HUTECH

Đại học Công nghệ Tp.HCM

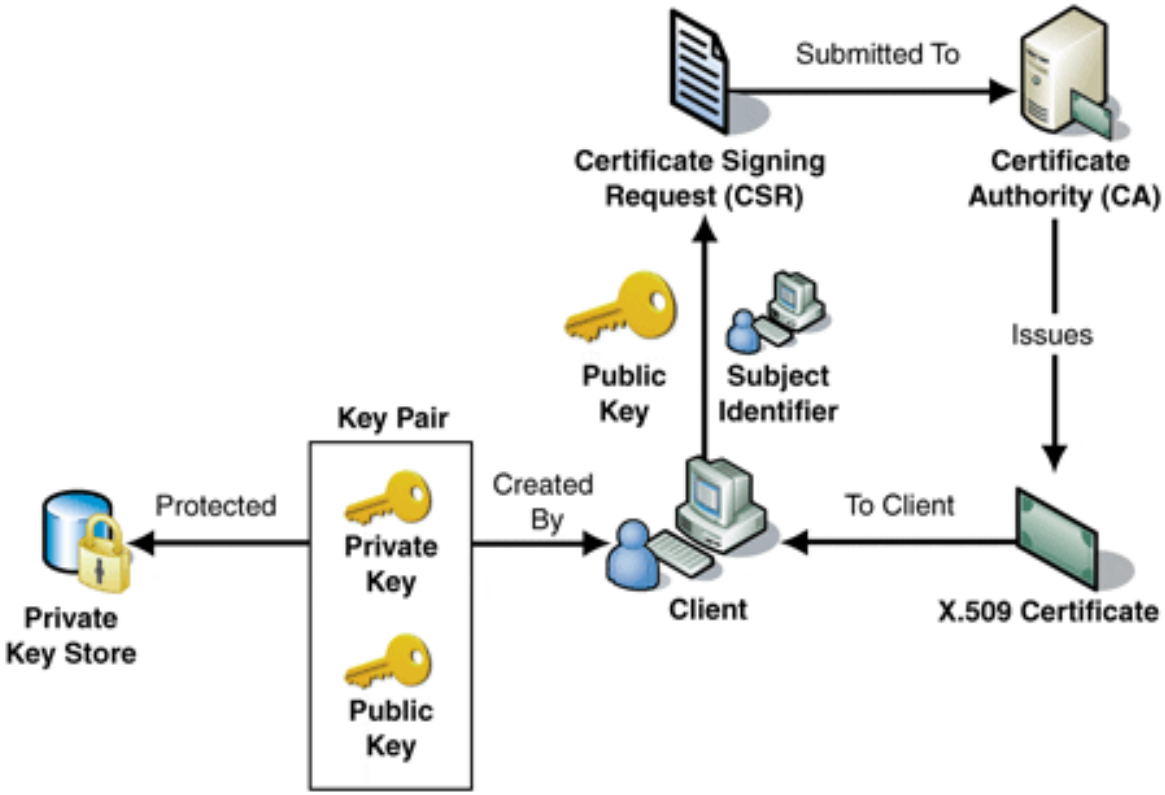
Bài 8:
Bảo mật Web & Email

Trình bày:
Ths. Lương Trần Hy Hiến
http://hienlth.info/hutech/baomatthongtin

Nội dung

1. Dịch vụ xác thực X.509
2. Giao thức bảo mật Web SSL
3. Bảo mật email PGP

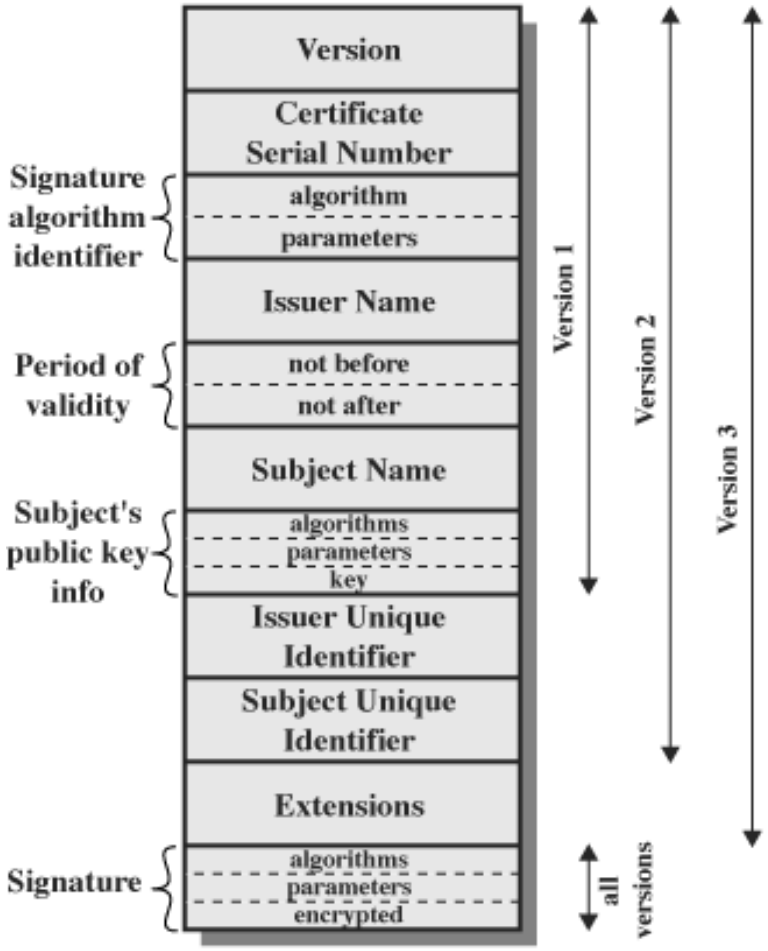
1. Dịch vụ xác thực X.509



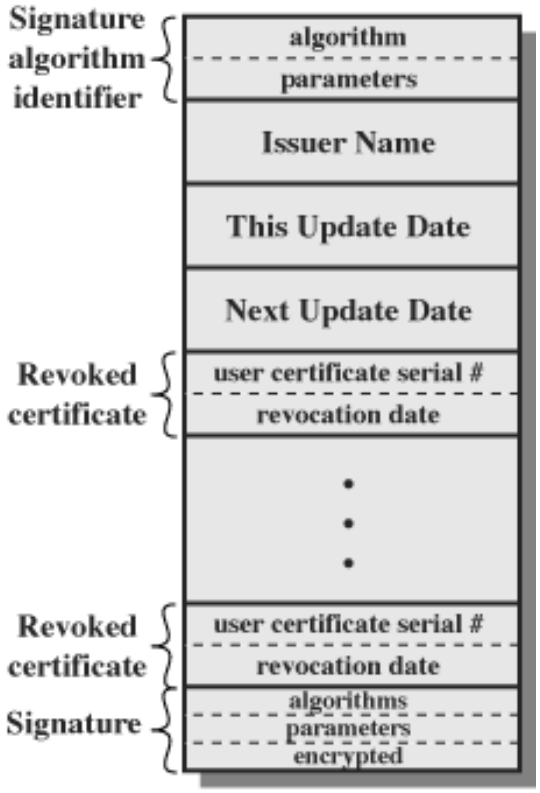
Dịch vụ xác thực X.509

- Nằm trong loạt khuyến nghị X.500 của ITU-T nhằm chuẩn hóa dịch vụ thư mục
  - Servers phân tán lưu giữ CSDL thông tin người dùng
- Định ra một cơ cấu cho dịch vụ xác thực
  - Danh bạ chứa các chứng thực khóa công khai
  - Mỗi chứng thực bao gồm khóa công khai của người dùng ký bởi một bên chuyên trách chứng thực đáng tin
- Định ra các giao thức xác thực
- Sử dụng mật mã khóa công khai và chữ ký số
  - Không chuẩn hóa giải thuật nhưng RSA khuyến nghị

