



BÀI GIẢNG MÔN

An ninh mạng thông tin*TEL1401*

Giảng viên:

TS. Phạm Anh Thư

Điện thoại/E-mail:

0912528188

thupa80@yahoo.com, thupaptit@gmail.com

Bộ môn:

Mạng viễn thông - Khoa Viễn thông 1

Học kỳ/Năm biên soạn: I/ 2022-2023



Chương 4: Xác thực

4.1 Quản lý và phân phối khóa

4.2 Xác thực người sử dụng



Phân phối và quản lý khóa

- ❖ Đối với phương pháp mật mã khóa đối xứng: các thành viên chia sẻ cùng một khóa bí mật.
- ❖ Hơn nữa, yêu cầu là khóa được thay đổi thường xuyên nhằm tránh các tấn công.
- ❖ Vì vậy, sức mạnh của bất kỳ một hệ thống mã hóa nào cũng đều liên quan tới kỹ thuật phân phối khóa.



Phân phối và quản lý khóa

❖ Phân cấp khóa:

■ Khóa phiên

- Là khóa tạm thời
- Thời gian tồn tại của khóa phiên càng ngắn càng tốt
- Được sử dụng cho việc mật mã dữ liệu trong mỗi phiên
- Bị xóa bỏ sau khi sử dụng

■ Khóa chủ

- Là khóa được sử dụng lâu dài
- Được sử dụng để mật mã khóa phiên
- Được dùng chung bởi người sử dụng và trung tâm phân phối khóa (KDC)



Phân phối và quản lý khóa

❖ Các cách phân phối khóa bí mật:

1. Trao đổi mọi khóa một cách nhân công:
 - A lựa chọn một khóa và chuyển phát nhân công tới B.
 - Bất tiện
2. Trao đổi khóa chủ một cách nhân công:
 - Một thành viên thứ ba (KDC: trung tâm phân phối khóa) lựa chọn khóa chủ và chuyển phát nhân công tới A và B.
 - Các khóa phiên được tự động trao đổi giữa các người sử dụng qua KDC
 - Vấn đề bảo mật và nghìn cổ chai tại KDC



Phân phối và quản lý khóa

❖ Các cách phân phối khóa bí mật:

3. Nếu A và B cùng sử dụng một khóa trước đó, một thành viên có thể chuyển một khóa mới dựa trên việc mã hóa khóa cũ.

4. Nếu A và B có một kết nối mã hóa với một thành viên C, C có thể chuyển phát khóa cho cả A và B.



Phân phối khóa đối xứng bằng mật mã khóa đối xứng

- ❖ Hai bên dùng chung khóa bí mật
- ❖ Các khóa cần được trao đổi một cách thường xuyên để tránh phá khóa
- ❖ Các cách phân phối khóa:
 - Phân phối khóa không tập trung: phân phối khóa chủ một cách nhân công giữa các thành viên, sau đó phân phối khóa phiên một cách tự động
 - Sử dụng trung tâm phân phối khóa (KDC): phân phối khóa chủ một cách nhân công với KDC, sau đó phân phối khóa phiên một cách tự động



Phân phối khóa đối xứng bằng mật mã khóa đối xứng

- ❖ Thay đổi khóa phiên một cách tự động và thường xuyên
- ❖ Thay đổi khóa chủ một cách nhân công và hiếm khi
- ❖ Thời gian sống của khóa phiên:
 - Càng ngắn thì càng an toàn
 - Đối với giao thức hướng kết nối (TCP): mỗi kết nối yêu cầu 1 khóa phiên mới
 - Đối với giao thức phi kết nối (UDP/IP): thay đổi sau khoảng thời gian xác định hoặc sau một số gói được gửi đi



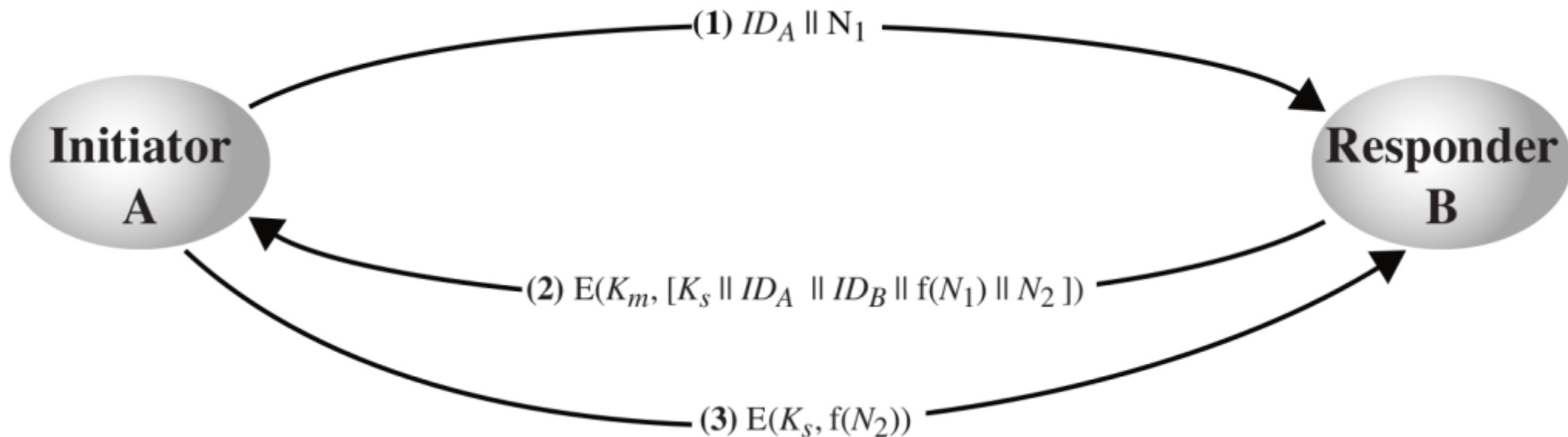
Phân phối khóa đối xứng bằng mật mã khóa đối xứng

❖ Các ký hiệu:

- Các đầu cuối: A và B có nhận dạng tương ứng là ID_A và ID_B
- Khóa chủ giữa A và B là K_m
- Các khóa chủ được chỉ định cho các đầu cuối: K_a , K_b
- Khóa phiên giữa A và B là K_s
- Các giá trị Nonce: N_1 , N_2
 - Là các số được sử dụng 1 lần
 - Có thể là số ngẫu nhiên, hàm f, số đếm
 - Phải khác nhau với mỗi yêu cầu
 - Kẻ tấn công khó đoán ra

Kịch bản phân phối khóa không tập trung

- ❖ Mỗi đầu cuối phải trao đổi một cách nhân công $n-1$ khóa chủ (K_m) với các đầu cuối khác
- ❖ Không dựa vào bên thứ 3 được chứng thực



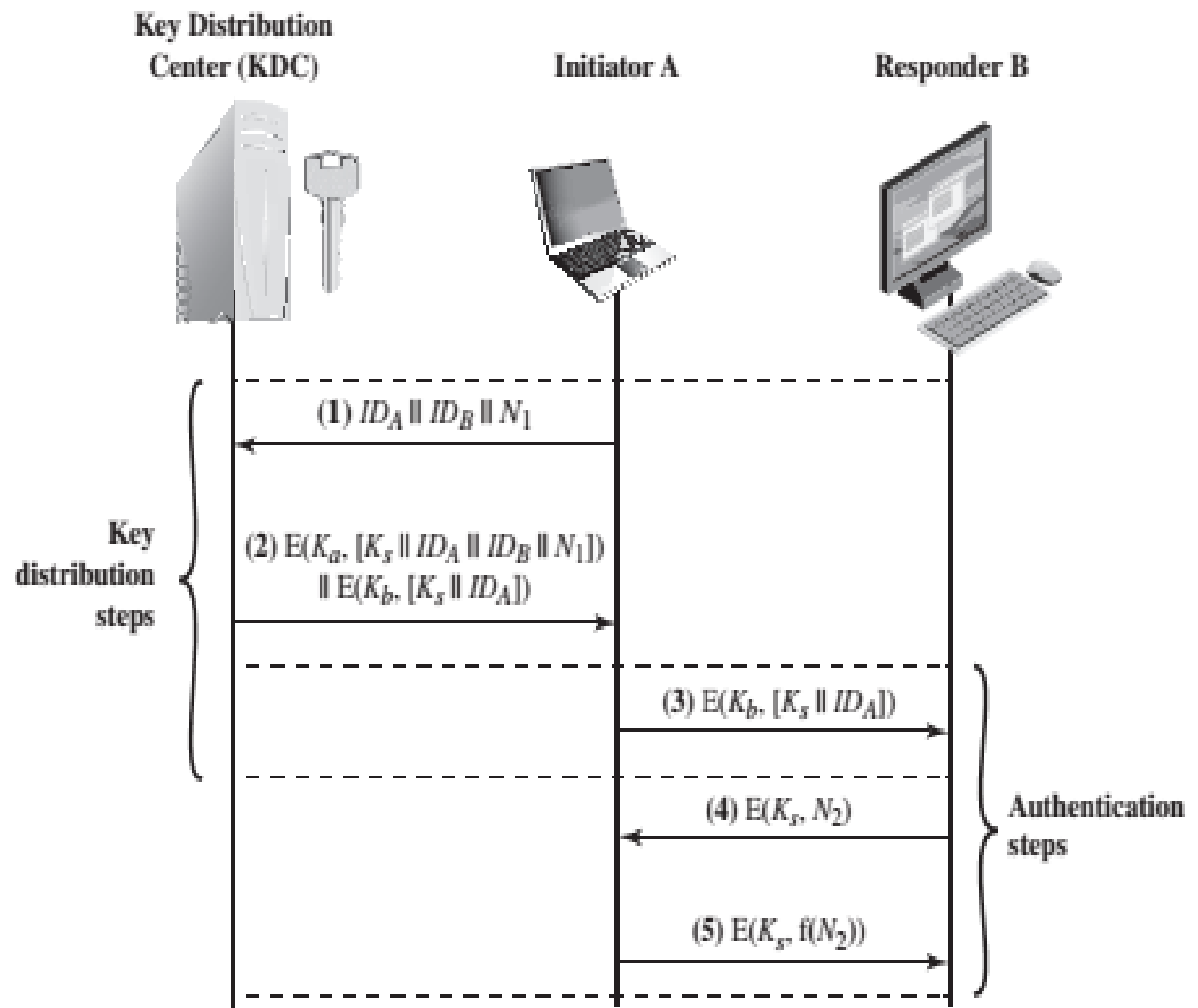


Kịch bản phân phối khóa dựa trên KDC

- ❖ KDC là bên thứ 3 được chứng thực
- ❖ Người sử dụng trao đổi khóa chủ một cách nhân công với KDC
- ❖ Người sử dụng có thể tự động lấy khóa phiên qua KDC để trao đổi thông tin với nhau

