Vietnam National University Ho Chi Minh City, University of Science
Department of Information Technology

Topic 8:
Digital Certificate &Certificate Authority

Assoc. Prof. Trần Minh Triết
PhD. Trương Toàn Thịnh

fit@hcmus

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

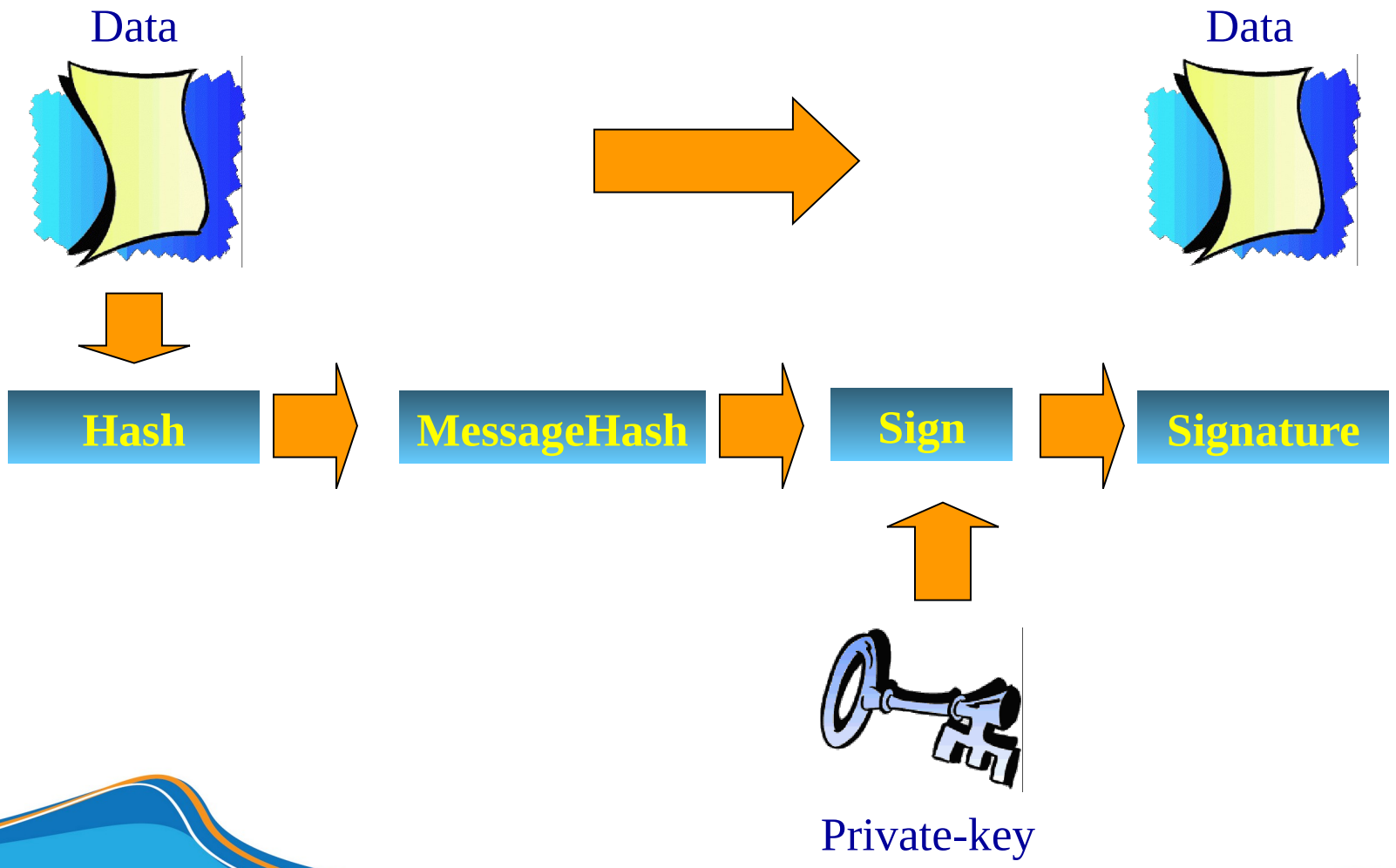
Contents

- Introduction
- Digital signature
- Digital certificate
- Certificate Authority (CA)
- PKI model
- Applications…