Khuôn dạng X.509

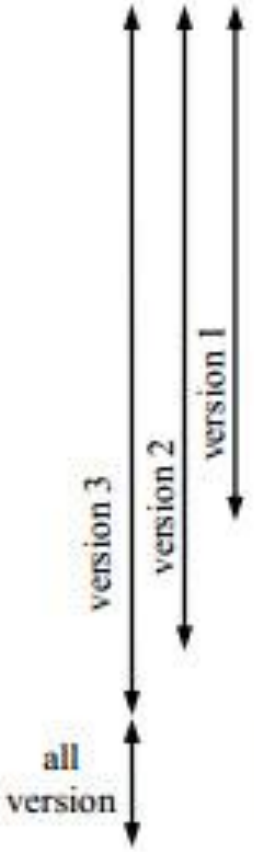


(a) X.509 Certificate



(b) Certificate Revocation List

Cấu trúc và ví dụ một chứng chỉ X.509

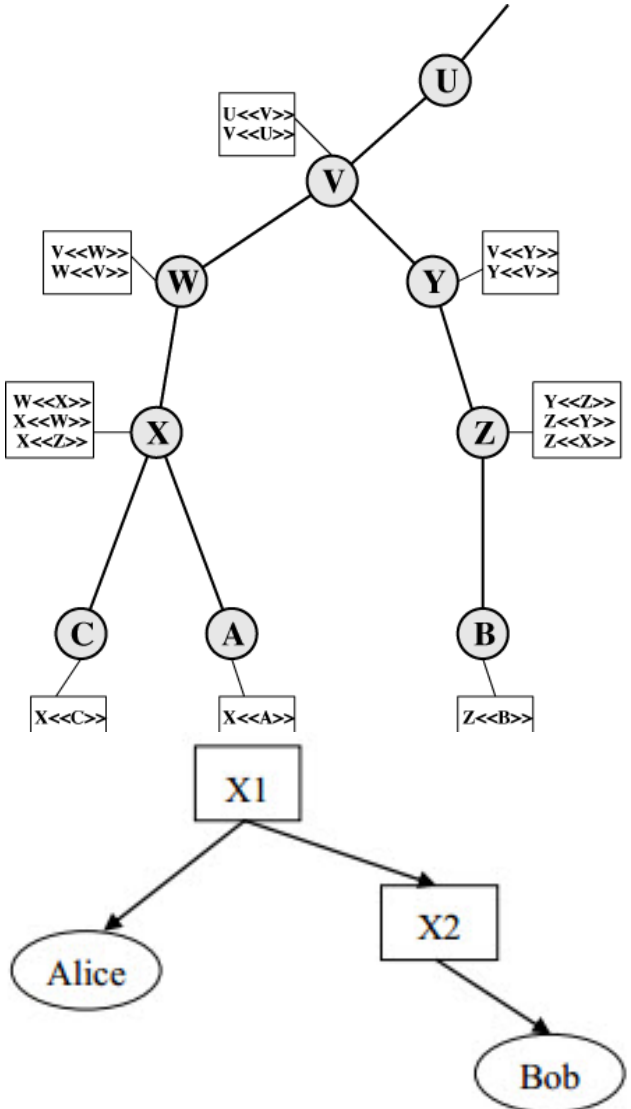


Version	Version 3
Serial Number	05:A0:4C
Certificate Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption
Issuer Name	OU = Equifax Secure Certificate Authority; O = Equifax
Validity (Not Before, Not After)	04/01/2006 17:09:06 PM GMT - 04/01/2011 17:09:06 PM GMT
Subject	CN= login.yahoo.com; OU= Yahoo; O= Yahoo! Inc.
Subject Public Key Algorithm	PKCS #1 RSA Encryption
Subject Public Key	30 81 89 02 81 81 00 b5 6c 4f ee ef 1b 04 5d be…
Issuer Unique Identifie	
Subject Unique Identifier	
Extension for version 3	
Certificate Signature Algorithm	PKCS #1 SHA-1 With RSA Encryption
Certificate Signature Value	50 25 65 10 43 e1 74 83 2f 8f 9c 9e dc 74 64 4e…

Nhận chứng thực CA

- Cứ có khóa công khai của CA (cơ quan chứng thực) là có thể xác minh được chứng thực
- Chỉ CA mới có thể thay đổi chứng thực
  - Chứng thực có thể đặt trong một thư mục công khai
- Cấu trúc phân cấp CA
  - Người dùng được chứng thực bởi CA đã đăng ký
  - Mỗi CA có hai loại chứng thực
    - Chứng thực thuận: Chứng thực CA hiện tại bởi CA cấp trên
    - Chứng thực nghịch: Chứng thực CA cấp trên bởi CA hiện tại
- Cấu trúc phân cấp CA cho phép người dùng xác minh chứng thực bởi bất kỳ CA nào

Phân cấp X.509



Không thể chỉ có một trung tâm chứng thực CA duy nhất mà có thể có nhiều trung tâm chứng thực. Mỗi người sử dụng khác nhau có thể đăng ký chứng thực tại các CA khác nhau.

