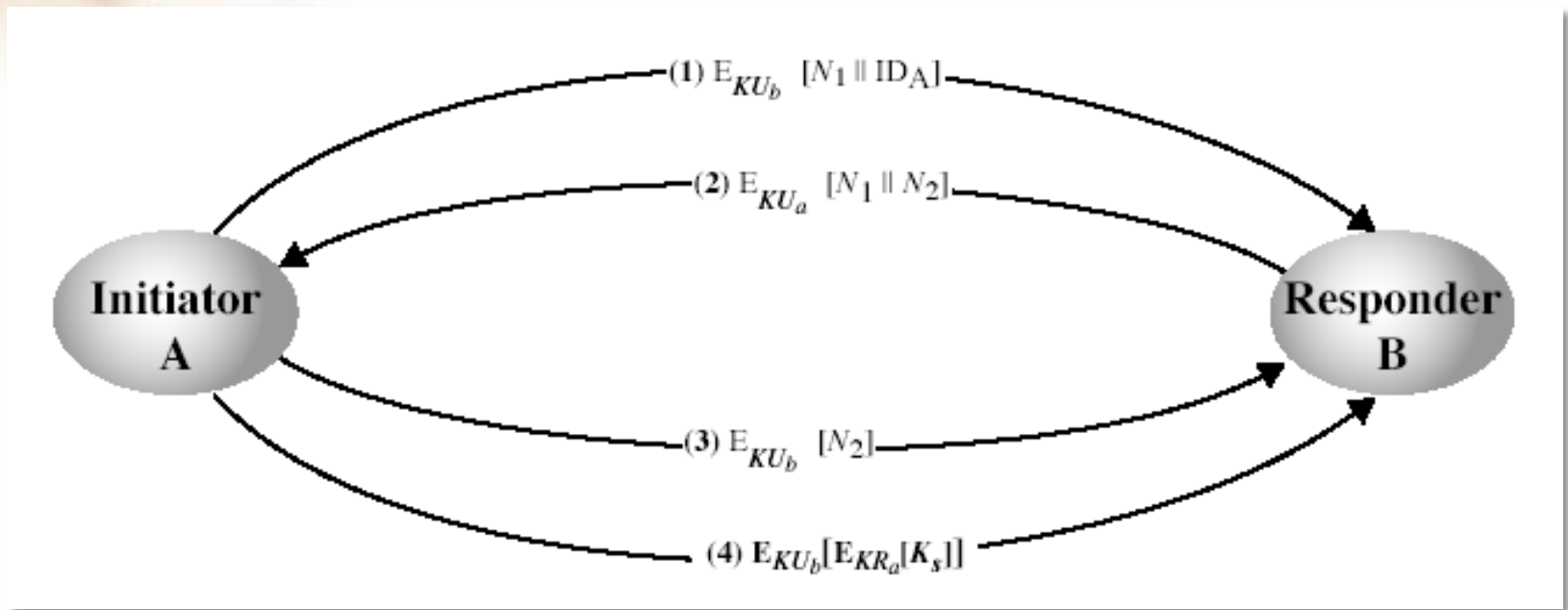


Simple Secret Key Distribution



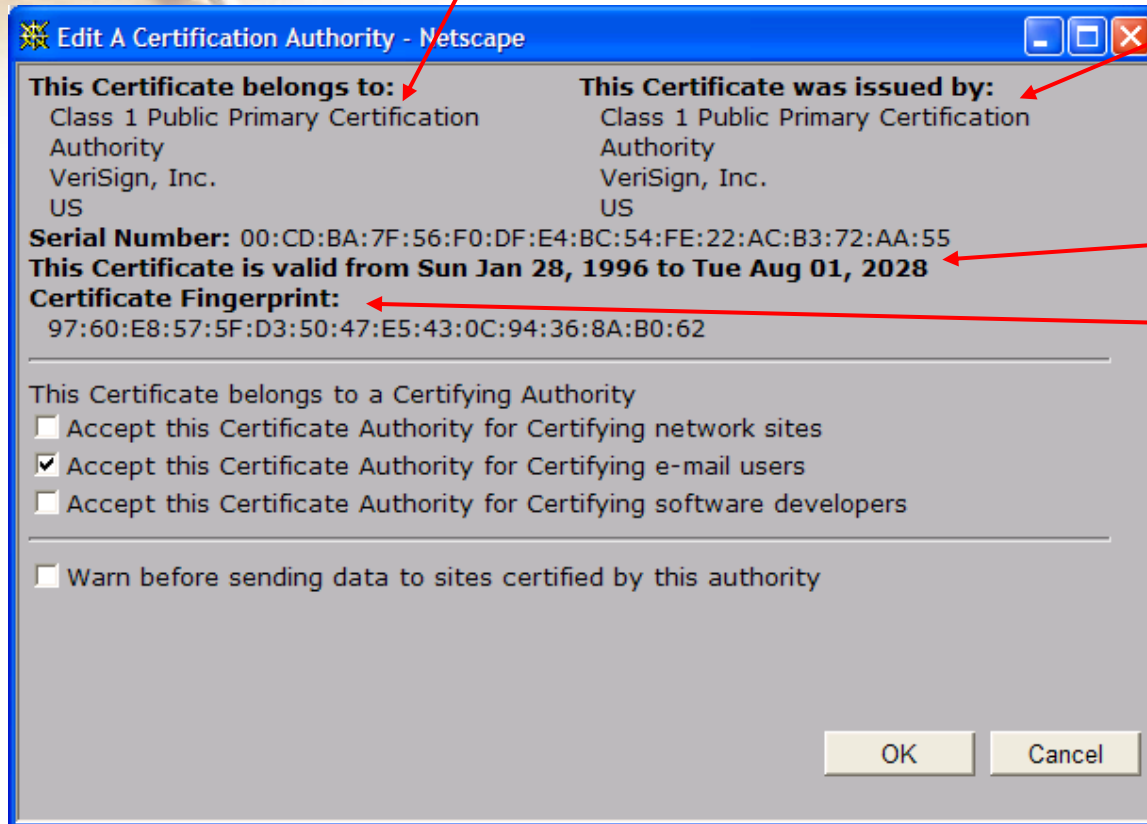
Needham Secret Key Distribution

- 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

A top-down view of a desk setup. In the upper left, a fountain pen with a black barrel and gold-colored accents lies diagonally. Next to it is a small, round, brown inkwell. A white sheet of paper is partially visible, with a ruler placed on it in the upper right. The ruler has markings in both inches and centimeters. The background is a light-colored, textured surface.

Q&A