# Chủ đề 9:
# Chứng nhận khóa công &
# Tổ chức chứng nhận khóa công
# (Digital Certificate &Certificate Authority)

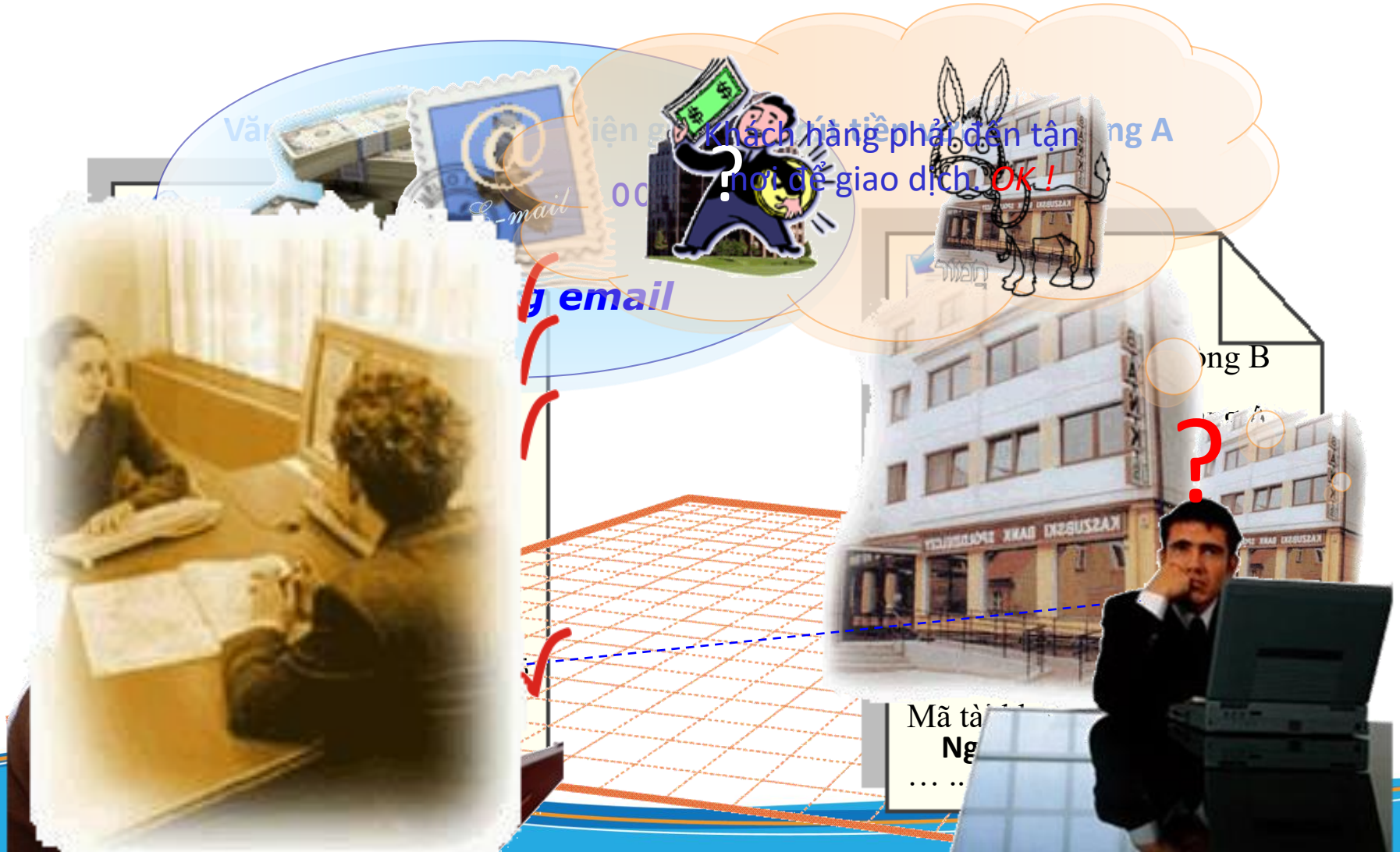
PGS.TS. Trần Minh Triết


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

# Nội dung

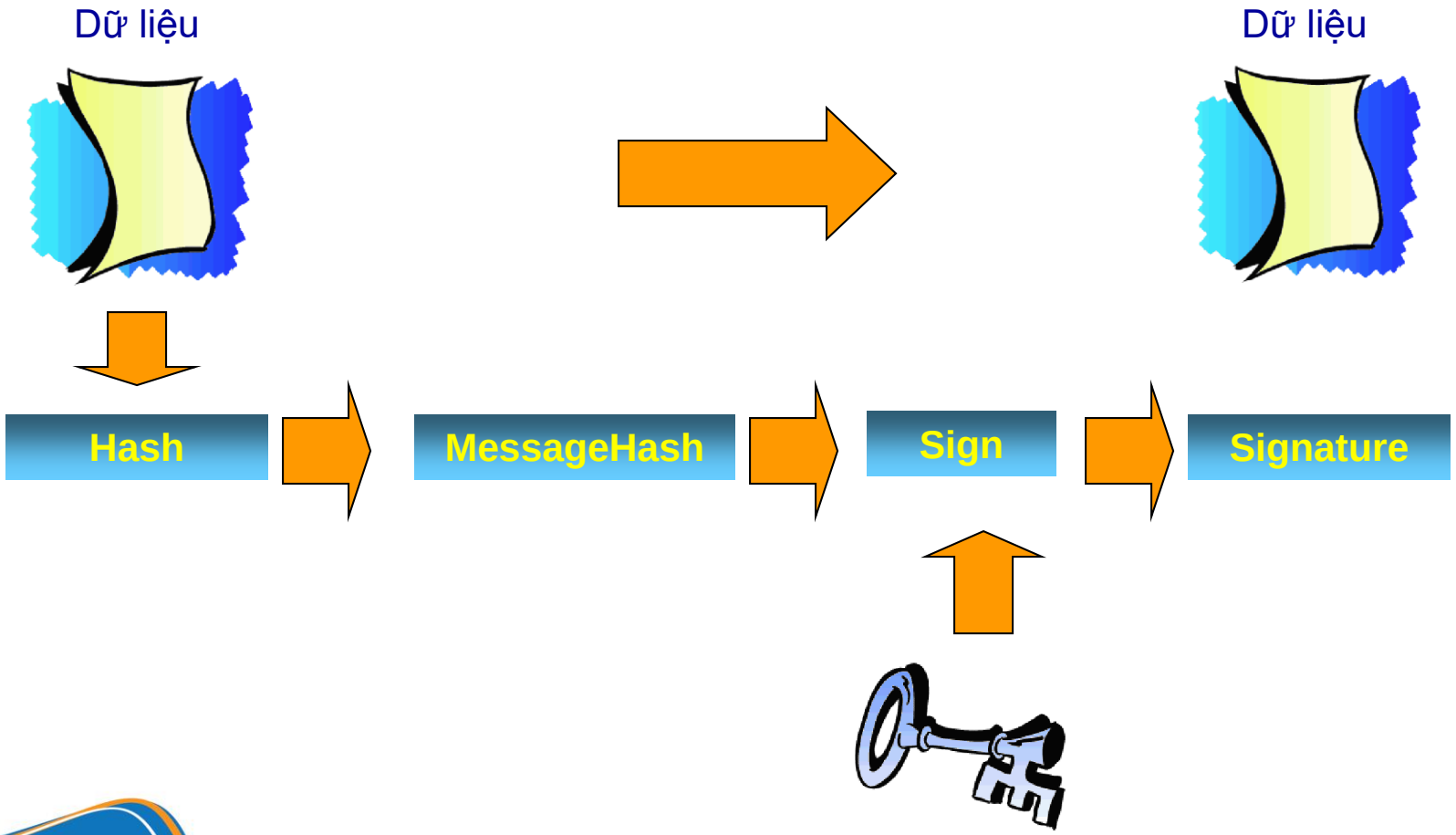
- Mở đầu
- Chữ ký điện tử
- Chứng nhận số
- Certificate Authority (CA)
- Mô hình PKI
- Ứng dụng…

