Dr. Ammar Haider
Assistant Professor
School of Computing

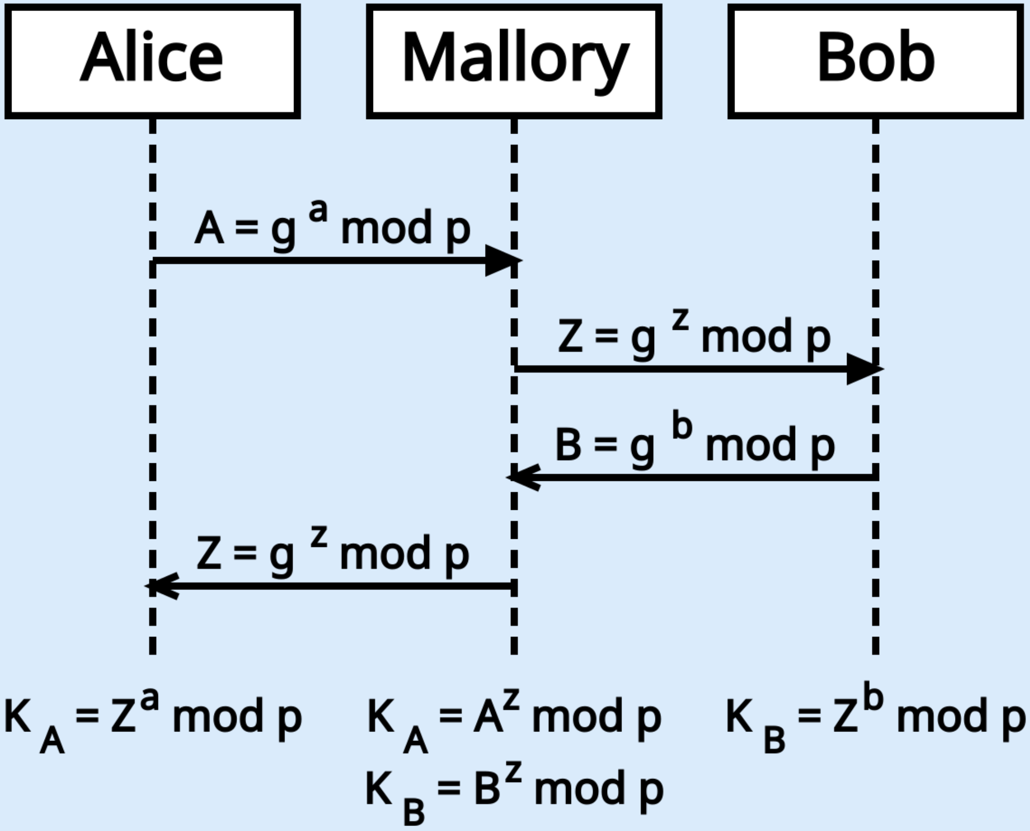
CS3002 Information Security

Public Key Infrastructure

Reference: Stallings SPP chap 23

MITM against Diffie-Hellman

- Vulnerable to main in the middle attack



https://commons.wikimedia.org/wiki/File:Man-in-the-middle_attack_of_Diffie-Hellman_key_agreement.svg

MITM in PKC

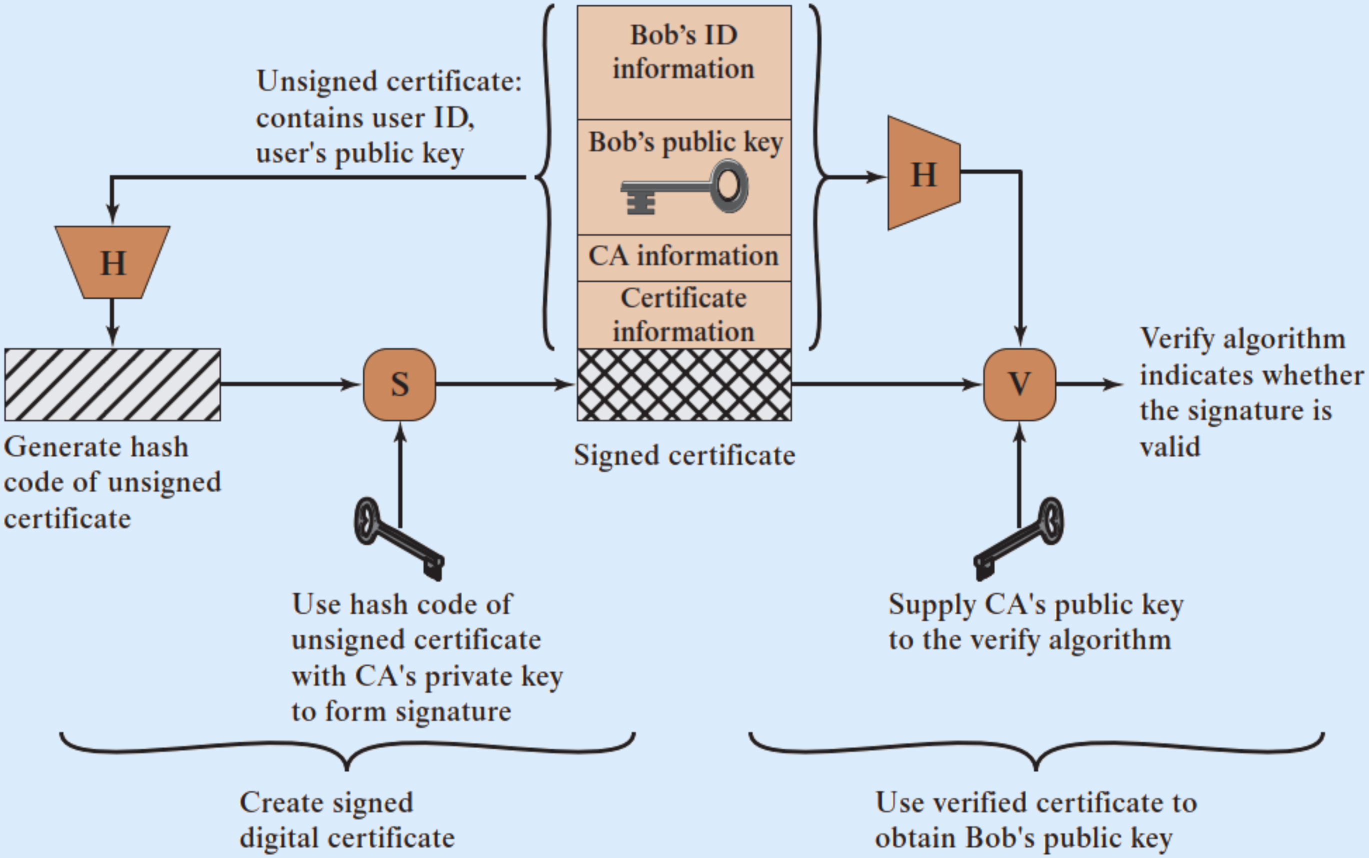
- MITM is not unique to Diffie-Hellman key exchange
- All kinds of asymmetric crypto (RSA, digital signatures, digital envelope etc.) is vulnerable to such attacks
- Whenever public keys are exchanged over an insecure channel, we can not blindly trust the received public key.

