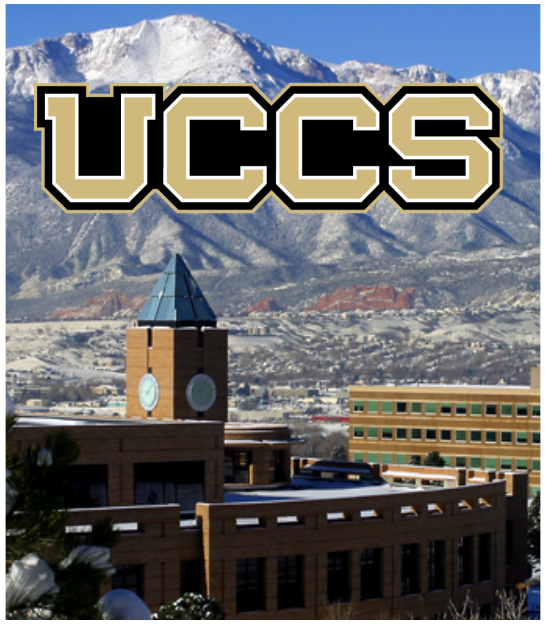


Asymmetric Cryptography and Key Management

Key Distribution and Management

Sang-Yoon Chang, Ph.D.

Module: Key Distribution and Management

Key distribution overview

Key hierarchy

Public-key authority

Public-key certificates

Key Distribution and Management

Key distribution/management are complex

Alice and Bob establish:

- Shared secret key for symmetric cryptography
- Valid/authenticated public keys for asymmetric cryptography

Key Distribution Approaches

1. User A can select a key and physically deliver it to User B
2. Third party can physically deliver the key to A and B

Key Distribution Approaches

1. User A can select a key and physically deliver it to User B
2. Third party can physically deliver the key to A and B
3. If they communicated previously, A and B can use a previous key to encrypt and communicate the new key

Key Distribution Approaches

1. User A can select a key and physically deliver it to User B
2. Third party can physically deliver the key to A and B
3. If they communicated previously, A and B can use a previous key to encrypt and communicate the new key
4. If A and B have secure communications w/ a trusted third party C, C can deliver key

Key Hierarchy

Session key:

- Temporary; used for one or few sessions
- Used between users for data encryption

Master key:

