Information Security

CS3002

Lecture 11

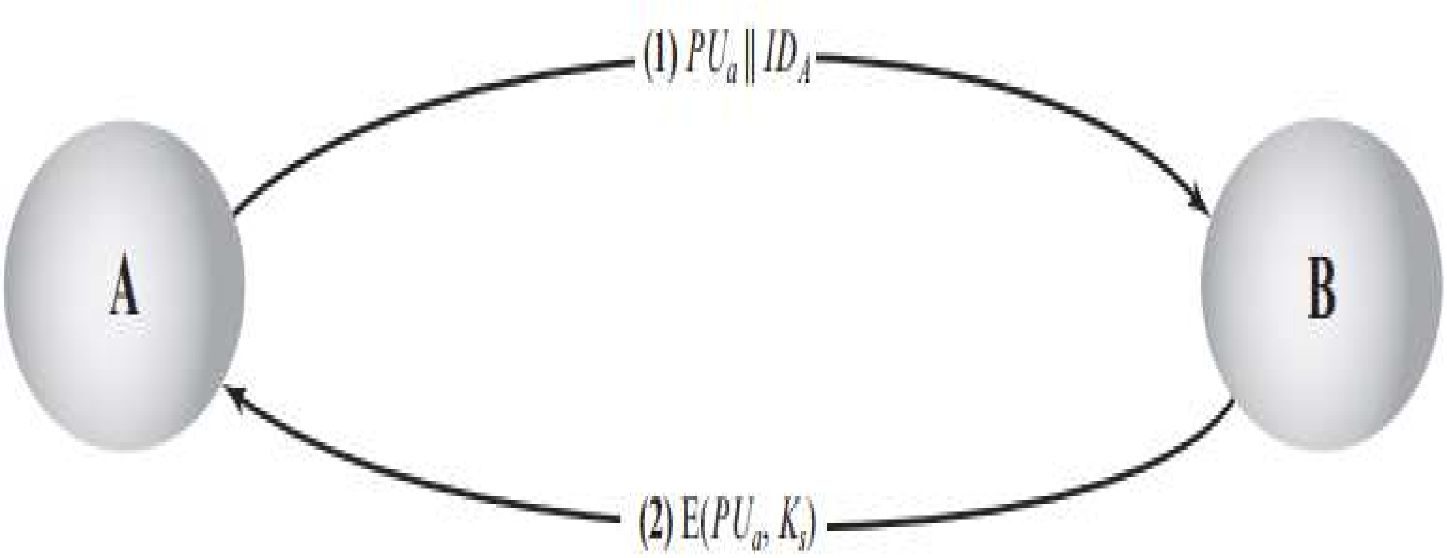
3rd October 2023

Dr. Rana Asif Rehman

