CRYPTOGRAPHY AND INFORMATION SECURITY

IT 3203

LECTURE 24

By

Varsha Himthani

Assistant Professor (Selection Grade)

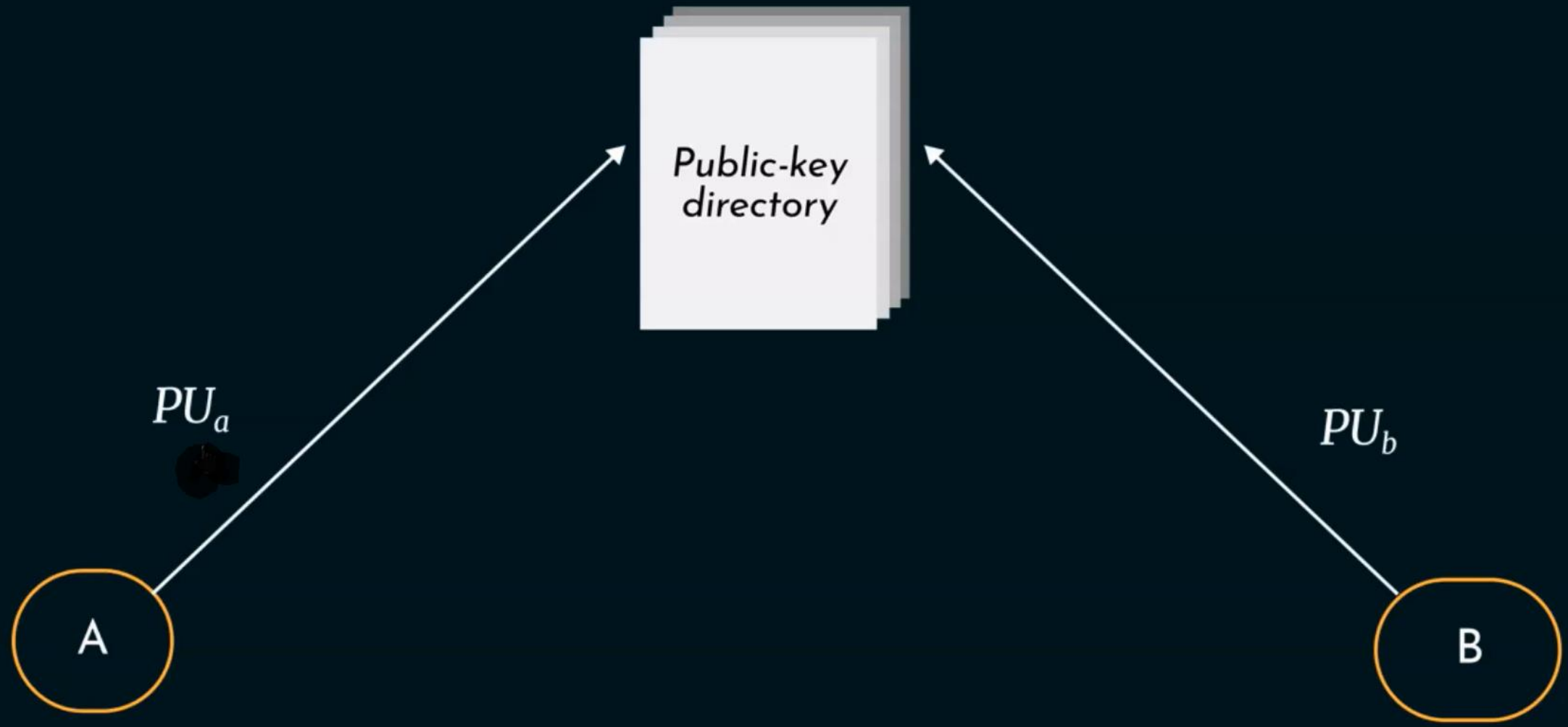
Manipal University Jaipur