- Encrypt session keys
- Shared between user and key distribution center

Decentralized Key Distribution

Assume symmetric key (K_m) distributed for both Alice and Bob

Use K_m to distribute and share K_s

Alice **Bob**

$ID_A||N_1$ --------->

Alice **Bob**

$ID_A||N_1$ --------->

<---------- $E(K_m,[\ K_s||ID_A||ID_B||f(N_1)||N_2\ ])$

Alice **Bob**

$ID_A||N_1$ --------->

<---------- $E(K_m,[\ K_s||ID_A||ID_B$
$||f(N_1)||N_2\ ])$

$E(K_s||f(N_2))$ ------->

Alice **Bob**

$ID_A||N_1$ --------->

<---------- $E(K_m,[\ K_s||ID_A||ID_B$
$||f(N_1)||N_2\ ])$

$E(K_s||f(N_2))$ ------->

Need n(n-1)/2 keys for n users

Public-Key Authority

Builds on public directory securely registering $\{ID_i, K_i\}$

K_i public key of user i
and k_i private key of user I

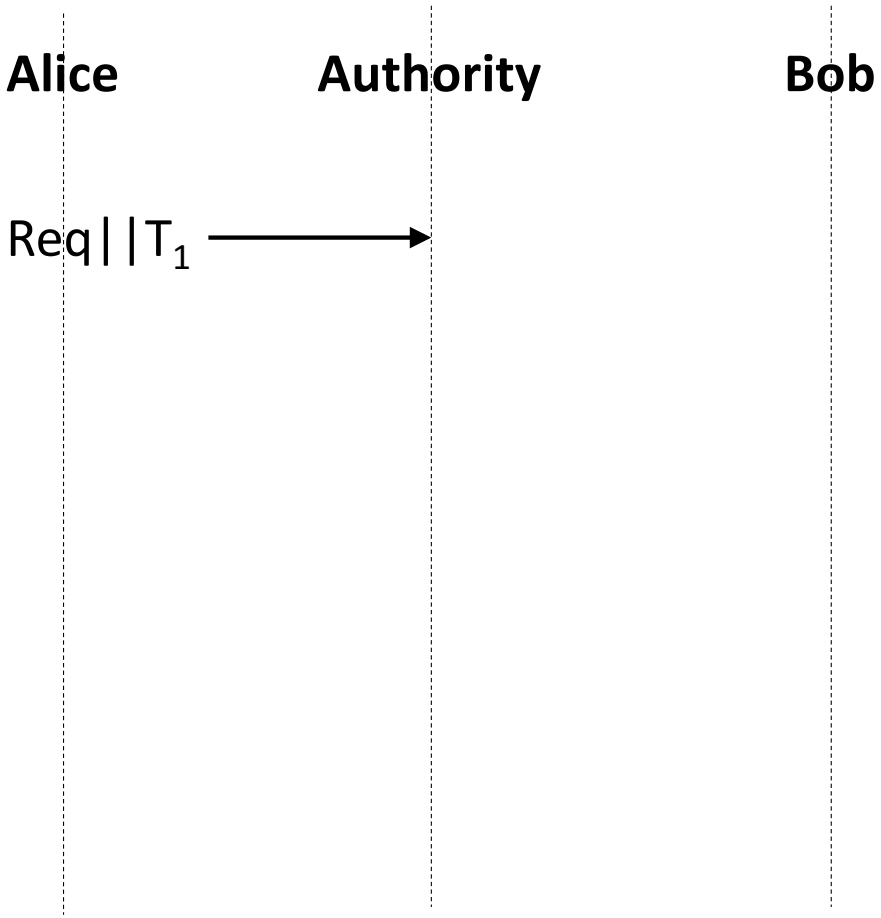
Public-Key Authority

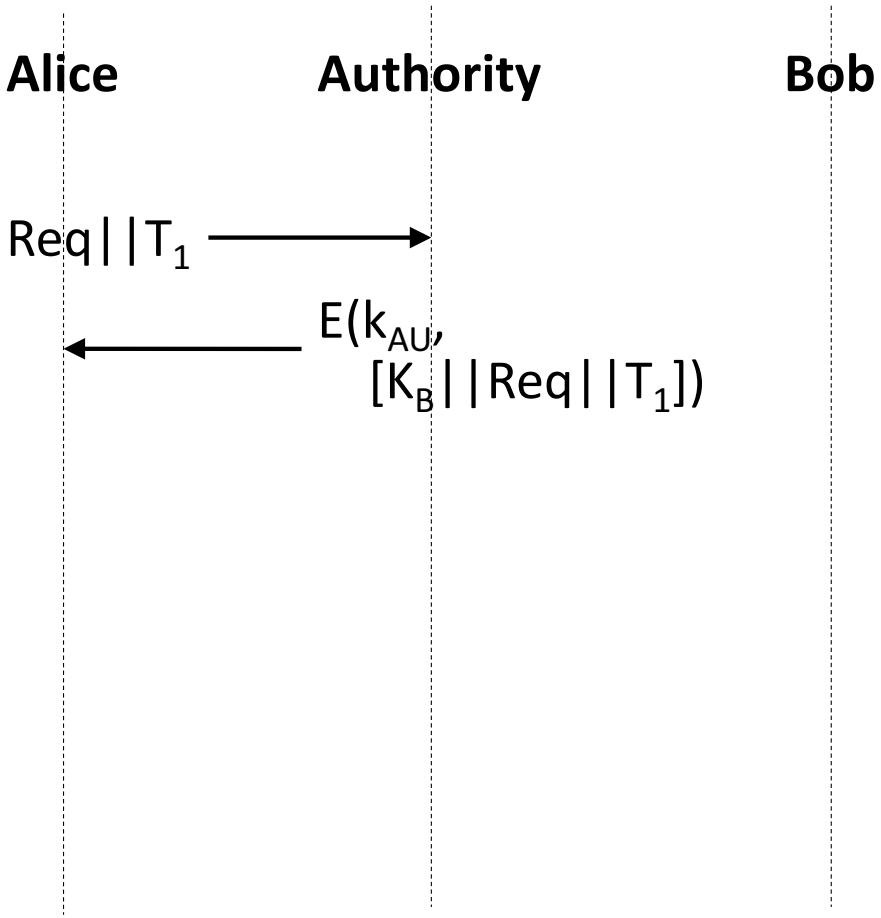
Builds on public directory securely registering $\{ID_i, K_i\}$