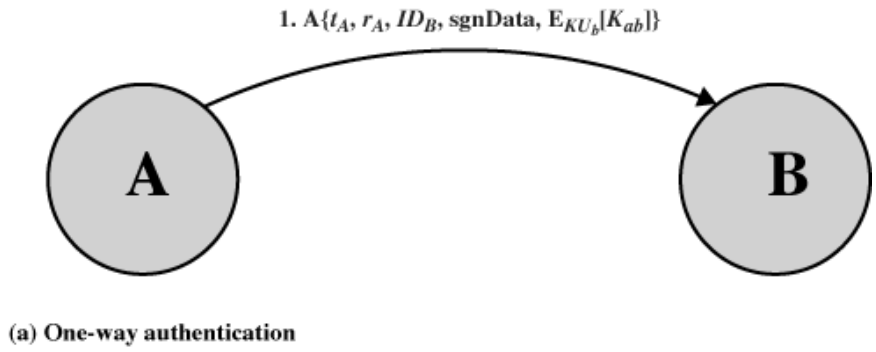
Để có thể trao đổi dữ liệu, một người cần phải tin tưởng vào khóa công khai của tất cả các trung tâm chứng thực.

Thu hồi chứng thực

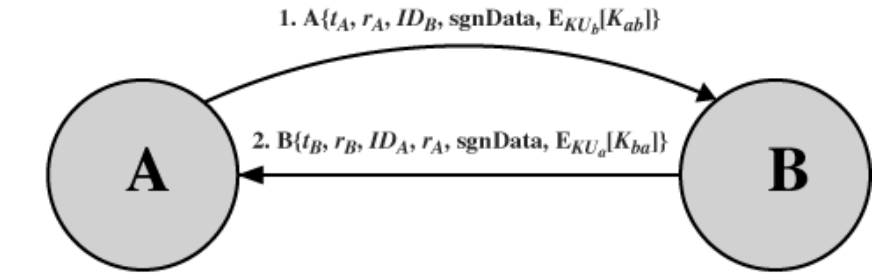
- Mỗi chứng thực có một thời hạn hợp lệ
- Có thể cần thu hồi chứng thực trước khi hết hạn
  - Khóa riêng của người dùng bị tiết lộ
  - Người dùng không còn được CA chứng thực
  - Chứng thực của CA bị xâm phạm
- Mỗi CA phải duy trì danh sách các chứng thực bị thu hồi (CRL)
- Khi nhận được chứng thực, người dùng phải kiểm tra xem nó có trong CRL không

Các thủ tục xác thực của X.509

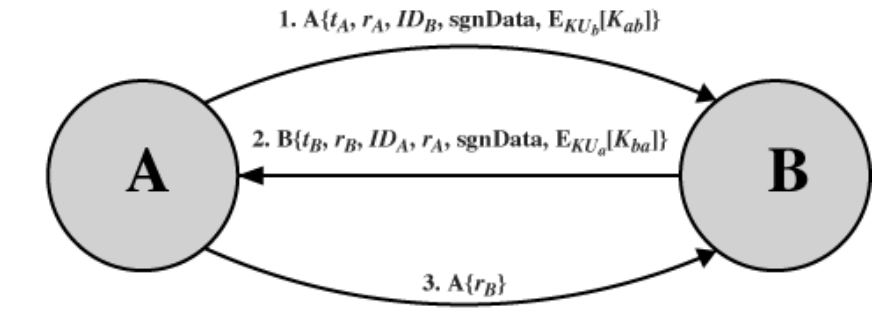
- Xác thực 1 chiều
- Xác thực 2 chiều
- Xác thực 3 chiều



(a) One-way authentication



(b) Two-way authentication



(c) Three-way authentication

Xác thực một chiều

- Một chiều A->B được sử dụng để thiết lập
  - Danh tính của A và rằng mẩu tin là từ A
  - Mẩu tin được gửi cho B
  - Tính toàn vẹn và gốc gác của mẩu tin
- Mẩu tin có thể bao gồm cả nhãn thời gian, ký hiệu đặc trưng của mẩu tin (nonce), danh tính của B và nó được ký bởi A. Có thể bao gồm một số thông tin bổ sung cho B như khoá phiên.