Various Public Key Distribution Techniques

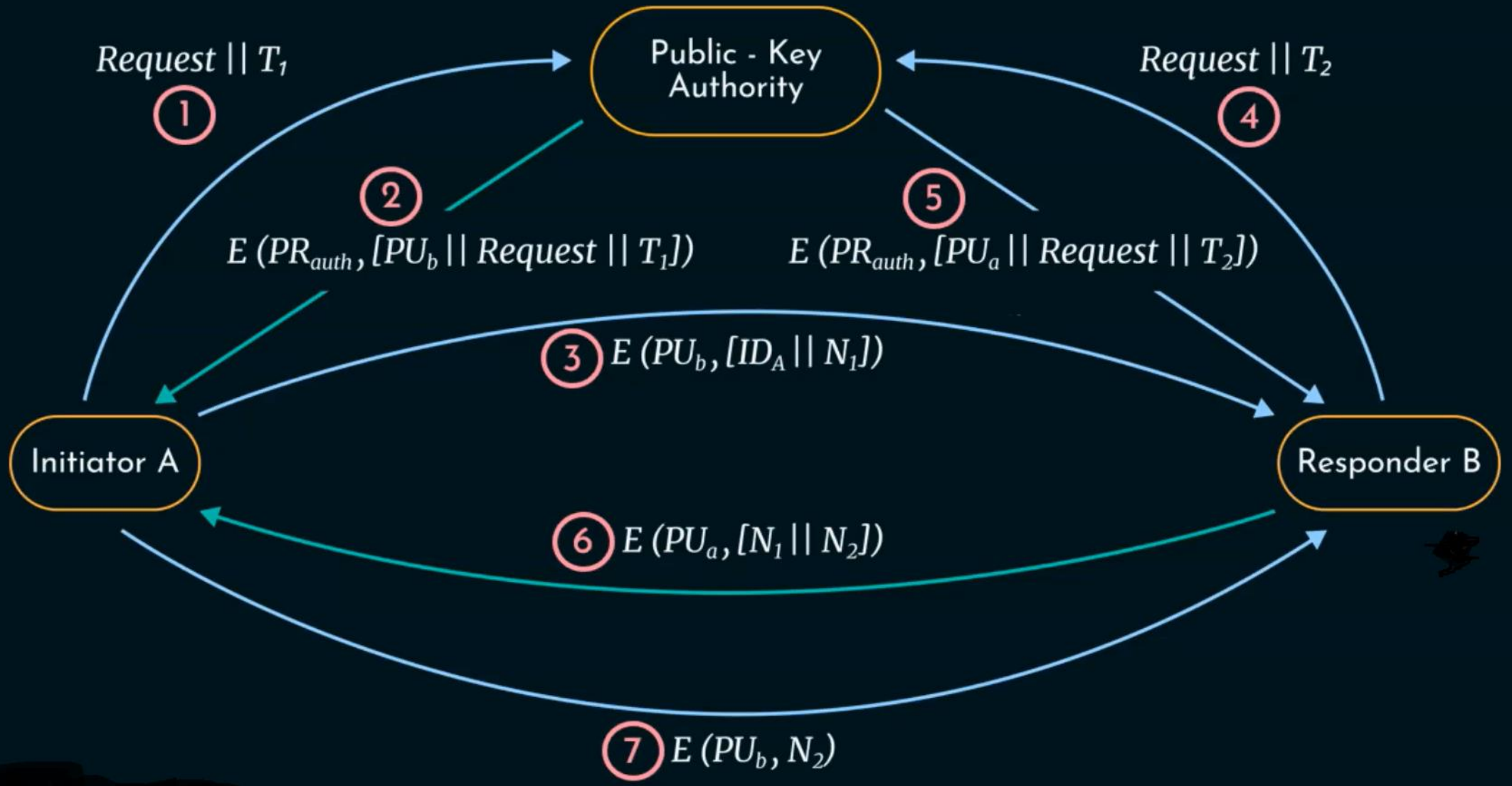
1. Public announcement
2. Publicly available directory
3. Public-key authority
4. Public-key certificates