Public-Key Certificates

- To prevent MITM against PKC, digital certificates are used.
- A certificate associates a public key with an individual/company
- Digital certificate is just a piece of data
  - A public key and ID of key owner, whole block signed by a **trusted third party**
- Issued by a Certificate Authority (CA)
- Helps in authentication

Public-Key Certificate

- Signing a certificate by CA


Unsigned certificate:
contains user ID,
user's public key
Bob's ID information
Bob's public key
CA information
Certificate information
H
H
Generate hash code of unsigned certificate
S
Signed certificate
V
Verify algorithm indicates whether the signature is valid
Use hash code of unsigned certificate with CA's private key to form signature
Supply CA's public key to the verify algorithm
Create signed digital certificate
Use verified certificate to obtain Bob's public key

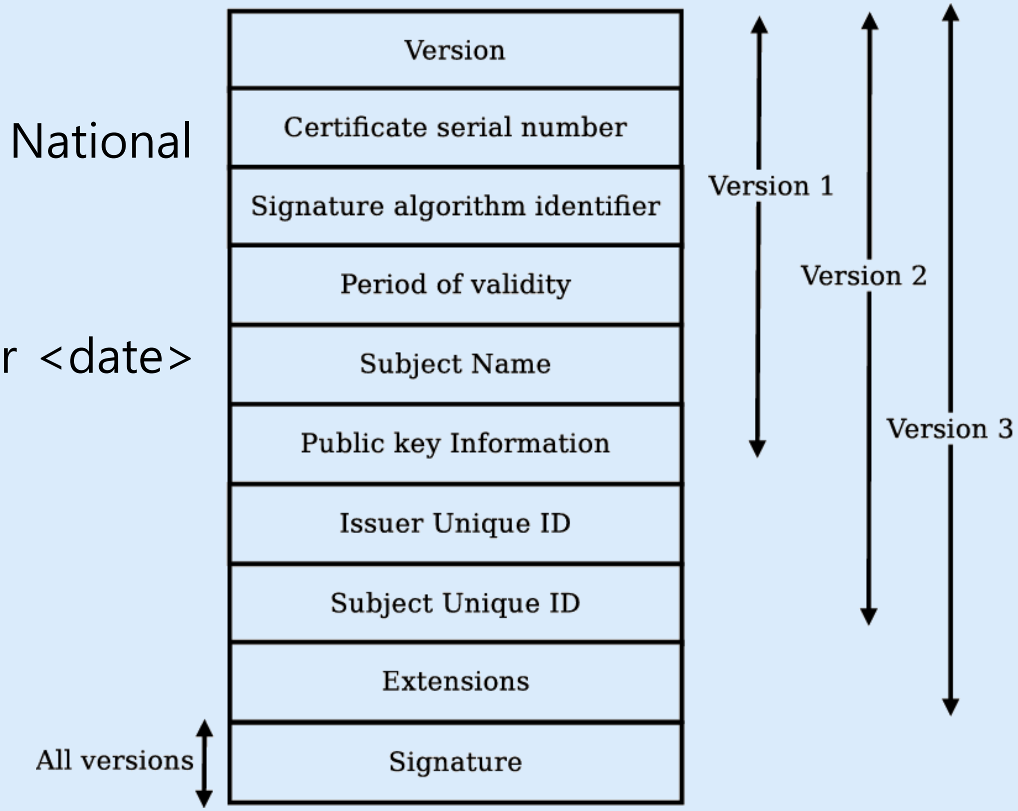
Public-Key Certificate

- Contains the following information:
  - who issued the certificate: Comodo, Symantec etc.
  - who the certificate is issued to (aka subject)
  - public key of the owner
  - validity period
  - digital signature by CA

- X.509: International Standard for the format of a public-key certificate

X.509 Identity Certificates

- Distinguished Name of user
  - C=US, O=Lawrence Berkeley National Laboratory, OU=DSD, CN=Mary R. Thompson
- DN of Issuer
  - C=US, O=Lawrence Berkeley National Laboratory, CN=LBNL-CA
- Validity dates:
  - Not before <date>, Not after <date>
- User's public key
- V3 extensions
- CA signatures
- Defined in **ASN.1 notation**
  - language independent



Version

Certificate serial number

Signature algorithm identifier

Period of validity

Subject Name

Public key Information

Issuer Unique ID

Subject Unique ID

Extensions

Signature

Version 1

Version 2

Version 3

All versions

Public Key Infrastructure (PKI)

- PKI is the set of hardware, software, and procedures needed to create, store, distribute and revoke digital certificates

