AN TOÀN & BẢO MẬT THÔNG TIN

Giảng viên: Ths Phạm Thanh Bình

Bộ môn Kỹ thuật máy tính & mạng

http://dhthuyloi.blogspot.com

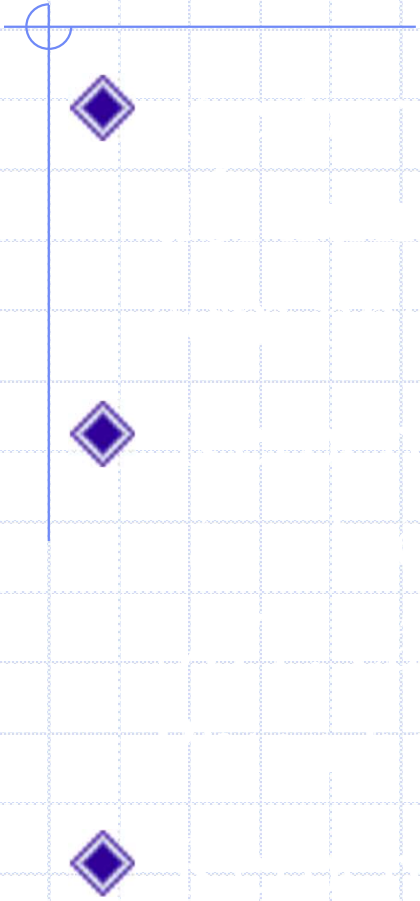
Chương 4:

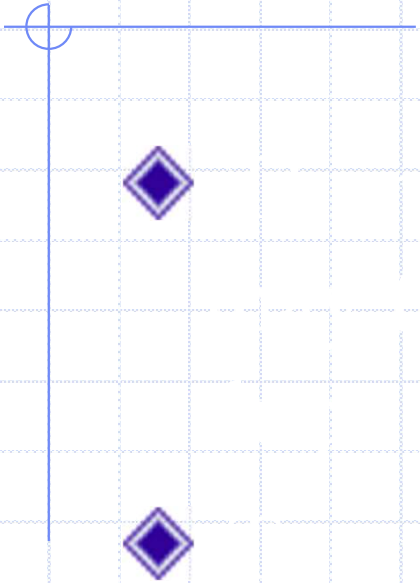
CÁC ỨNG DỤNG TRONG AN NINH MẠNG

- Các ứng dụng chứng thực
- An ninh Web
- An ninh giao dịch điện tử

Bài 4.1 Các ứng dụng chứng thực

- Chứng chỉ khoá công khai
- Dịch vụ chứng thực X.509
- Hạ tầng khoá công khai





Khoá công khai bảo mật, được sử dụng tốt hơn
Nhưng khoá công khai dễ bị giả mạo

Chứng chỉ khoá công khai

Việc phân phối khoá công khai cũng cần phải có phương pháp. Một số cách để phân phối khoá công khai như:

- Yết thị công khai
- Đặt trong một thư mục công cộng
- Dùng chứng chỉ khoá công khai

Yết thị công khai

- Người sở hữu khoá (A) có thể gửi khoá công khai của mình cho đối tác, hoặc công bố rộng rãi cho cộng đồng
- Nhược điểm: Do không có cơ chế xác thực, bất cứ ai cũng có thể đóng giả làm A và gửi khoá công khai cho đối tác của A, khiến đối tác nhầm tưởng là đang liên lạc với A.

Phong bì chứa khoá công khai bên trong: gọi là chứng chỉ
Không lo giả mạo chữ ký

Đặt trong một thư mục công cộng

- Các khoá công khai được đặt trong một thư mục công cộng do một tổ chức đáng tin cậy quản lý.
- Người dùng muốn công bố khoá công khai của mình thì phải đăng kí với tổ chức đó.
- Nhược điểm: Nếu kẻ tấn công (bằng cách nào đó) chiếm được quyền truy cập của tổ chức, anh ta có thể thay thế các khoá công khai trong thư mục bằng các khoá giả mạo.