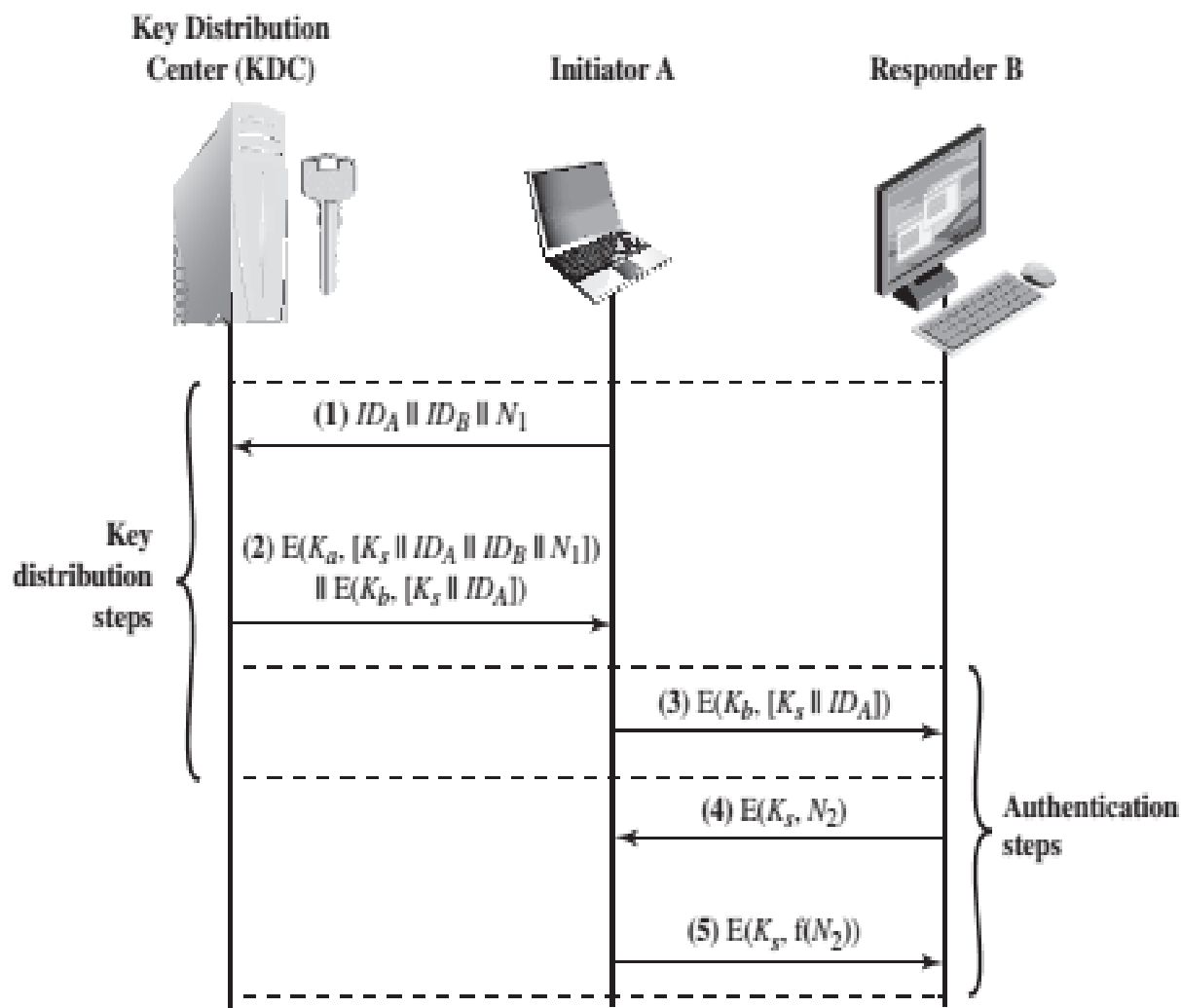
Kịch bản phân phối khóa dựa trên KDC

- ❖ B1: A gửi yêu cầu đến KDC cho một khóa phiên để bảo vệ một kết nối logic tới B: định dạng A, định dạng B, số ngẫu nhiên N_1 .
- ❖ B2: KDC phản hồi với một bản tin được mã hóa bằng cách sử dụng khóa K_a và thông tin để gửi cho B



Kịch bản phân phối khóa

- ❖ B3: A lưu trữ khóa phiên cho phiên sắp tới và chuyển tiếp đến B thông tin có nguồn gốc tại KDC cho B, cụ thể là, $E(K_b, [K_s \parallel ID_A])$.
- ❖ B4: Sử dụng khóa phiên mới được tạo ra để mã hóa, B sẽ gửi một nonce N_2 tới A
- ❖ B5: sử dụng khóa phiên K_s , A trả lời B với $f(N_2)$ với f là một hàm thực hiện một số biến đổi trên N_2 (ví dụ: cộng một)





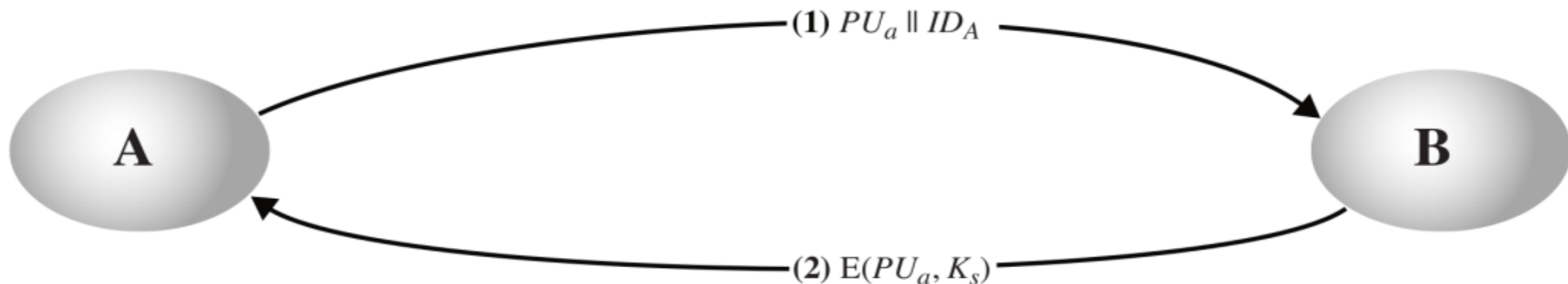
Phân phối khóa đối xứng bằng mật mã khóa bất đối xứng

- ❖ Mật mã khóa bất đối xứng thường là quá chậm khi mật mã hóa khối lượng lớn dữ liệu
- ❖ Thường thì ứng dụng của mật mã khóa bất đối xứng là để trao đổi khóa bí mật
- ❖ Gồm 3 cách:
 - Phân phối khóa bí mật một cách đơn giản
 - Phân phối khóa bí mật với tính bảo mật và xác thực
 - Sử dụng mật mã khóa công khai để trao đổi các khóa chủ giữa KDC và các user

Phân phối khóa đối xứng bằng mật mã khóa bất đối xứng

❖ Cách 1:

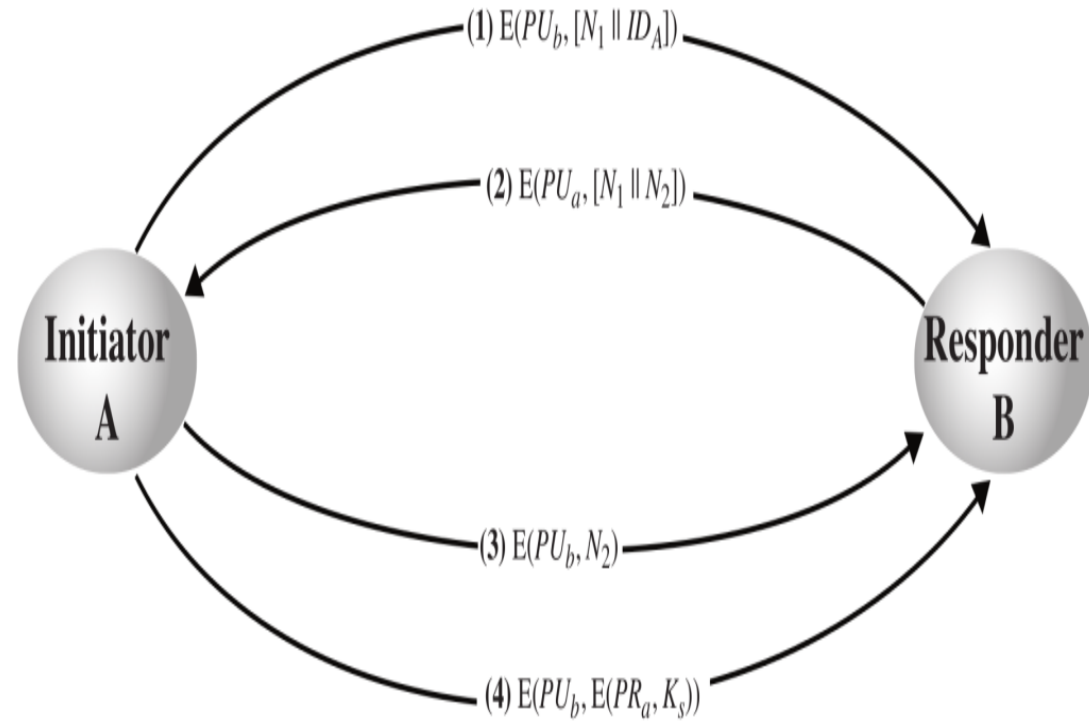
1. A tạo ra một cặp khóa công khai / bí mật $\{PU_a, PR_a\}$ và phát đi một bản tin tới B gồm PU_a và định danh của A, ID_A .
2. B tạo ra một khóa bí mật K_s và truyền nó cho A, được mã hóa với khóa công khai của A.
3. A tính $D(PR_a, E(PU_a, K_s))$ để khôi phục lại các khóa bí mật. Bởi vì chỉ có A có thể giải mã bản tin, chỉ có A và B sẽ biết nhận dạng của K_s .
4. A loại bỏ PU_a và PR_a và B loại bỏ PU_a .



Phân phối khóa bí mật cung cấp bảo mật và nhận thực

Cách 2: Giả định rằng A và B đã trao đổi khóa công khai theo một lược đồ nào đó:

1. A sử dụng khóa công khai của B để mã hóa một bản tin đến B có chứa ID_A và N_1 .
2. B gửi một bản tin đến A được mã hóa với PU_a và chứa N_1, N_2 .
3. A trả lại N_2 , mã hóa bằng khóa công khai của B, để đảm bảo B biết đáp ứng đó là từ A.
4. A chọn một khóa bí mật K_s và gửi $M = E(PU_b, E(PR_a, K_s))$ đến B
5. B tính $D(PU_a, D(PR_b, M))$ để khôi phục lại khóa bí mật.