Xác thực hai chiều

- Hai mẩu tin A->B và B->A được thiết lập, ngoài mẩu tin từ A đến B như trên còn có:
  - Danh tính của B và trả lời từ B
  - Trả lời này dành cho A
  - Tính toàn vẹn và gốc gác của trả lời
- Trả lời bao gồm cả ký hiệu đặc trưng của mẩu tin (nonce) từ A, cả nhãn thời gian và ký hiệu đặc trưng trả lời từ B. Có thể bao gồm một số thông tin bổ sung cho A.

Xác thực ba chiều

- Ba mẩu tin A->B, B->A và A->B được thiết lập như trên mà không có đồng hồ đồng bộ.
- Ngoài 2 chiều như trên còn có trả lời lại từ A đến B chứa bản sao nonce của trả lời từ B, nghĩa là các nhãn thời gian mà không cần kiểm tra.

X.509 phiên bản 3

Trong phiên bản 3 được bổ sung một số thông tin cần thiết trong giấy chứng nhận như: Email/URL, chi tiết về đợt phát hành, các ràng buộc sử dụng. Tốt hơn hết là đặt tên tường minh cho các cột mới xác định trong phương pháp mở rộng tổng quát. Các mở rộng bao gồm:

- Danh tính mở rộng
- Chỉ dẫn tính quan trọng
- Giá trị mở rộng

Các mở rộng xác thực

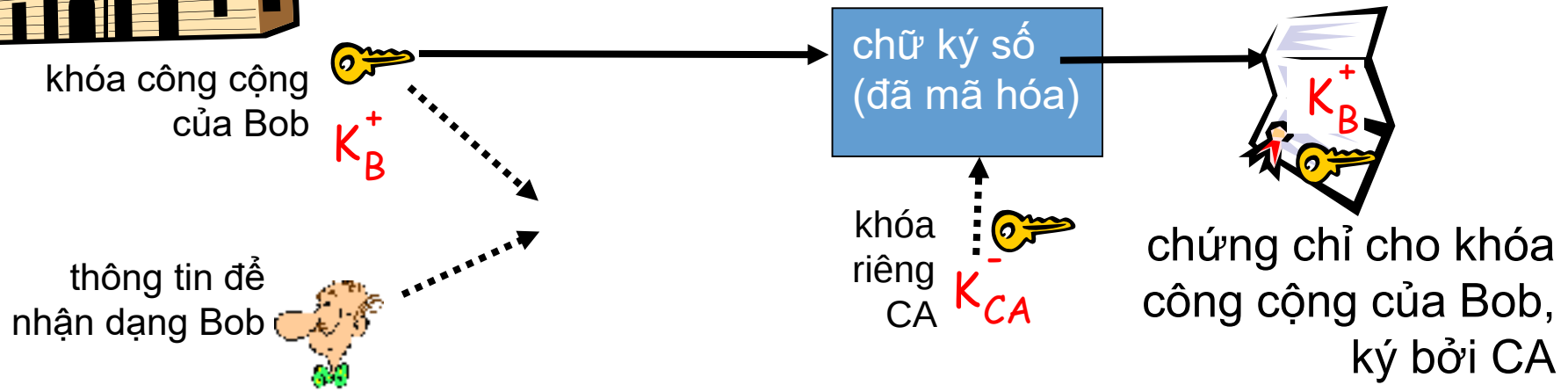
- Khoá và các thông tin đợt phát hành
- Bao trùm thông tin về đối tượng, khoá người phát hành, chỉ thị kiểu phát hành, chứng nhận

  Đối tượng chứng nhận và các thuộc tính người phát hành
- Hỗ trợ có tên phụ, định dạng phụ cho các đối tượng và người phát hành

  Chứng nhận các ràng buộc phát hành
- Cho phép sử dụng các ràng buộc trong chứng nhận bởi các CA khác