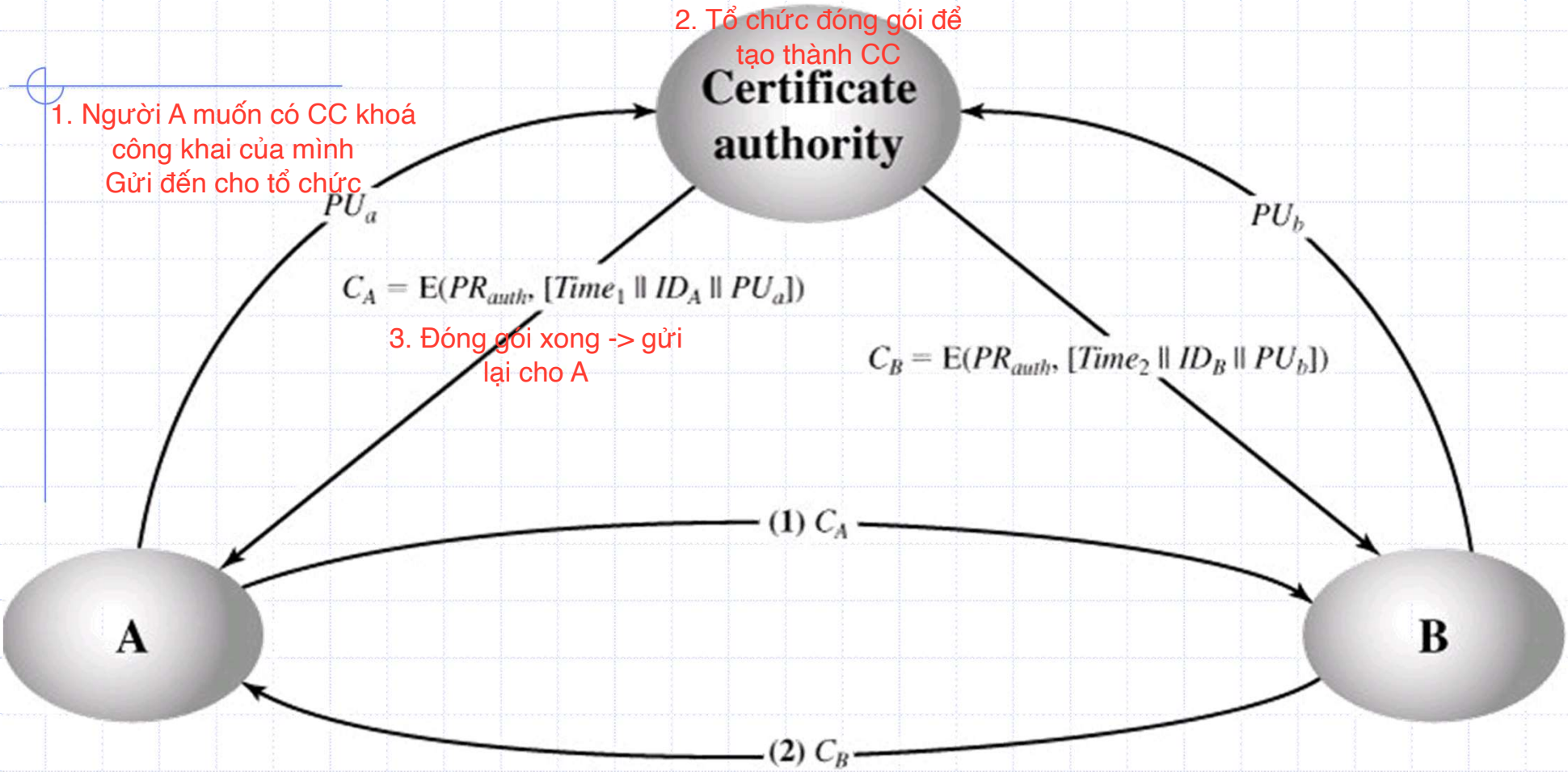
Dùng chứng chỉ khoá công khai

- Khoá công khai không được đặt trực tiếp trong thư mục công cộng, mà được đặt trong "chứng chỉ khoá công khai"
- Người dùng A muốn công bố khoá công khai của mình thì phải đăng kí với một tổ chức đáng tin cậy có thẩm quyền cấp chứng chỉ, tổ chức này sẽ cấp cho A một chứng chỉ bao gồm khoá công khai của A (PU_a), định danh của A (ID_A), và chữ kí của tổ chức.