1. Public Announcement

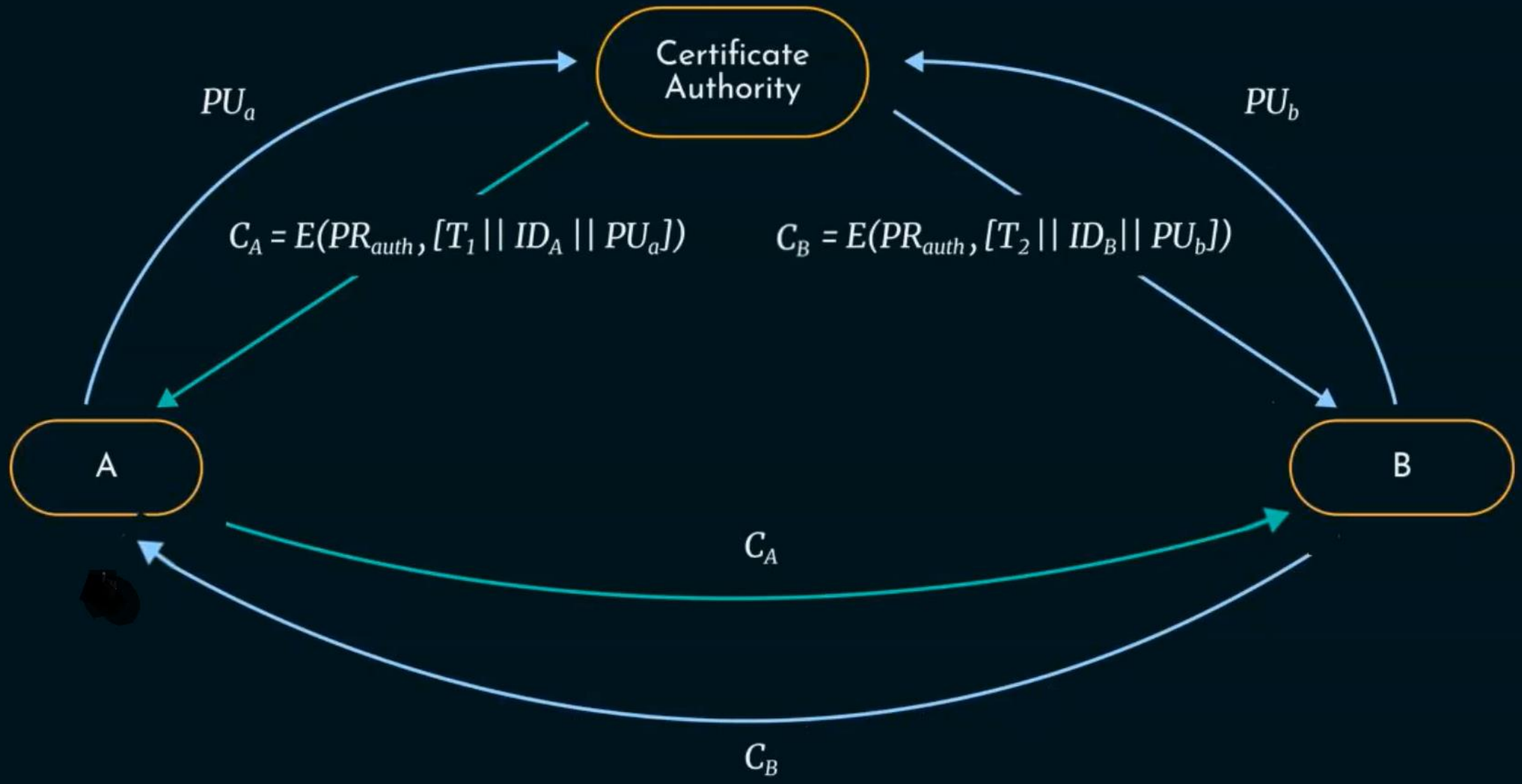
2. Publicly available directory



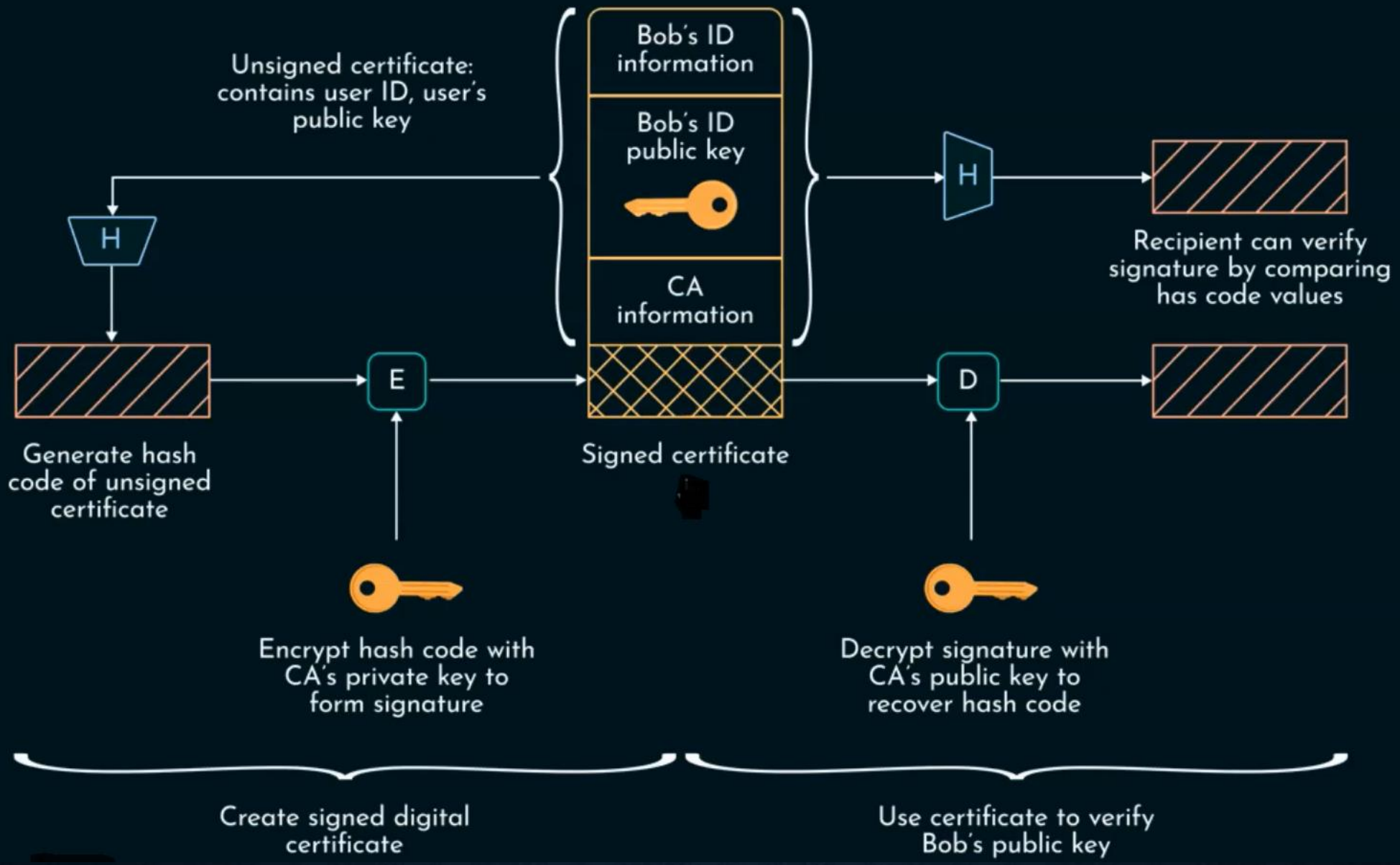
3. Public Key Authority