Demo 1

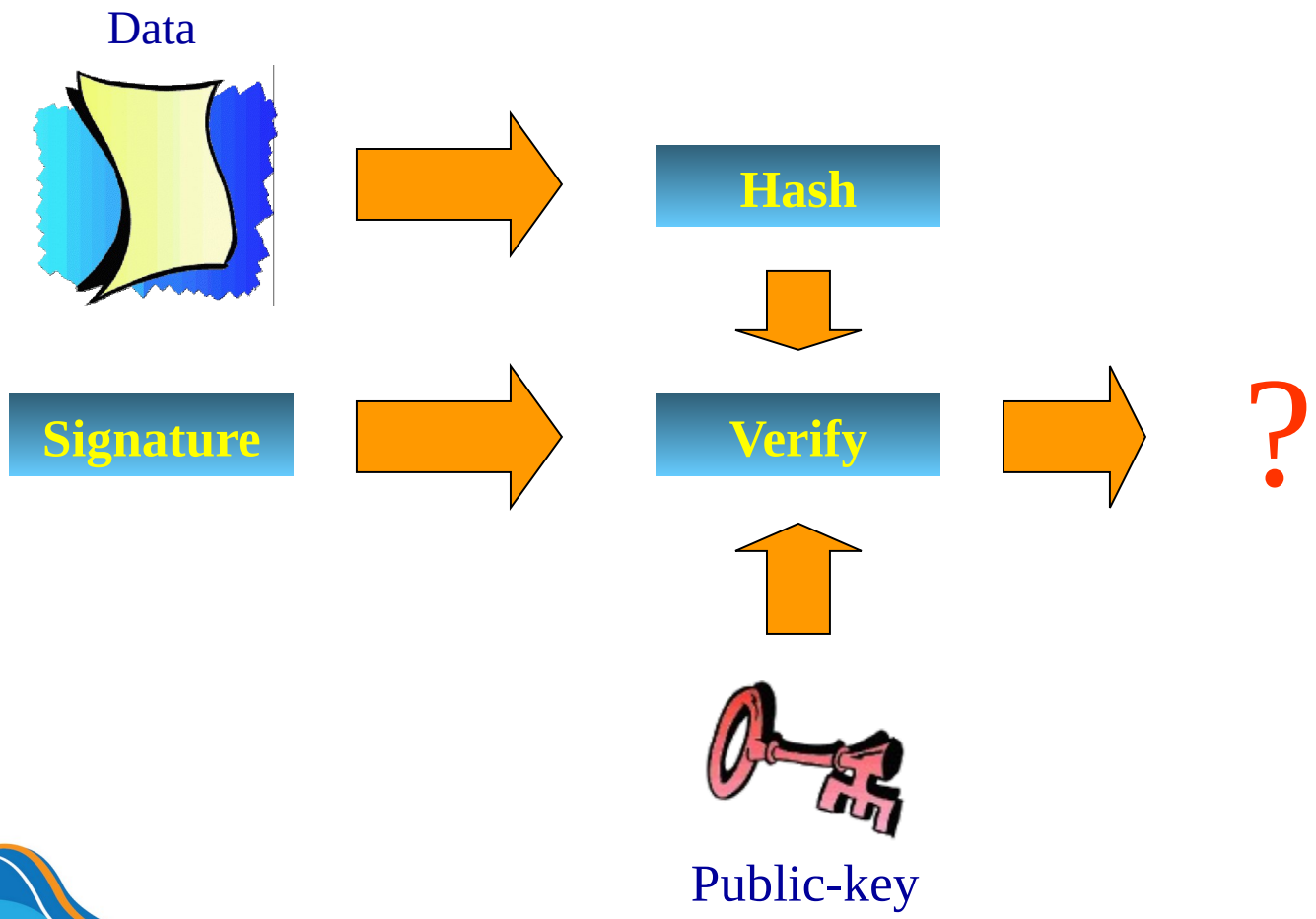
Recall digital signature

Create signature

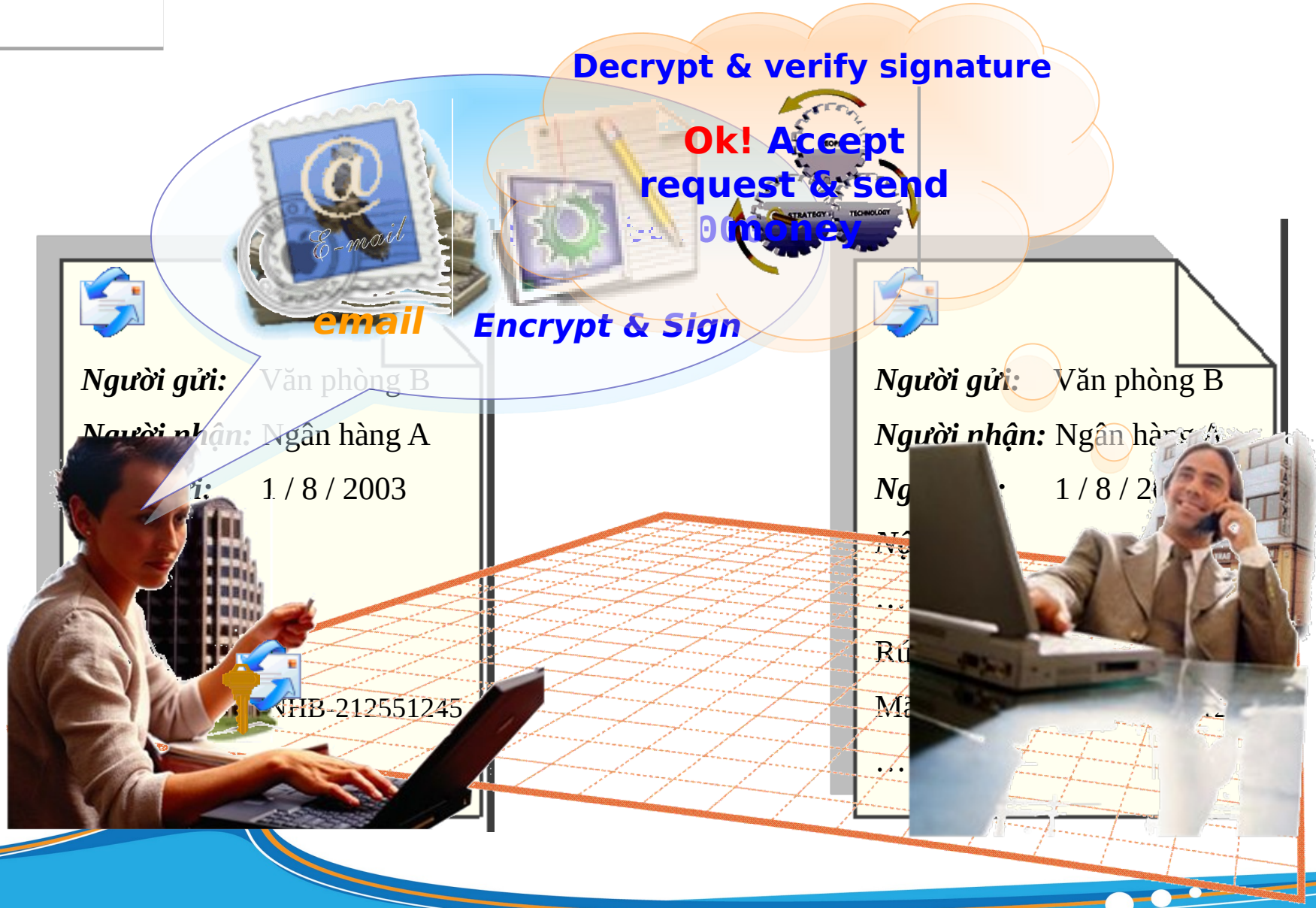


Recall digital signature

- Verify signature

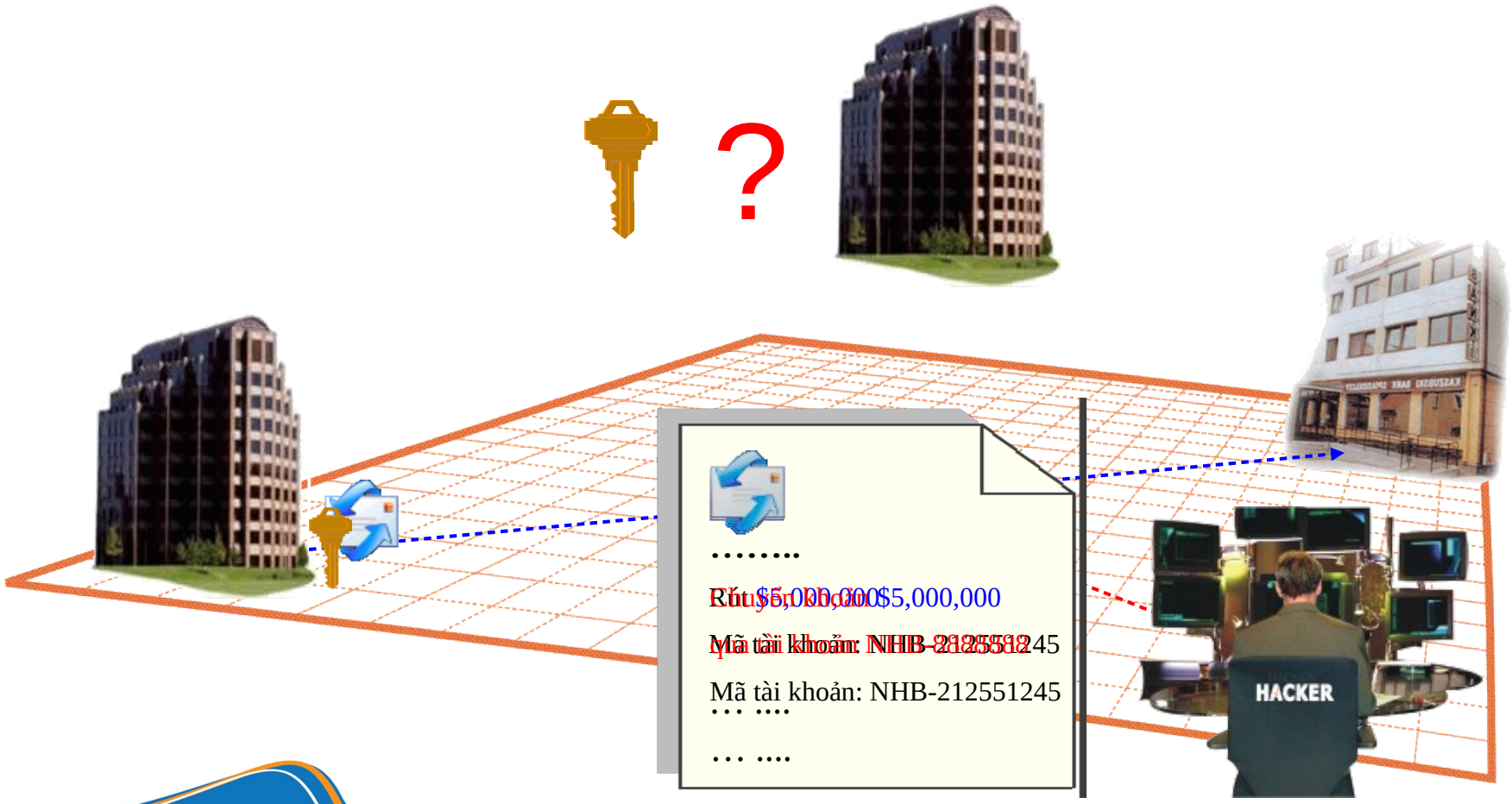


Demo 2


Decrypt & verify signature
Ok! Accept request & send money
email
Encrypt & Sign
Người gửi: Văn phòng B
Người nhận: Ngân hàng A
1 / 8 / 2003
Người gửi: Văn phòng B
Người nhận: Ngân hàng A
1 / 8 / 2

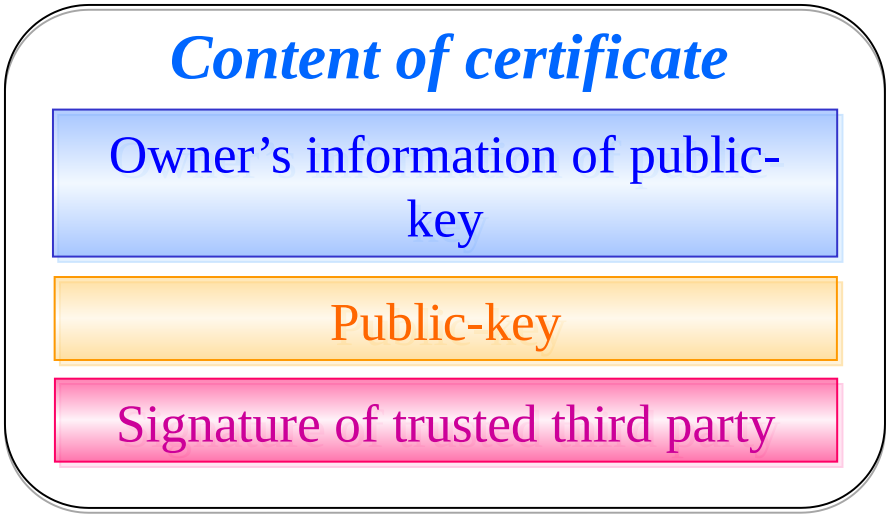
Demo 3

- Data is attacked in transit (MIM-Man in Middle)