# Demo1



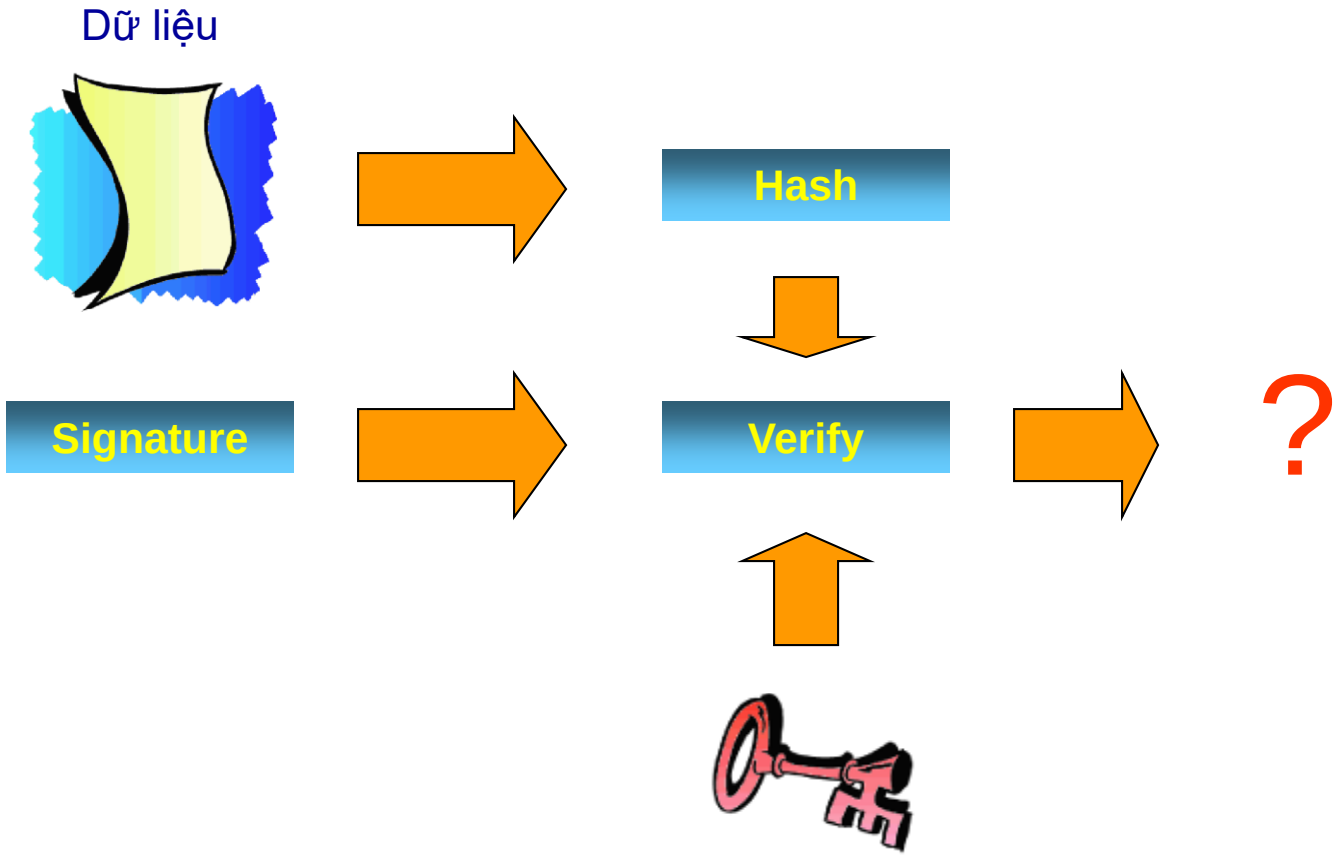
# Nhắc lại về Chữ ký điện tử

## Tạo chữ ký



# Nhắc lại về Chữ ký điện tử

Kiểm tra chữ ký

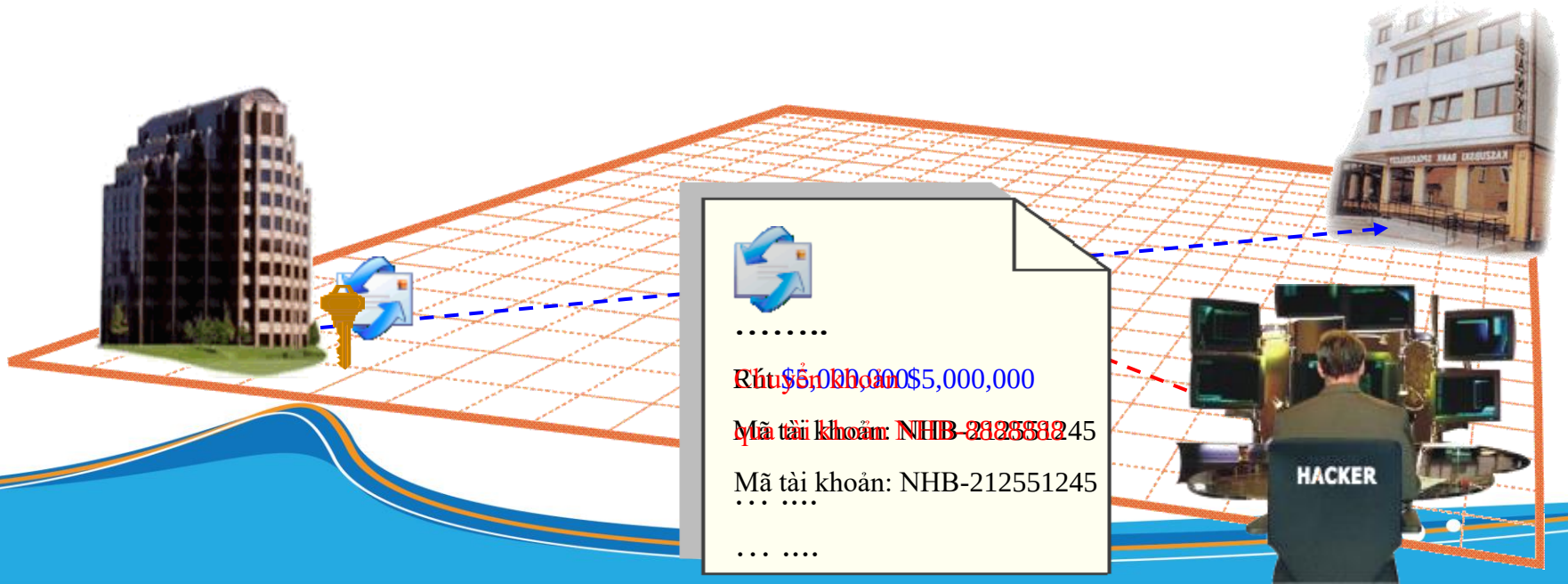


# Demo2


Giải mã & kiểm tra chữ ký
Ok! Chấp nhận yêu cầu & gửi tiền
email
Mã hóa & Ký
Người gửi: Văn phòng B
Người nhận: Ngân hàng A
Ngày gửi: 1 / 8 / 2003
Người gửi: Văn phòng B

# Demo3

Dữ liệu bị tấn công trên đường truyền.
MIM (Man in Middle)