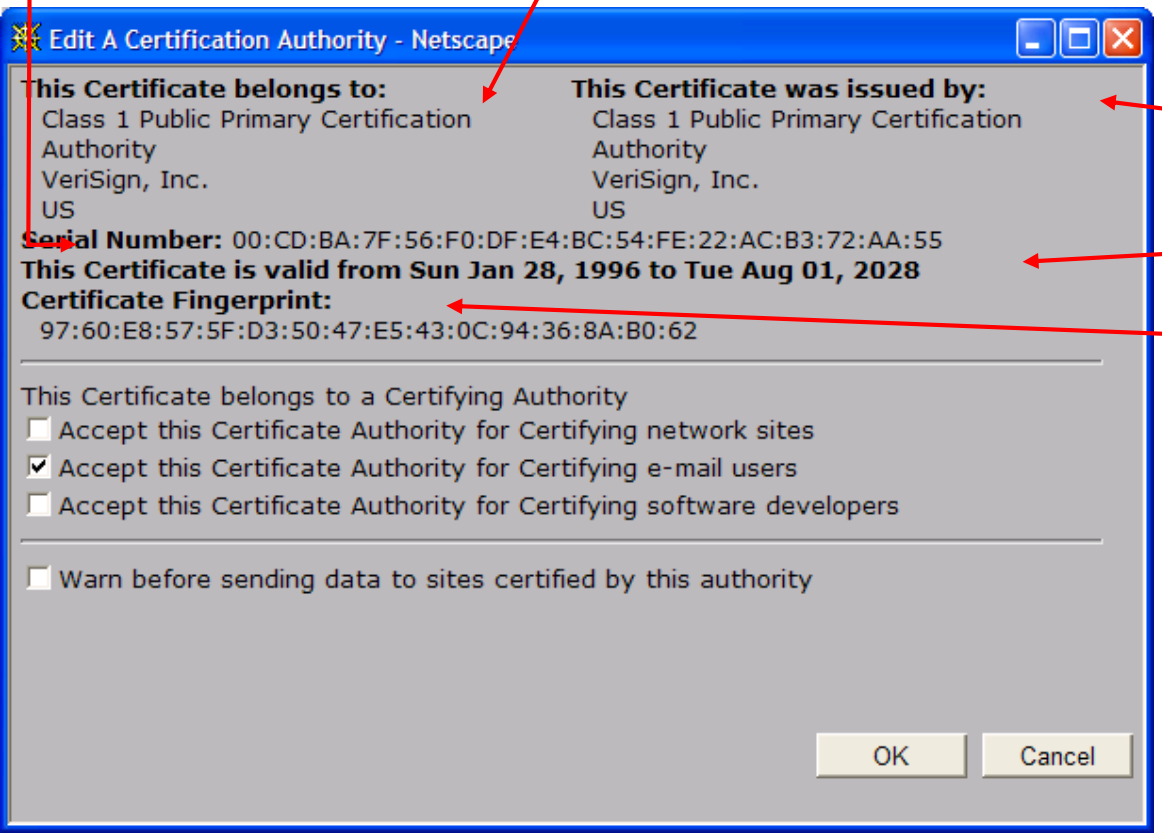
Cấp chứng chỉ

- Certification authority (CA): gắn kết khóa công cộng với thực thể E nào đó.
- E (người, router) đăng ký khóa công cộng của họ với CA.
  - E cung cấp "bằng chứng để nhận dạng" cho CA.
  - CA tạo ra chứng chỉ ràng buộc E với khóa công cộng của nó.
  - chứng chỉ chứa khóa công cộng của E được ký số bởi CA – CA nói "đây là khóa công cộng của E"