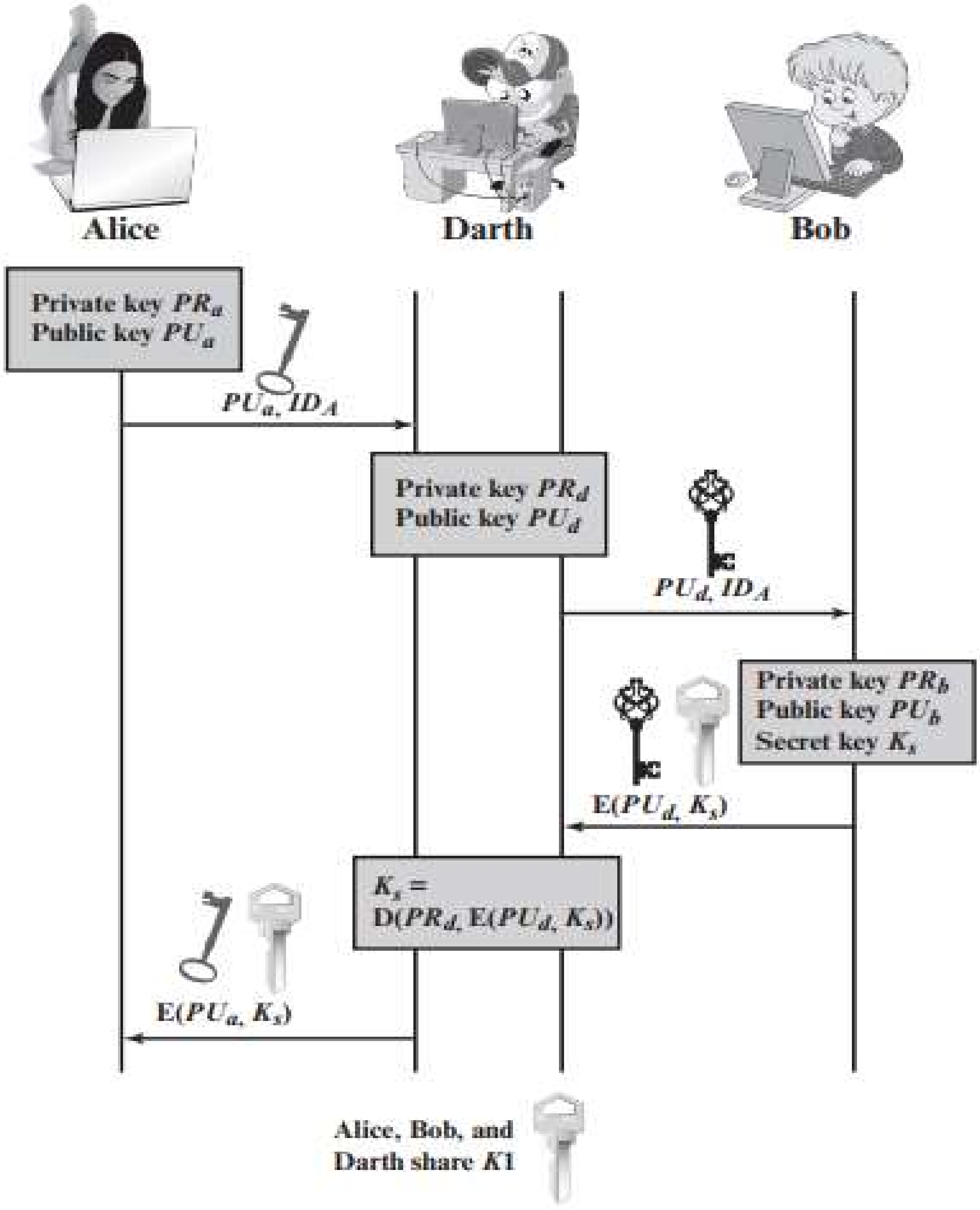
Email: r.asif@lhr.nu.edu.pk

PUBLIC KEY INFRASTRUCTURE (PKI)