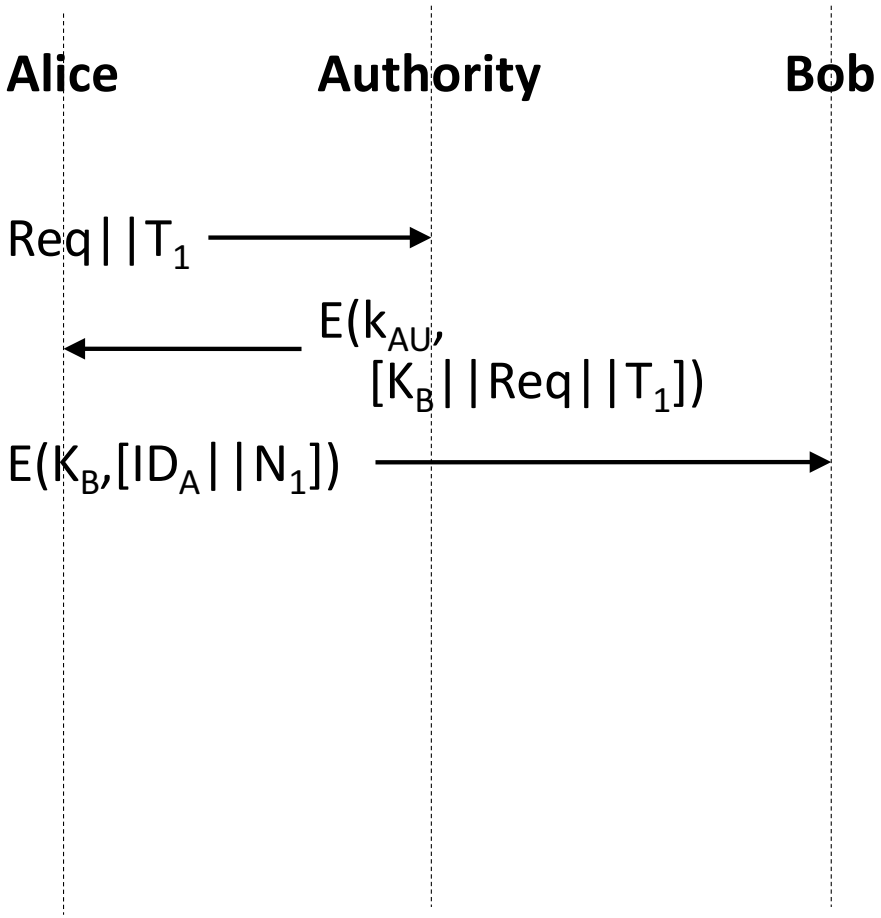
Securely distribute keys from directory

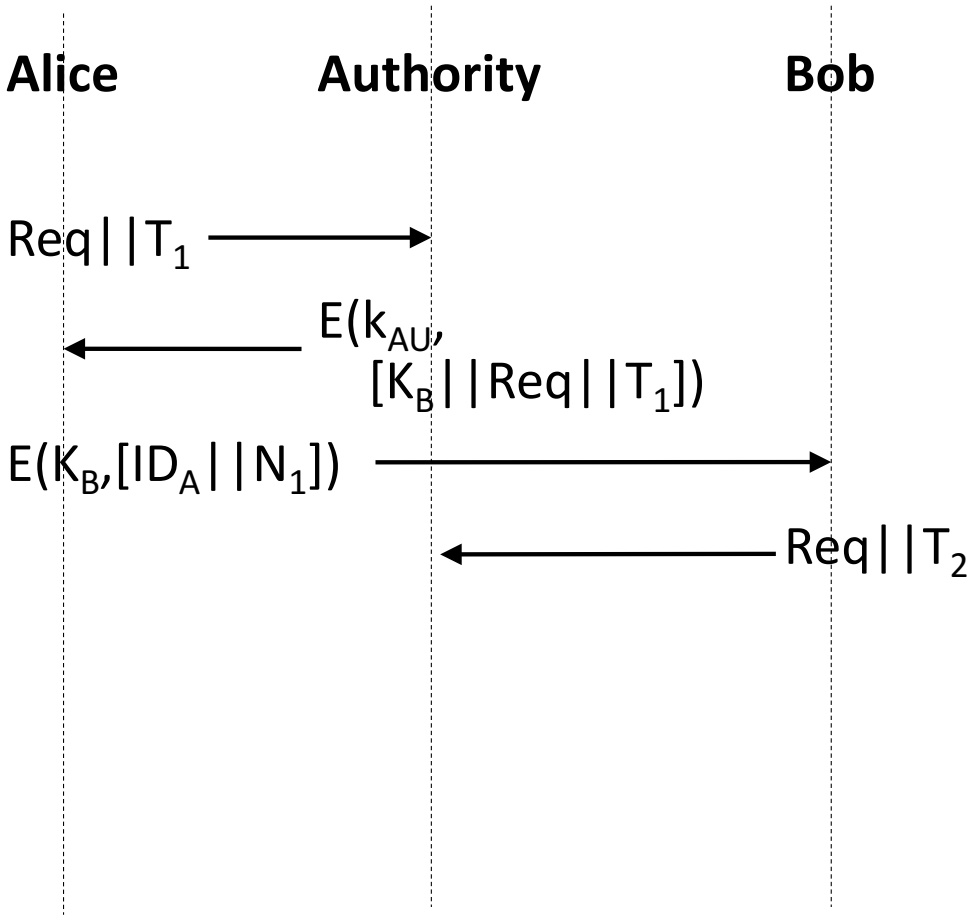
Require users to know authority's K_{AU}