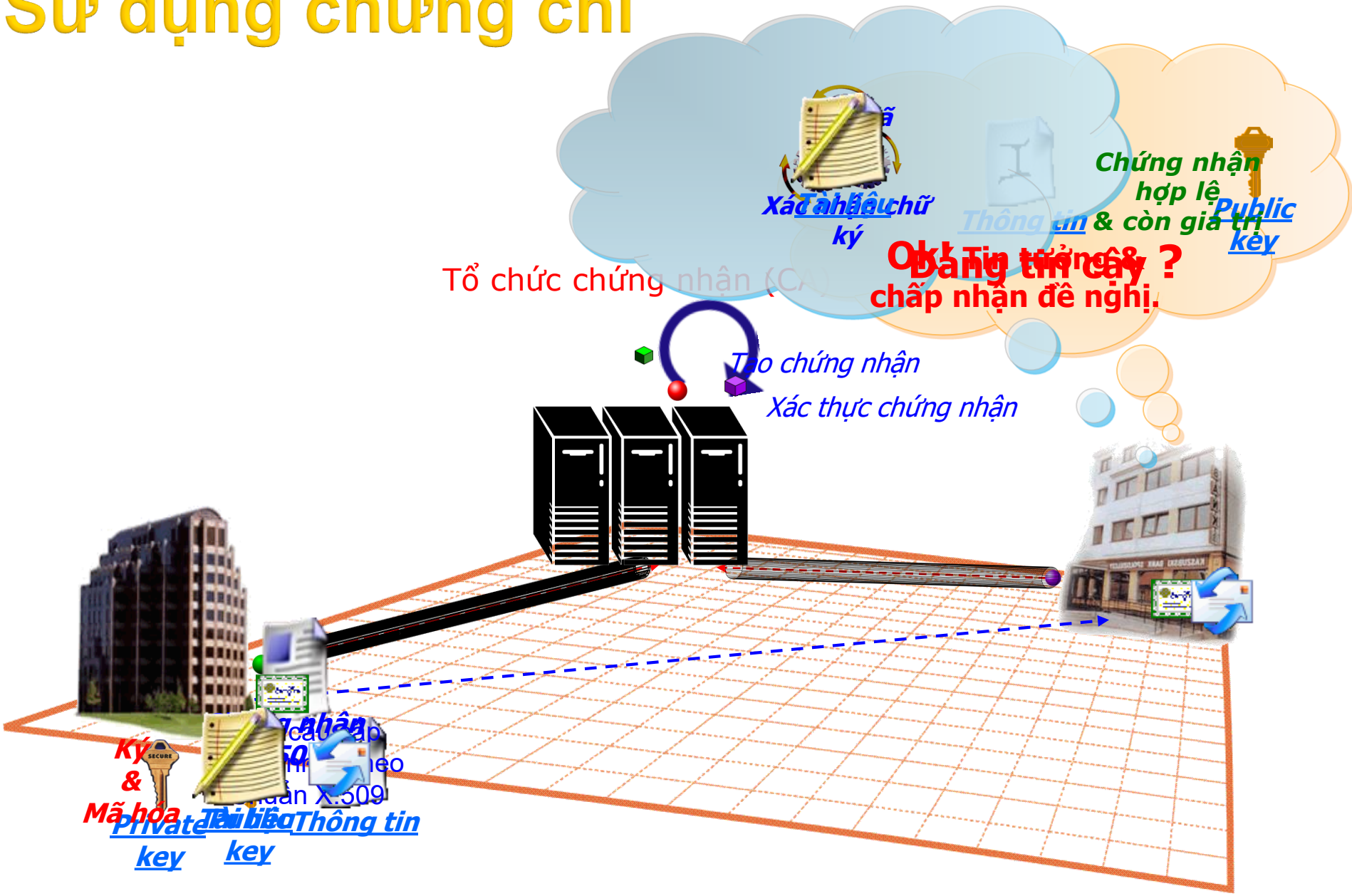
Mô tả chứng chỉ

- Số thứ tự (duy nhất)
- thông tin về người sở hữu chứng chỉ, bao gồm giải thuật và chính giá trị khóa (không hiển thị ra)