Simple Secret Key Distribution



Man-in-the-Middle Attack



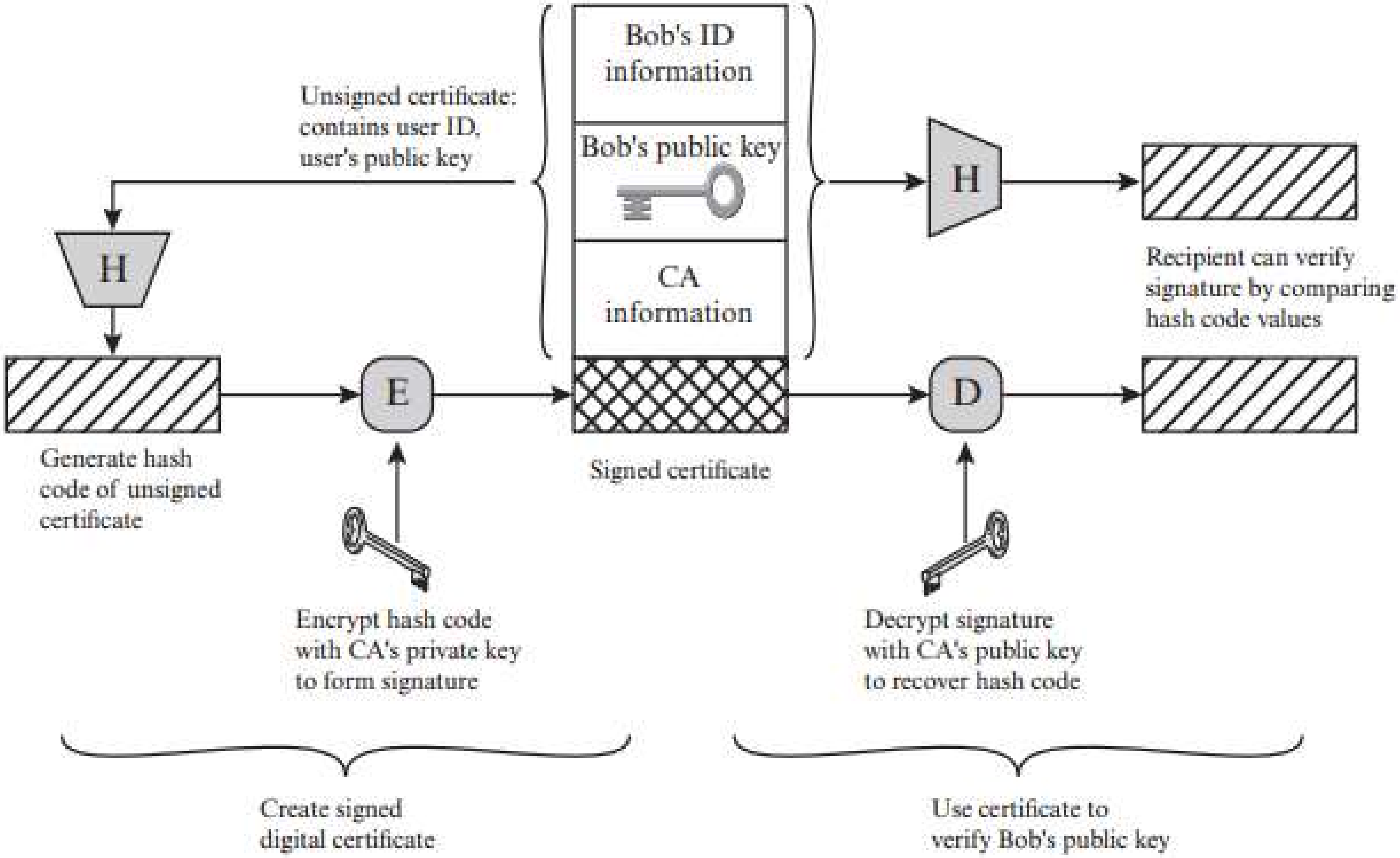
How we can make sure,
the Public Key belongs to legitimate user?

DIGITAL CERTIFICATE

Digital Certificate

- To decrypt the signature, the corresponding public key is required.
- A *digital certificate* is used to bind public keys to persons or other entities. If there were no certificates, the signature could easily be forged, as the recipient could not check if the public key belongs to the sender.
- The certificate itself is signed by a trusted third party, a *Certificate Authority* like VeriSign/ DigiCert Inc.

Digital Certificates



Bob's ID information
Bob's public key
CA information
Unsigned certificate: contains user ID, user's public key
H
H
E
D
Generate hash code of unsigned certificate
Signed certificate
Recipient can verify signature by comparing hash code values
Encrypt hash code with CA's private key to form signature
Decrypt signature with CA's public key to recover hash code
Create signed digital certificate
Use certificate to verify Bob's public key