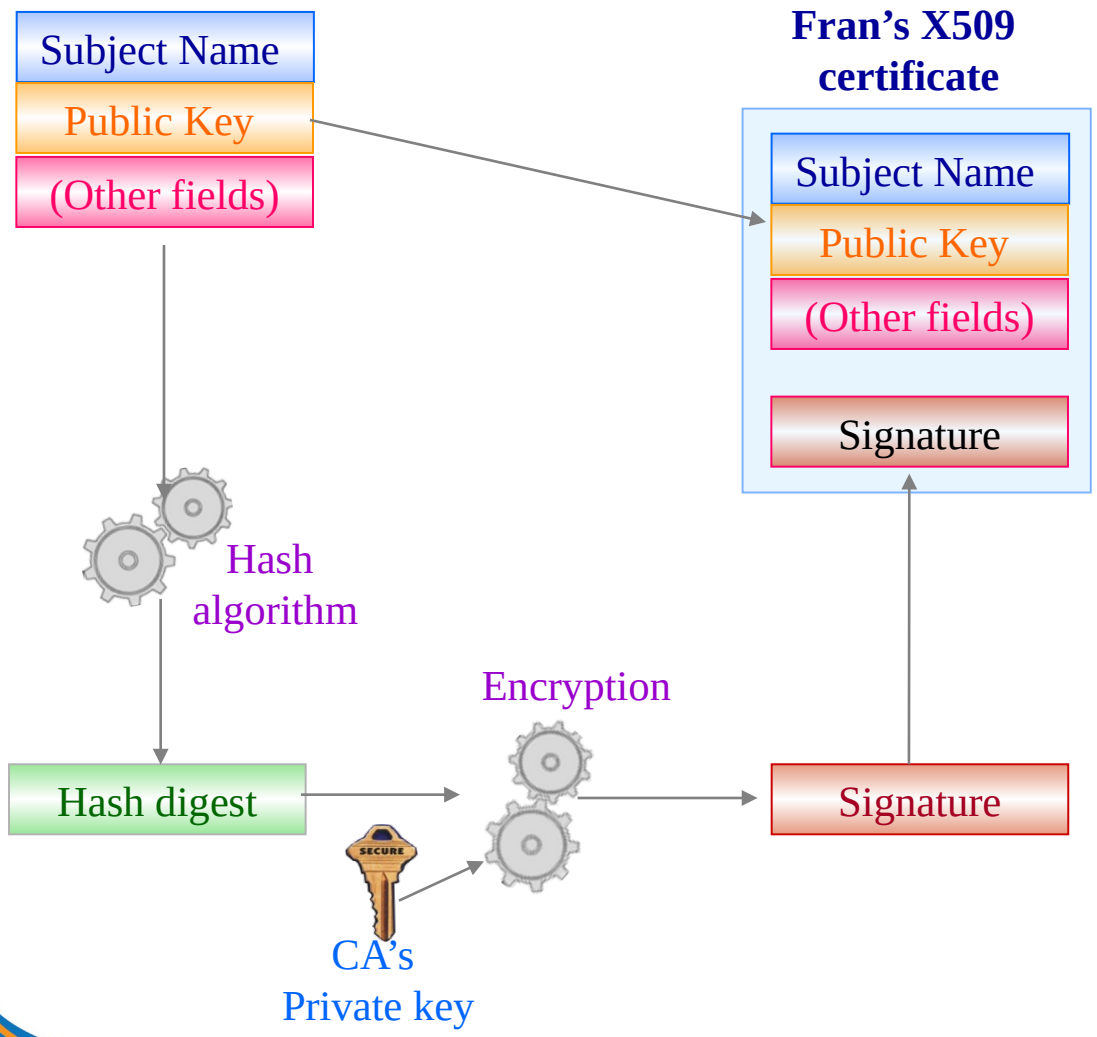
Digital Certificate

- Digital certificate is a certificate of ownership of public-key

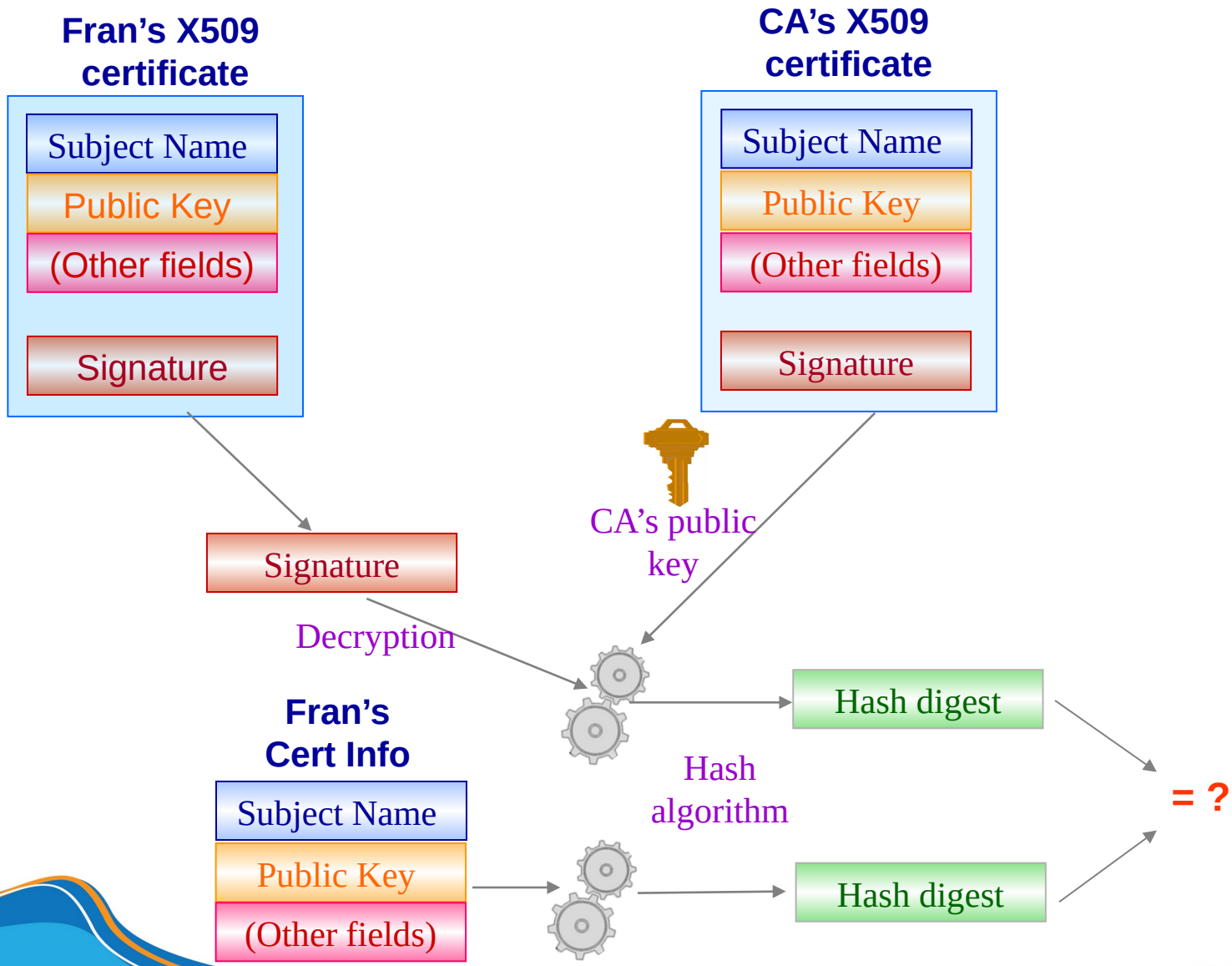


⇒ E-certificate solves the problem MIM

Create certificate

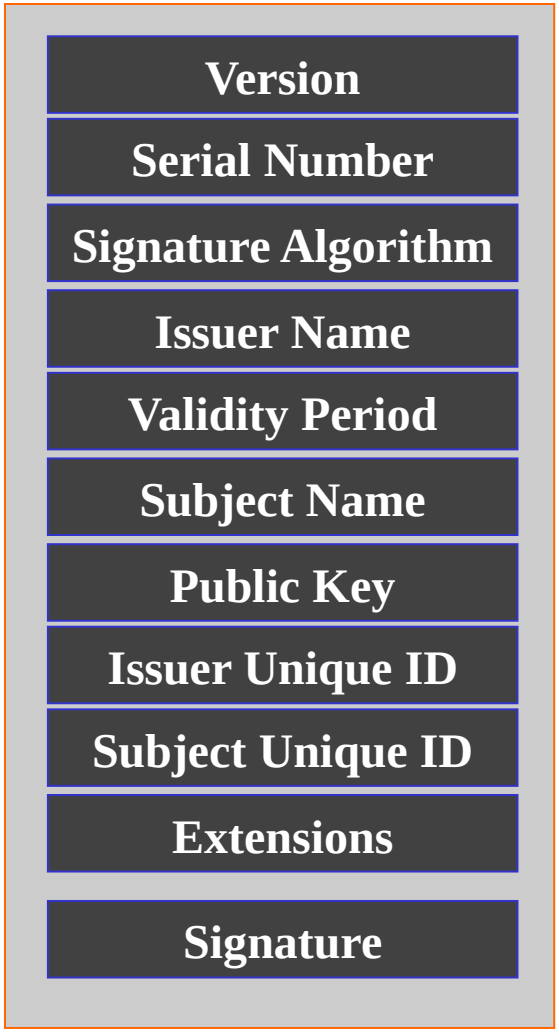


Verify certificate



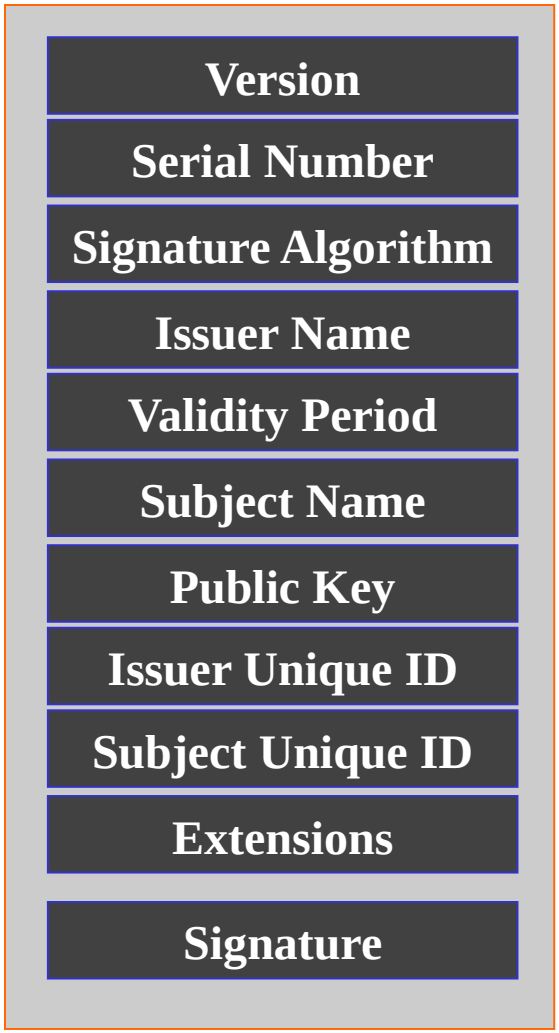
Standard X.509 (ver. 3.0)

- *Version*: Specify the version of the certificate X.509.
- *Serial Number*: The issue serial number is assigned by the CA. Each CA should assign a unique batch number to each certificate it issues.
- *Signature Algorithm*: Signature algorithm specifies the encryption algorithm used by the CA to sign the certificate. In an X.509 certificate it is usually a combination of a hash algorithm (such as MD5) and a public key algorithm (such as RSA).