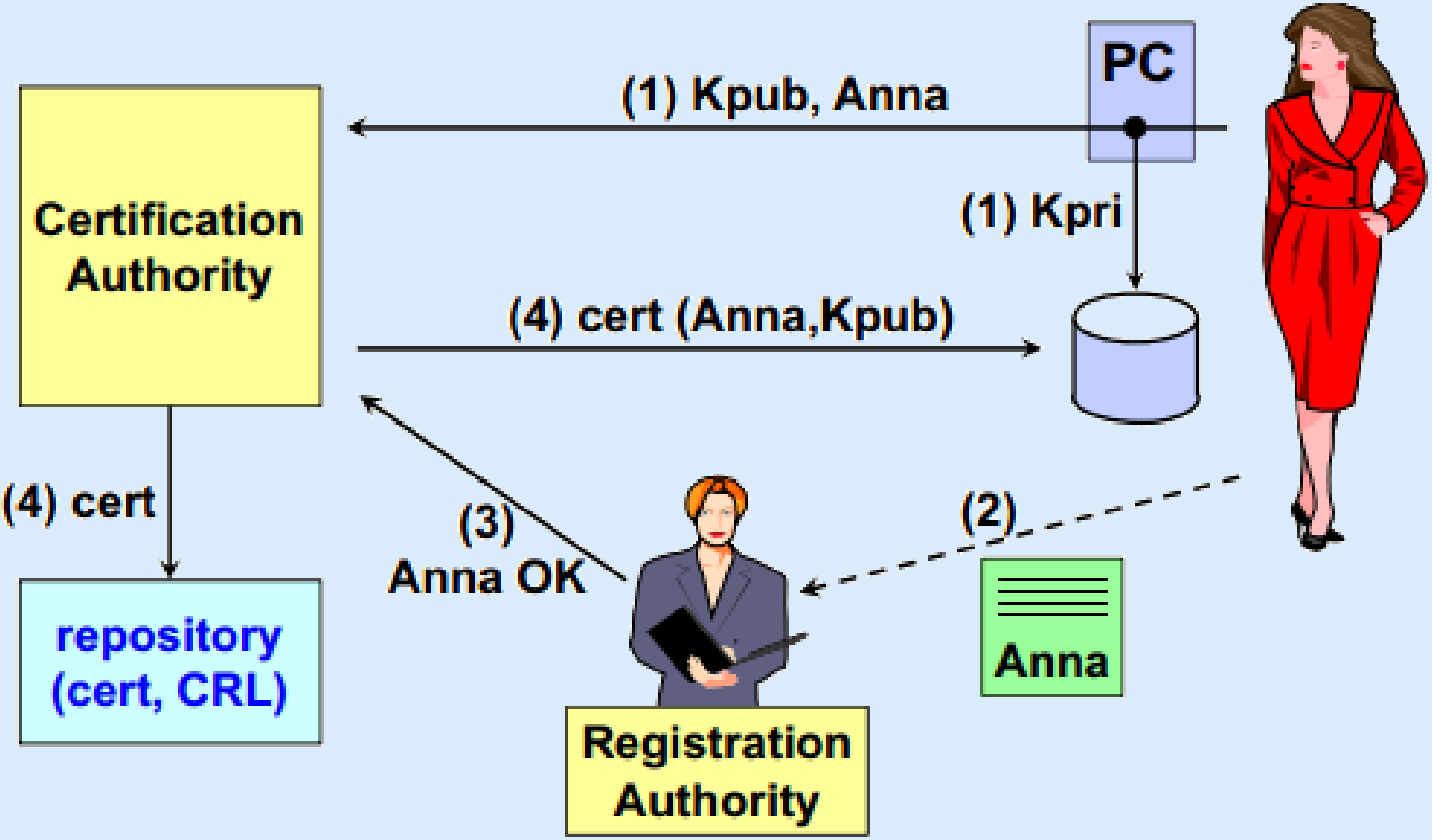
Elements of PKI

- X.509 Certificates
- Certificate Authorities (CA)
- Registration Authorities (RA)
- Public/Private Key Pairs
- Certificate Revocation Lists

Certificate Authority

- A third party. Must be a secure server
  - Signs and publishes X.509 Identity certificates
  - Revokes certificates and publishes a Certification Revocation List (CRL)
- Anyone can sign certificates (act as CA), but their certificates will have no value unless the users **trust** them.
- Trusting means the certificate inspector (receiver) already knows about this CA, and has pre-saved the CA's public key in its records.
  - so that they can verify CA's signatures

Certificate Issuance Process



Registration Authority

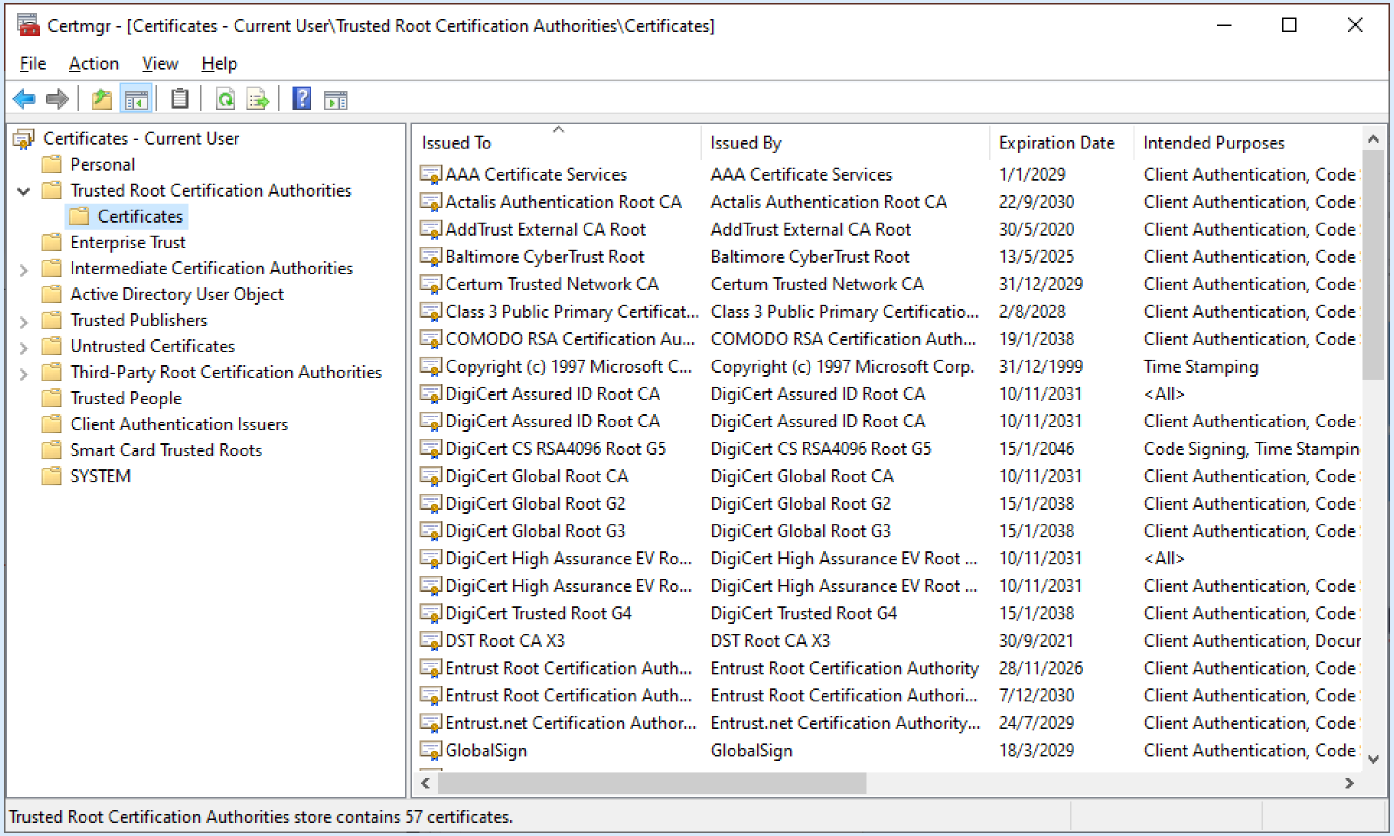
- An RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.
- You provide RA with information and fees
- RA verifies the information before the CA issues the certificate
- RA does not sign the certificate
- Your key pair maybe created by RA or yourself

Trusted CAs

- All operating systems come with a pre-installed list of trusted CAs.
- There are several vendors
  - IdenTrust
  - DigiCert
  - Sectigo (Comodo)
  - Lets Encrypt: issues free certificates
- OpenSSL is a free and open source library. Can be used to setup your own CA server.