- A có thể công bố rộng rãi chứng chỉ này hoặc gửi chứng chỉ cho đối tác, mà không phải lo lắng bị kẻ khác làm giả chứng chỉ.
- Đối tác của A có thể kiểm tra tính hợp lệ của chứng chỉ dựa trên chữ kí của tổ chức.

2. Tổ chức đóng gói để tạo thành CC

1. Người A muốn có CC khoá công khai của mình Gửi đến cho tổ chức



3. Đóng gói xong -> gửi lại cho A

Kí hiệu:

- CA: Certificate Authority (Tổ chức cấp phát chứng chỉ)
- C_A: là chứng chỉ khoá công khai của A

$$C_A = E(PR_{auth}, [T||ID_A||PU_a])$$

- PR_{auth} là khóa riêng của tổ chức cấp phát chứng chỉ.
- T là một nhãn thời gian cho biết thời gian hiệu lực của chứng chỉ

- Đối tác của A có thể dùng PU_{auth} để giải mã C_A, nhằm kiểm tra tính hợp lệ của C_A và thu được PU_a:

$$D(PU_{auth}, C_A) = D(PU_{auth}, E(PR_{auth}, [T||ID_A||PU_a]))$$
$$= [T||ID_A||PU_a]$$

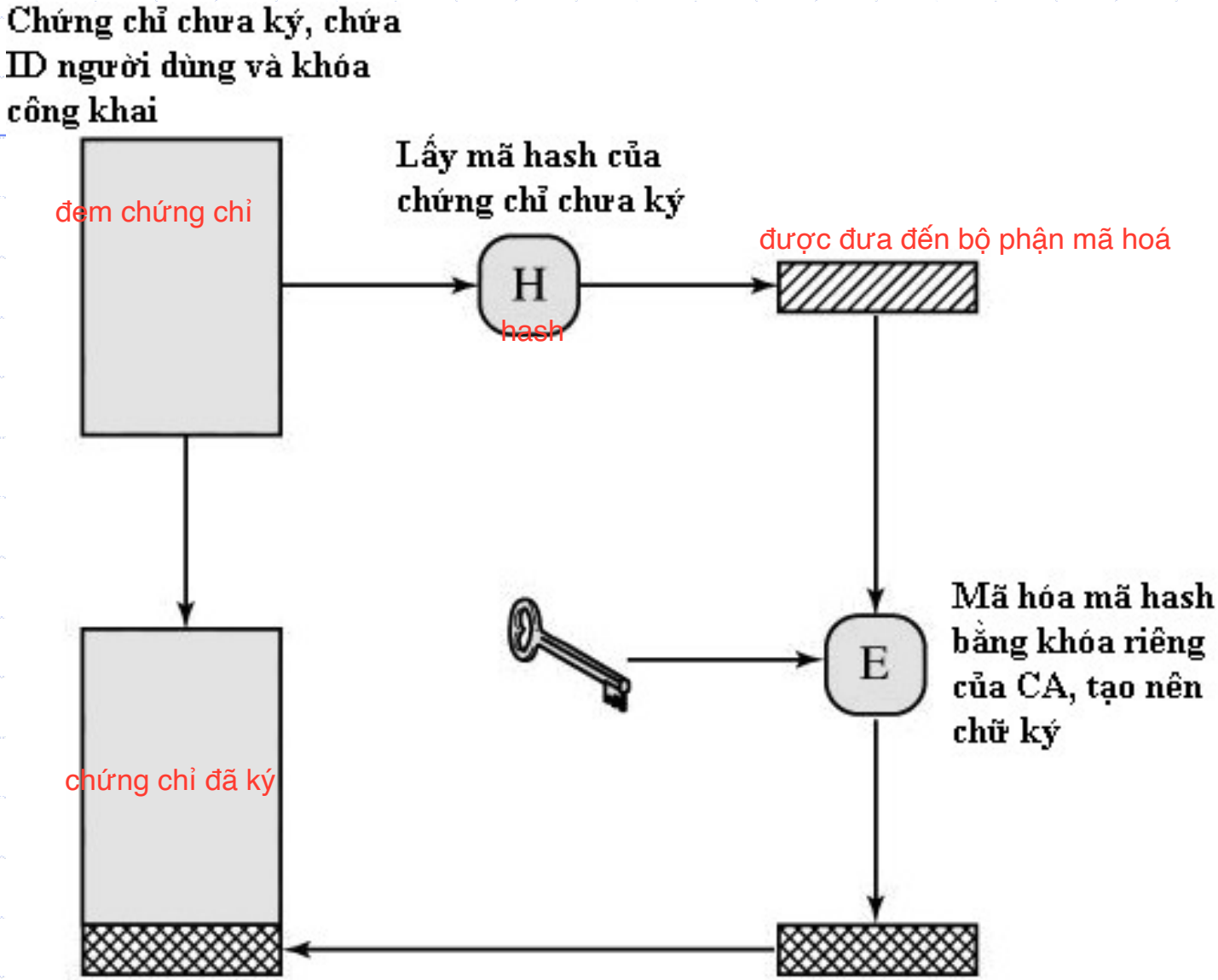
- Sau đó đối tác có thể liên lạc với A nhờ PU_a.