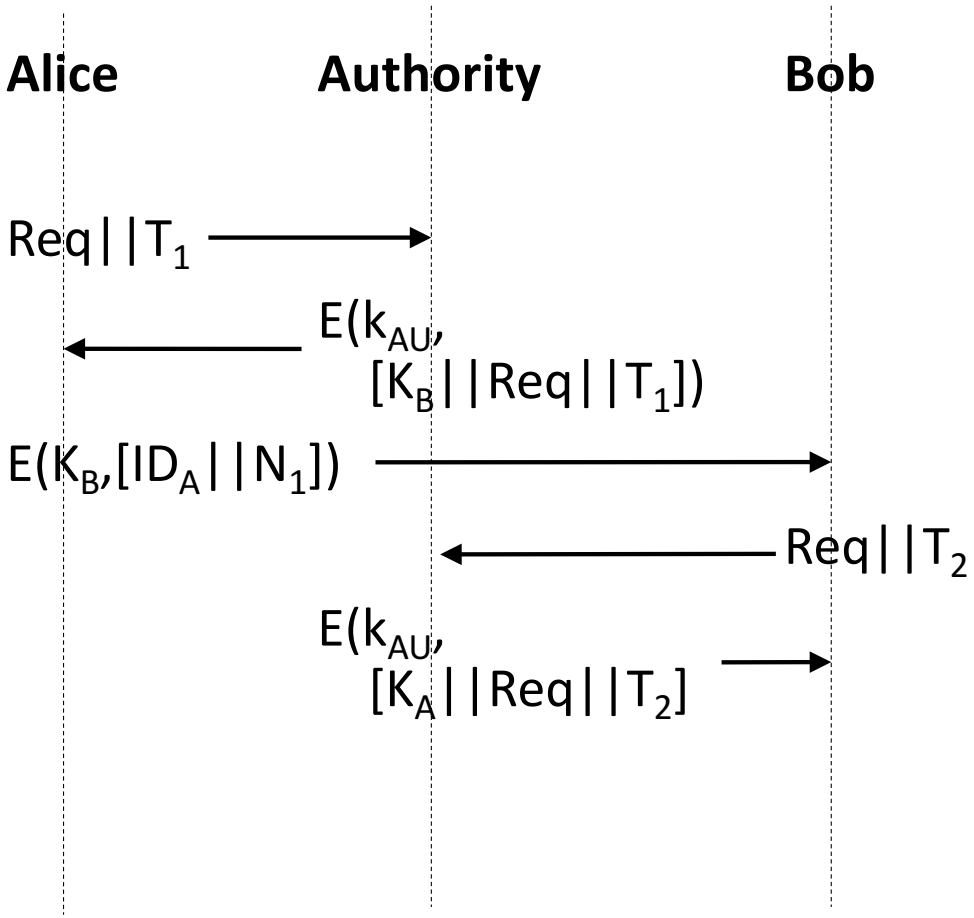
Require real-time access to authority

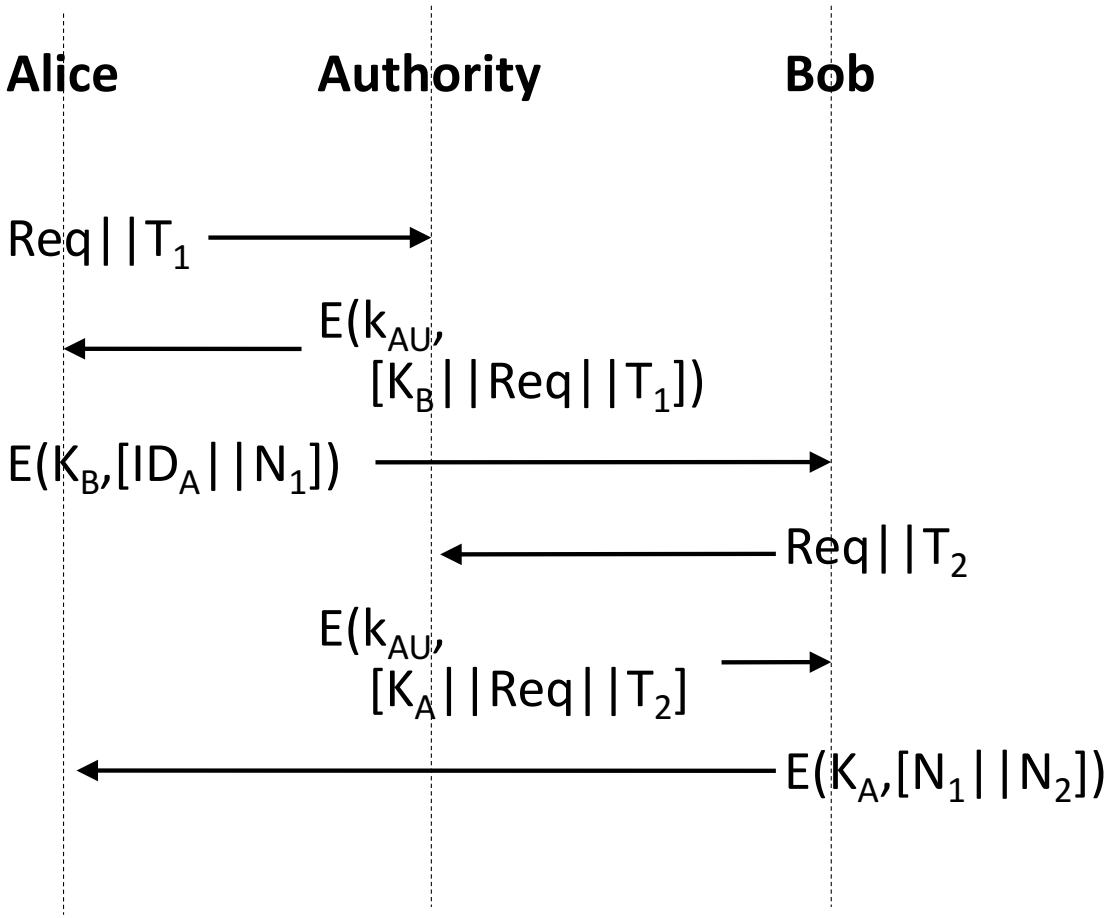