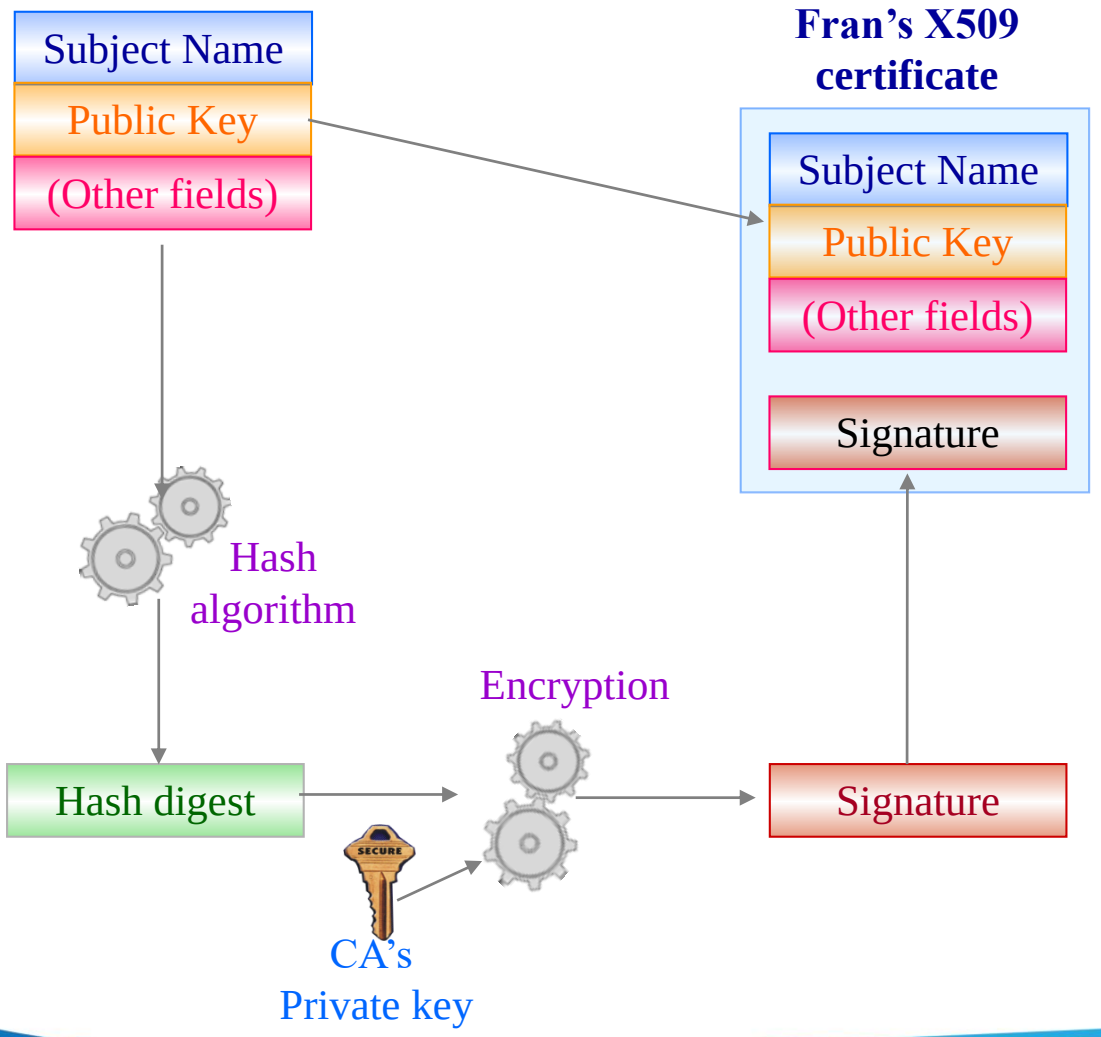



# Digital Certificate

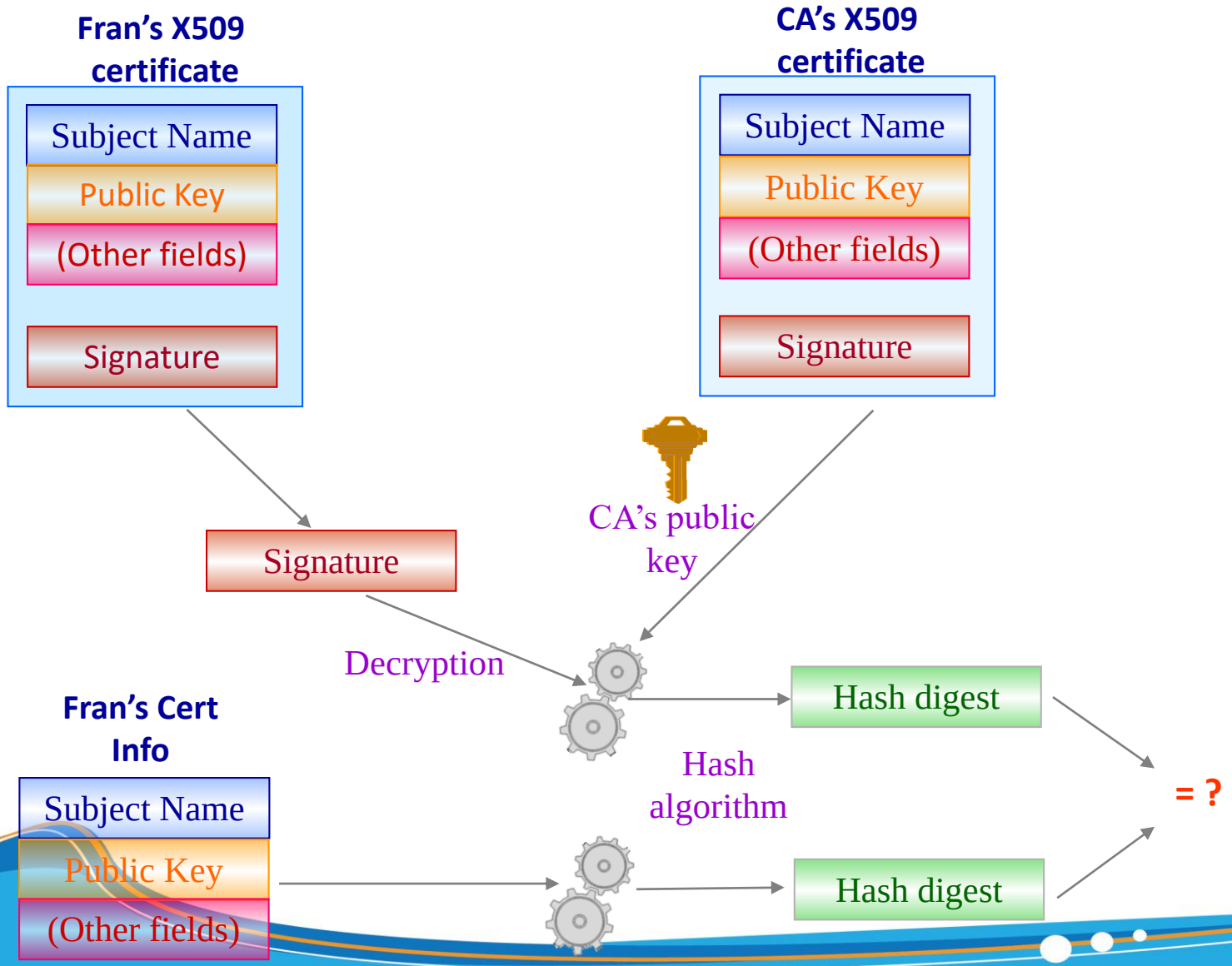
- Chứng nhận điện tử là chứng thực sự sở hữu khóa công khai


→ **Chứng nhận điện tử giải quyết được vấn đề MIM**

# Tạo chứng nhận

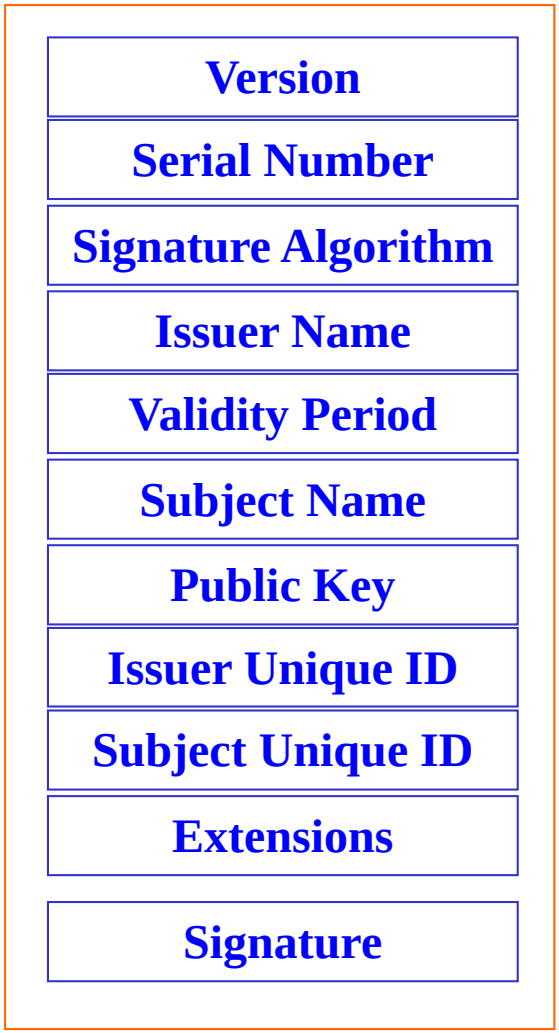


# Kiểm tra chứng nhận



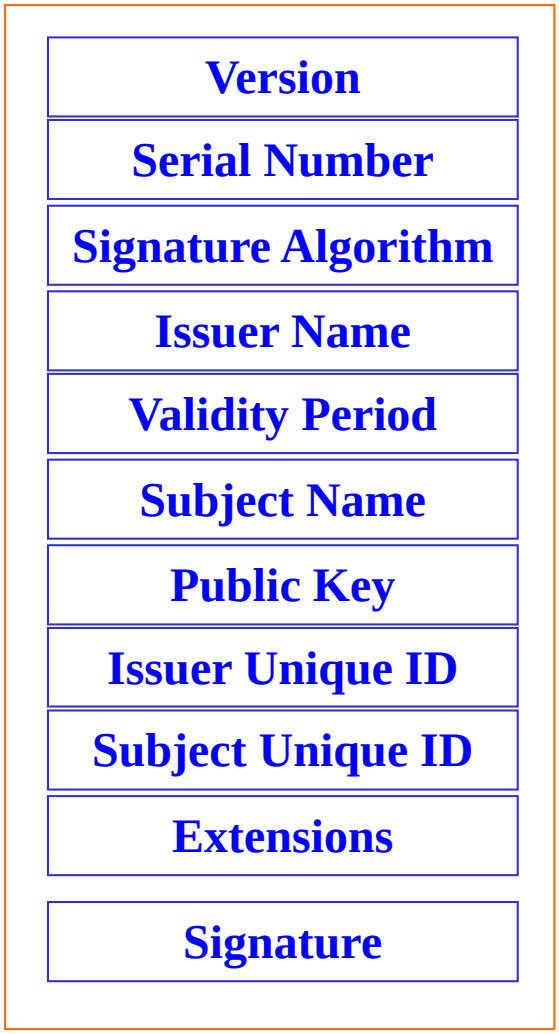
# Chuẩn X.509 (ver. 3.0)

- *Version*: Chỉ định phiên bản của chứng nhận X.509.
- *Serial Number*: Số loạt phát hành được gán bởi CA. Mỗi CA nên gán một mã số loạt duy nhất cho mỗi giấy chứng nhận mà nó phát hành.
- *Signature Algorithm*: Thuật toán chữ ký chỉ rõ thuật toán mã hóa được CA sử dụng để ký giấy chứng nhận. Trong chứng nhận X.509 thường là sự kết hợp giữa thuật toán băm (chẳng hạn như MD5) và thuật toán khóa công cộng (chẳng hạn như RSA).



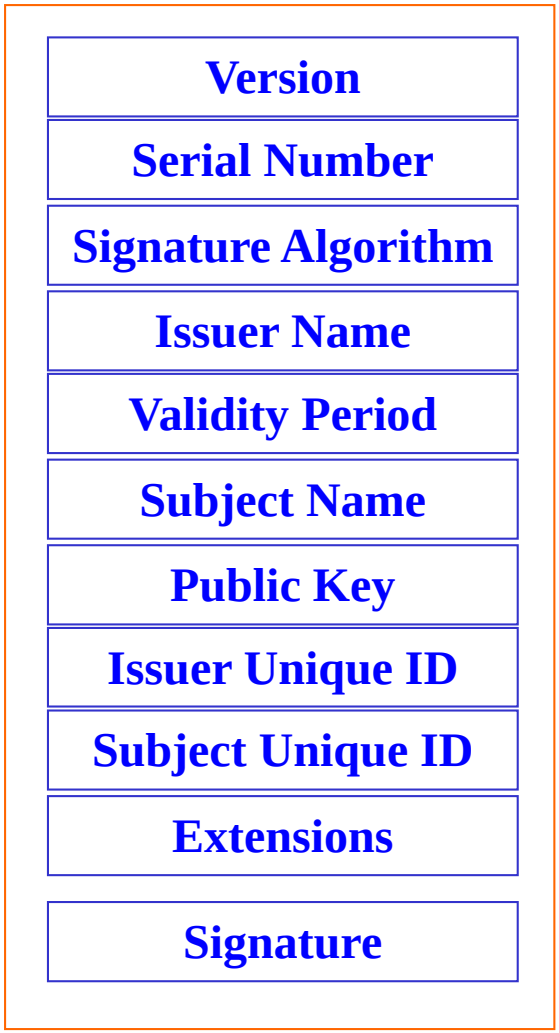
# Chuẩn X.509 (ver. 3.0)

- *Issuer Name*: Tên tổ chức CA phát hành giấy chứng nhận, đây là một tên phân biệt theo chuẩn X.500 (X.500 Distinguised Name – X.500 DN). Hai CA không được sử dụng cùng một tên phát hành.
- *Validity Period*: Trường này bao gồm hai giá trị chỉ định khoảng thời gian mà giấy chứng nhận có hiệu lực. Hai phần của trường này là not-before và not-after. Not-before chỉ định thời gian mà chứng nhận này bắt đầu có hiệu lực, Not-after chỉ định thời gian mà chứng nhận hết hiệu lực. Các giá trị thời gian này được đo theo chuẩn thời gian Quốc tế, chính xác đến từng giây.