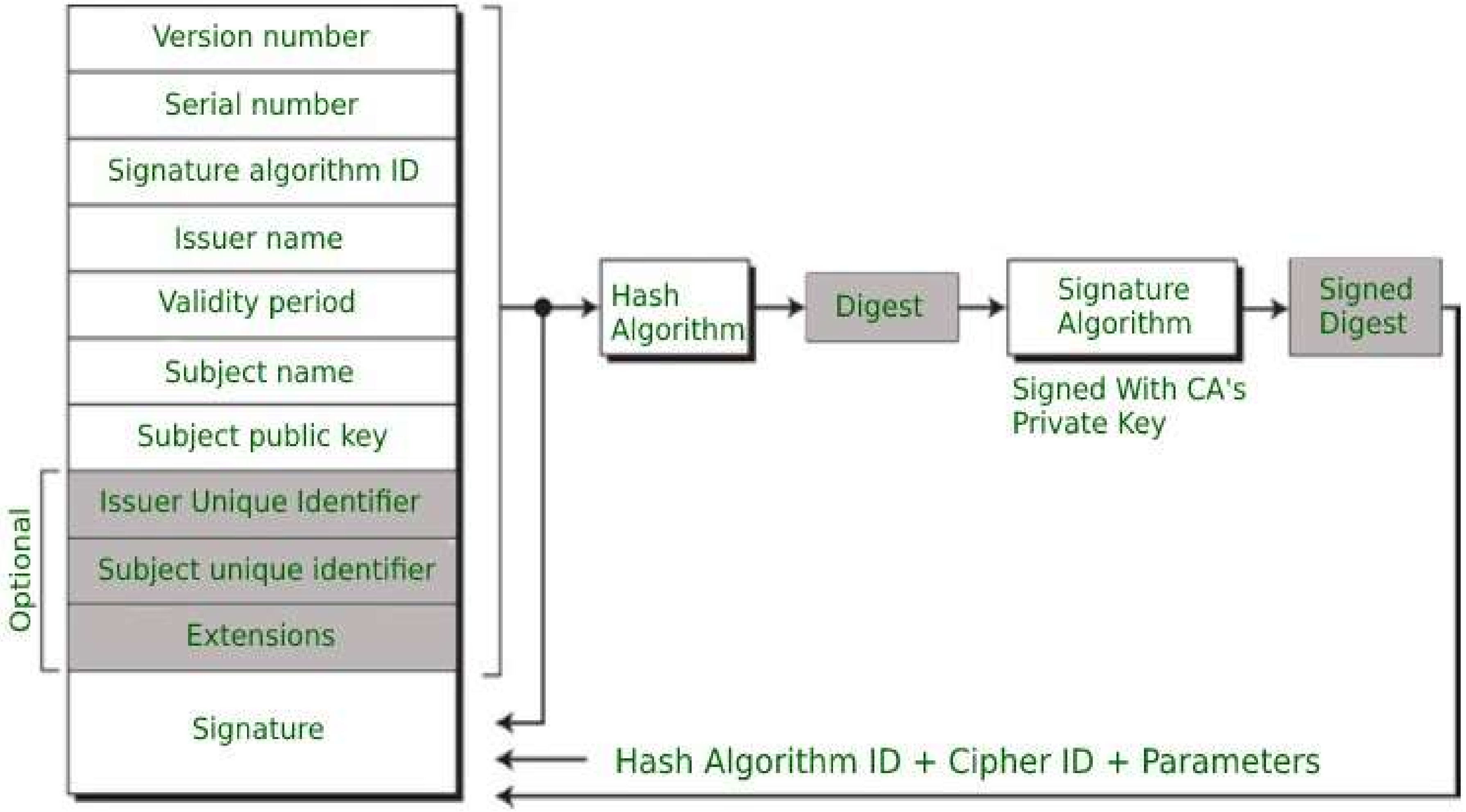
Elements of PKI

- Digital Certificate
  - X.509 standard
- Certificate Authorities (CA)
  - OpenSSL, Netscape, Verisign, Entrust, RSA Keon
- Registration Authority (RA)
- Public/Private Key Pairs - Key management
- Certificate Revocation Lists (CRL)

1. Digital Certificate

- Electronic file/data structure that contains the following information:
  - who issued the certificate: Comodo, Symantec etc
  - who the certificate is issued to
  - Public key of the owner
  - Validity period
  - Digital signature
- Issued by CA
- Helps in authentication
- Associate public key with an individual/company
- X.509 Standard