Phân phối khóa bí mật cung cấp bảo mật và nhận thực

Cách 3:

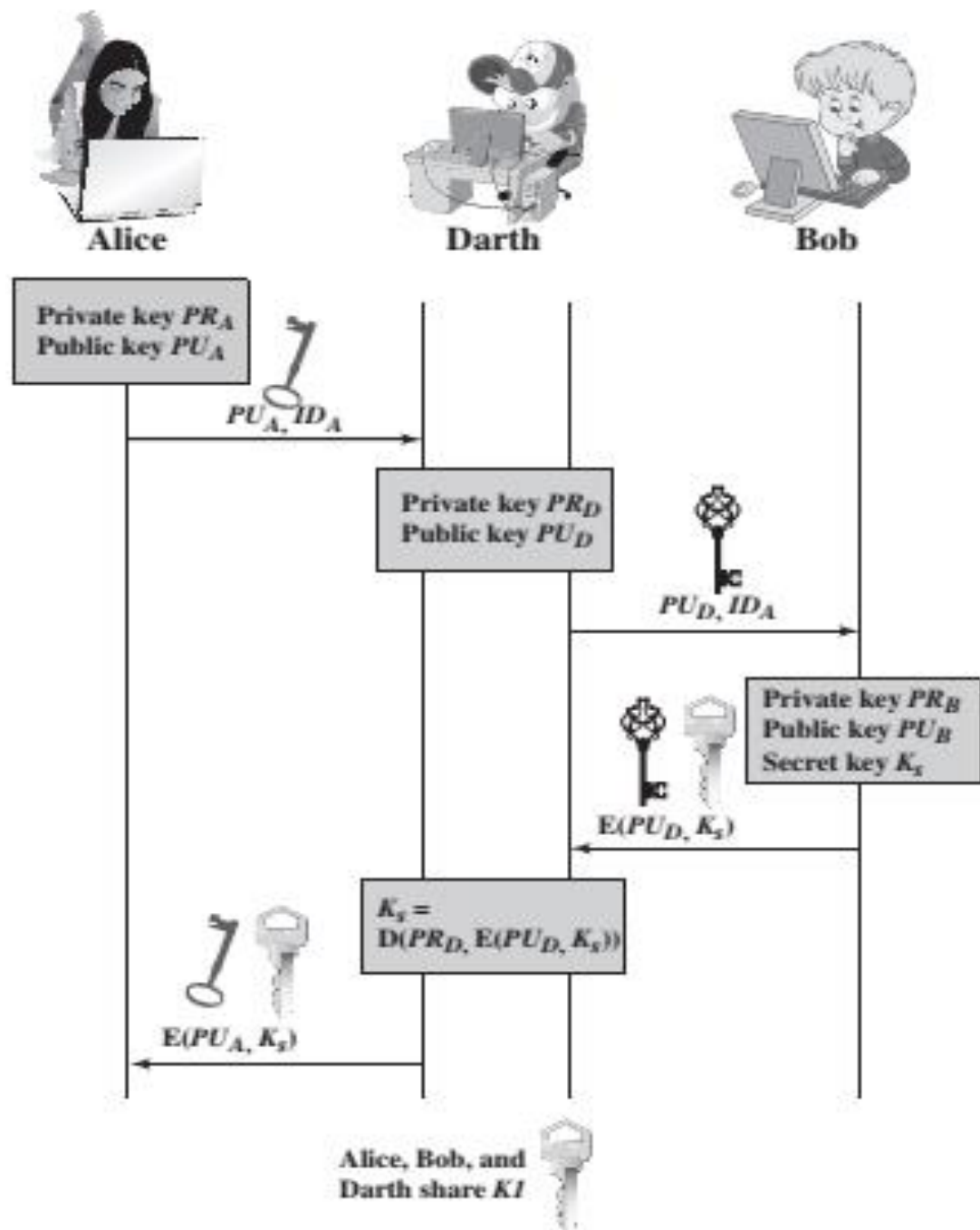
- Sử dụng mật mã khóa công khai để trao đổi các khóa chủ giữa KDC và các user
- Đây là phương pháp hiệu quả để phân phối các khóa chủ (tốt hơn nhiều phân phối nhân công)
- Hữu ích đối với các mạng lớn



Phân phối khóa công khai

- ❖ Theo thiết kế thì các khóa công khai được công khai cho tất cả người sử dụng
- ❖ Vấn đề là làm sao có thể đảm bảo khóa công khai của A thực sự thuộc về A?
- ❖ Làm sao để không ai có thể giả dạng A

Tấn công phân phối khóa





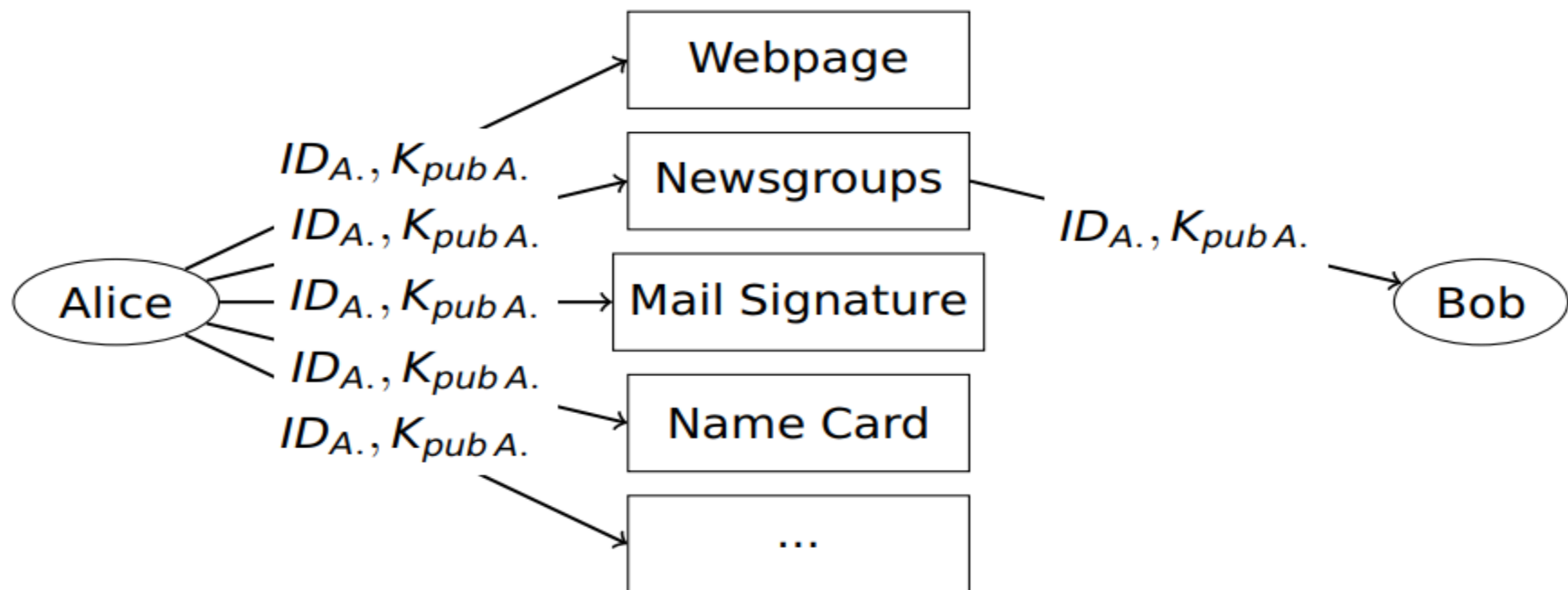
Phân phối khóa công khai

- ❖ Một số giải pháp kỹ thuật đã được đề xuất cho việc phân phối khóa công khai có thể nhóm lại thành các loại chung sau:
 - Thông báo công khai
 - Thư mục khóa công khai
 - Trung tâm thẩm quyền khóa công khai
 - Chứng thư khóa công khai

Thông báo công khai

Ưu điểm?
Nhược điểm?

- ❖ Bất kỳ một thành viên tham gia nào cũng có thể gửi khóa công khai của mình cho bất kỳ thành viên tham gia khác.