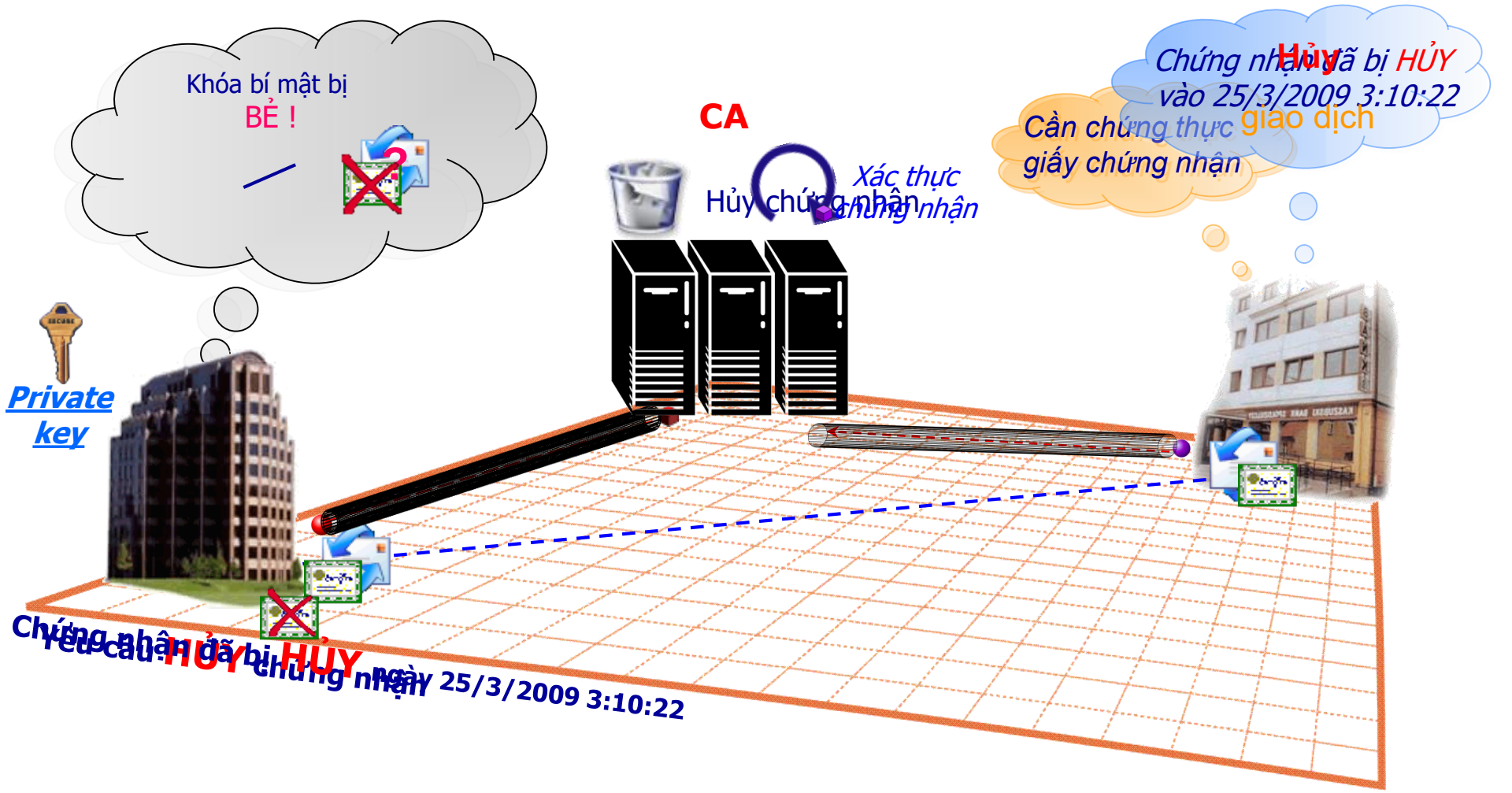


- thông tin về người phát hành chứng chỉ
- ngày kiểm tra tính hợp lệ
- chữ ký số bởi người phát hành chứng chỉ

Sử dụng chứng chỉ



Sử dụng chứng chỉ



2. Giao thức bảo mật web SSL

Tại sao cần bảo mật Web???

- Web được sử dụng rộng rãi bởi các công ty, tổ chức, và các cá nhân
- Các vấn đề đặc trưng đối với an ninh Web
  - Web dễ bị tấn công theo cả hai chiều
  - Tấn công Web server sẽ gây tổn hại đến danh tiếng và tiền bạc của công ty
  - Các phần mềm Web thường chứa nhiều lỗi an ninh
  - Web server có thể bị khai thác làm căn cứ để tấn công vào hệ thống máy tính của một tổ chức
  - Người dùng thiếu công cụ và kiến thức để đối phó với các hiểm họa an ninh