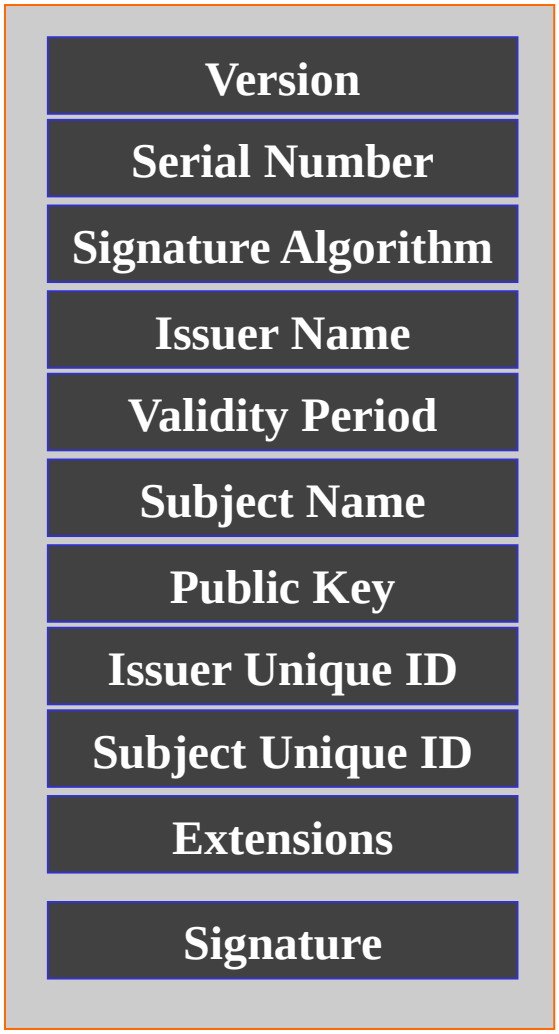
Standard X.509 (ver. 3.0)

- *Issuer Name*:
  - Name of the CA issuing the certificate
  - X.500 Distinguised Name – X.500 DN.
  - Two CAs cannot use the same issue name.
- *Validity Period*: consists of 2 values specifying the period for which the certificate is valid: not-before and not-after.
  - *Not-before*: certification period begins to take effect.
  - *Not-after*: certification period expires.
  - These time values are measured according to the International time standard, accurate to the second.



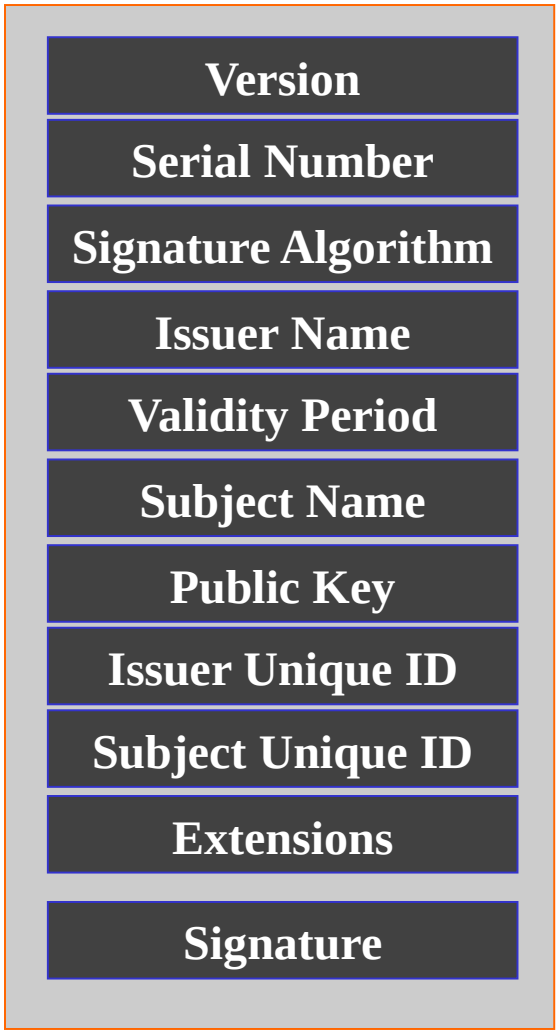
Standard X.509 (ver. 3.0)

- *Issuer Unique ID&Subject Unique ID*:
  - Using from X.509 version 2,
  - Used to identify two CAs or two entities when they have the same DN.
  - RFC 2459 recommends not to use these two fields.
- *Extensions*:
  - Contains the necessary additional information the CA operator wants to place in the certificate.
  - Released in X.509 version 3.



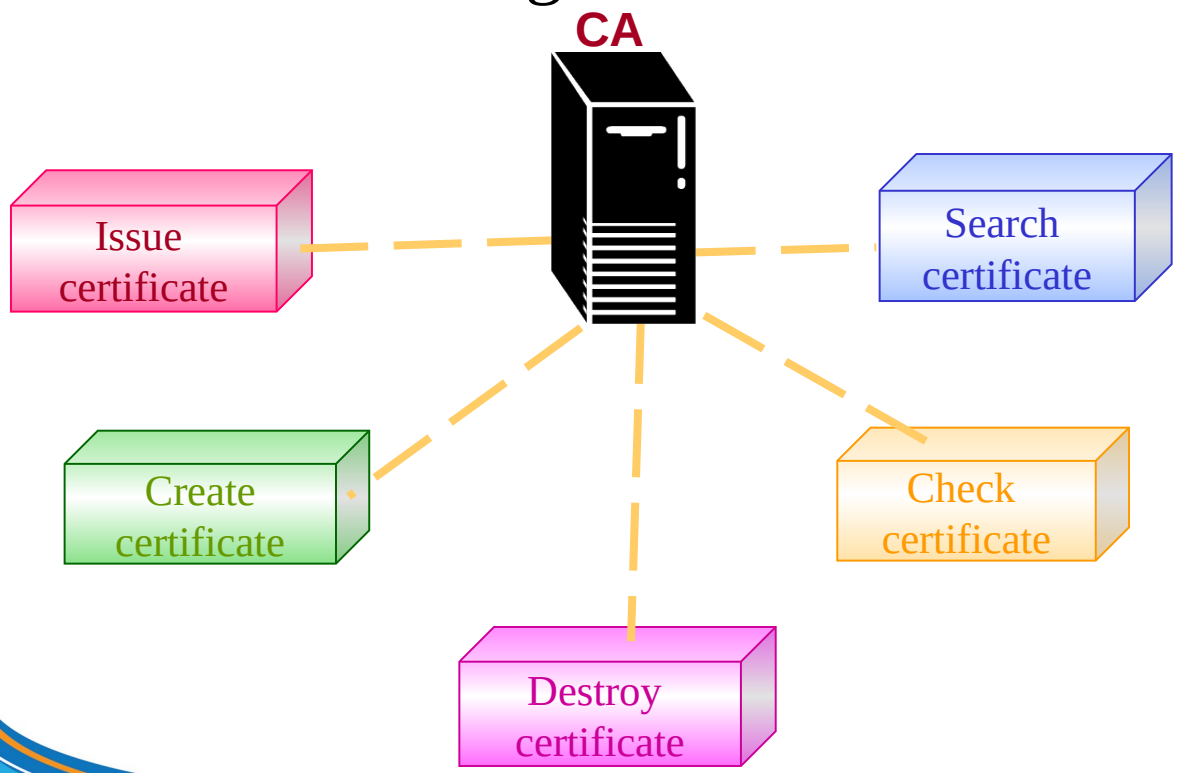
Chuẩn X.509 (ver. 3.0)

- *Signature*:
  - E-signatures applied by CA organizations.
  - CA organization uses a secret key of the type specified in the signature algorithm field.
  - The signature includes all other parts of the certificate.
  - ⇒ CA certifies for all other information in the certificate, not just the subject name and public key.



Certificate Authority System

- A trusted third party
- E-signature management
- Digital certificate management



Certificate Authority System CA(S)

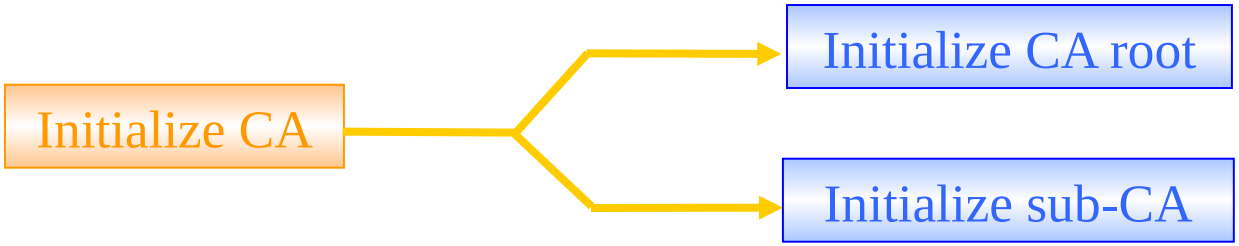
Centralized model

Web of Trust

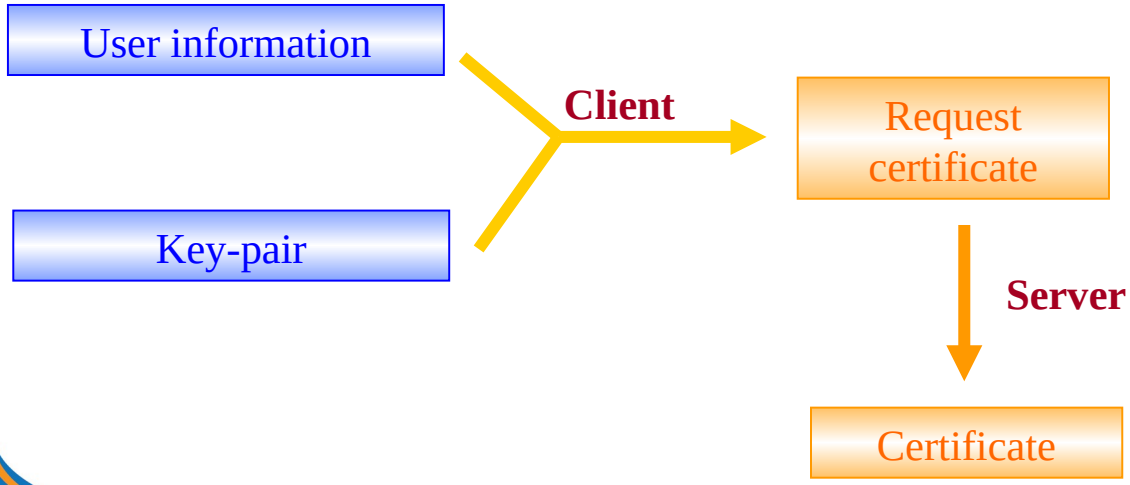
Hierarchical model

Certificate Authority System CA(S)