Trusted CAs – Check your PC

Windows: launch Certmgr.msc



Certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

- Certificates - Current User
  - Personal
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Client Authentication Issuers
  - Smart Card Trusted Roots
  - SYSTEM

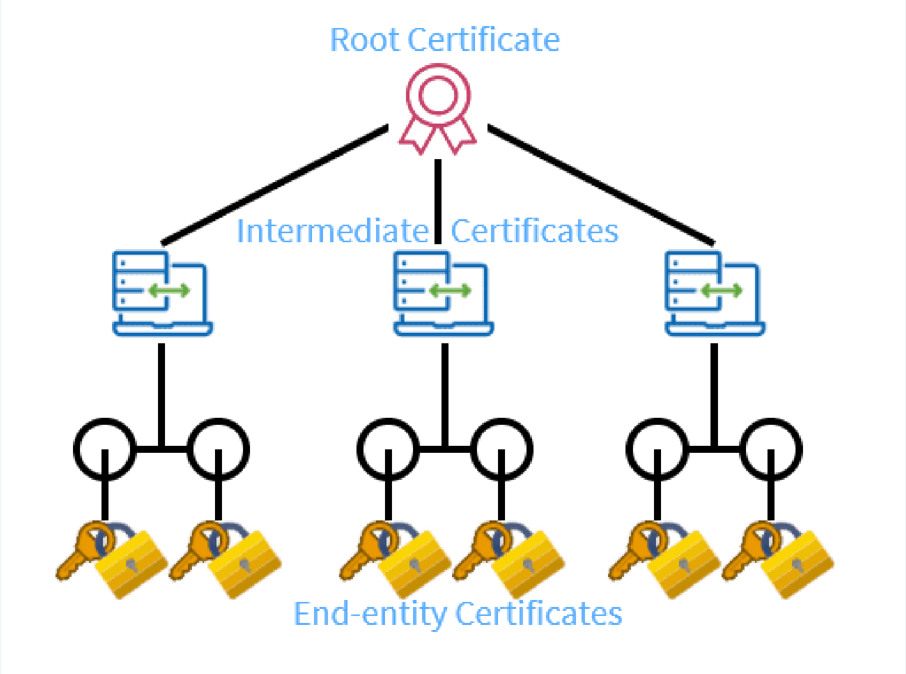
Issued To	Issued By	Expiration Date	Intended Purposes
AAA Certificate Services	AAA Certificate Services	1/1/2029	Client Authentication, Code
Actalis Authentication Root CA	Actalis Authentication Root CA	22/9/2030	Client Authentication, Code
AddTrust External CA Root	AddTrust External CA Root	30/5/2020	Client Authentication, Code
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/5/2025	Client Authentication, Code
Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029	Client Authentication, Code
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	2/8/2028	Client Authentication, Code
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	19/1/2038	Client Authentication, Code
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Time Stamping
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	<All>
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	Client Authentication, Code
DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	15/1/2046	Code Signing, Time Stampin
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Client Authentication, Code
DigiCert Global Root G2	DigiCert Global Root G2	15/1/2038	Client Authentication, Code
DigiCert Global Root G3	DigiCert Global Root G3	15/1/2038	Client Authentication, Code
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10/11/2031	<All>
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10/11/2031	Client Authentication, Code
DigiCert Trusted Root G4	DigiCert Trusted Root G4	15/1/2038	Client Authentication, Code
DST Root CA X3	DST Root CA X3	30/9/2021	Client Authentication, Docur
Entrust Root Certification Auth...	Entrust Root Certification Authority	28/11/2026	Client Authentication, Code
Entrust Root Certification Auth...	Entrust Root Certification Authori...	7/12/2030	Client Authentication, Code
Entrust.net Certification Author...	Entrust.net Certification Authority...	24/7/2029	Client Authentication, Code
GlobalSign	GlobalSign	18/3/2029	Client Authentication, Code

Trusted Root Certification Authorities store contains 57 certificates.

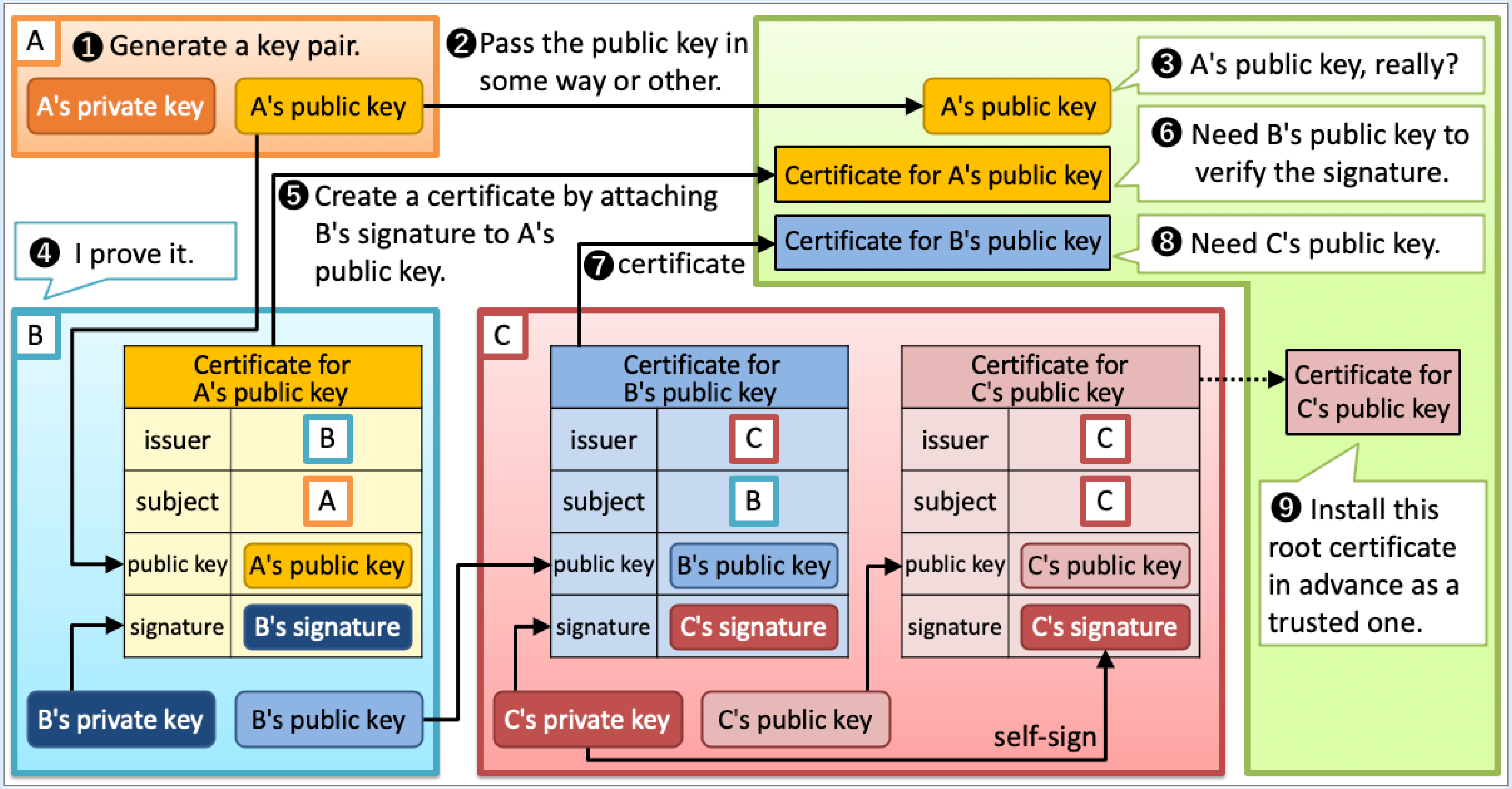
All trusted authorities are present in system’s **certificates store**, aka **trust store**. This is a highly security-critical component of system. What would happen if attackers could manipulate the certificate store?