Alice
Authority
Bob
Req||T1

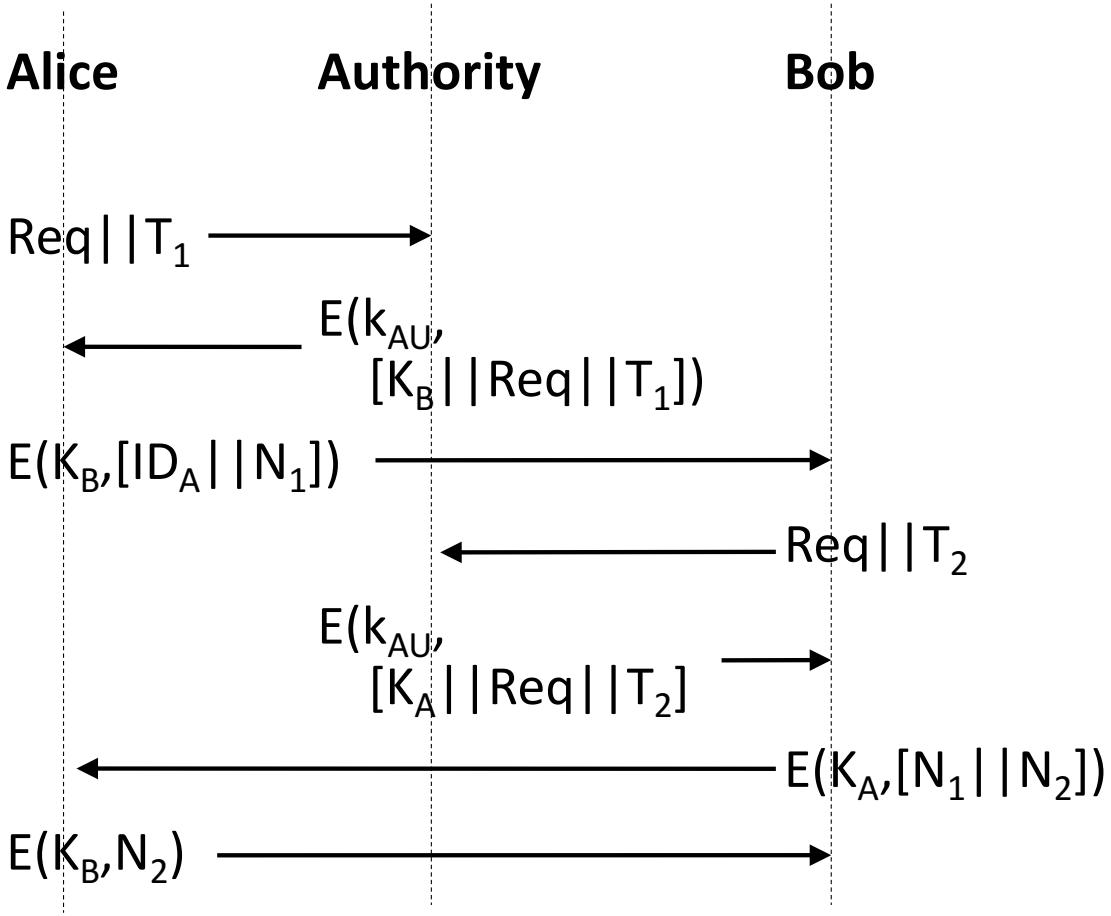

Alice
Authority
Bob
Req||T1
E(kAU,
[KB||Req||T1])