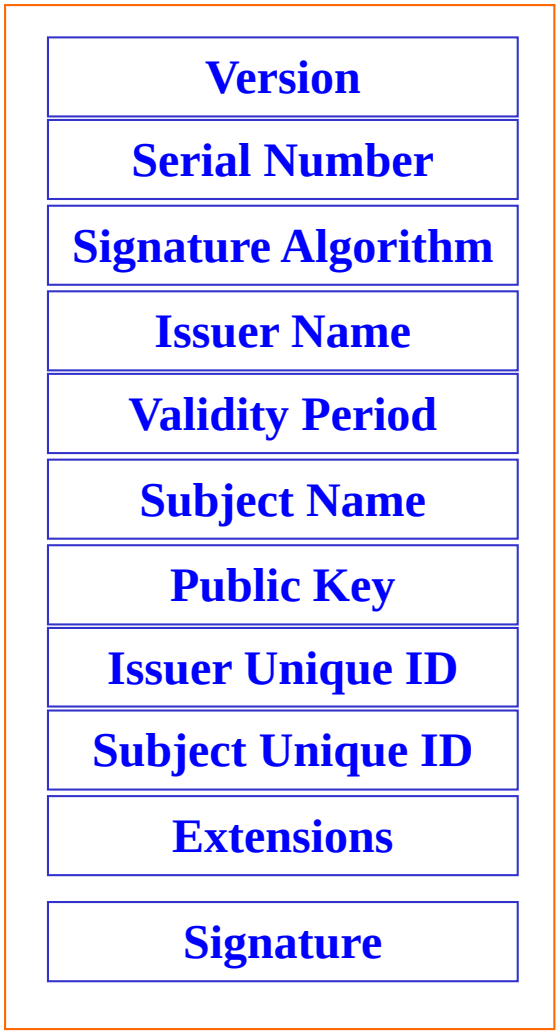
# Chuẩn X.509 (ver. 3.0)

- *Issuer Unique ID* và *Subject Unique ID*: Hai trường này được giới thiệu trong X.509 phiên bản 2, được dùng để xác định hai tổ chức CA hoặc hai chủ thể khi chúng có cùng DN. RFC 2459 đề nghị không nên sử dụng hai trường này.
- *Extensions*: Chứa các thông tin bổ sung cần thiết mà người thao tác CA muốn đặt vào chứng nhận. Trường này được giới thiệu trong X.509 phiên bản 3.



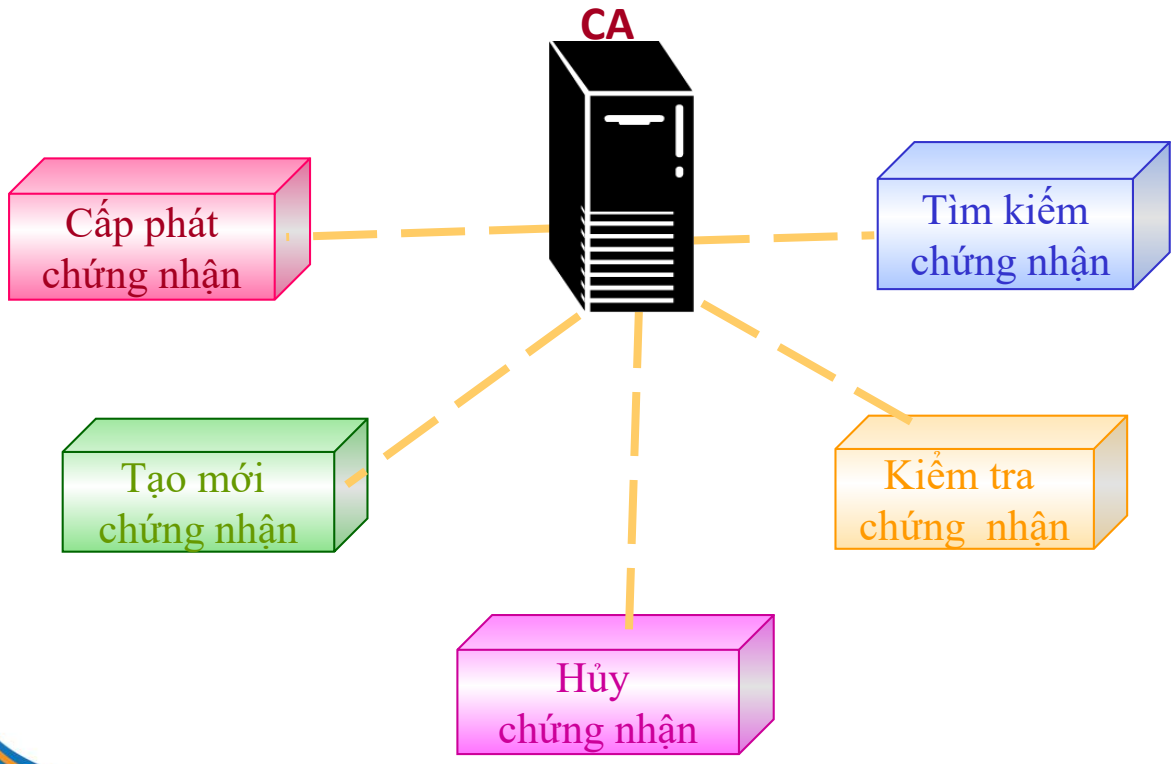
# Chuẩn X.509 (ver. 3.0)

- *Signature*: Đây là chữ ký điện tử được tổ chức CA áp dụng. Tổ chức CA sử dụng khóa bí mật có kiểu quy định trong trường thuật toán chữ ký. Chữ ký bao gồm tất cả các phần khác trong giấy chứng nhận. Do đó, tổ chức CA chứng nhận cho tất cả các thông tin khác trong giấy chứng nhận chứ không chỉ cho tên chủ thể và khóa công cộng.

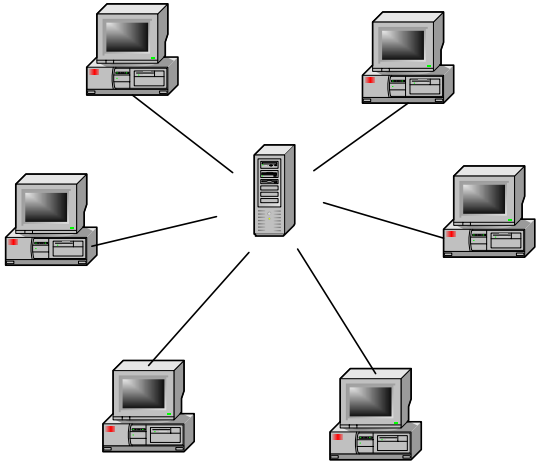


# Certificate Authority System

- Một tổ chức thứ ba đáng tin cậy
- Quản lý chữ ký điện tử
- Quản lý chứng nhận số

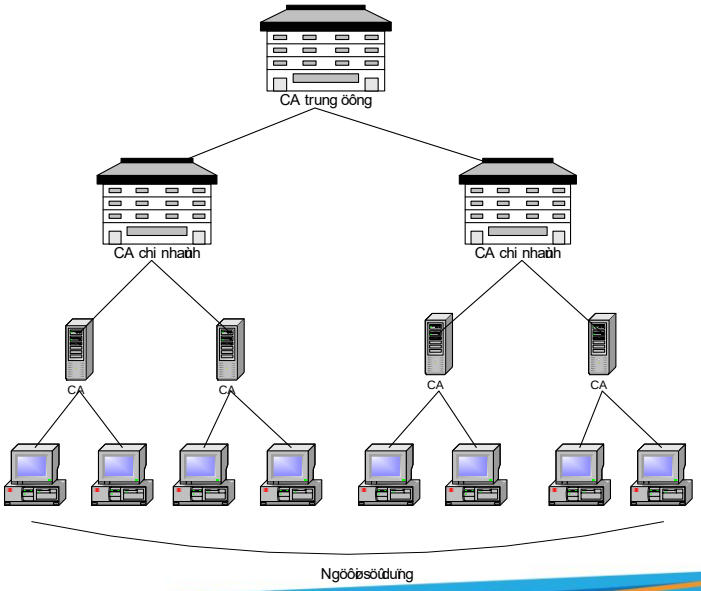


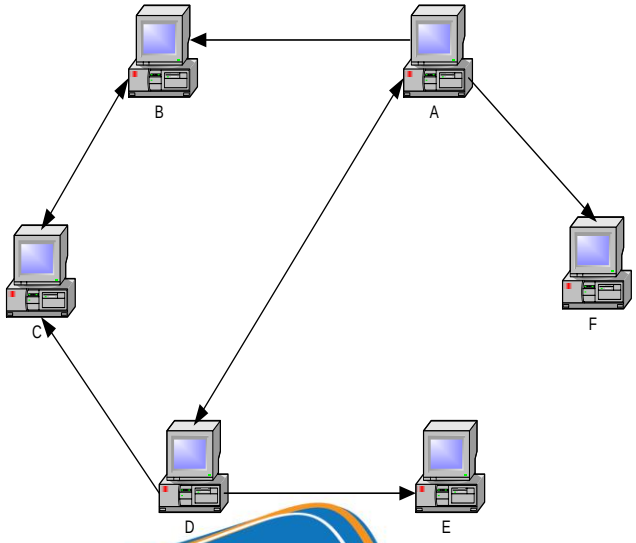
# Certificate Authority System CA(S)