Chain of Trust

- Instead of getting a certificate directly from a root CA, it is more practical to get one from an intermediate CA which already has a certificate from root CA.
- This hierarchy can go many levels deep



Chain of Trust

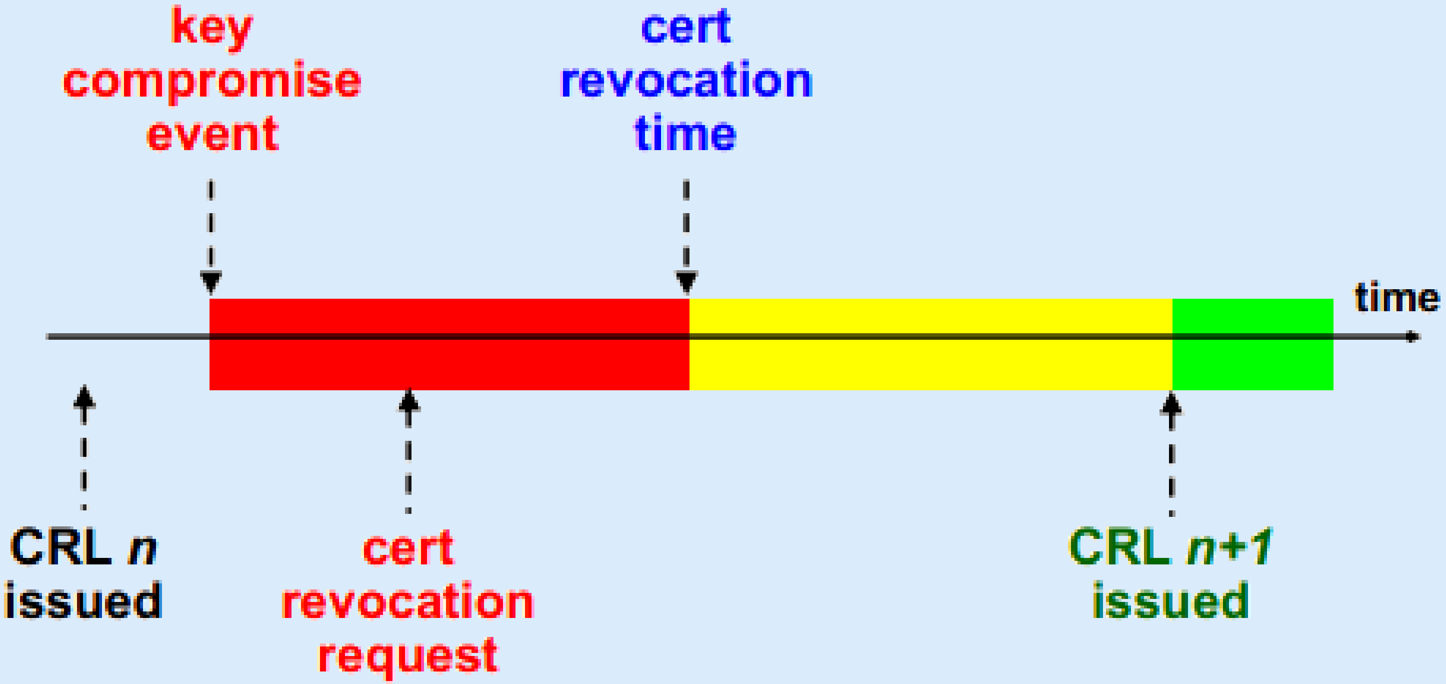

A
❶ Generate a key pair.
A's private key
A's public key
❷ Pass the public key in some way or other.
A's public key
❸ A's public key, really?
Certificate for A's public key
❻ Need B's public key to verify the signature.
Certificate for B's public key
❽ Need C's public key.
❺ Create a certificate by attaching B's signature to A's public key.
❹ I prove it.
❼ certificate
B
Certificate for A's public key
issuer
B
subject
A
public key
A's public key
signature
B's signature
B's private key
B's public key
C
Certificate for B's public key
issuer
C
subject
B
public key
B's public key
signature
C's signature
Certificate for C's public key
issuer
C
subject
C
public key
C's public key
signature
C's signature
C's private key
C's public key
self-sign
Certificate for C's public key
❾ Install this root certificate in advance as a trusted one.

https://darutk.medium.com/illustrated-x-509-certificate-84aece2c5c2e

Certificate Revocation List (CRL)

- Certificates may need to be revoked (prior to expiration) for several reasons
- Subject may request revocation because
  - Subject's private key was compromised
  - HR reasons, e.g. employee left the company
  - Temporary revocation (on "hold") e.g. resource on leave
  - Subject changed names, physical address, DNS
- CA themselves may decide to revoke because
  - Subject provided false information
  - CA's private key was compromised!
- CAs maintain lists of revoked/cancelled certificates. These lists are published by CA frequently