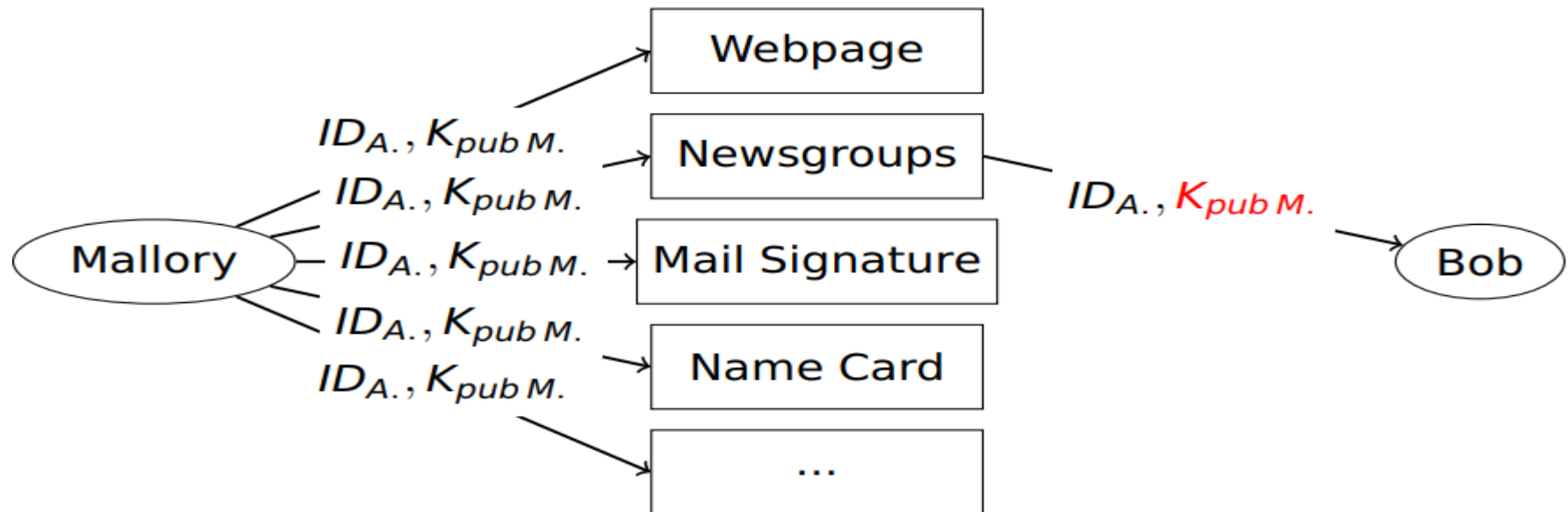


Thông báo công khai

❖ Ưu điểm: đơn giản, thuận tiện

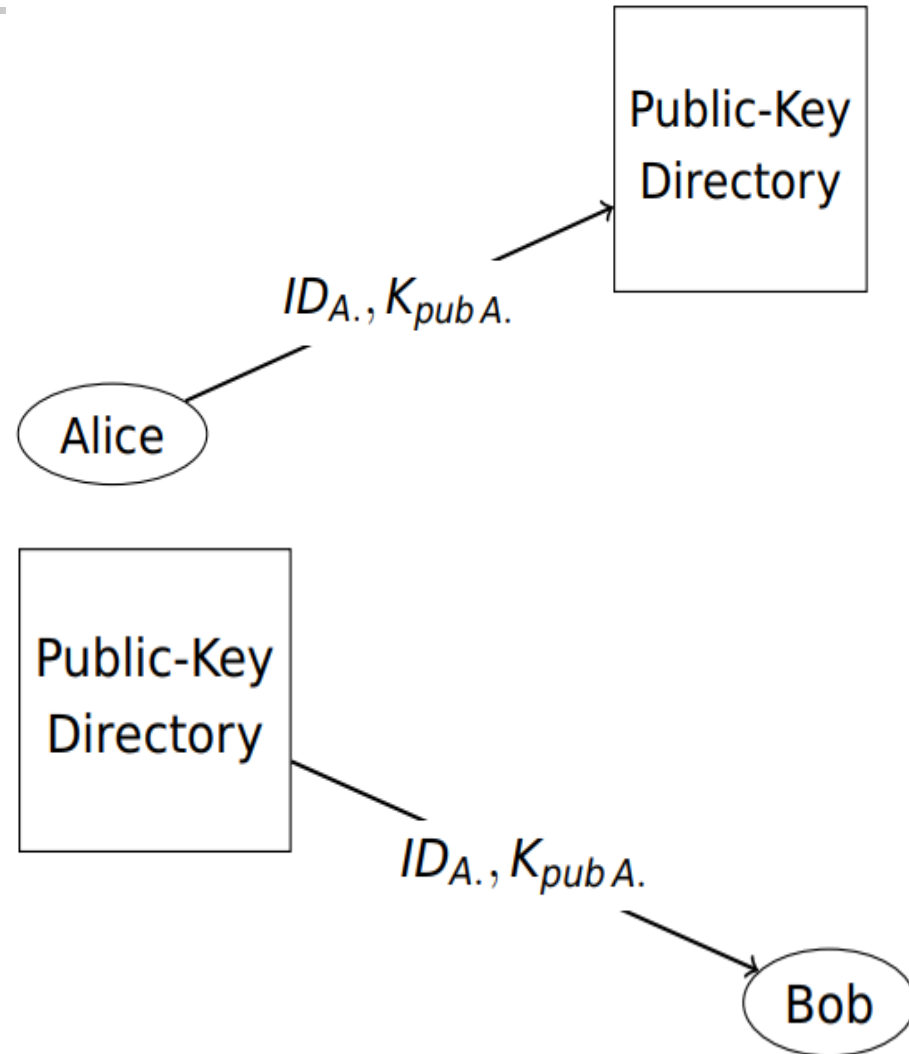
❖ Nhược điểm:

- Kẻ giả mạo có thể giả vờ là người sử dụng A và gửi một khóa công khai cho thành viên khác



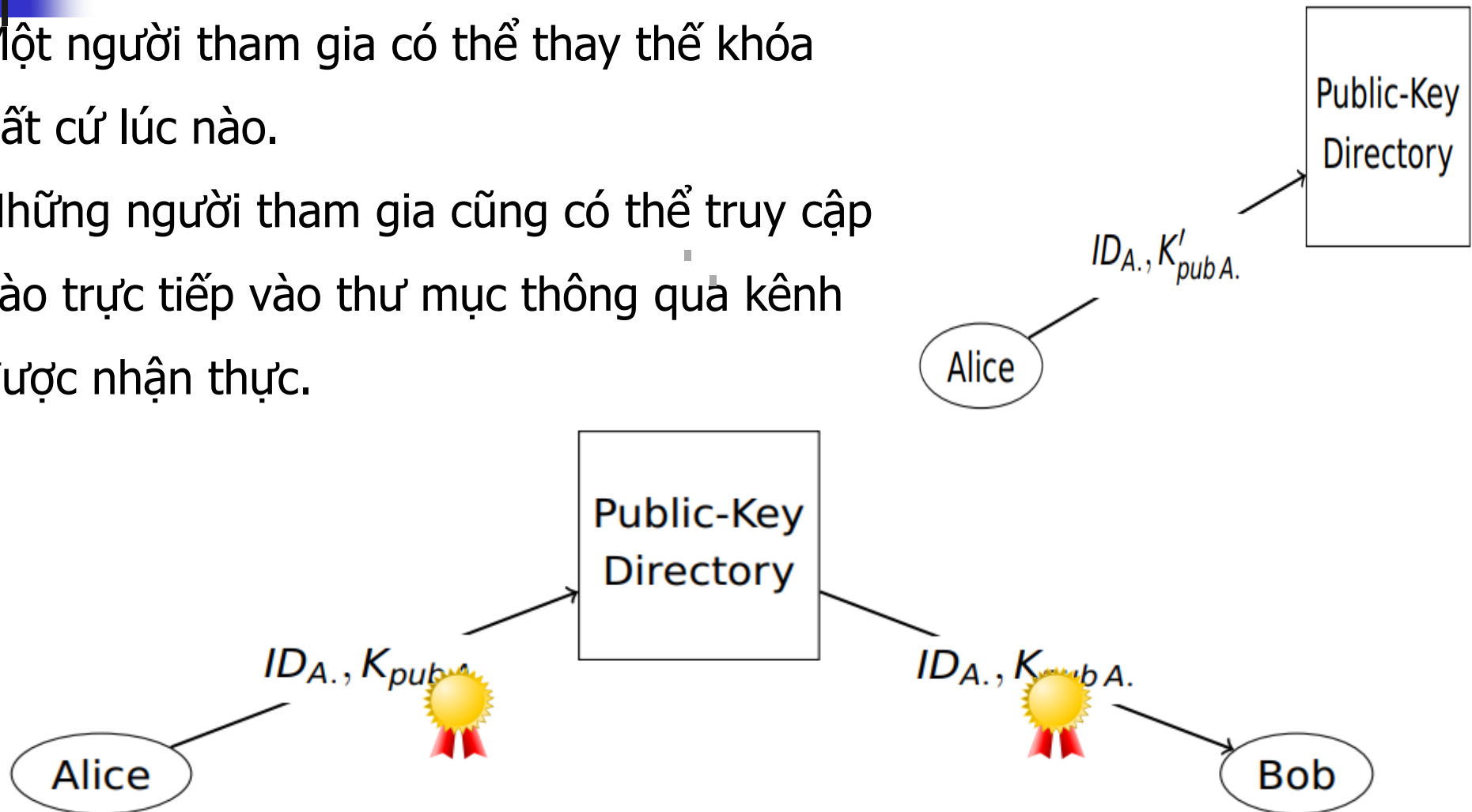
Thư mục khóa công khai

- Người có thẩm quyền duy trì một danh mục với mỗi khoản mục {tên, khóa công khai} cho từng thành viên tham gia.
- Mỗi người tham gia đăng ký một khóa công khai với bên thẩm quyền quản lý danh mục. Việc đăng ký thư mục qua các hình thức truyền thông được chứng thực an toàn.



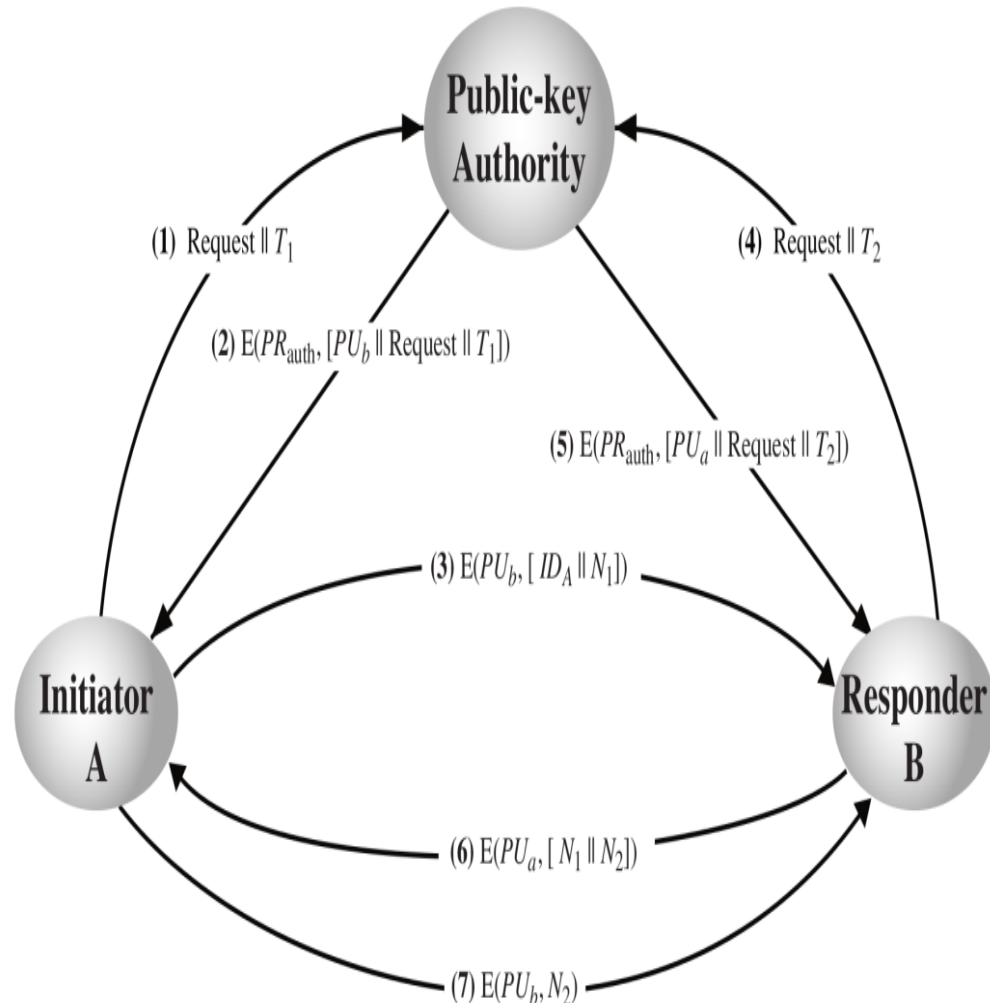
Thư mục khóa công khai

- Một người tham gia có thể thay thế khóa bất cứ lúc nào.
- Những người tham gia cũng có thể truy cập vào trực tiếp vào thư mục thông qua kênh được nhận thực.