**Mô hình tập trung**

**Mô hình phân cấp**

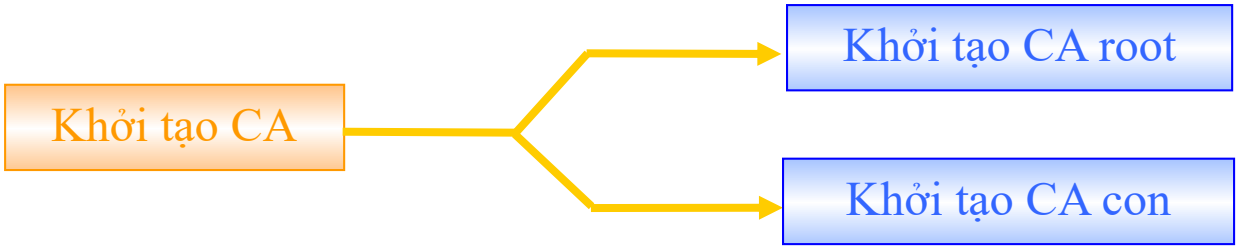


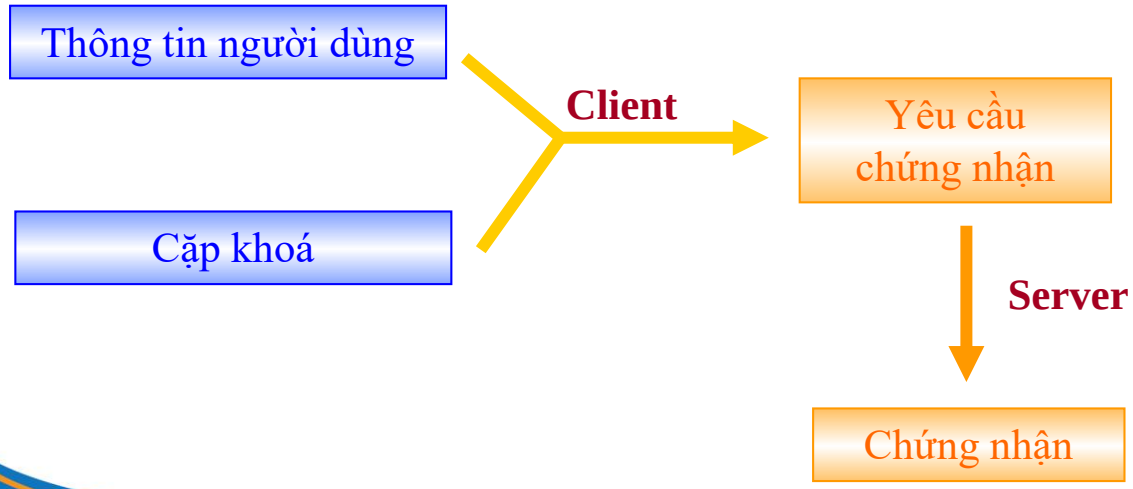

**Web of Trust**

# Certificate Authority System CA(S)

## Initialize CA

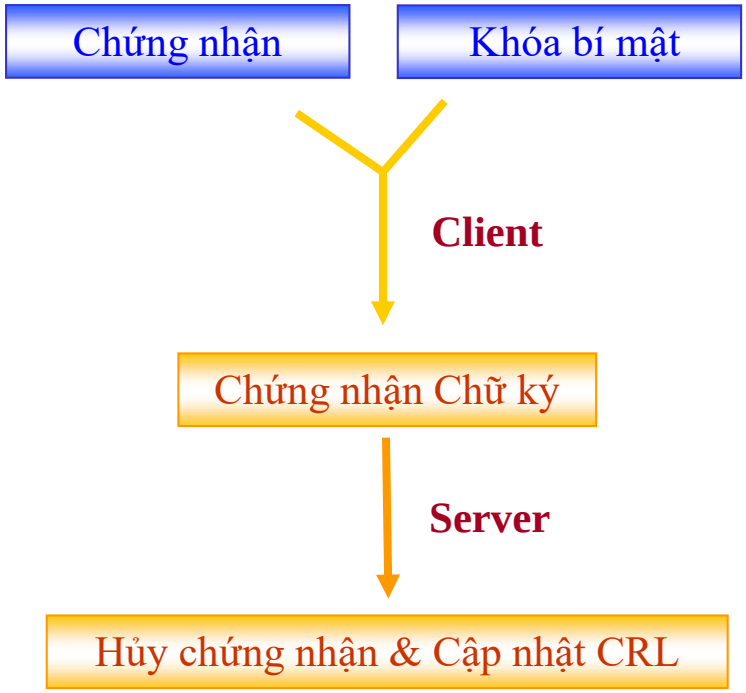


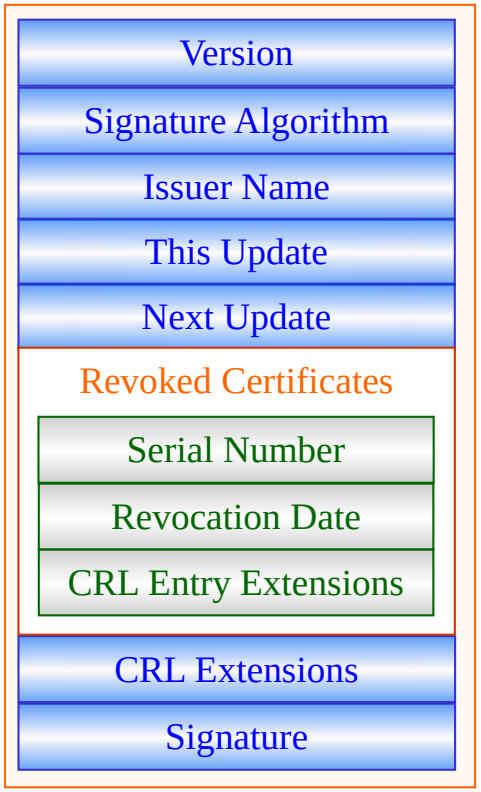

## Create Cert



# Certificate Authority System – CA(S)

## Revoke Cert

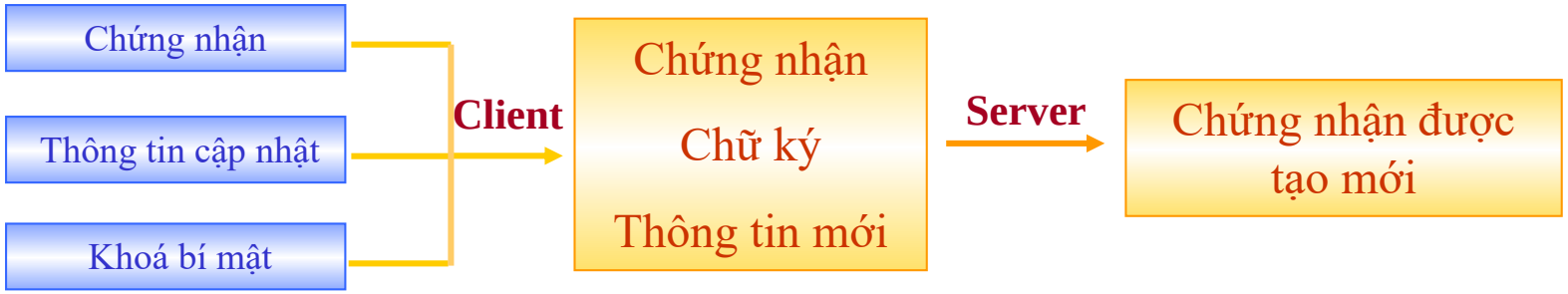


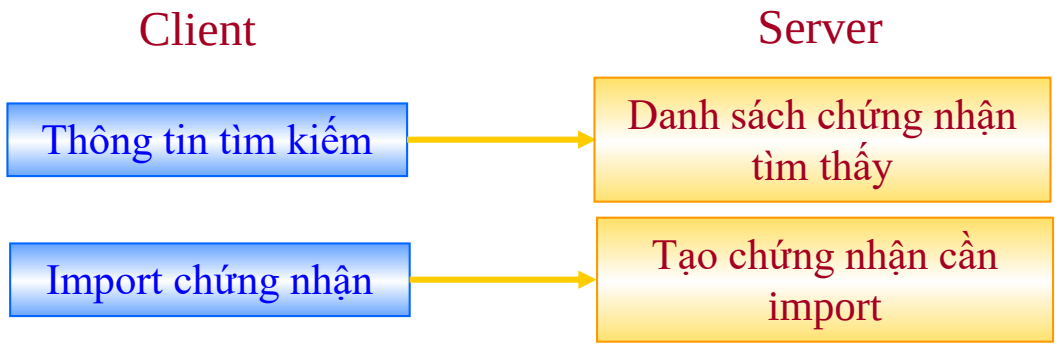

*Phiên bản 2 theo chuẩn của CRL*

# Certificate Authority System – CA(S)

## Update Cert

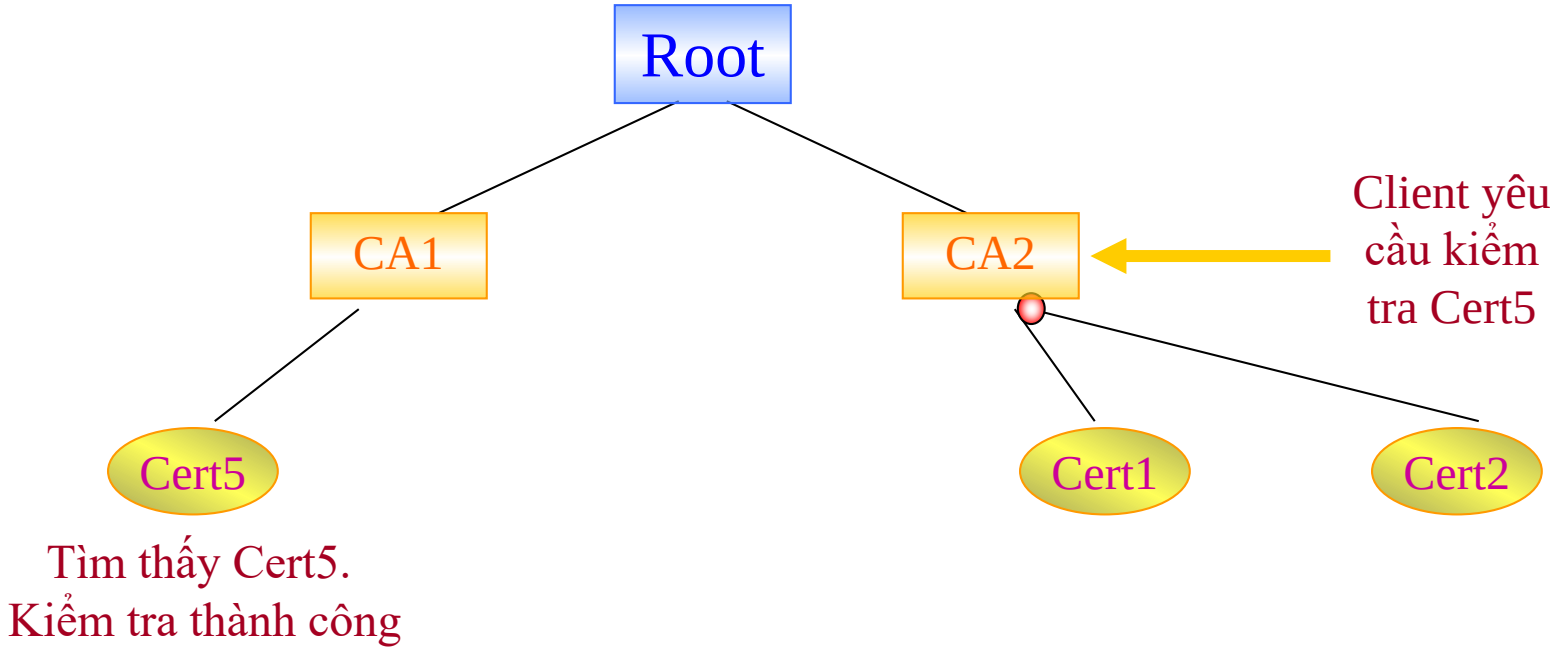



## Search Cert



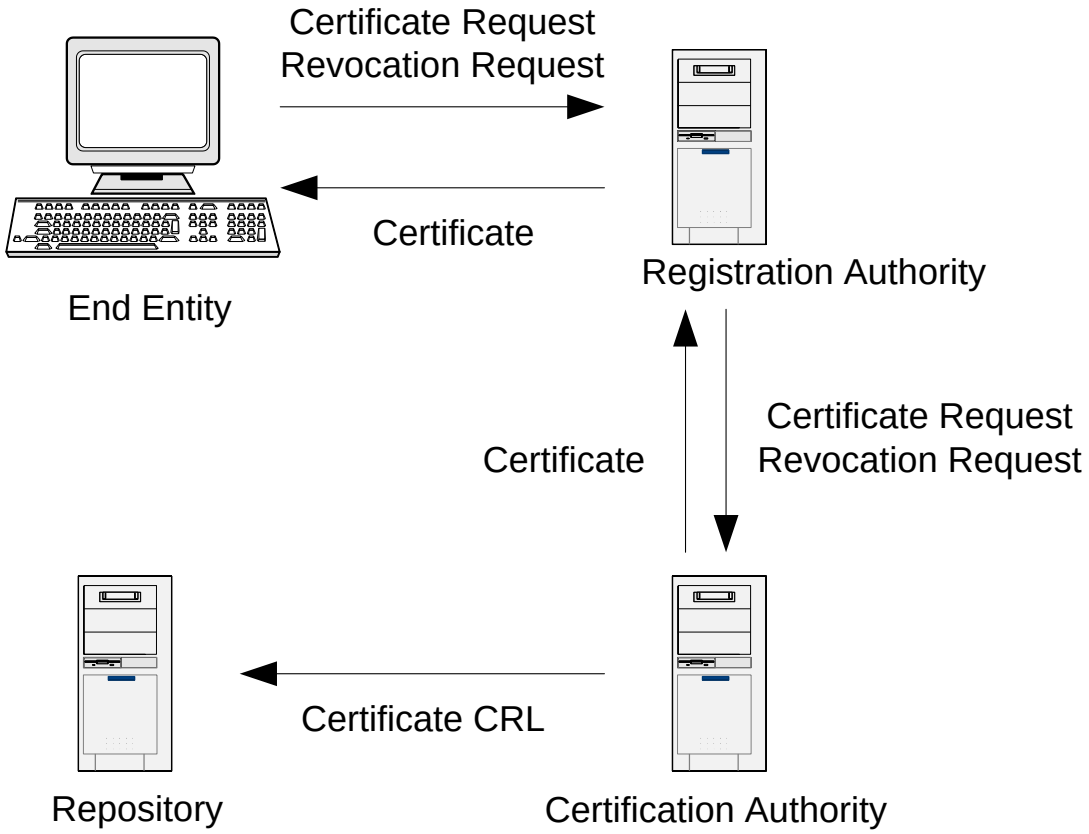
# Certificate Authority System – CA(S)