Certificate Revocation Timeline



CRL Drawbacks

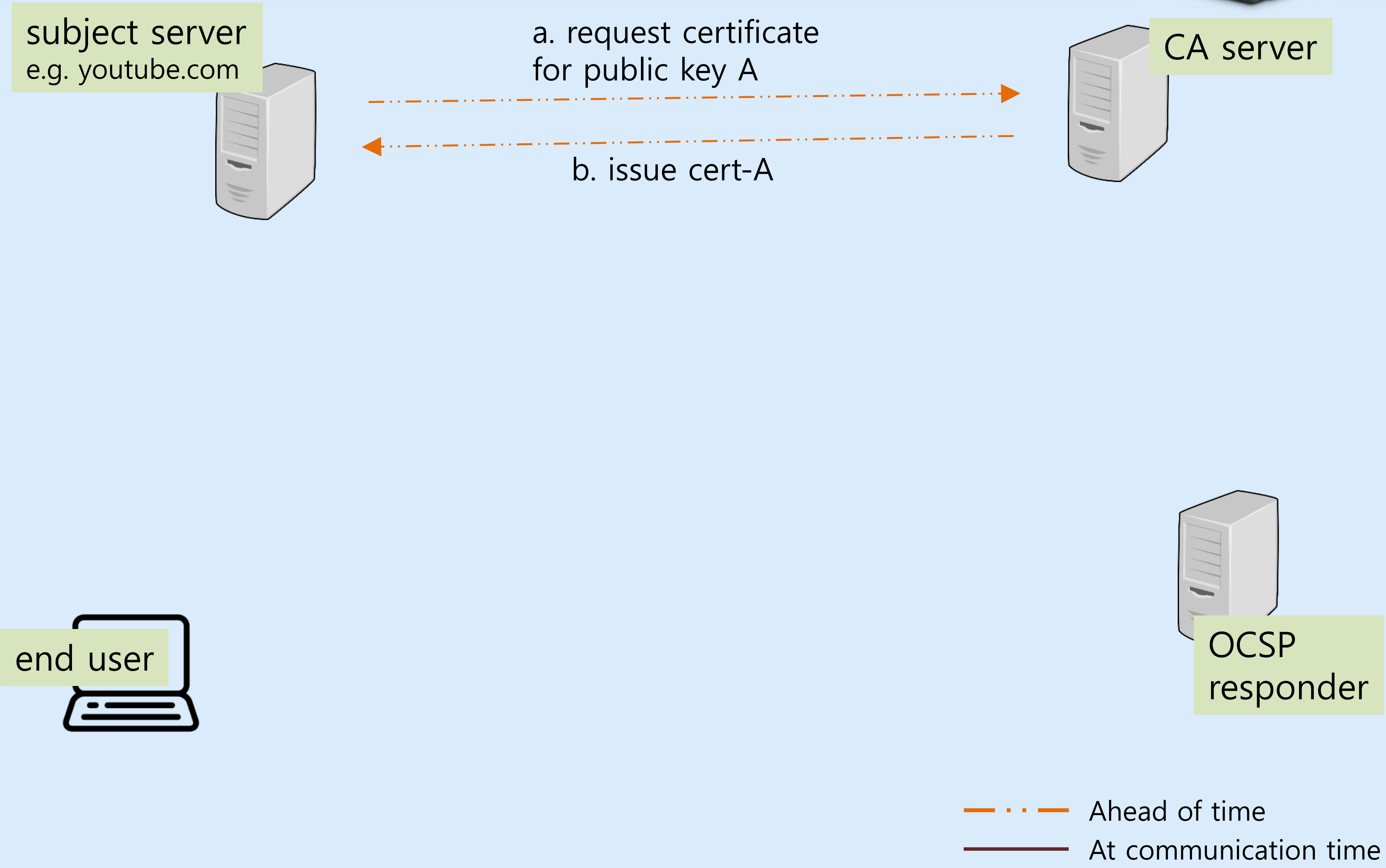
- Certificate revocation lists
  - Too much work on the client
  - Too much traffic on internet
    - Not used

- Alternate: Online Certificate Status Protocol
  - CA's always-online revocation server
  - Provides current information
  - Saves traffic on the internet

OCSP

- Online certificate status protocol
- IETF-PKIX standard to verify online if a certificate is valid:
  - good/verified
  - revoked
    - revocation time
    - revocation reason
  - unknown
- response must be signed by the responder server (not by the CA!)
  - the OCSP server certificate cannot be verified with OCSP itself!