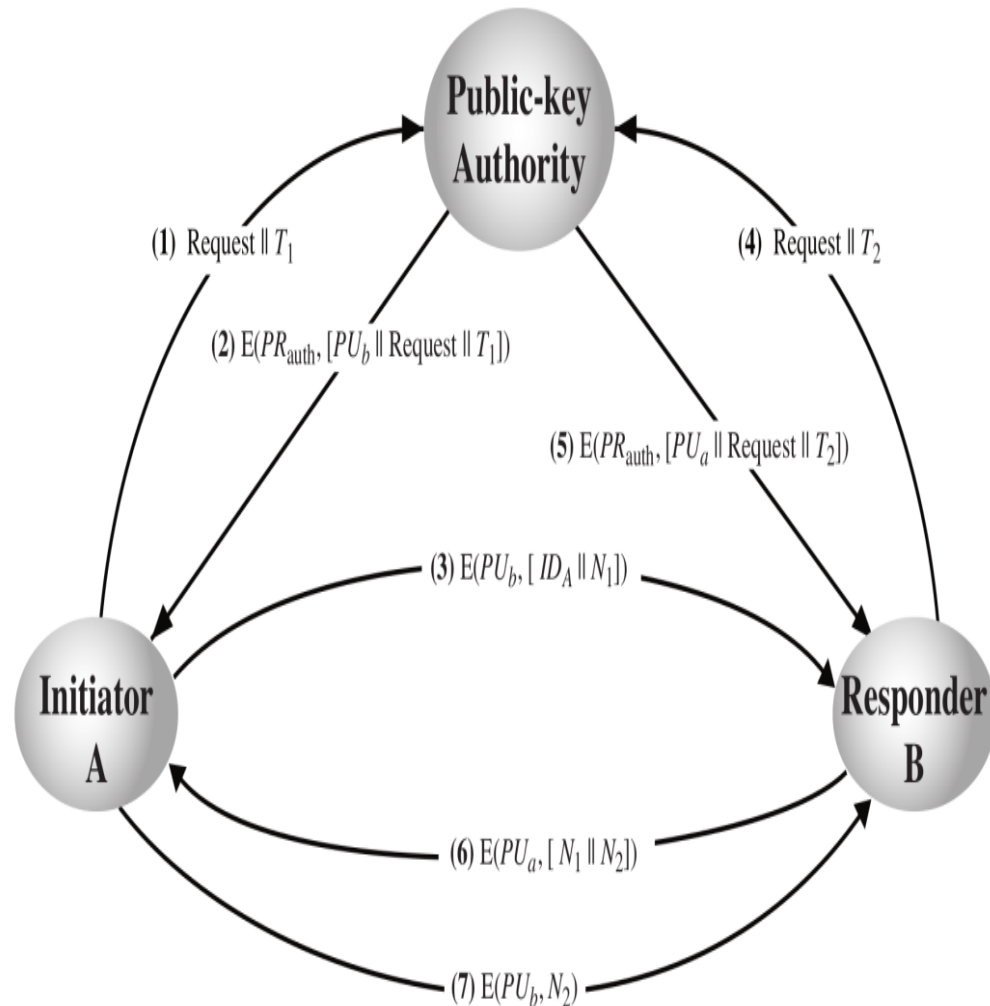
Trung tâm thẩm quyền khóa công khai

1. A gửi một bản tin chứa tem thời gian tới trung tâm thẩm quyền khóa công khai có chứa một yêu cầu khóa công khai của B.
2. Trung tâm ủy quyền trả lời một bản tin được mã hóa bằng khóa riêng của chính trung tâm, PR_{auth} . Như vậy, A có thể giải mã các bản tin bằng khóa công khai của trung tâm thẩm quyền.
3. A lưu trữ công khai của B và sử dụng nó để mã hóa một bản tin đến B chứa định danh của A (ID_a) và một nonce (N_1) để xác định giao dịch duy nhất này.



Trung tâm thẩm quyền khóa công khai

4. B thu lấy khóa công khai của A từ trung tâm thẩm quyền theo cách thức tương tự như A lấy khóa công khai của B.
5. Khóa công khai đã được chuyển giao một cách an toàn để A và B có thể bắt đầu trao đổi các thông tin an toàn.
6. B gửi một bản tin đến A được mã hóa với PU_a và chứa $N1$ và $N2$. Do chỉ có B có thể có bản tin giải mã (3), sự hiện diện của N_1 trong bản tin tại bước (6) đảm bảo rằng A biết trả lời từ B.
7. A trả lại nonce N_2 được mã hóa bằng khóa công khai của B, để B biết rằng bản tin đó đến từ A





Chứng thư số khóa công khai

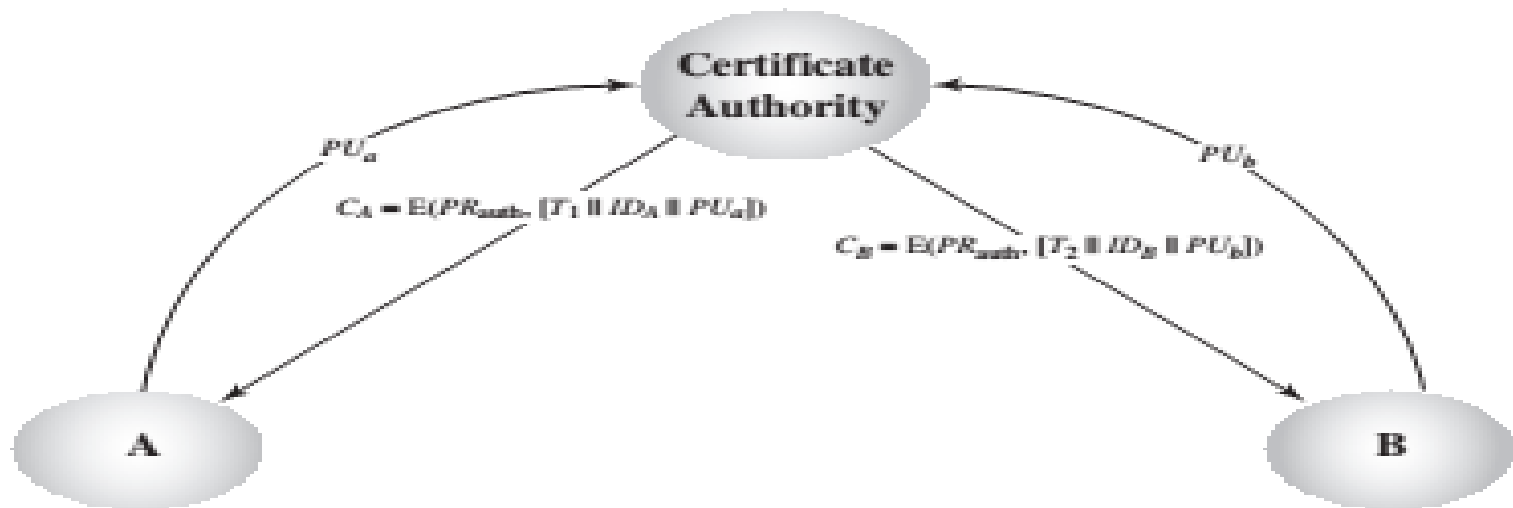
- Một cách tiếp cận khác, lần đầu tiên được đề xuất bởi Kohnfelder sử dụng chứng thư cho những người tham gia để trao đổi các khóa
- Một giấy chứng thư: bao gồm một khóa công khai, một nhận dạng của chủ sở hữu chính và toàn bộ khối chữ ký của một bên thứ ba đáng tin cậy.



Chứng thư số khóa công khai

- Bên thứ ba: là một cơ quan cấp chứng thư như một cơ quan chính phủ hoặc một tổ chức tài chính
- Người dùng có thể gửi khoá công khai tới cơ quan cấp chứng chỉ một cách an toàn và có được một giấy chứng nhận.
- Các thành viên khác có thể xác minh rằng chứng chỉ đã được tạo ra bởi nơi có thẩm quyền.