Dịch vụ chứng thực X.509

- X.509 là một tiêu chuẩn về chứng chỉ khoá công khai được chấp nhận rộng rãi trên toàn thế giới
- Các chứng chỉ X.509 được sử dụng trong hầu hết các ứng dụng về an ninh mạng
- X.509 được đề nghị vào năm 1988, và được sửa đổi nhiều lần trong các năm 1993, 1995 và 2000, tạo ra các phiên bản khác nhau

- Mỗi chứng chỉ X.509 ứng với một người dùng, được tạo ra bởi CA (Tổ chức cấp chứng chỉ tin cậy)
- Các chứng chỉ sẽ được đặt vào một thư mục công khai của CA, hoặc đặt vào thư mục của người dùng
- Người dùng có thể truy xuất thư mục của CA để lấy chứng chỉ của người khác, hay tự phân phối chứng chỉ của mình cho người khác, mà không lo bị giả mạo.

Quá trình sinh chứng chỉ X.509

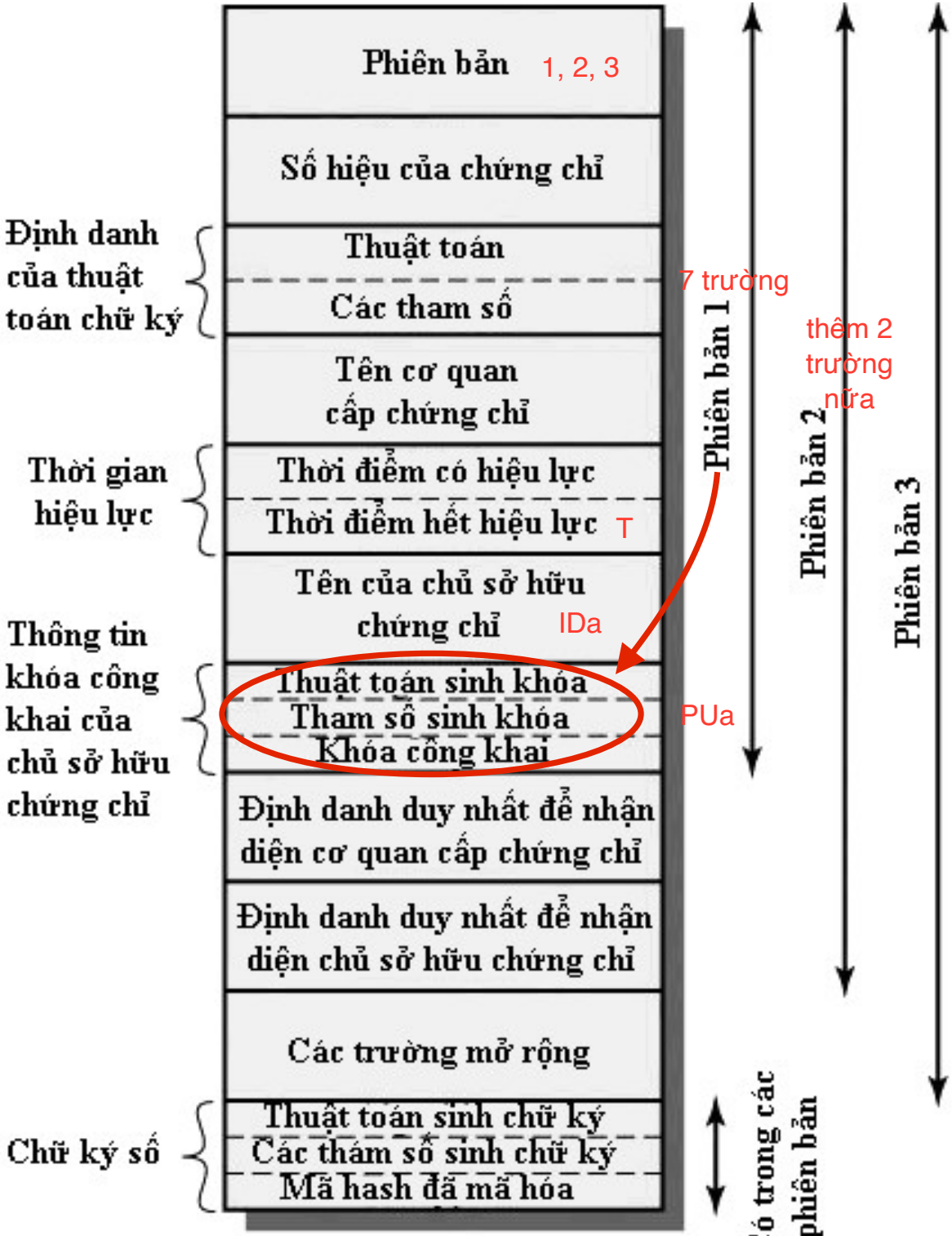


Bài tập:

- Hãy biểu diễn quá trình sinh chứng chỉ trong sơ đồ trên bằng công thức.

Bài Tập: Viết công thức biểu diễn chứng chỉ X509 đã ký

(PUa ll IDa ll T) ll E(PRca, H (PUa ll IDa ll T))