Initialize CA

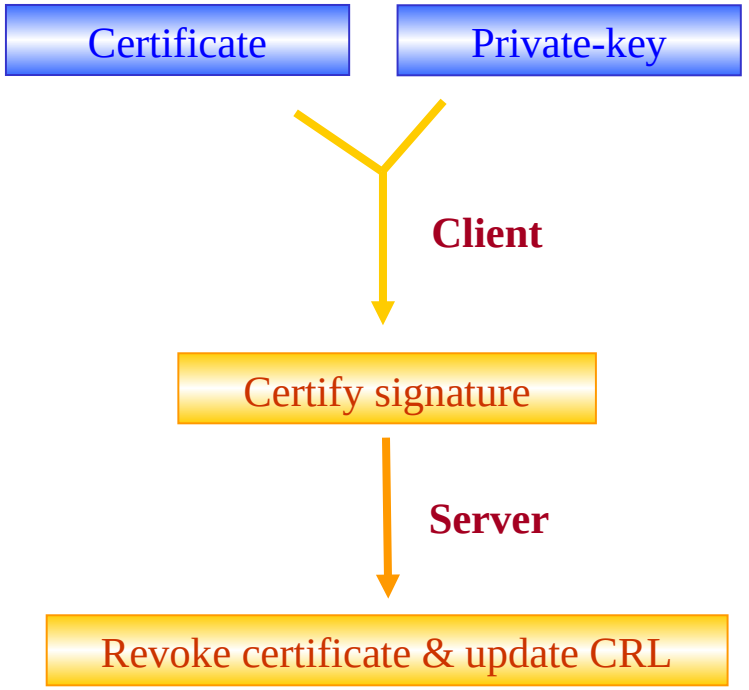


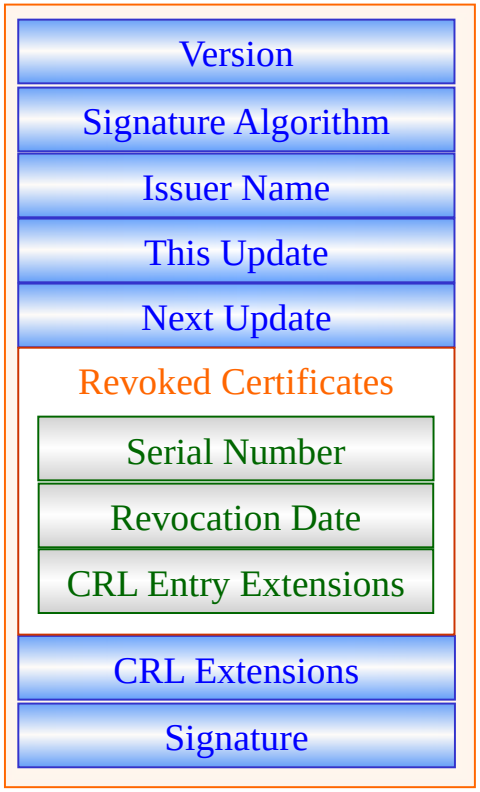
Create Cert



Certificate Authority System – CA(S)

Revoke Cert

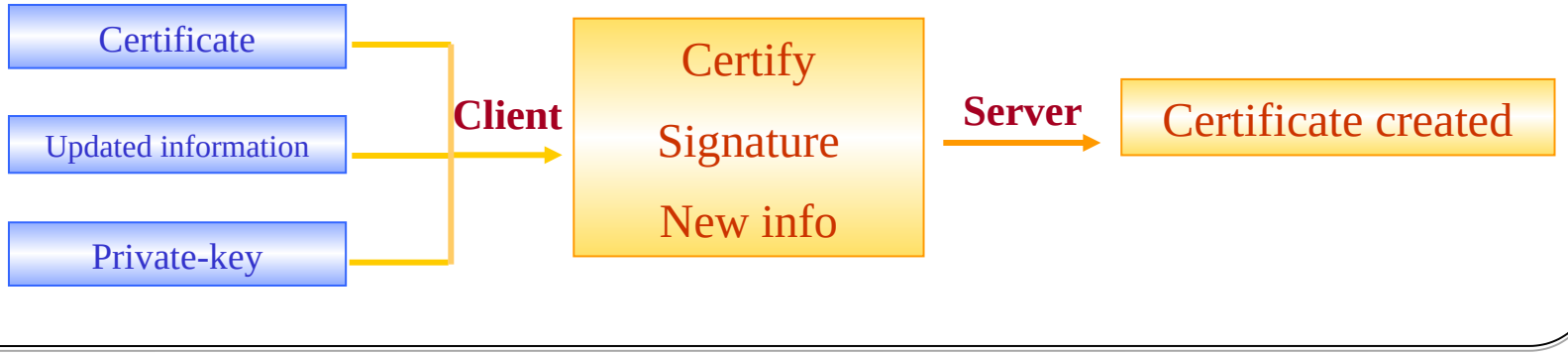




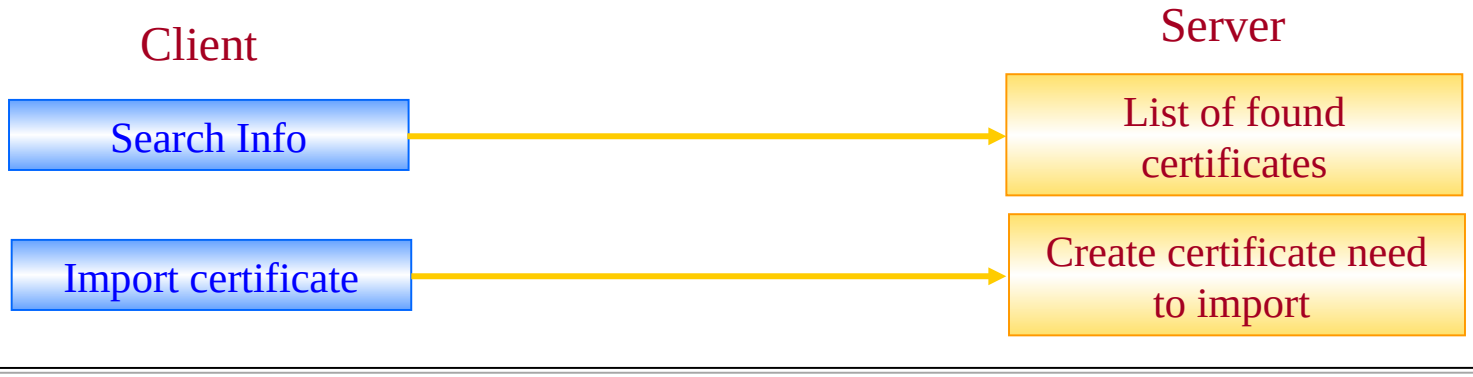
Version 2 of CRL's standard

Certificate Authority System – CA(S)