Chứng thư khóa công khai



(a) Obtaining certificates from CA



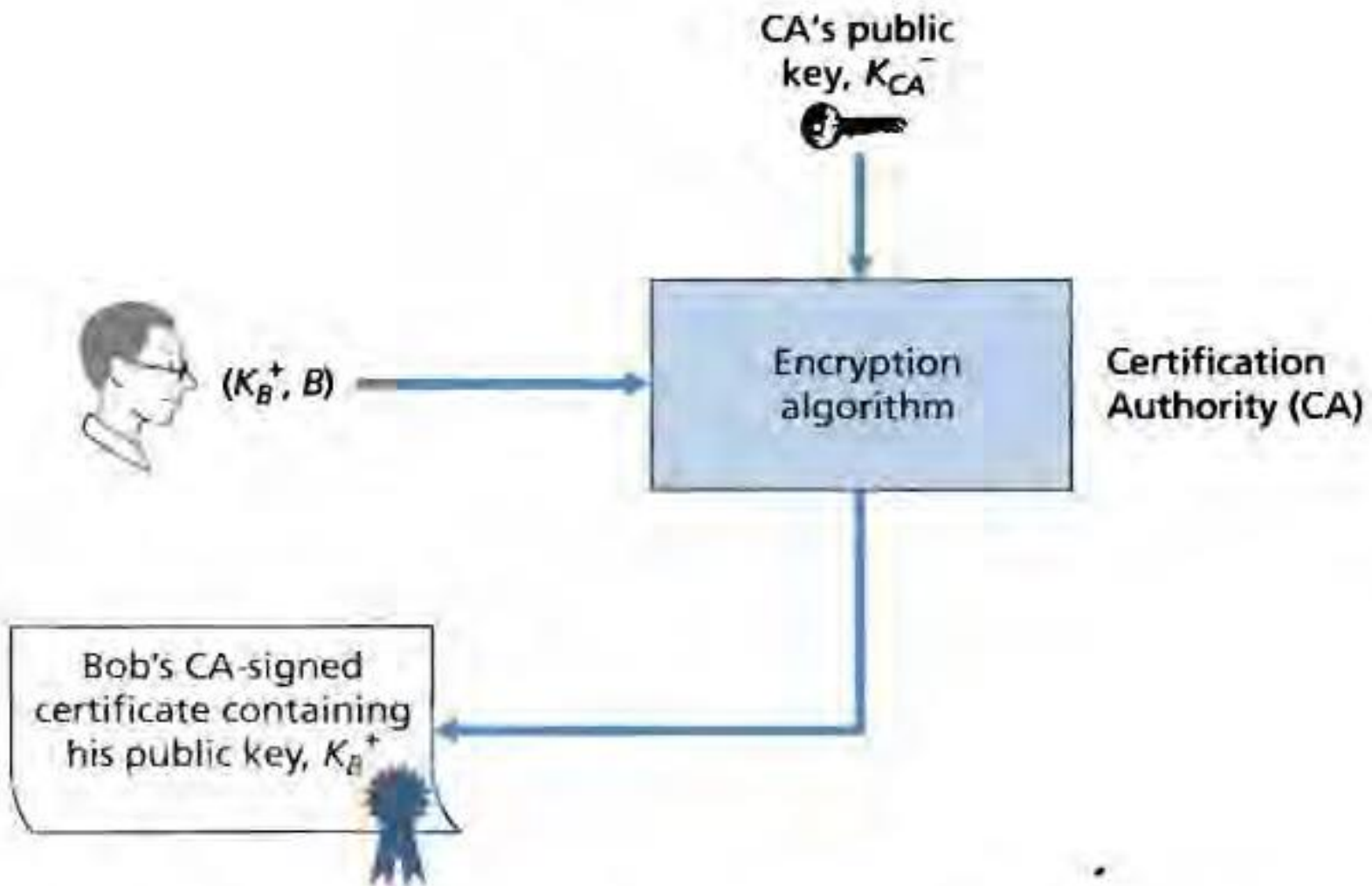
(b) Exchanging certificates



Chứng thực số CA

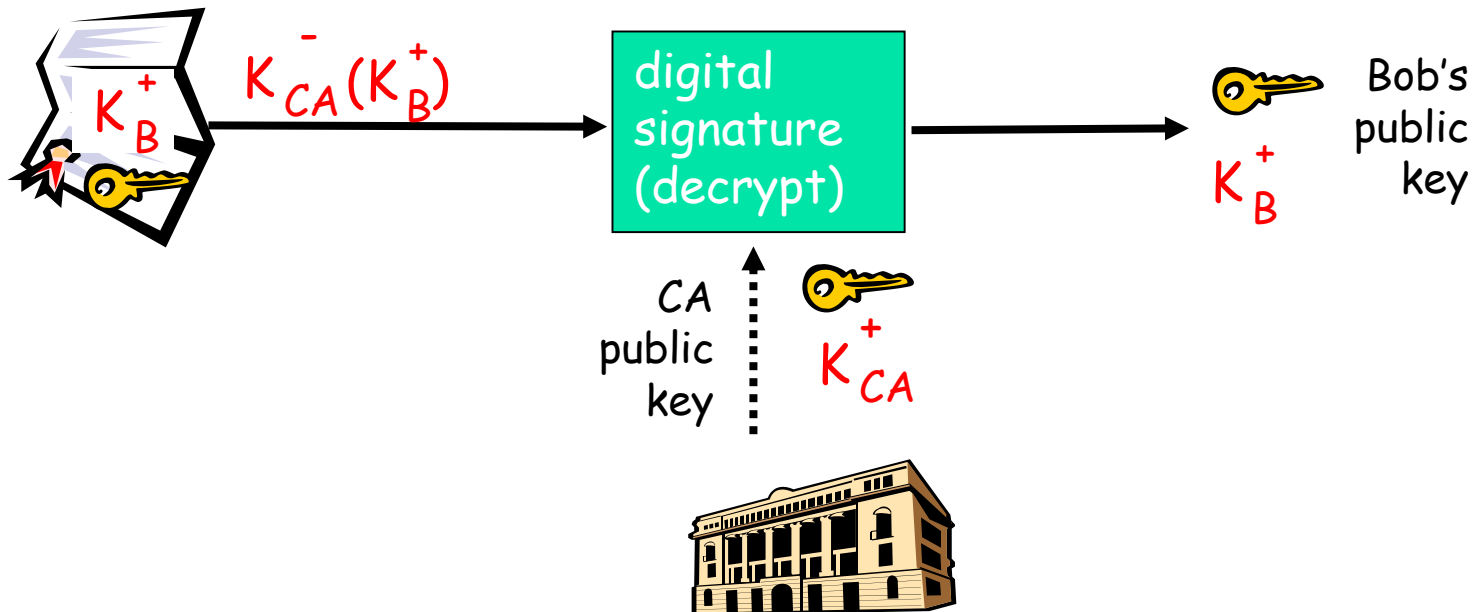
- **Certification Authority (CA):** liên kết khóa công khai với thực thể cụ thể E.
- E đăng ký khóa công khai với CA.
 - E cung cấp “bằng chứng định danh” (proof of identity) cho CA.
 - CA mở chứng thư (certificate) ràng buộc E với khóa công khai của nó.
 - Chứng thư chứa khóa công khai của E được ký số bởi CA: CA thông báo “Đây chính là khóa công khai của E”.

Tạo chứng thư khóa công khai

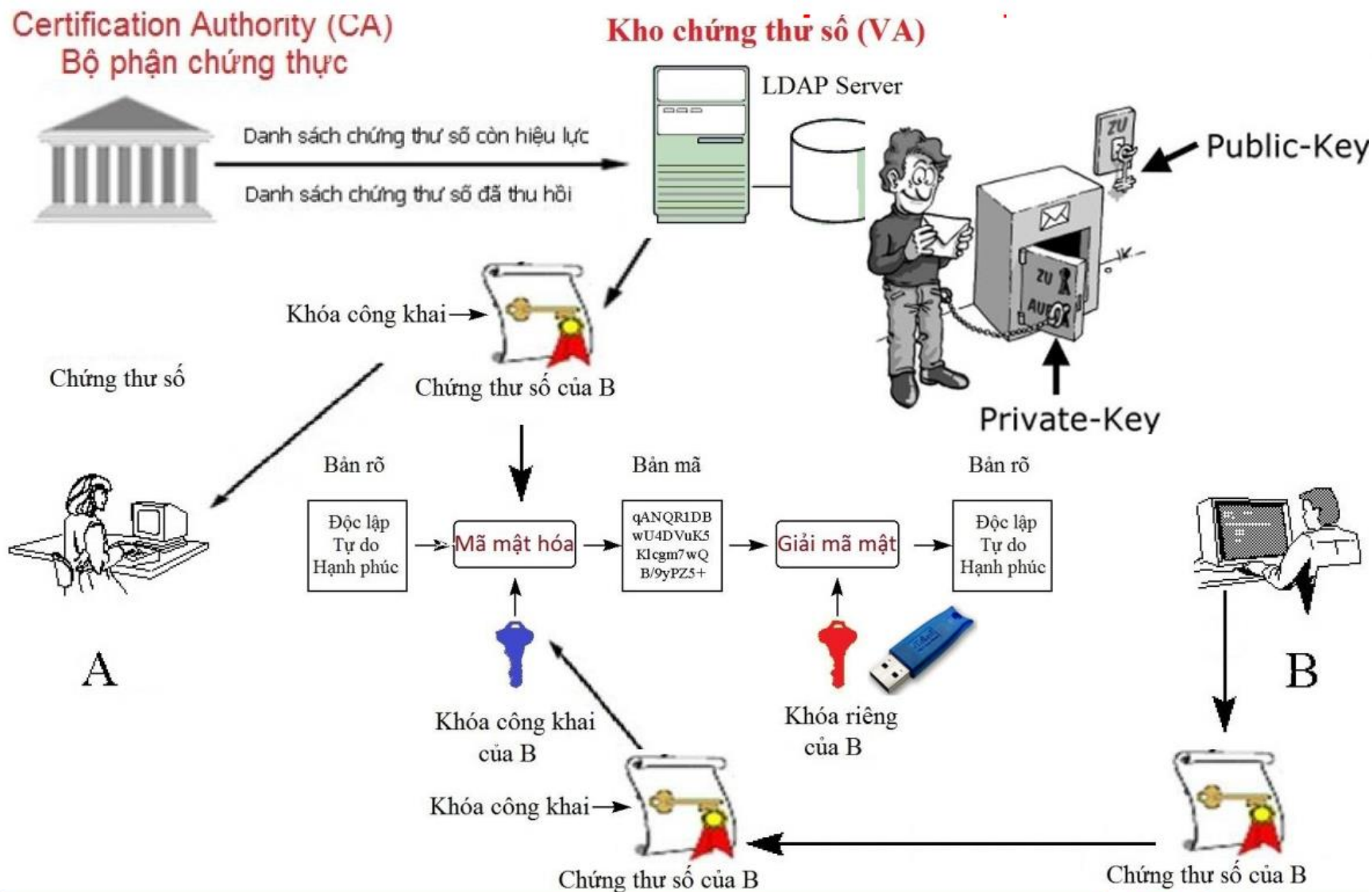


Chứng thực khóa công khai

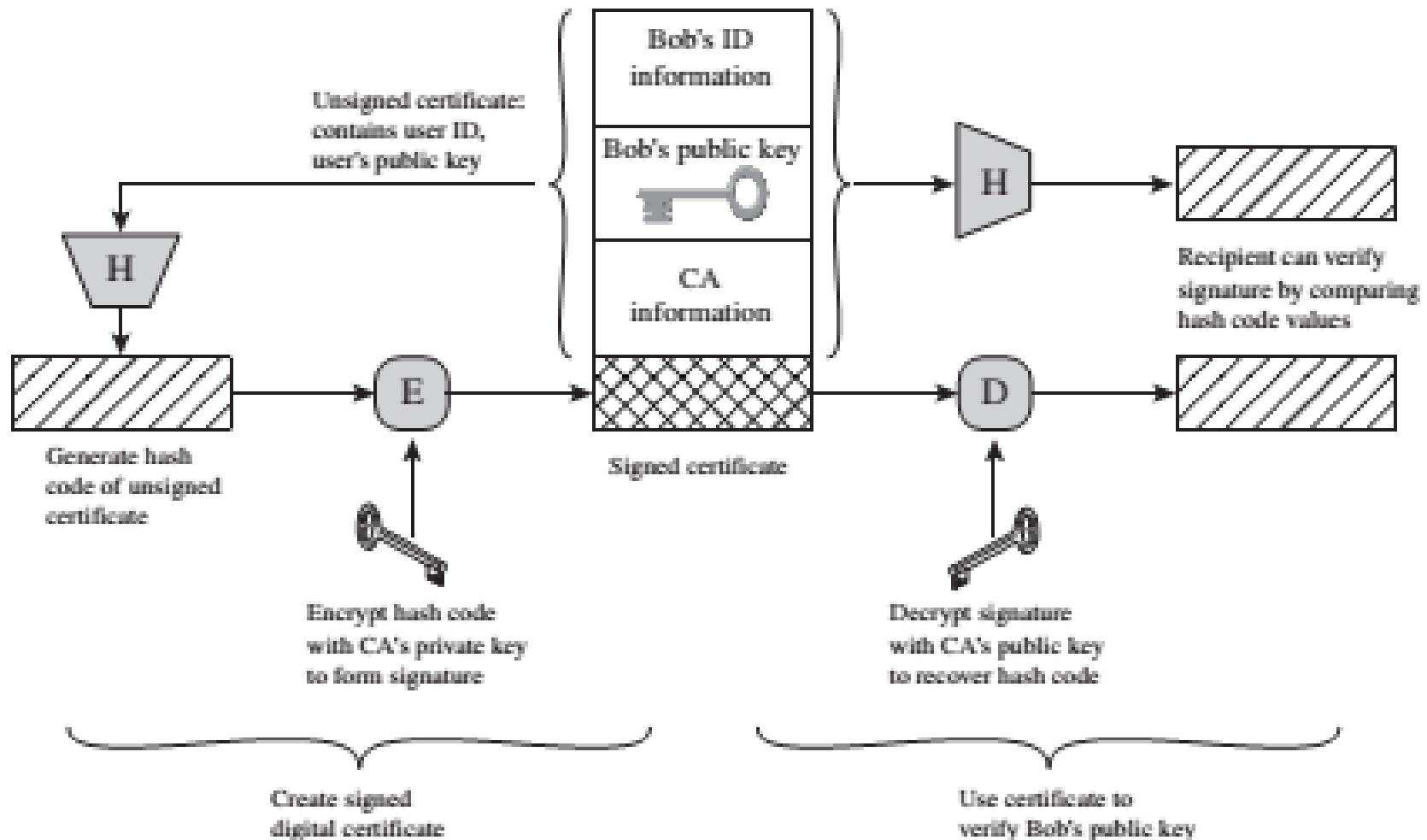
- Khi A muốn khóa công khai của B:
 - Lấy chứng thư số của B (từ B hoặc từ đâu đó).
 - Áp dụng khóa công khai của CA cho chứng thư của B, giải mã để lấy khóa công khai của B.