X.509 Standard



2. Certificate Authority

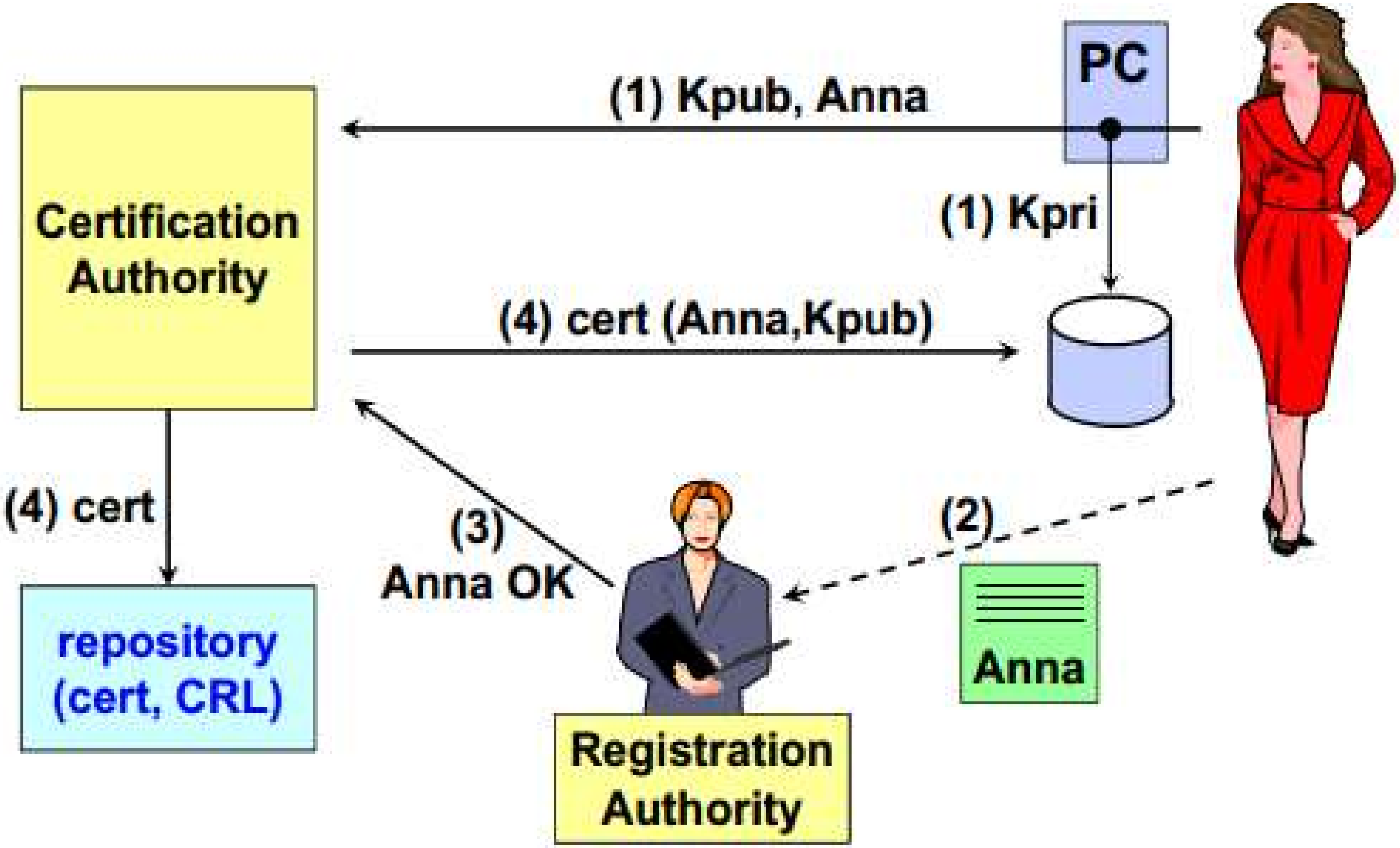
- A trusted third party - must be a secure server
- Signs and publishes X.509 Identity certificates
- Revokes certificates and publishes a Certification Revocation List (CRL)