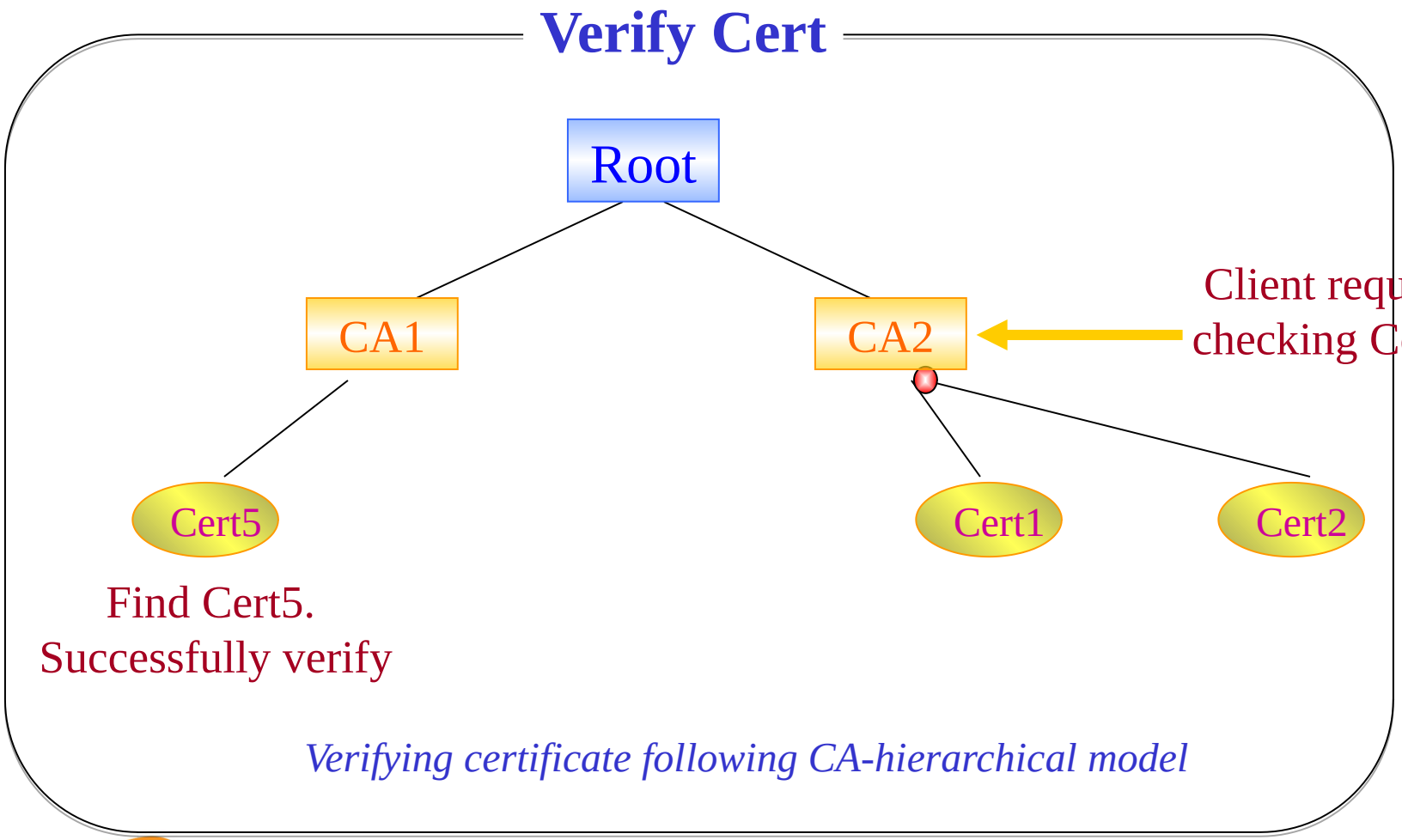
Update Cert



Search Cert

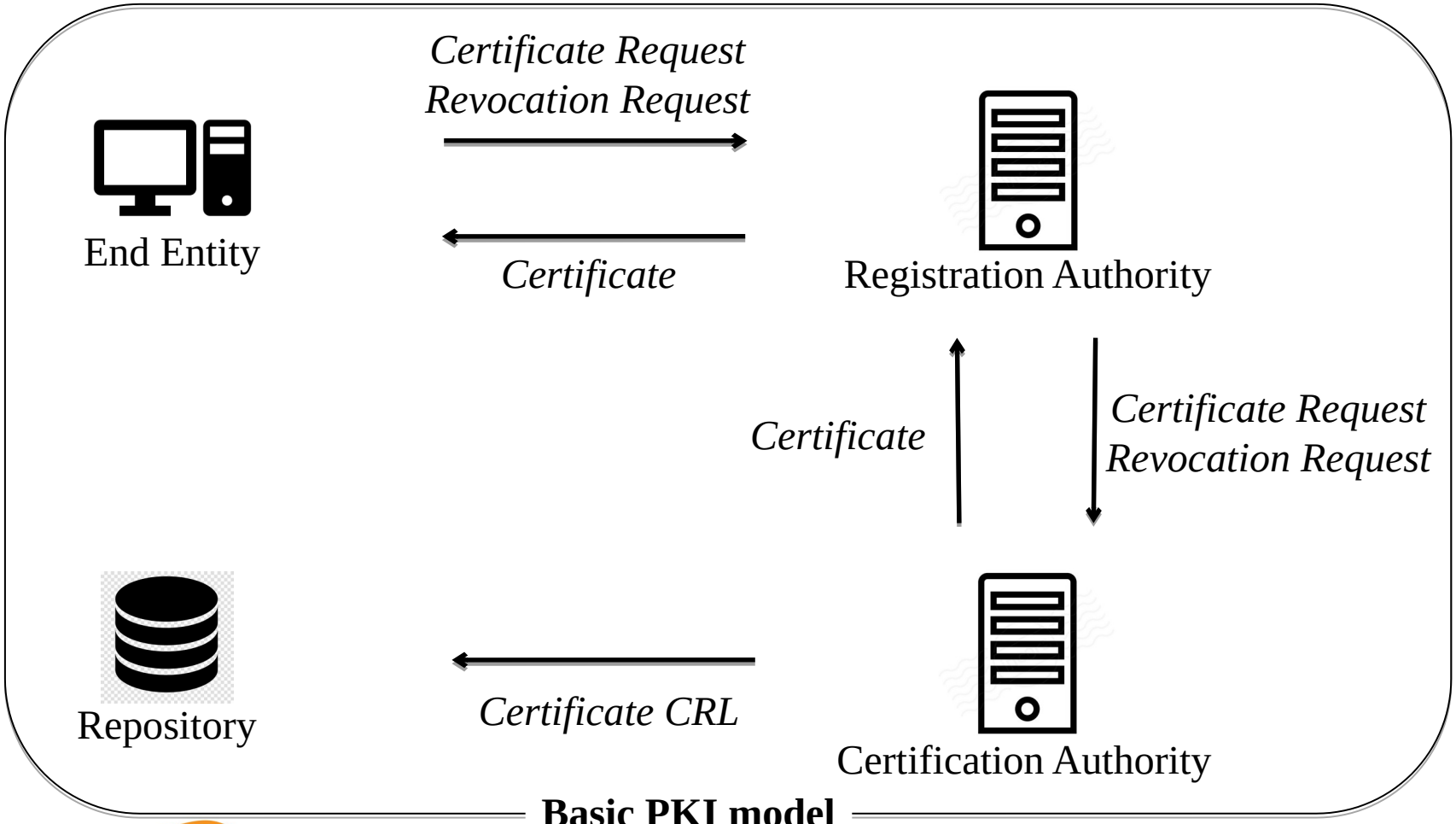


Certificate Authority System – CA(S)



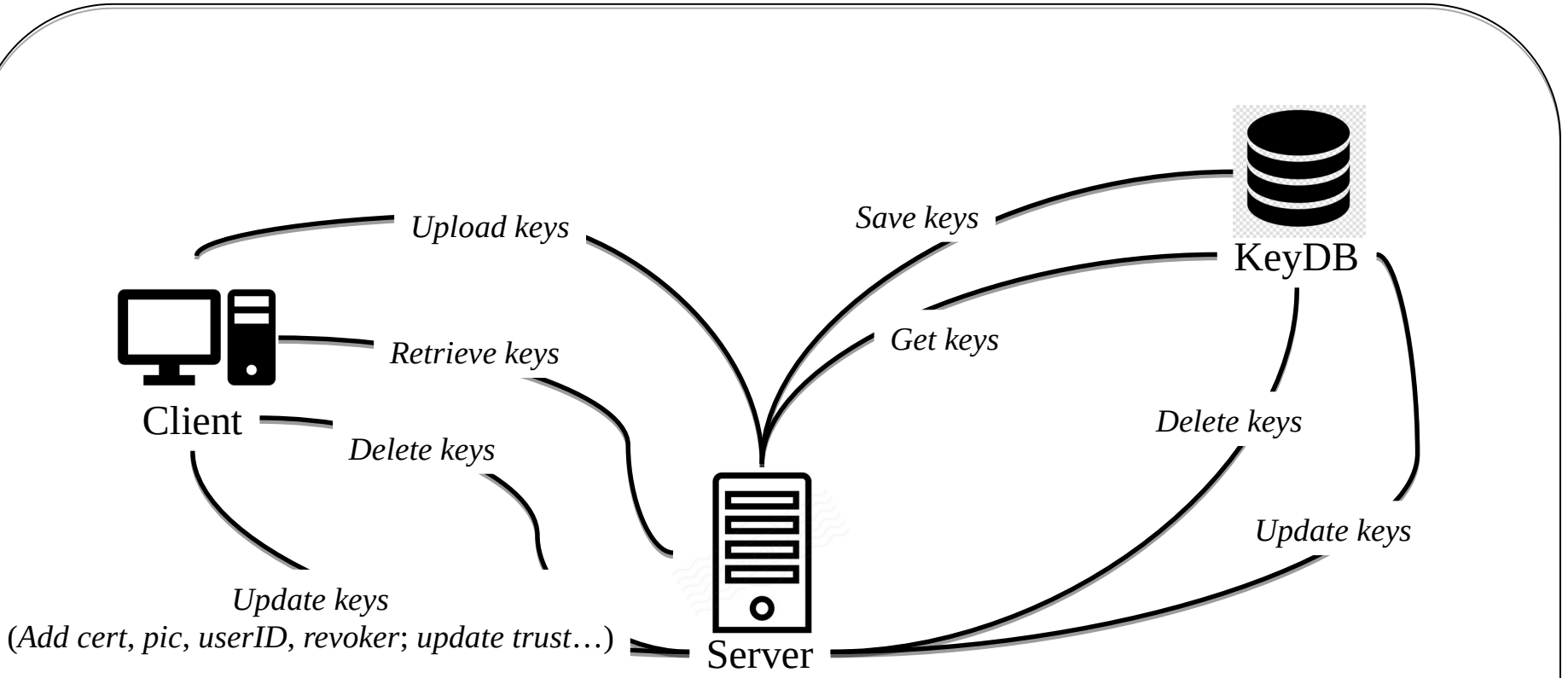
Verifying certificate following CA-hierarchical model