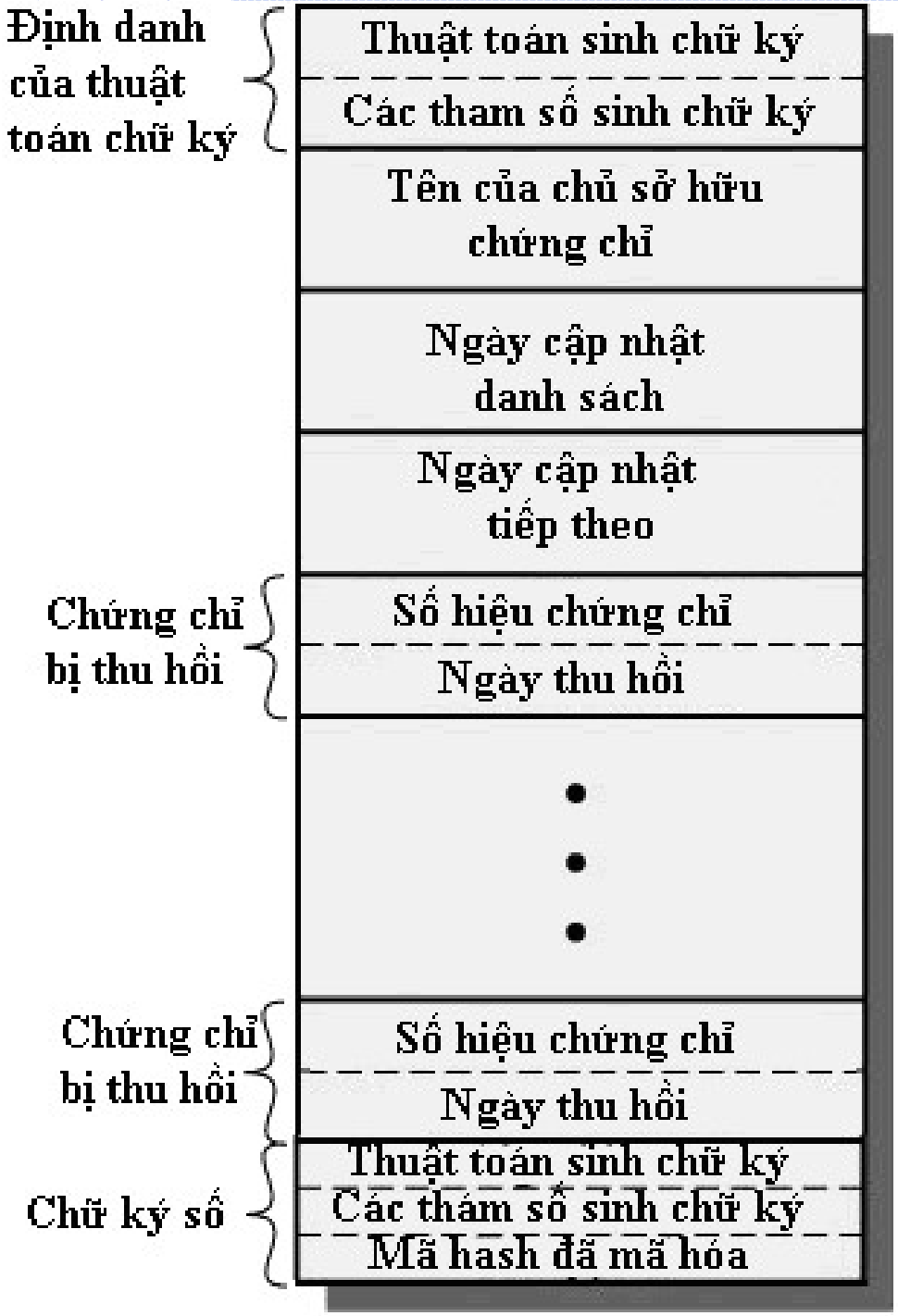
(a) Cấu trúc chứng chỉ X.509

Thu hồi chứng chỉ

- Mỗi chứng chỉ có hiệu lực trong một khoảng thời gian xác định (tương tự như thẻ tín dụng). Khi hết hạn thì sẽ phải cấp một chứng chỉ mới
- Đôi khi cần thu hồi chứng chỉ trước khi hết hạn, do nghi ngờ bị lộ khoá riêng của người dùng, hoặc người dùng không được CA chứng nhận nữa, hay chứng chỉ bị coi là thiếu tin cậy.

- Danh sách các chứng chỉ bị thu hồi trước khi hết hạn (CRL - Certificate Revocation List) phải được CA công bố công khai, và có chữ kí xác nhận của CA
- Khi người dùng nhận được một chứng chỉ (còn hạn) do người khác gửi tới, anh ta cần kiểm tra danh sách nói trên xem chứng chỉ đã bị thu hồi hay chưa