4. Public-Key Certificates



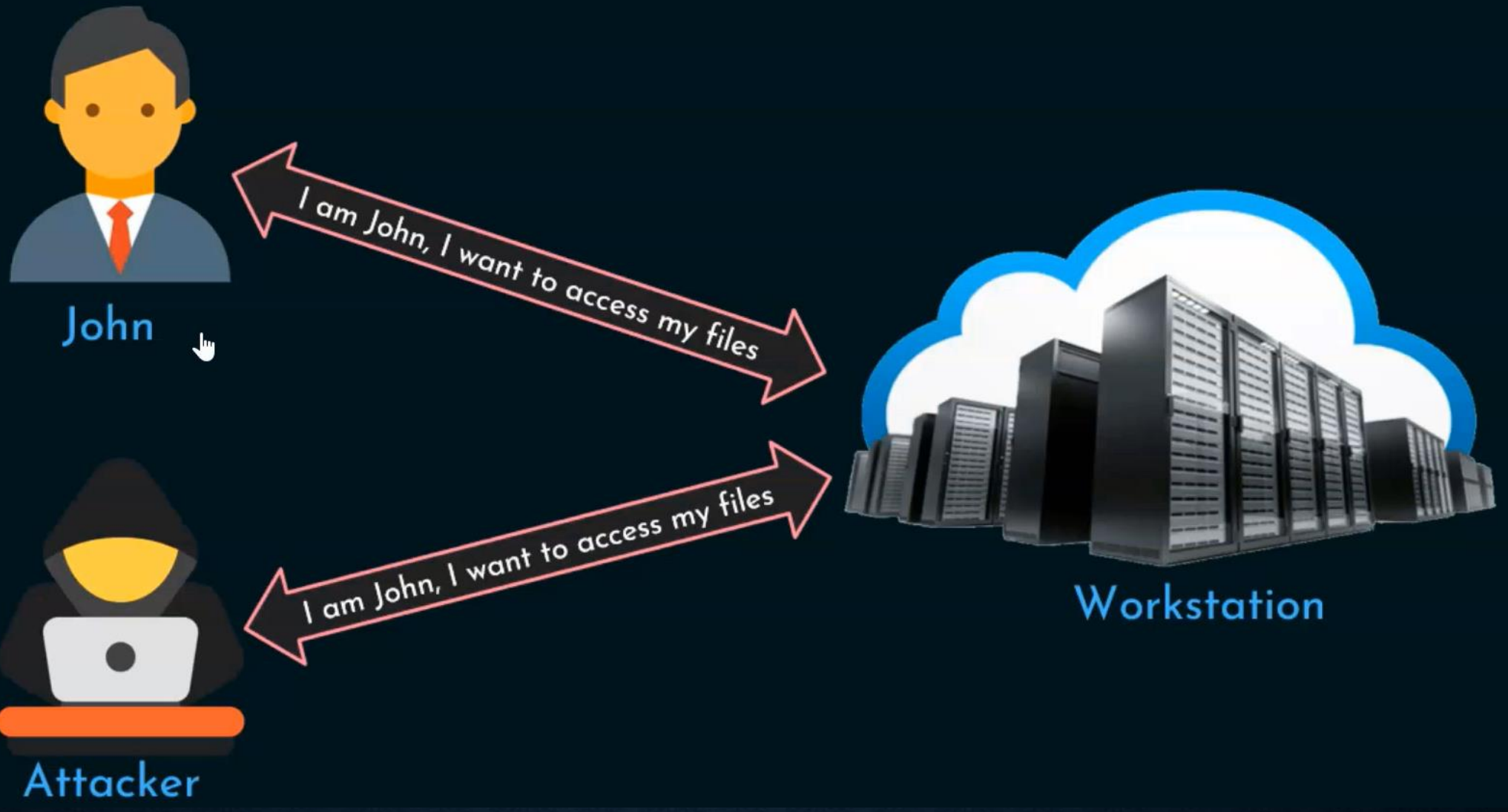
X.509 Certificates



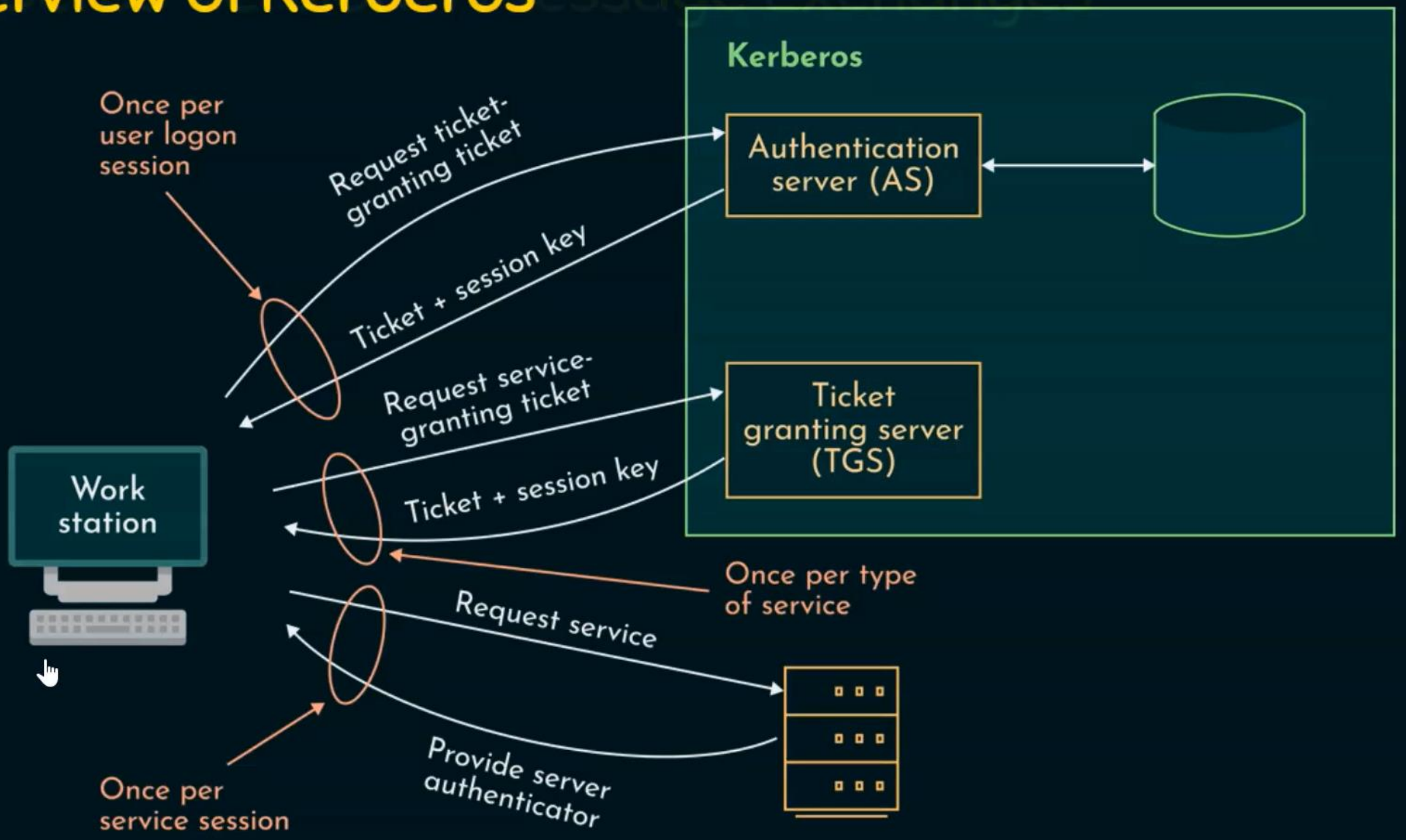
Kerberos

- ★ Kerberos is an authentication service.
- ★ Users at workstations can access services on servers distributed throughout the network.
- ★ Kerberos restrict access to authorized users and authenticate requests for service.
- ★ A workstation cannot be trusted to identify its users correctly to network services.

Why Kerberos?



Overview of Kerberos



Thank you