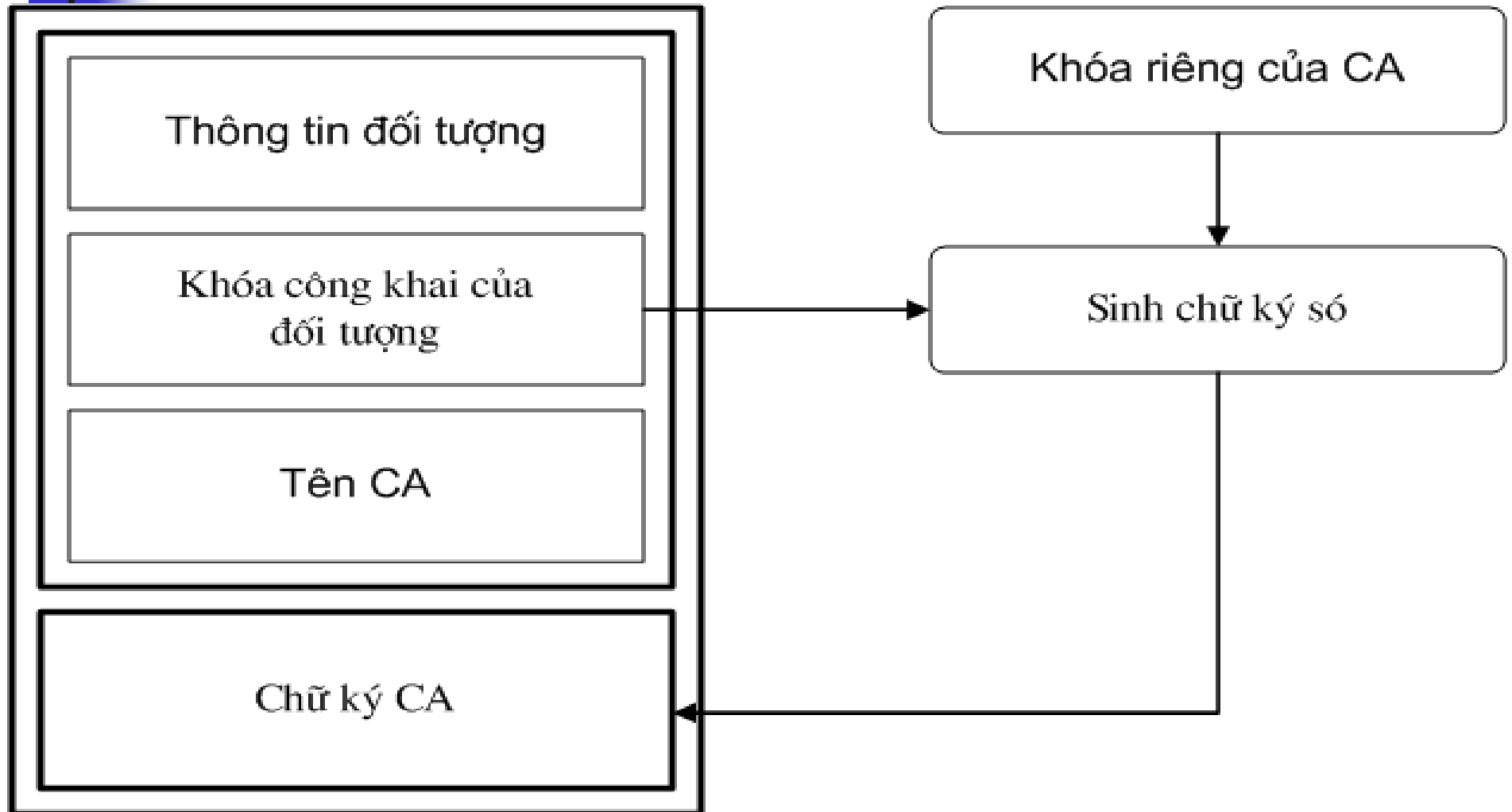
Sử dụng chứng thư khóa công khai



Sử dụng chứng thư khóa công khai



Cấu trúc chung chứng thư khóa công khai



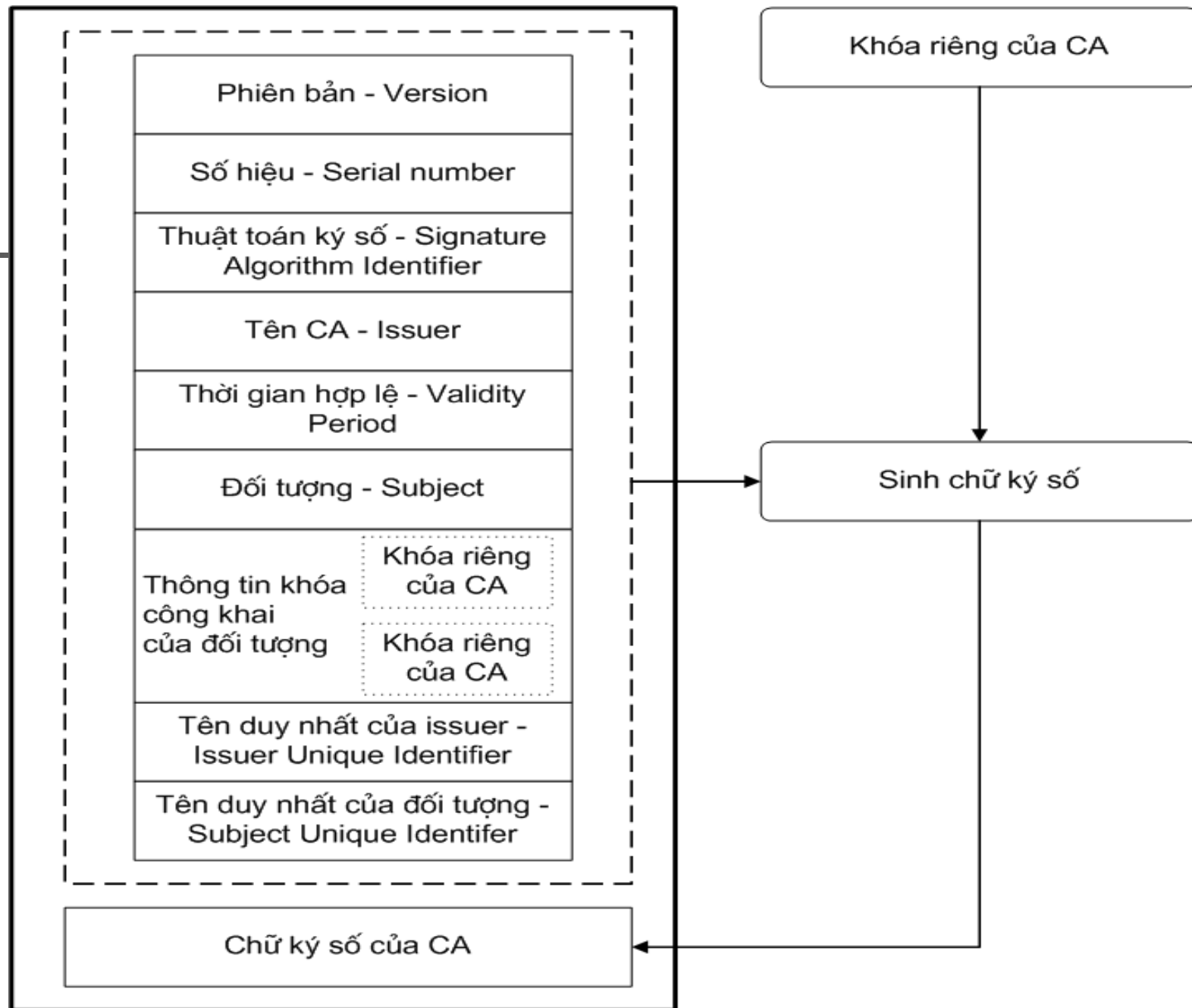


Chứng thư số X.509

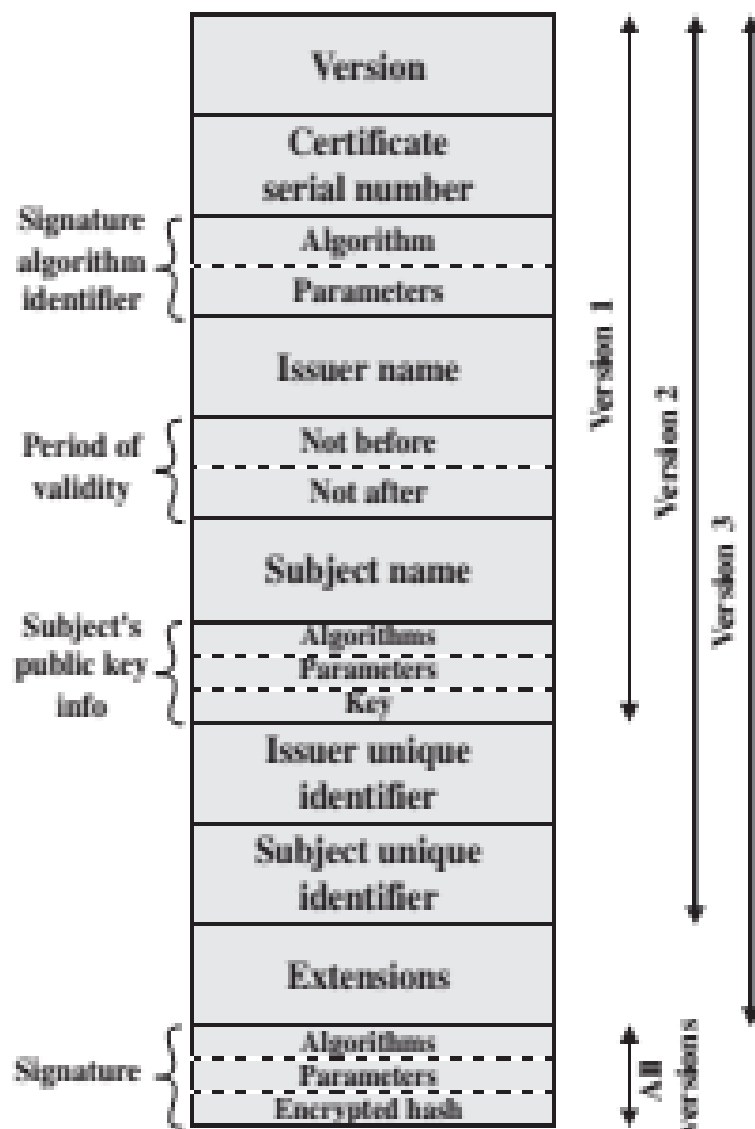
- Chứng nhận X.509 là chứng nhận khóa công khai phổ biến nhất.
- Tổ chức ITU (International Telecommunications Union) đã đưa ra chuẩn X.509 vào năm 1988.
- Một chứng nhận khóa công khai kết buộc một khóa công khai với sự nhận diện của một người (hoặc một thiết bị). Khóa công khai và tên thực thể sở hữu khóa này là hai mục quan trọng trong một chứng nhận.