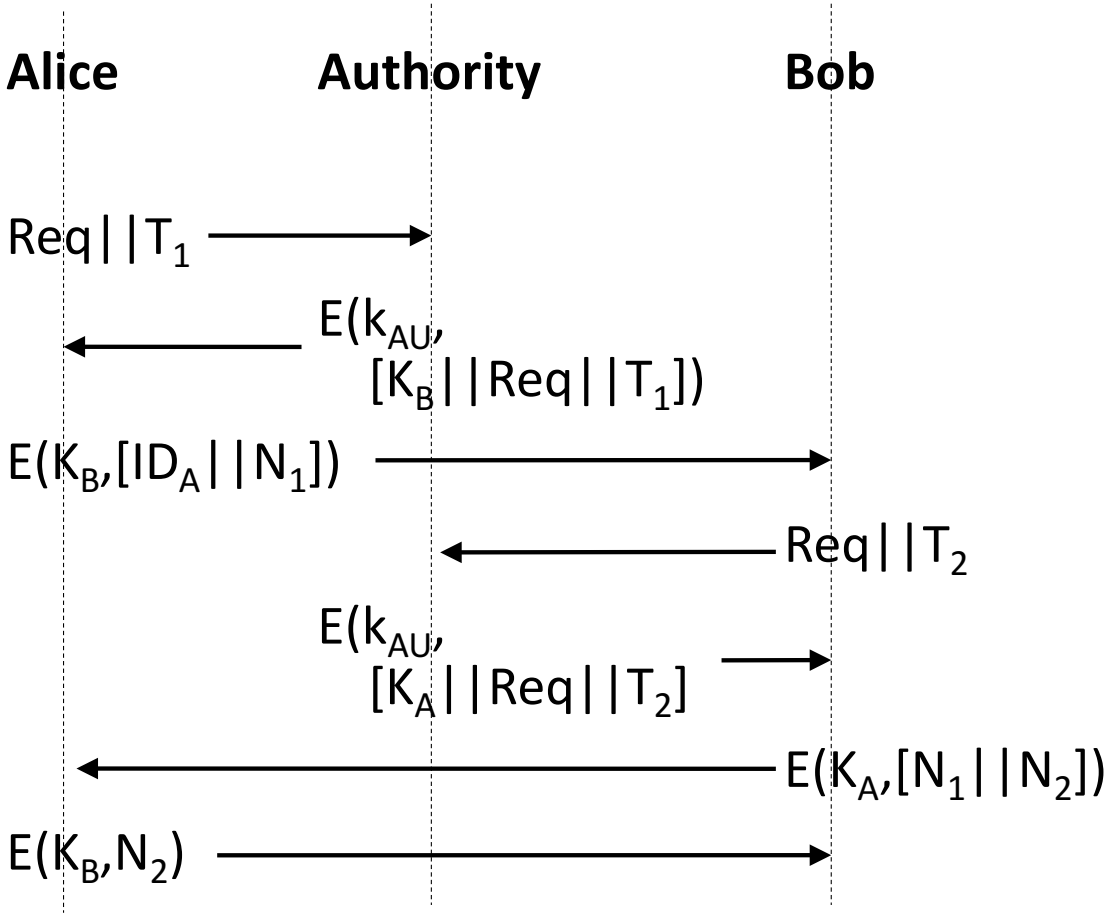

Alice
Authority
Bob
Req||T1
E(kAU,
[KB||Req||T1])
E(KB,[IDA||N1])


Alice
Authority
Bob
Req||T1
E(kAU,
[KB||Req||T1])
E(KB,[IDA||N1])
Req||T2


Alice
Authority
Bob
Req||T1
E(kAU,
[KB||Req||T1])
E(KB,[IDA||N1])
Req||T2
E(kAU,
[KA||Req||T2]


Alice
Authority
Bob
Req||T1
E(kAU,
[KB||Req||T1])
E(KB,[IDA||N1])
Req||T2
E(kAU,
[KA||Req||T2]
E(KA,[N1||N2])


Alice
Authority
Bob
Req||T1
E(kAU,
[KB||Req||T1])
E(KB,[IDA||N1])
Req||T2
E(kAU,
[KA||Req||T2]
E(KA,[N1||N2])
E(KB,N2)



Real-time access of authority when key is needed

Public-Key Certificate

Builds on p.-k. authority; binds i to K_i

But allows key exchange without
real-time access to the authority

Contains validity period, rights of use

Signed by Certificate Authority (CA)

Public-Key Certificate Requirements

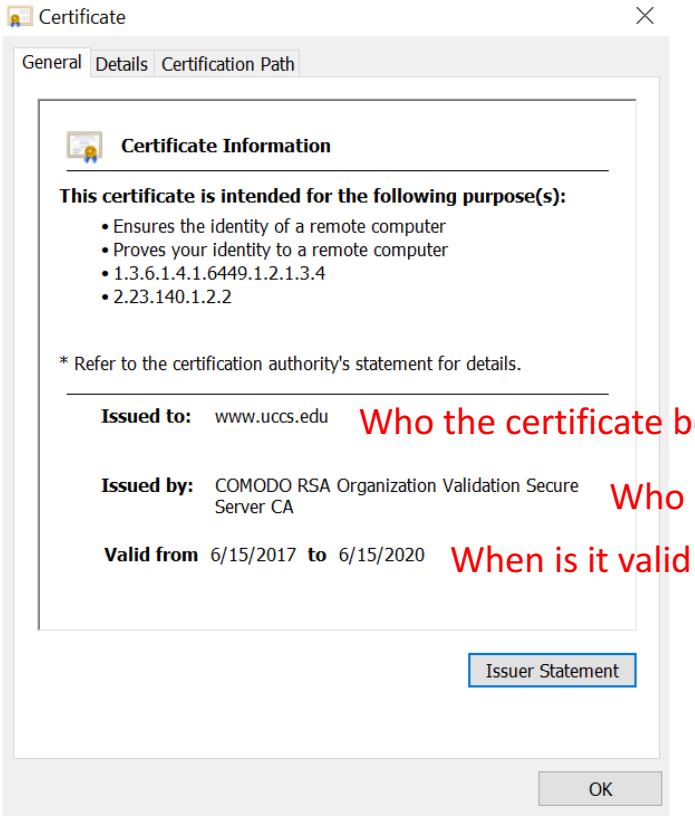
1. Any user can read a certificate
2. Any user can verify the certificate
3. Only CA can create/update certificates
4. Any user can verify the currency/validity of the certificate

Public-Key Certificate Requirements

1. Any user can read a certificate
2. Any user can verify the certificate
3. Only CA can create/update certificates
4. Any user can verify the currency/validity of the certificate