## Verify Cert



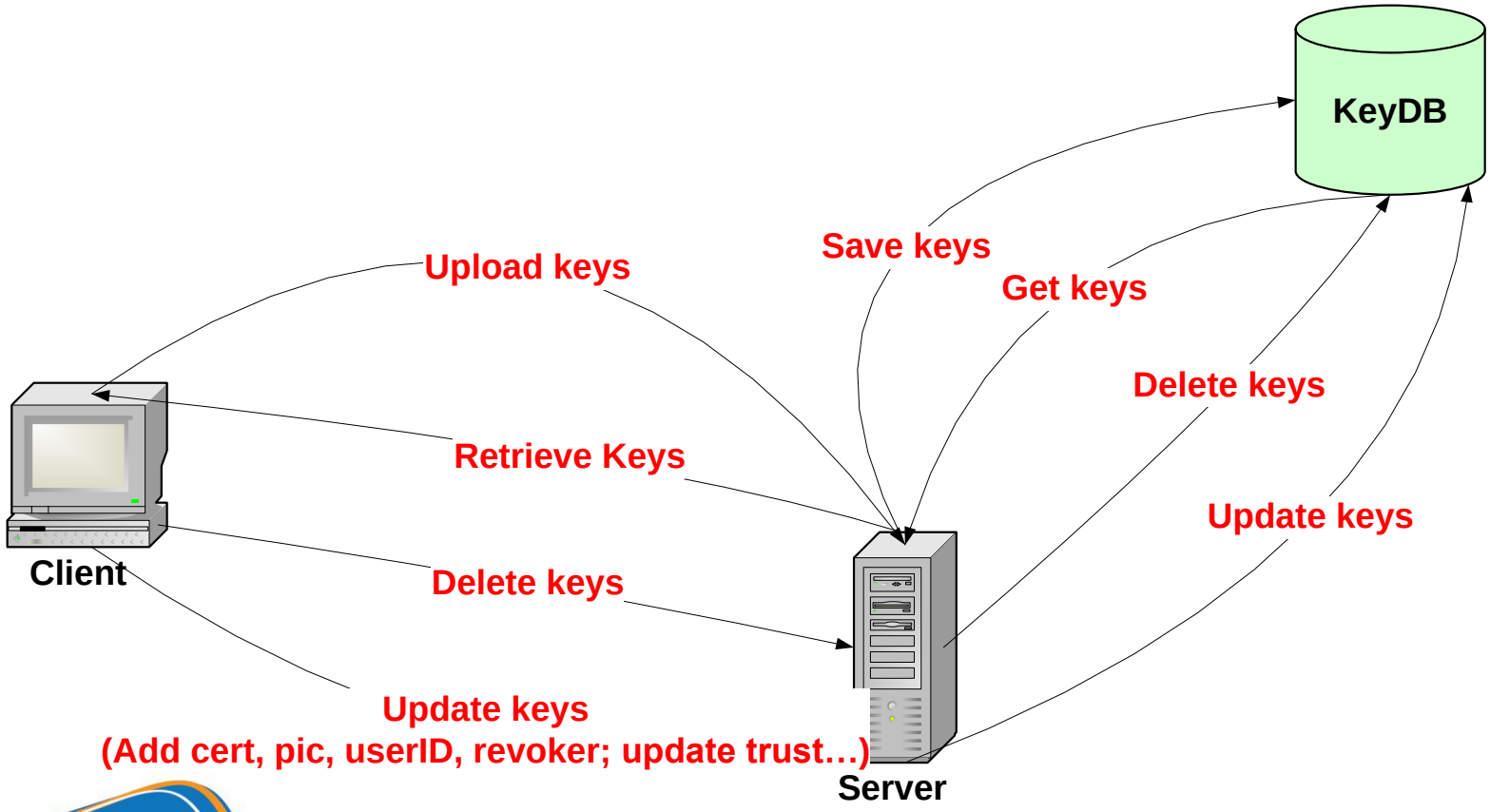

*Kiểm tra chứng nhận theo mô hình CA phân cấp*

# Public-key Infrastructure



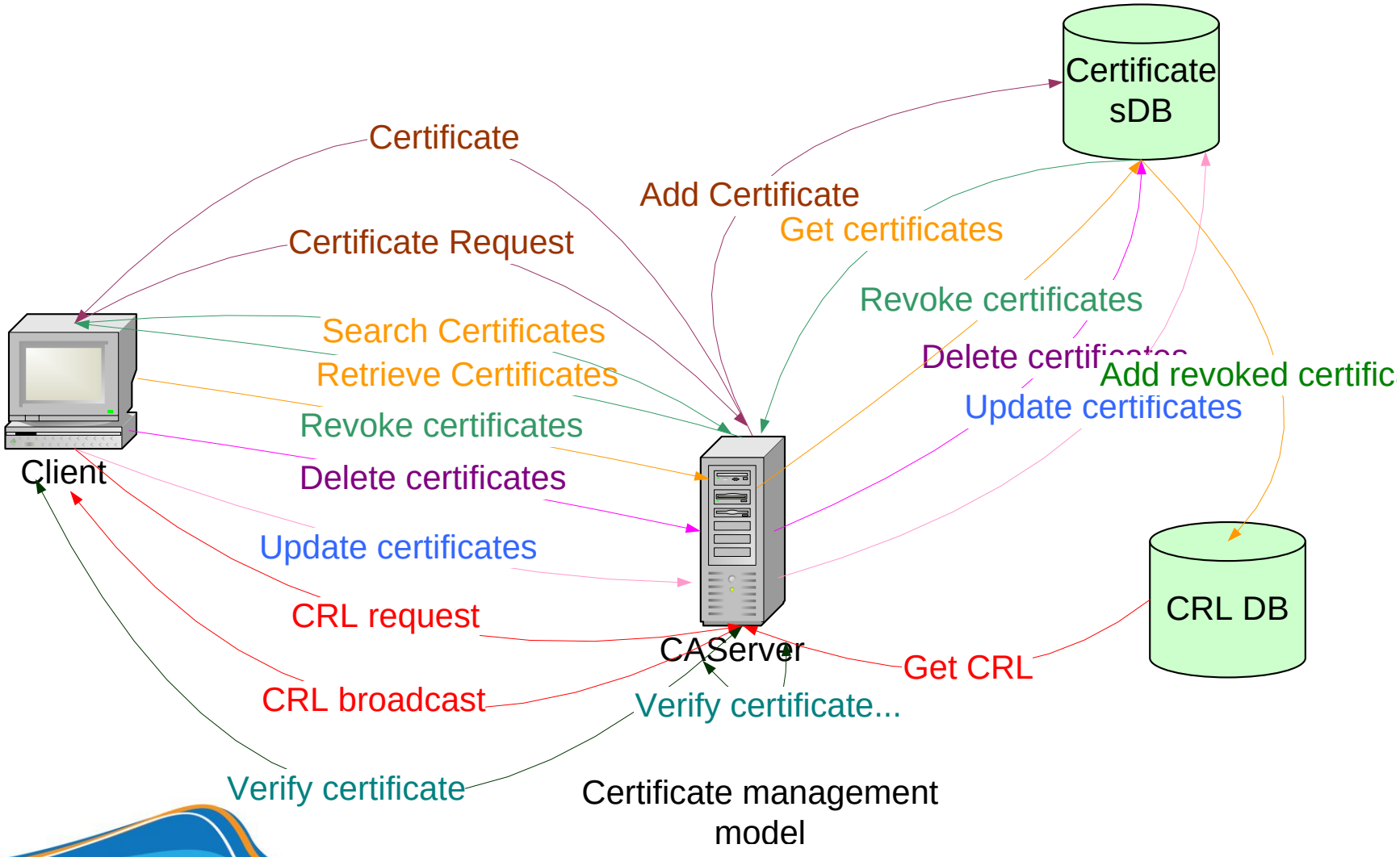

*Moâhình PKI cô baûn*

# Mô hình quản lý khóa

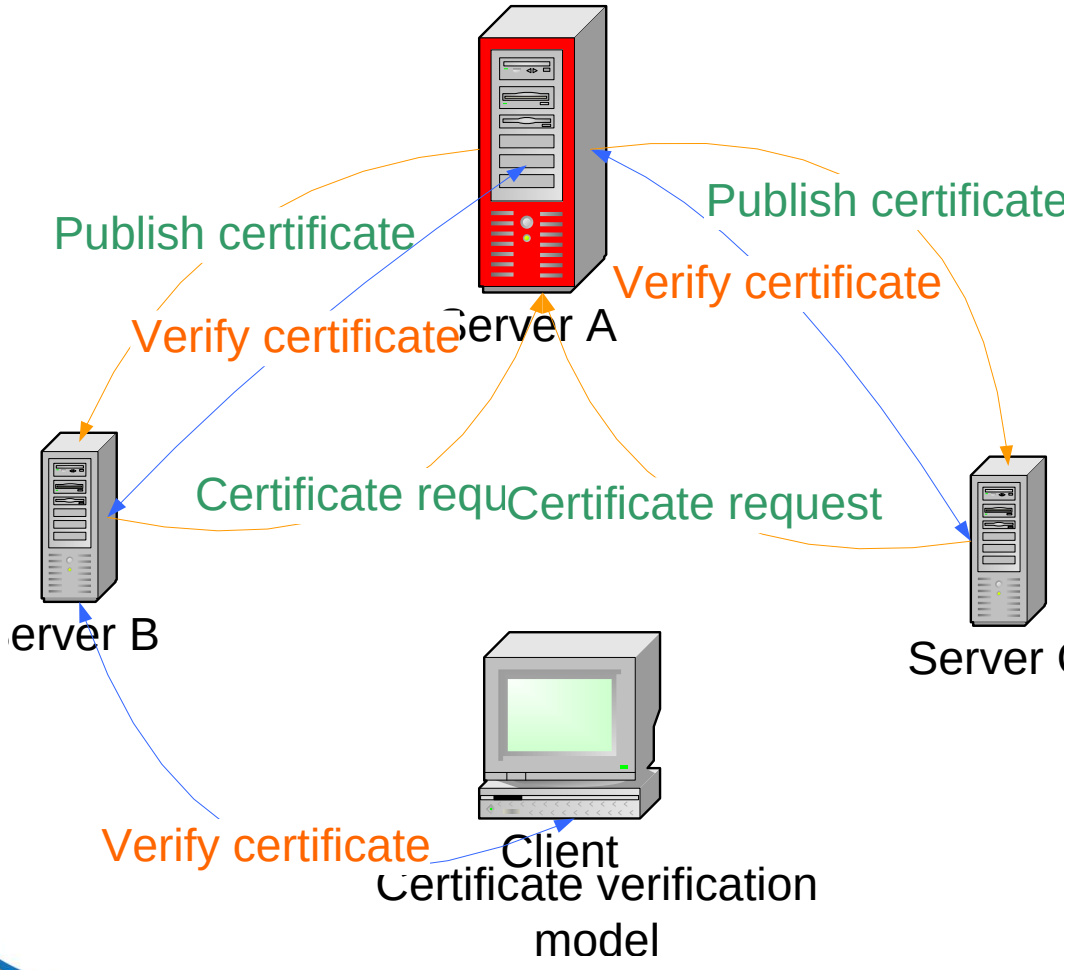



Key management model

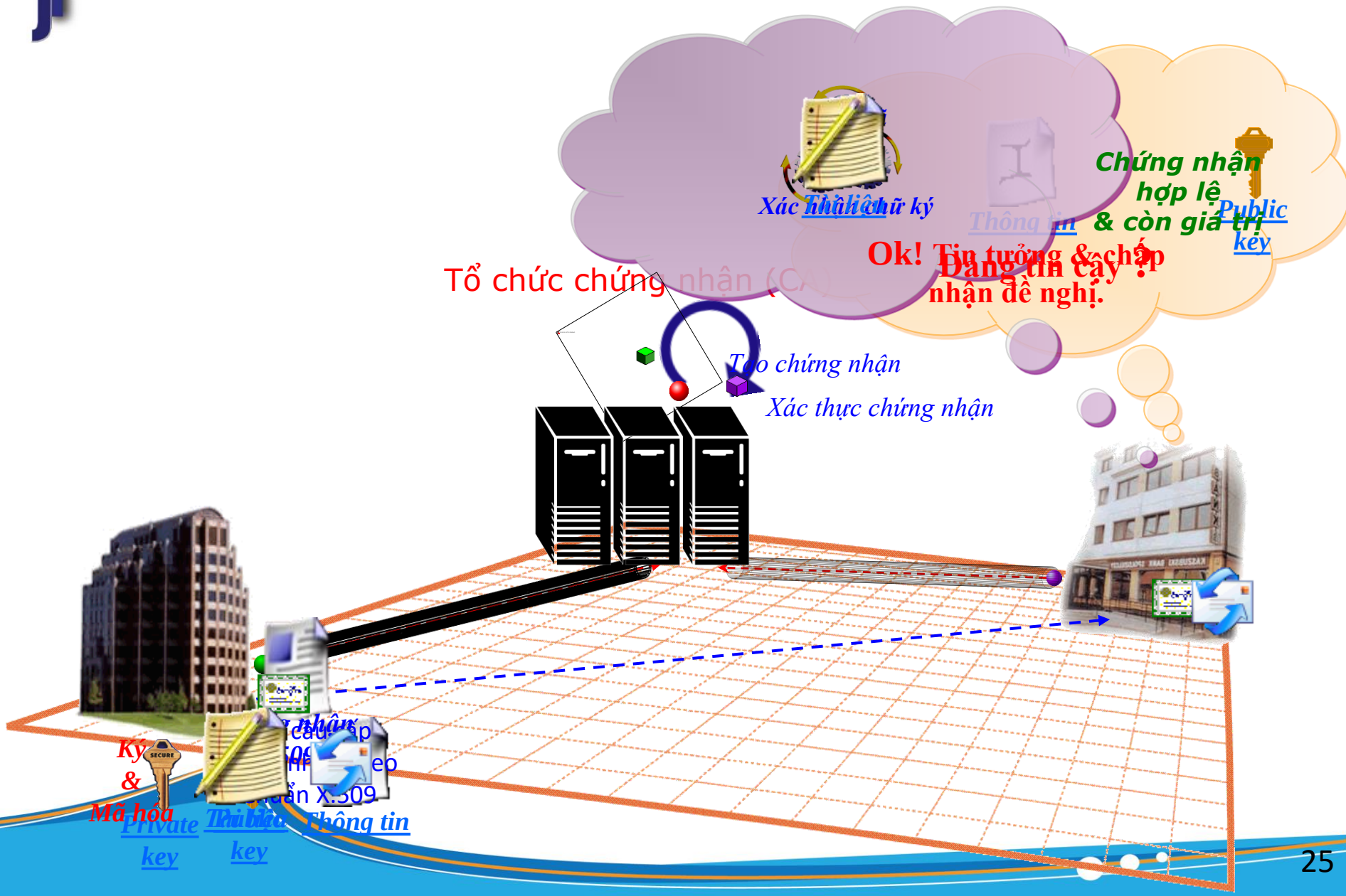
# Mô hình quản lý chứng nhận



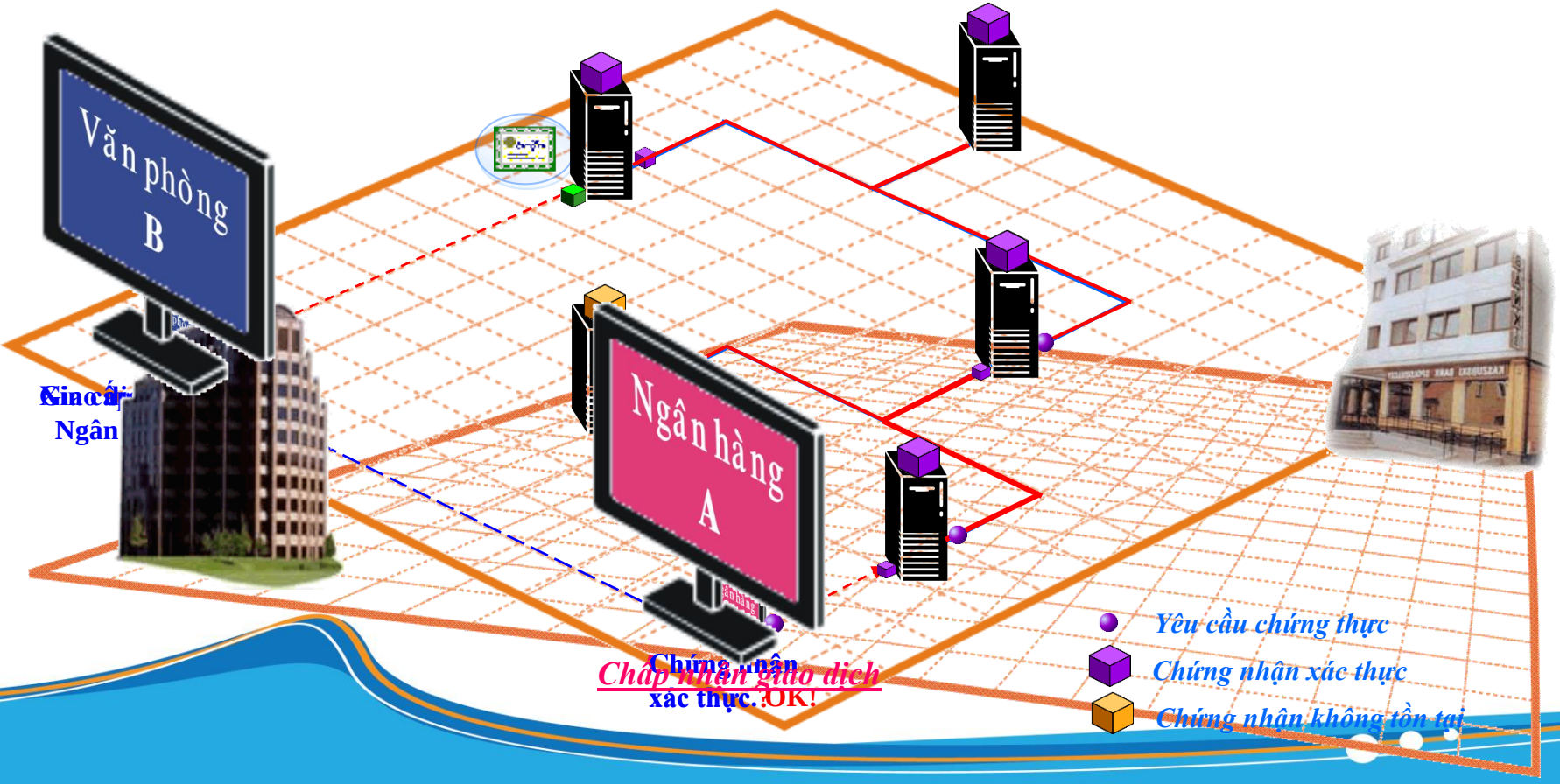
# Mô hình chứng thực phân cấp



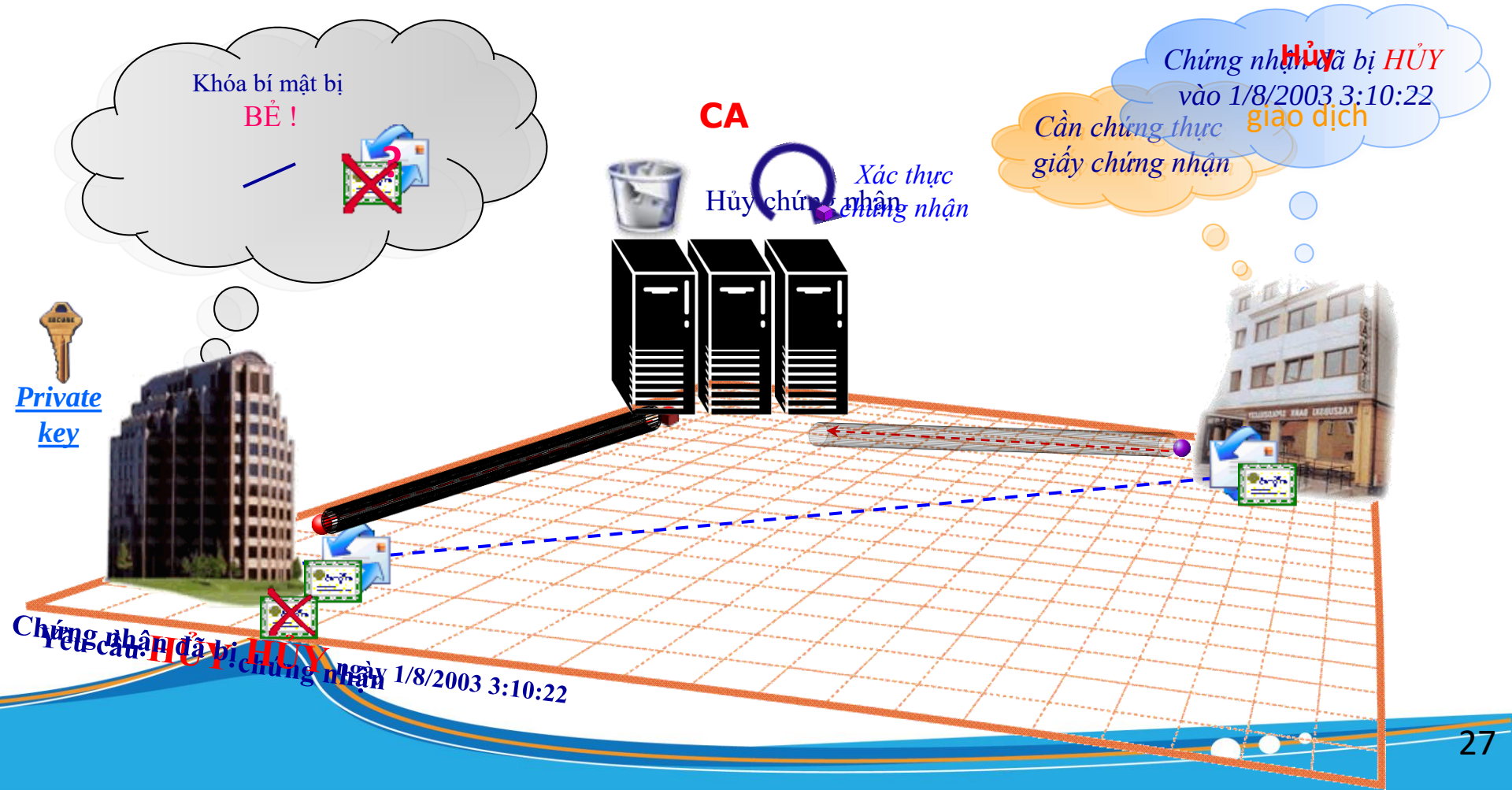
# Demo4


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 !
Tổ chức chứng nhận (CA)
Tạo chứng nhận
Xác thực chứng nhận
Ký & Mã hóa
Private key
Public key
Thông tin

# Demo5


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

# Demo6


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
Hủy
giao dịch
Cần chứng thực
giấy chứng nhận
Private
key
Chứng nhận đã bị HỦY
Yêu cầu: HỦY chứng nhận
ngày 1/8/2003 3:10:22