OCSP Usage



subject server
e.g. youtube.com

a. request certificate
for public key A

b. issue cert-A

CA server

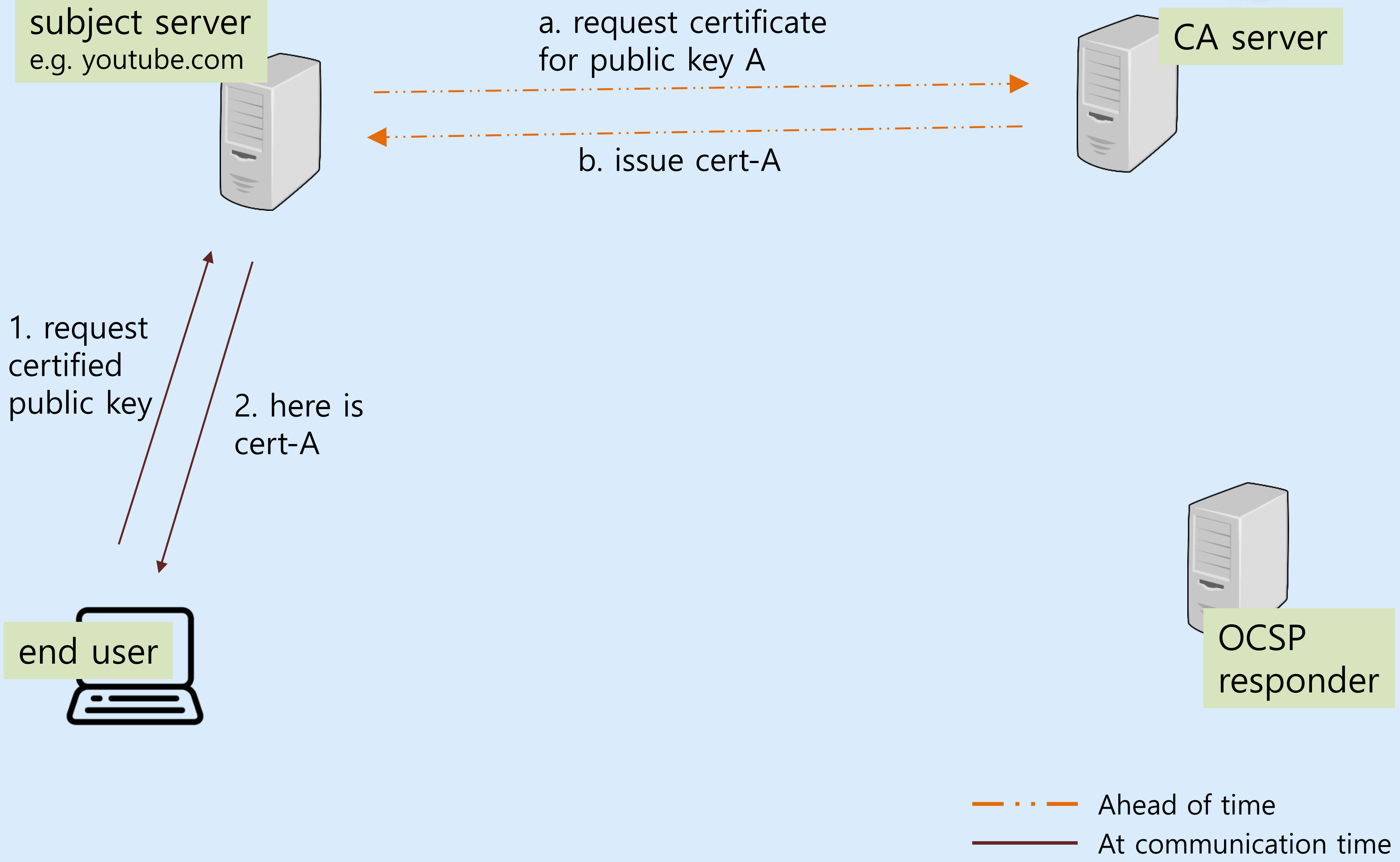
end user

OCSP
responder

▬ · · ▬ Ahead of time

▬▬ At communication time

OCSP Usage



subject server
e.g. youtube.com

a. request certificate
for public key A

CA server

b. issue cert-A

1. request
certified
public key

2. here is
cert-A

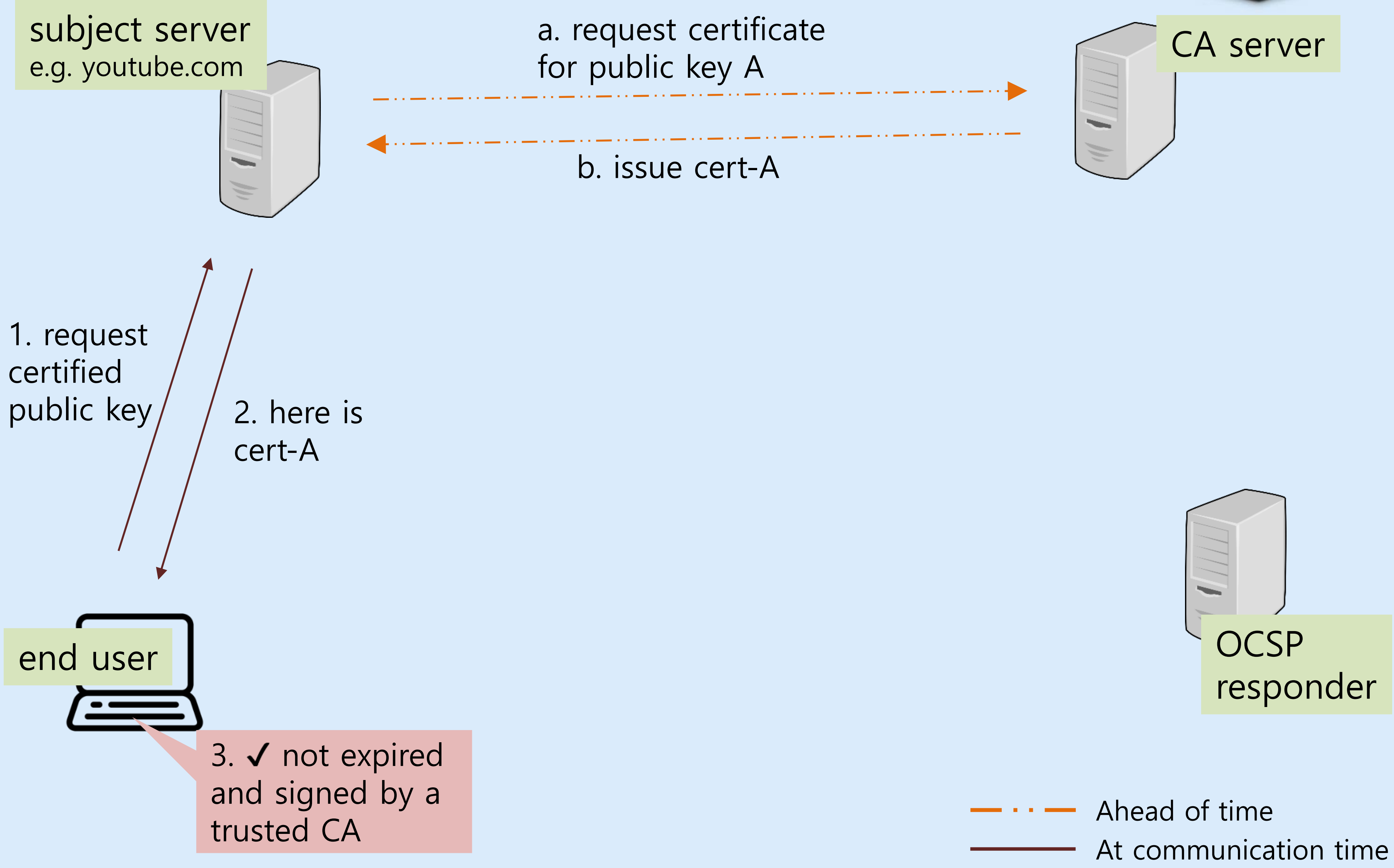
end user

OCSP
responder

Ahead of time

At communication time

OCSP Usage



subject server
e.g. youtube.com

a. request certificate
for public key A

CA server

b. issue cert-A

1. request
certified
public key

2. here is
cert-A

end user

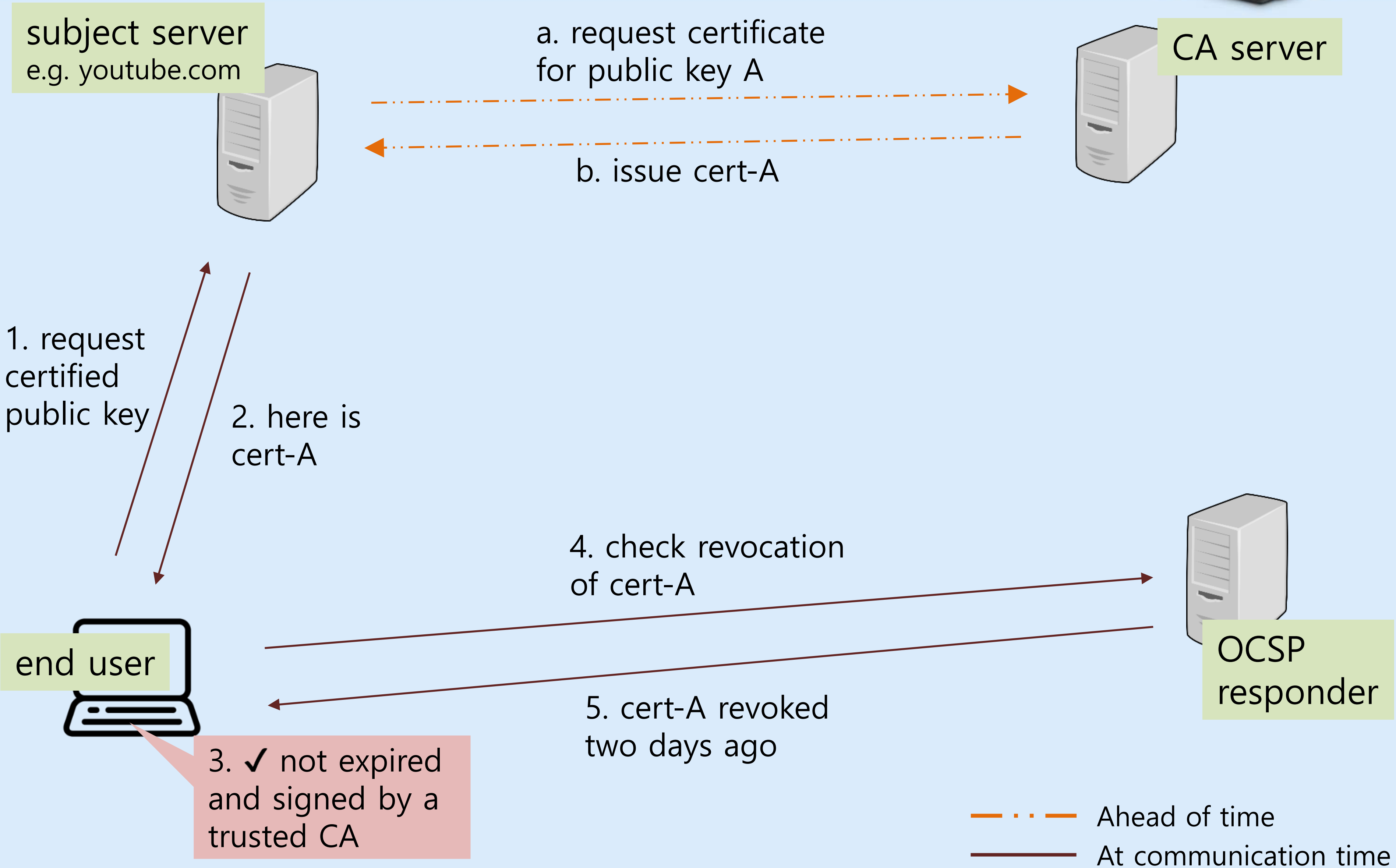
3. ✓ not expired
and signed by a
trusted CA

OCSP
responder

Ahead of time

At communication time