Public-key Infrastructure



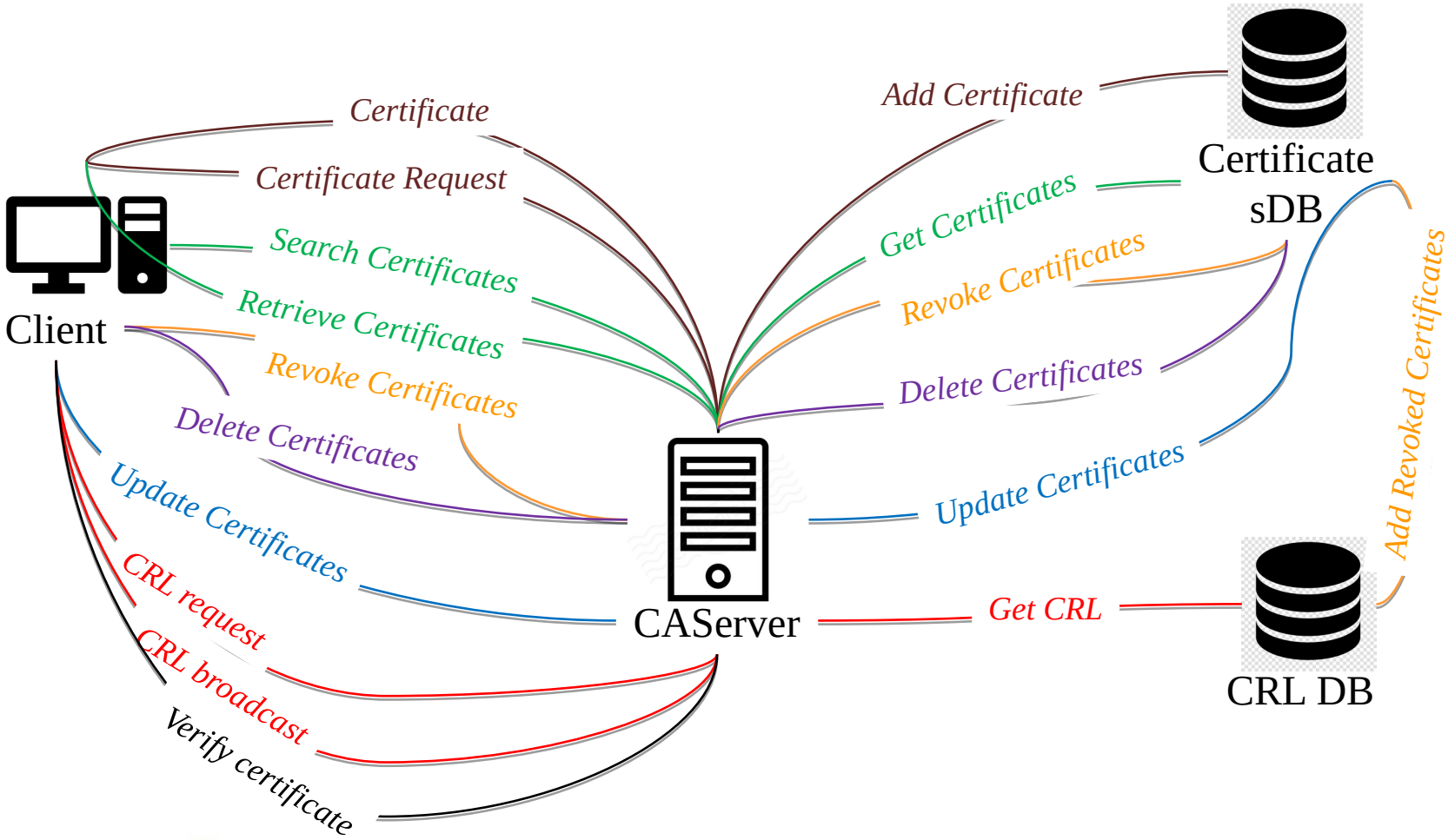
Basic PKI model

Key management model



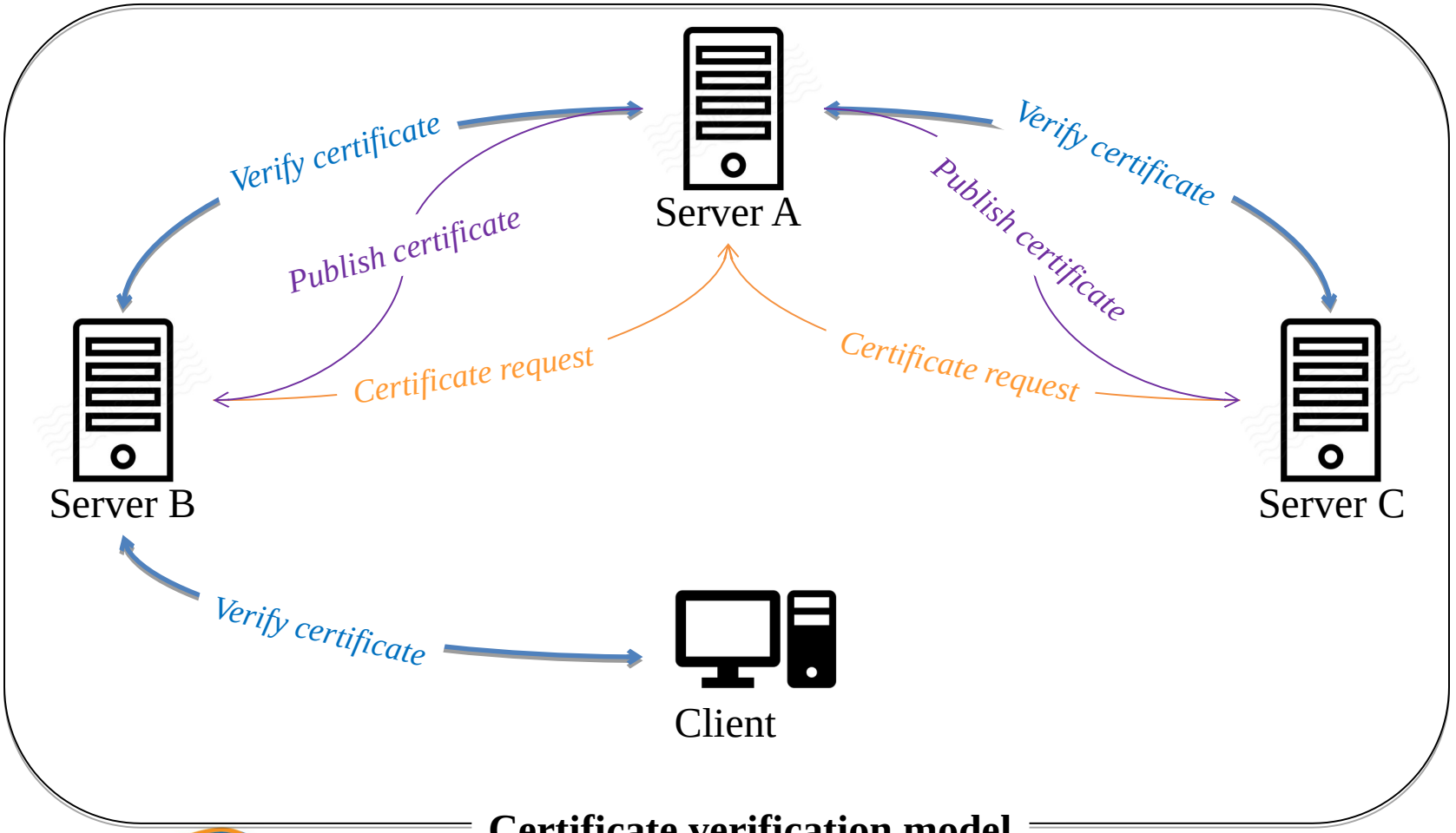
Key management model

Certificate management model



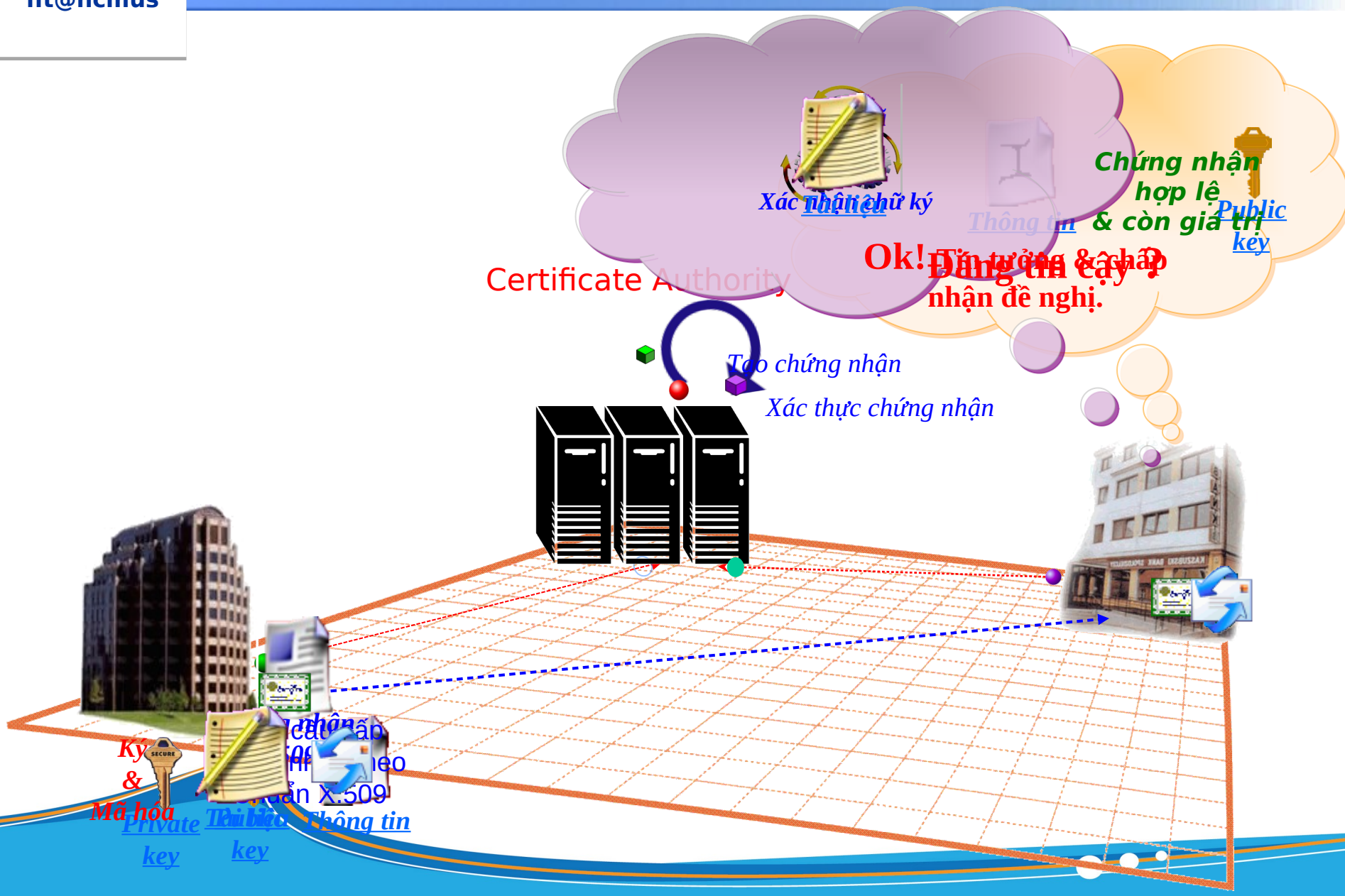
Certificate management model

Verification model of CA-hierarchical model

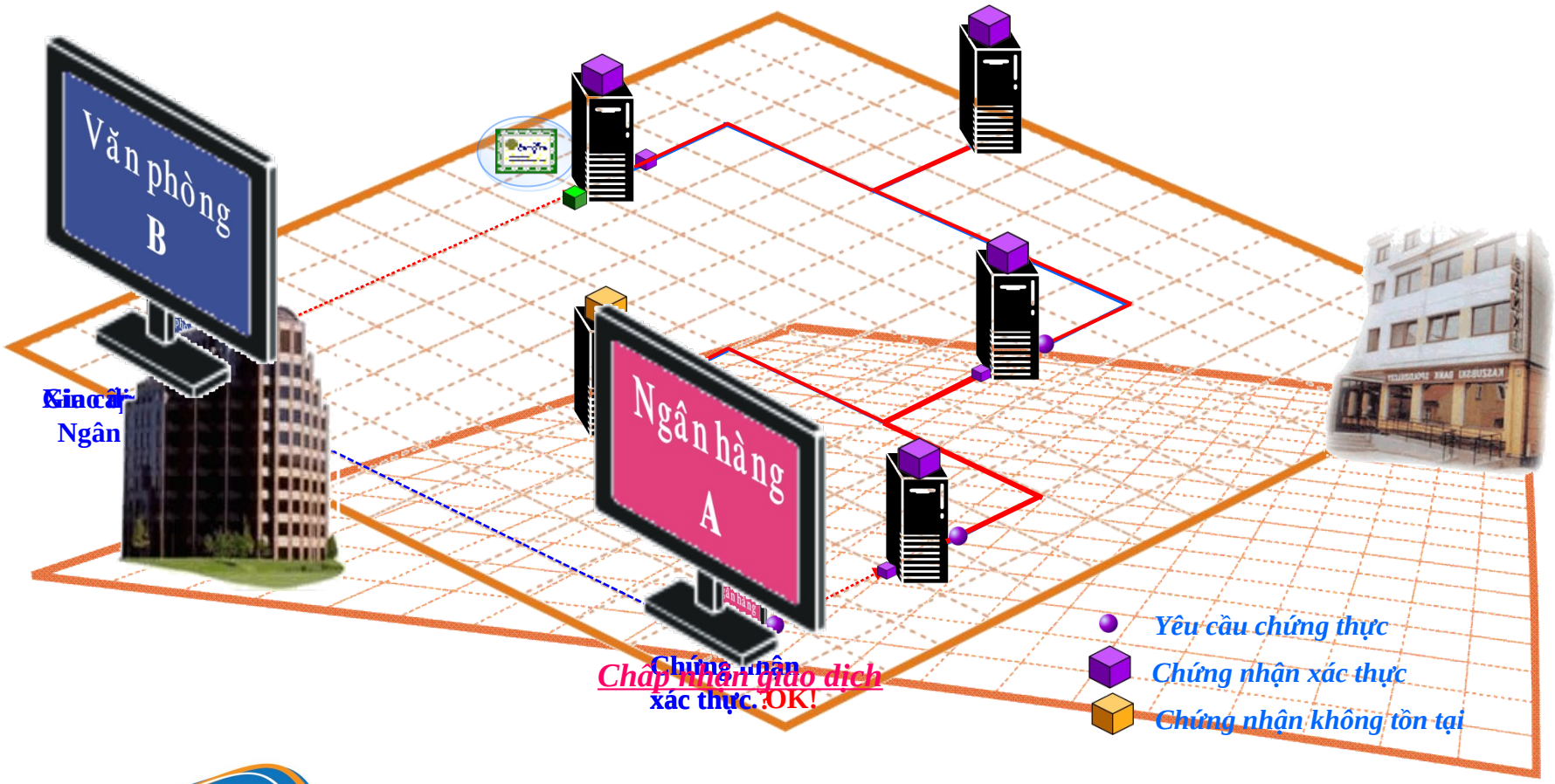


Certificate verification model

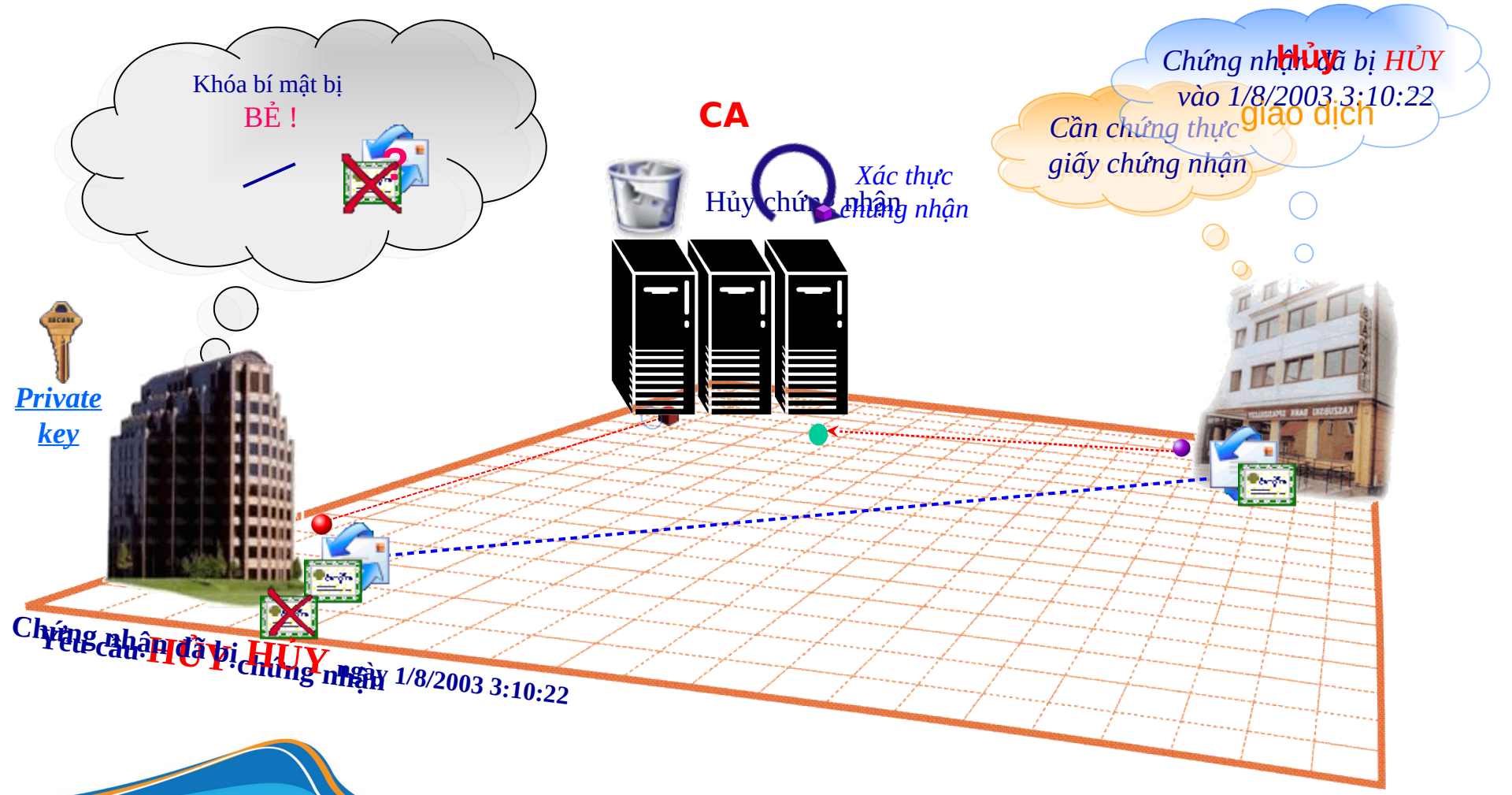
Demo 4


Xác nhận chữ ký
Thông tin
Chứng nhận hợp lệ & còn giá trị
Public key
Ok! Tin tưởng & chấp nhận đề nghị.
Đáng tin cậy ?
Certificate Authority
Tạo chứng nhận
Xác thực chứng nhận
Ký & Mã hóa
Private key
Public key
Thông tin

Demo 5


Văn phòng
B
Ngân hàng
A
Chấp nhận giao dịch
Yêu cầu chứng thực
Chứng nhận xác thực
Chứng nhận không tồn tại

Demo 6


Khóa bí mật bị
BẺ !
CA
Hủy chứng nhận
Xác thực
chứng nhận
Chứng nhận đã bị HỦY
vào 1/8/2003 3:10:22
Cần chứng thực
giấy chứng nhận
giao dịch
Private
key
Yêu cầu: HỦY chứng nhận ngày 1/8/2003 3:10:22