Giống file CSDL, chia ra thành các bản ghi

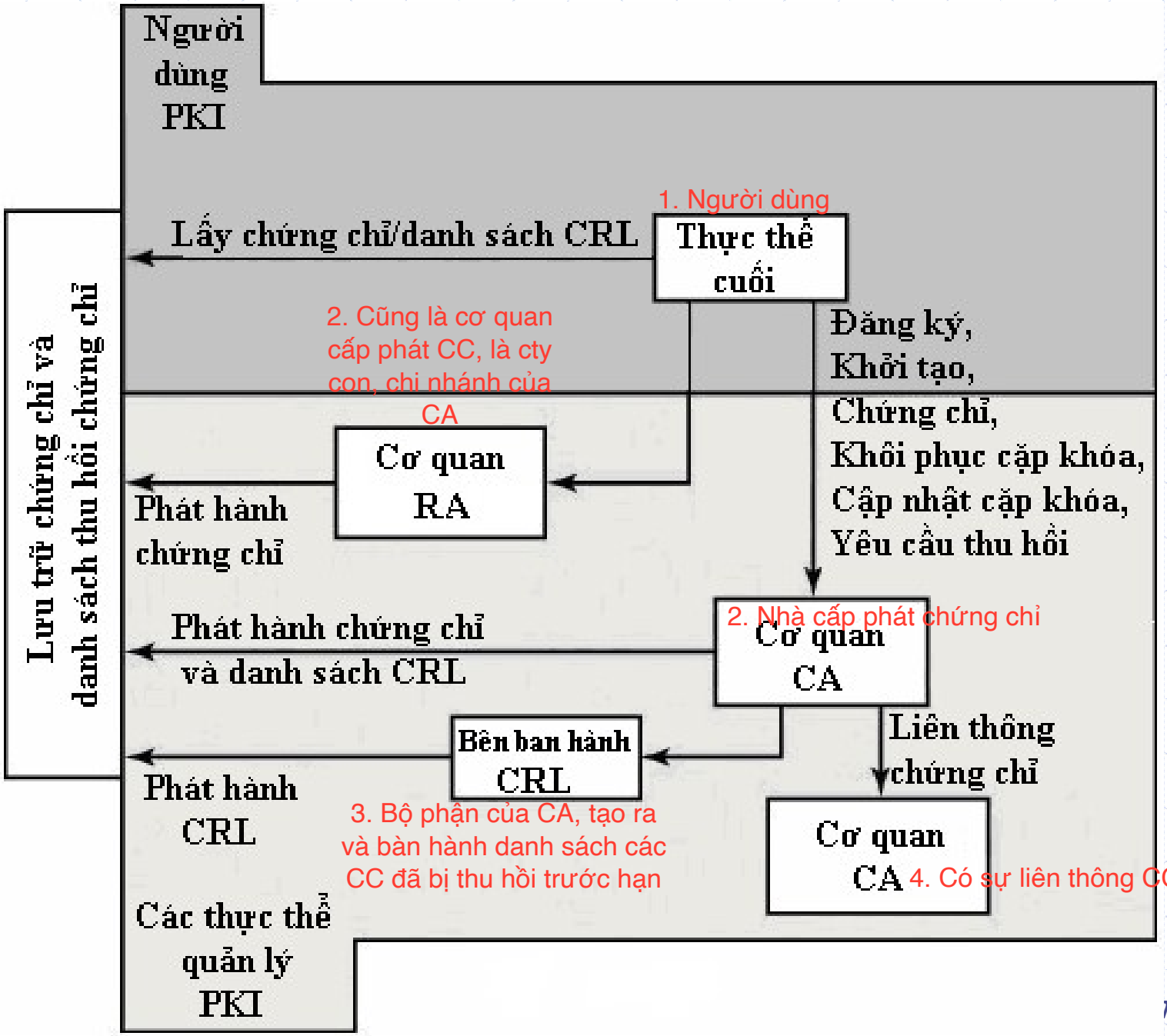


(b) Danh sách các chứng chỉ thu hồi

Hạ tầng khoá công khai

- Hạ tầng khoá công khai (PKI - Public Key Infrastructure) là một tập phần cứng, phần mềm, con người, chính sách và các thủ tục cần thiết để tạo ra, quản lý, lưu trữ, phân phối và thu hồi các chứng chỉ số dựa trên kỹ thuật mật mã bất đối xứng.
- Hạ tầng khoá công khai dựa trên tiêu chuẩn X.509 được kí hiệu là PKIX

Mô hình kiến trúc của PKIX



Giải thích:

- **CA (Certification Authority)**: Cơ quan cấp phát chứng chỉ, quản lý, thu hồi và công bố danh sách các chứng chỉ bị thu hồi (CRL)
- **RA (Registration Authority)**: Cơ quan đăng kí cấp phát chứng chỉ, có nhiệm vụ tiếp nhận và xác minh các yêu cầu về chứng chỉ số của người dùng, rồi gửi các yêu cầu đã xác minh cho CA để thực hiện yêu cầu đó.

- **Thực thể cuối (End Entity)**: là người dùng hay các bên sử dụng dịch vụ. Người dùng có thể gửi yêu cầu xin cấp chứng chỉ trực tiếp cho CA hoặc gián tiếp qua RA
- **Bên ban hành CRL (CRL issuer)**: CA có thể trực tiếp công bố danh sách các chứng chỉ bị thu hồi (CRL), hoặc giao cho CRL issuer công bố

Hết Phần 4_1