OCSP Usage



subject server
e.g. youtube.com

CA server

a. request certificate
for public key A

b. issue cert-A

1. request
certified
public key

2. here is
cert-A

end user

3. ✓ not expired
and signed by a
trusted CA

4. check revocation
of cert-A

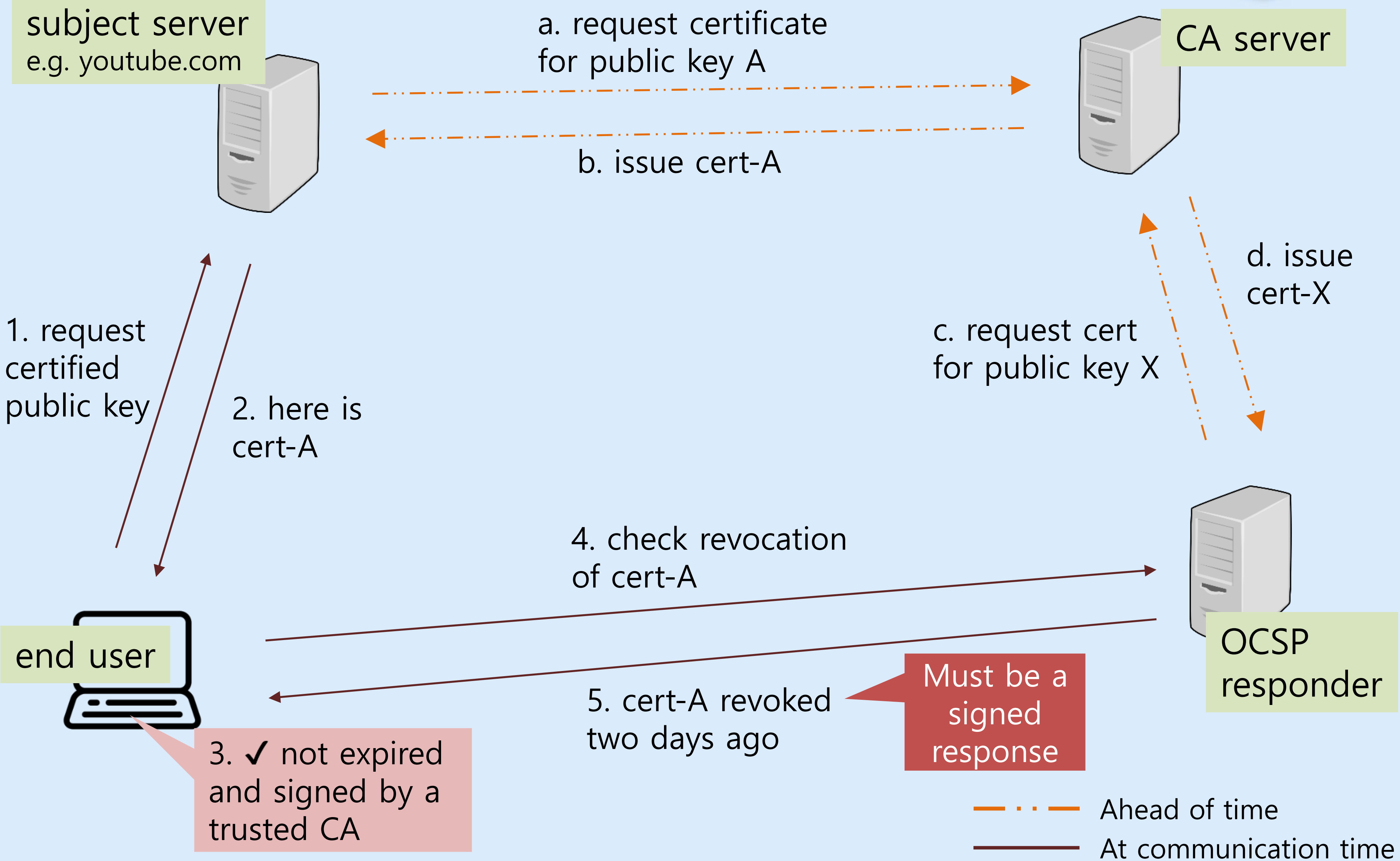
5. cert-A revoked
two days ago

OCSP
responder

— · · — Ahead of time

—— At communication time

OCSP Usage



subject server
e.g. youtube.com

CA server

a. request certificate
for public key A

b. issue cert-A

c. request cert
for public key X

d. issue
cert-X

OCSP
responder

end user

1. request
certified
public key

2. here is
cert-A

3. ✓ not expired
and signed by a
trusted CA

4. check revocation
of cert-A

5. cert-A revoked
two days ago

Must be a
signed
response

– · – Ahead of time

— At communication time