- Many vendors
  - OpenSSL - open source, very simple
  - Netscape - free for limited number of certificates
  - Entrust - Can be run by enterprise or by Entrust
  - Verisign - Run by Verisign under contract to enterprise
  - RSA Security - Keon servers

3. Registration Authority

- An RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.
- You provide RA with information and money
- Verifies the information before the CA issues the certificate
- Does not sign the certificate
- Key pair maybe created by RA or you

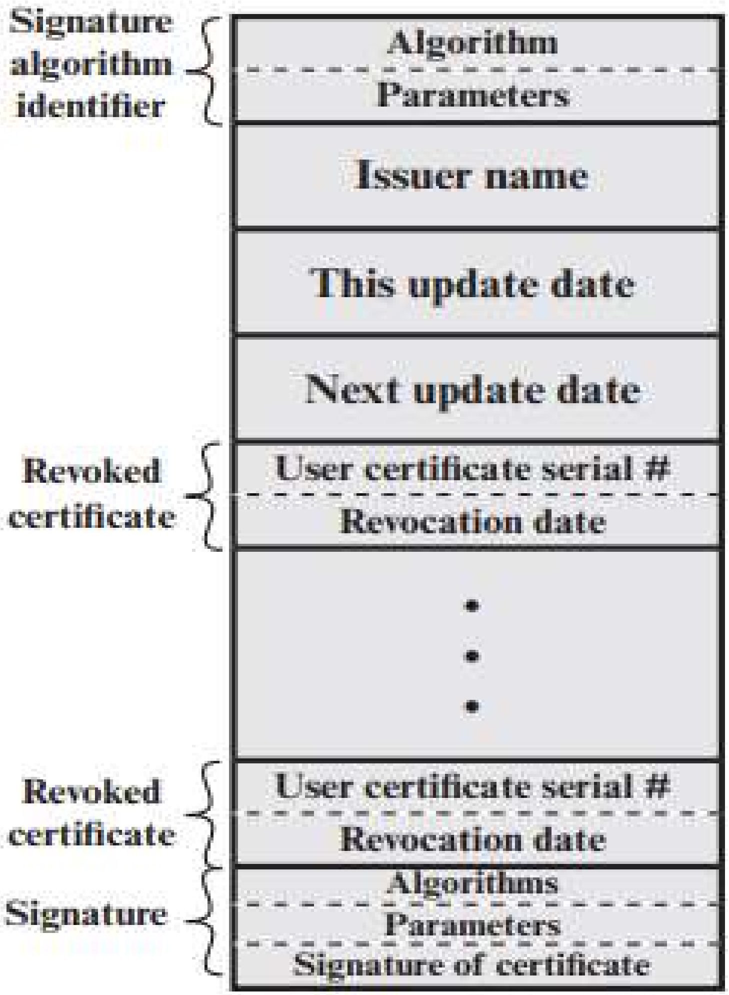
Certificate Issuance Process



4. Certificate Revocation List (CRL)

- List of revoked/cancelled certificates
- List published by CA frequently
- Reasons for revocation:
  - Certificate expiration
  - Certificate revocation (permanent)
    - Compromised private key
    - HR reasons
    - Company changed names, physical address, DNS
    - Any reason prior to expiration
  - Certificate suspended
    - "Certificate hold" as reason for revocation. E.g: resource on leave
- Owner can request the revocation of certificate