E.g., X.509 certificate standard

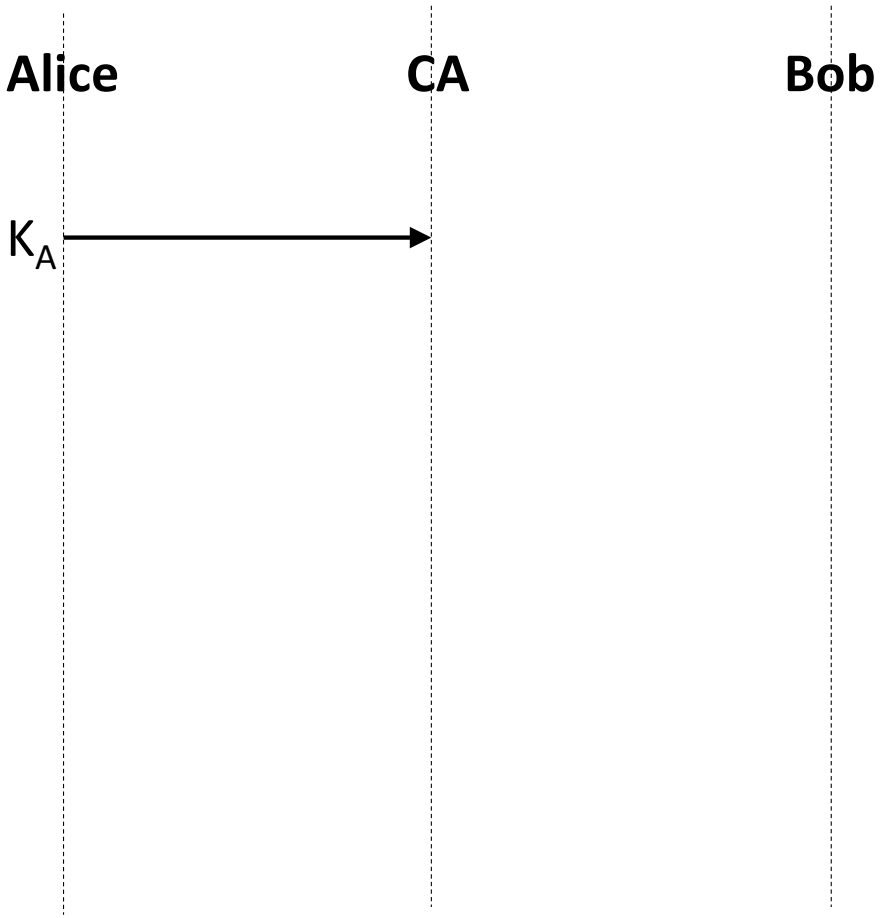
TLS Digital Certificate Example

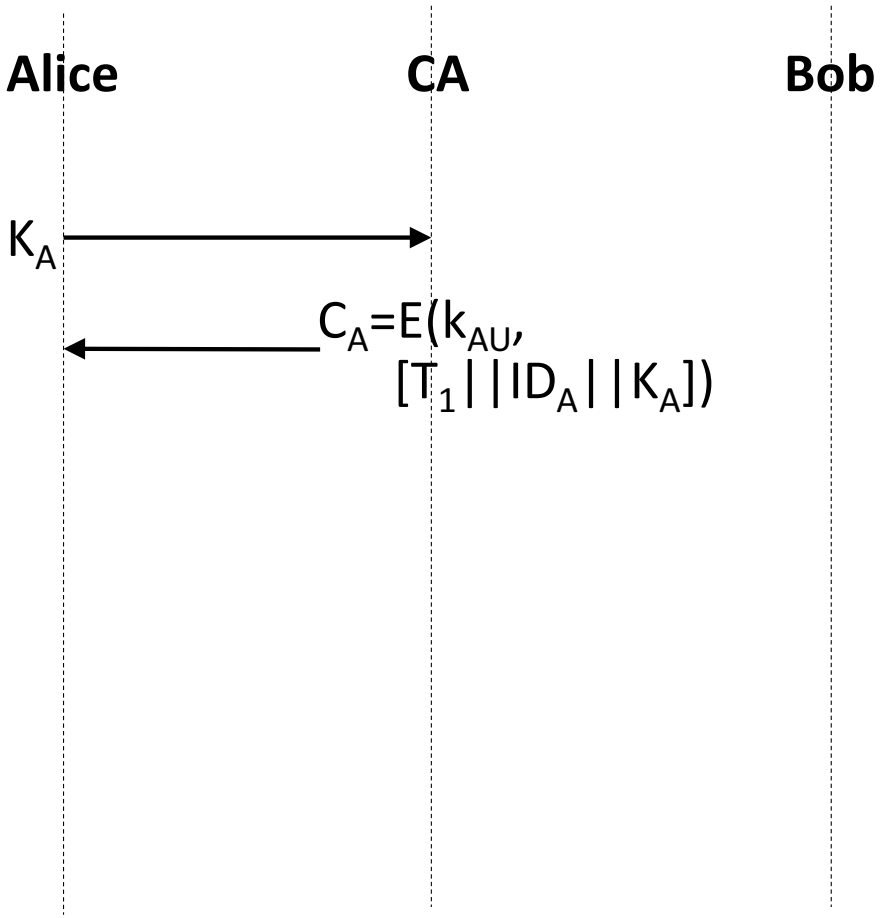


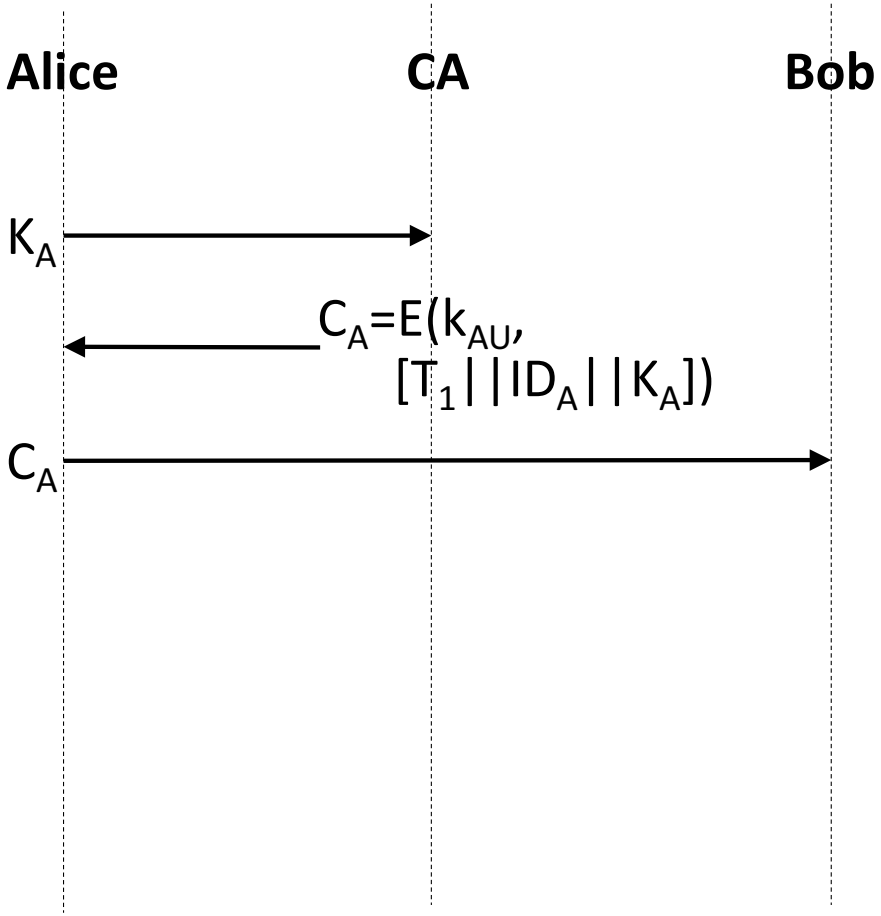
Who the certificate belongs to

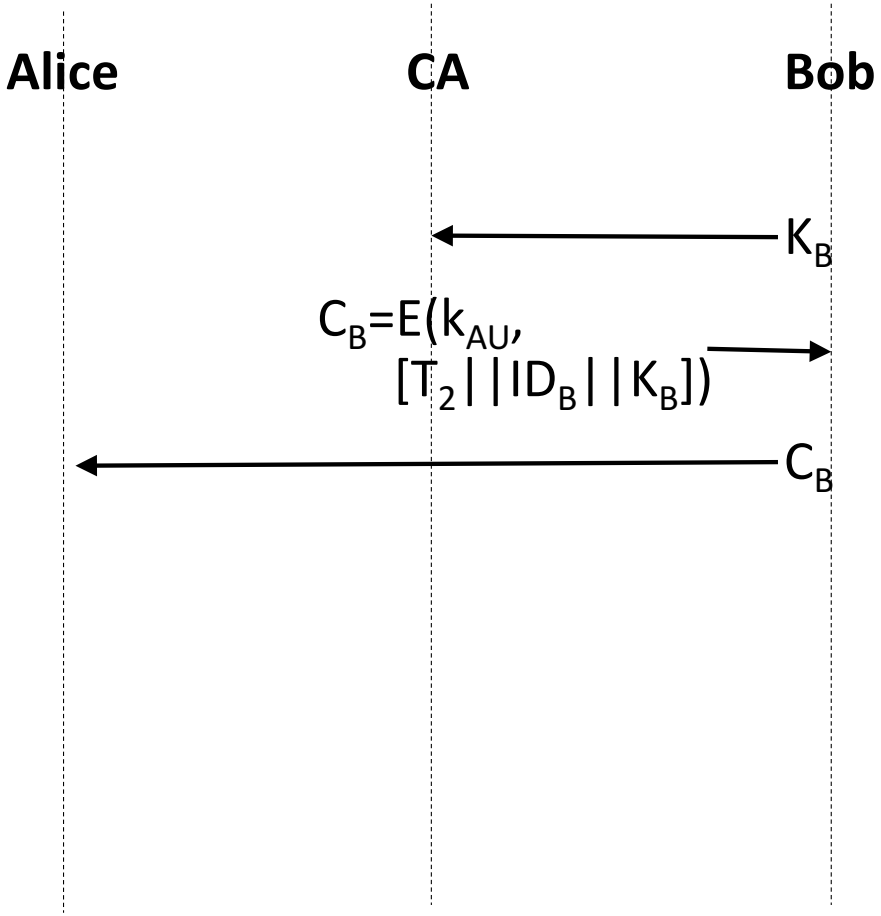
Who signed the certificate

When is it valid


Alice
CA
Bob
K_A


Alice
CA
Bob
K_A
$C_A=E(k_{AU},$
$[T_1||ID_A||K_A])$


Alice
CA
Bob
K_A
$C_A=E(k_{AU},$
$[T_1||ID_A||K_A])$
C_A


Alice
CA
Bob
K_B
$C_B=E(k_{AU},$
$[T_2||ID_B||K_B])$
C_B

Public Key Infrastructure

PKI is the system comprised of hardware, software, people policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates

Enable secure, convenient, and efficient acquisition of public keys