Certificate Revocation List

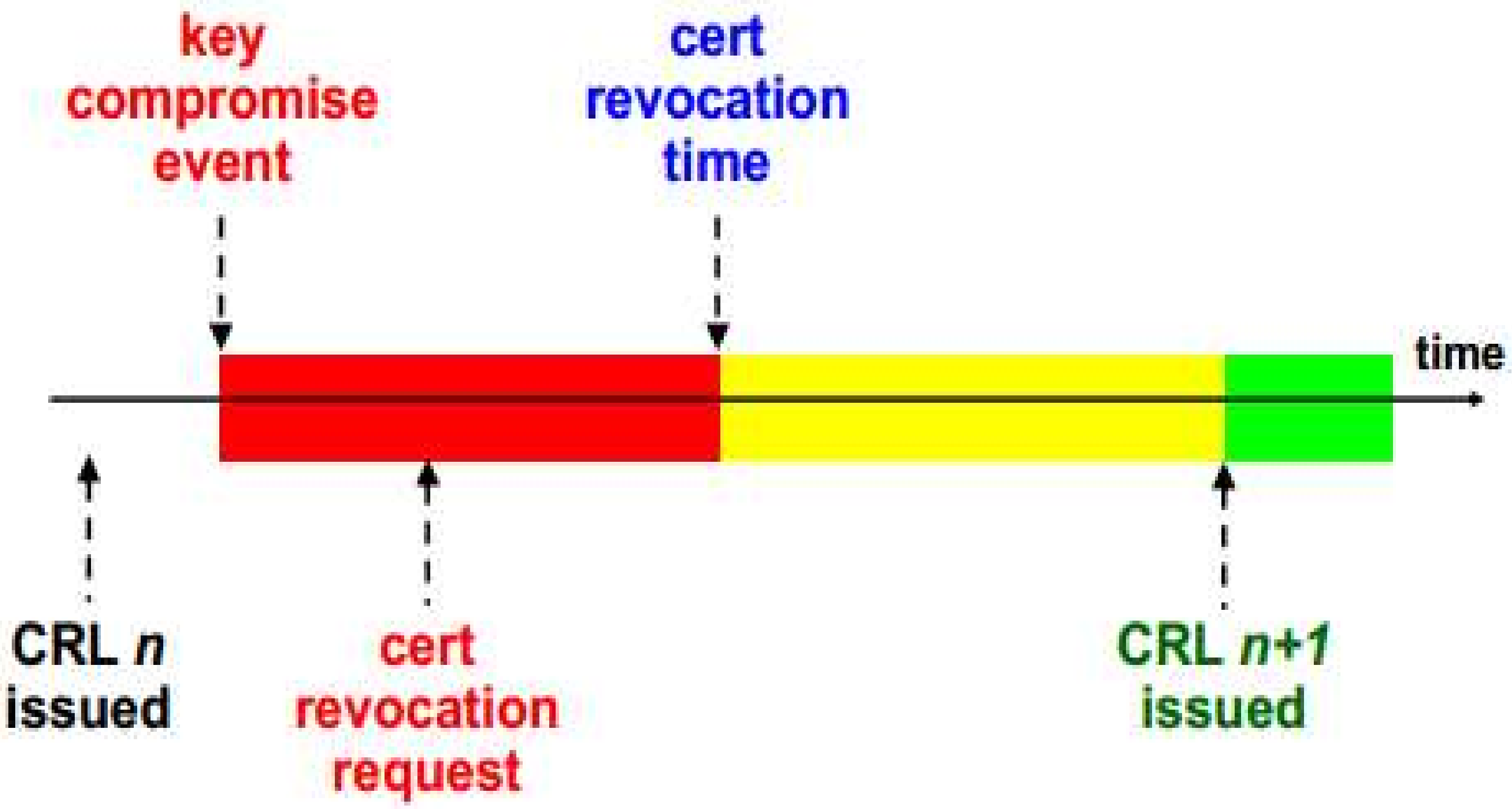


(b) Certificate revocation list

Certificate Revocation Lists

- Certificate revocation lists
  - Too much work on the client
  - Too much traffic on internet
    - Not used
- On-line Revocation Server (OLRS)
  - On-line certificate status protocol (OCSP)
  - Provides current information
  - Saves traffic on the internet
  - Allows chaining of OCSP responders

Certificate Revocation Timeline


key compromise event
cert revocation time
time
CRL *n* issued
cert revocation request
CRL *n*+1 issued