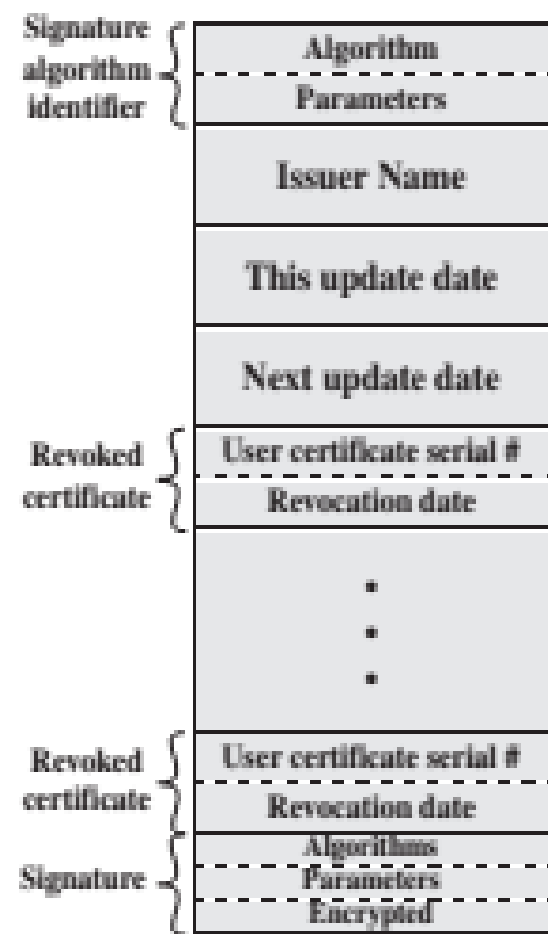
Chứng thư số X.509 v.1 và v.2



Chứng thư số X.509 v.1 và v.2



(a) X.509 certificate

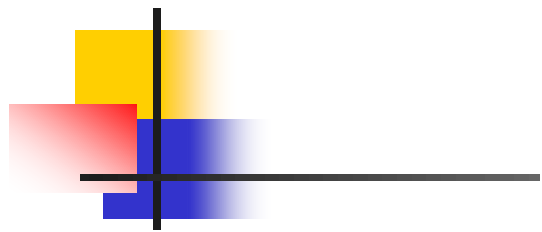


(b) Certificate revocation list

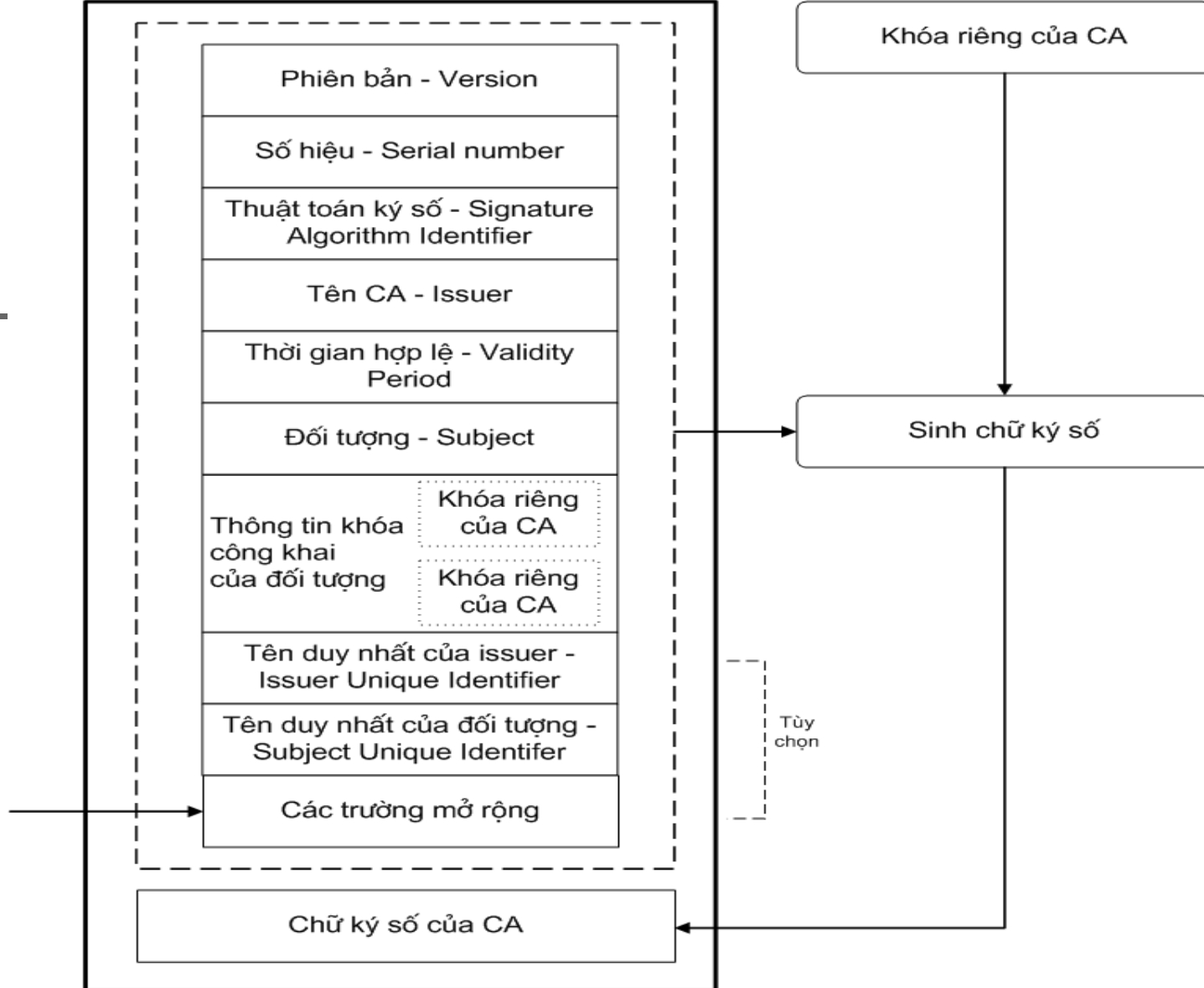


X.509 v.3

- ❖ Đối tượng có thể có các chứng chỉ khác nhau với các khóa công khai khác nhau và giả thiết rằng các cặp khóa cần được cập nhật định kỳ, do vậy cần phải có cách để phân biệt các chứng chỉ khác nhau của đối tượng này một cách dễ dàng.
- ❖ Một tên đối tượng trở thành tên duy nhất nhưng nó không có đủ thông tin cho những người sử dụng chứng chỉ khác nhận dạng đối tượng, do đó cần có thêm thông tin nhận dạng đối tượng.
- ❖ Một số các ứng dụng cần nhận dạng những người sử dụng thông qua các dạng tên xác định ứng dụng. Ví dụ: trong an toàn thư tín điện tử; trong việc gắn kết một khóa công khai với một địa chỉ thư tín điện tử.



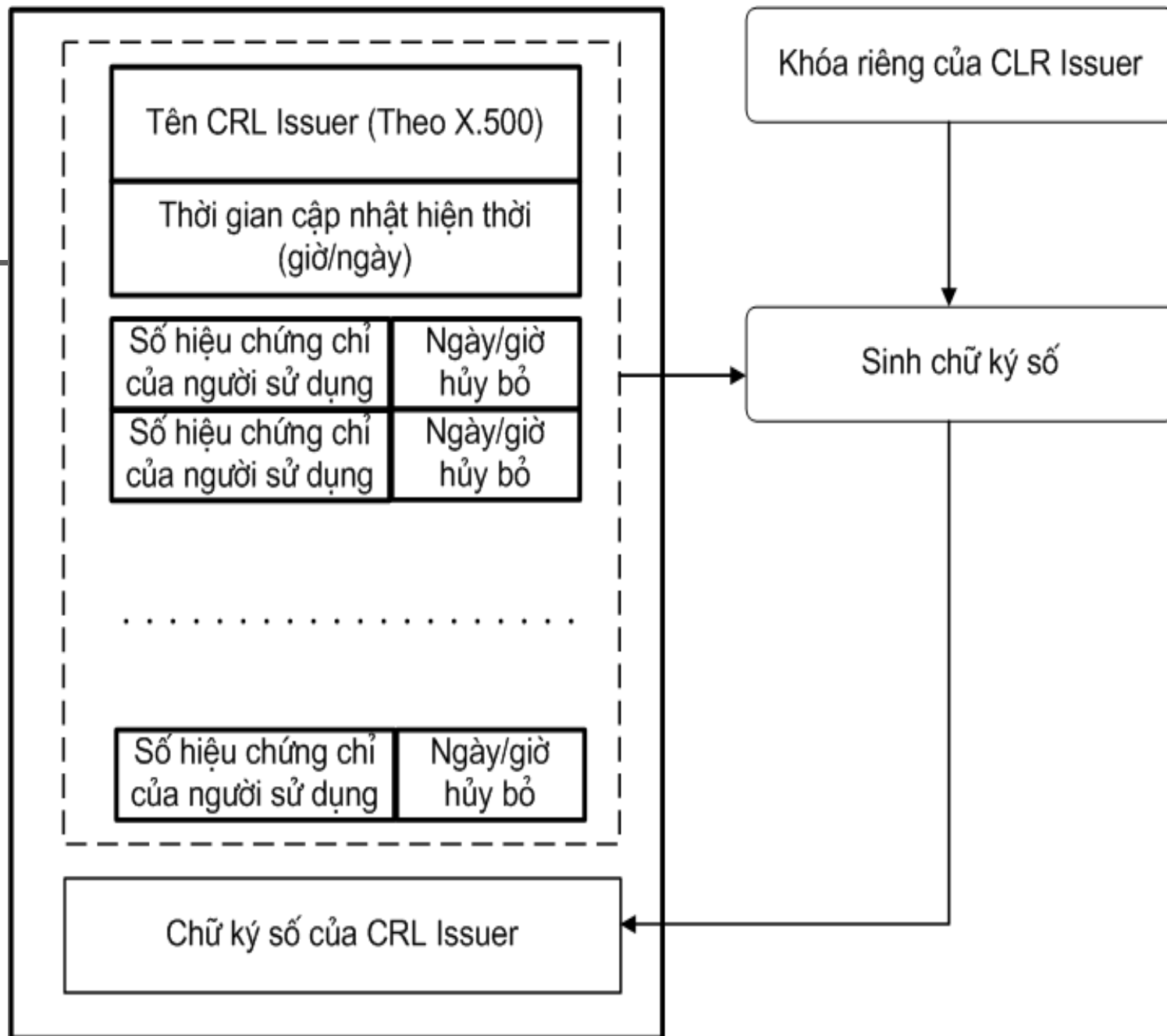
Cấu trúc X.509 v.3

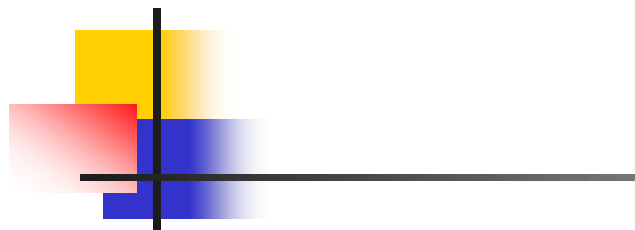


Định dạng trường mở rộng

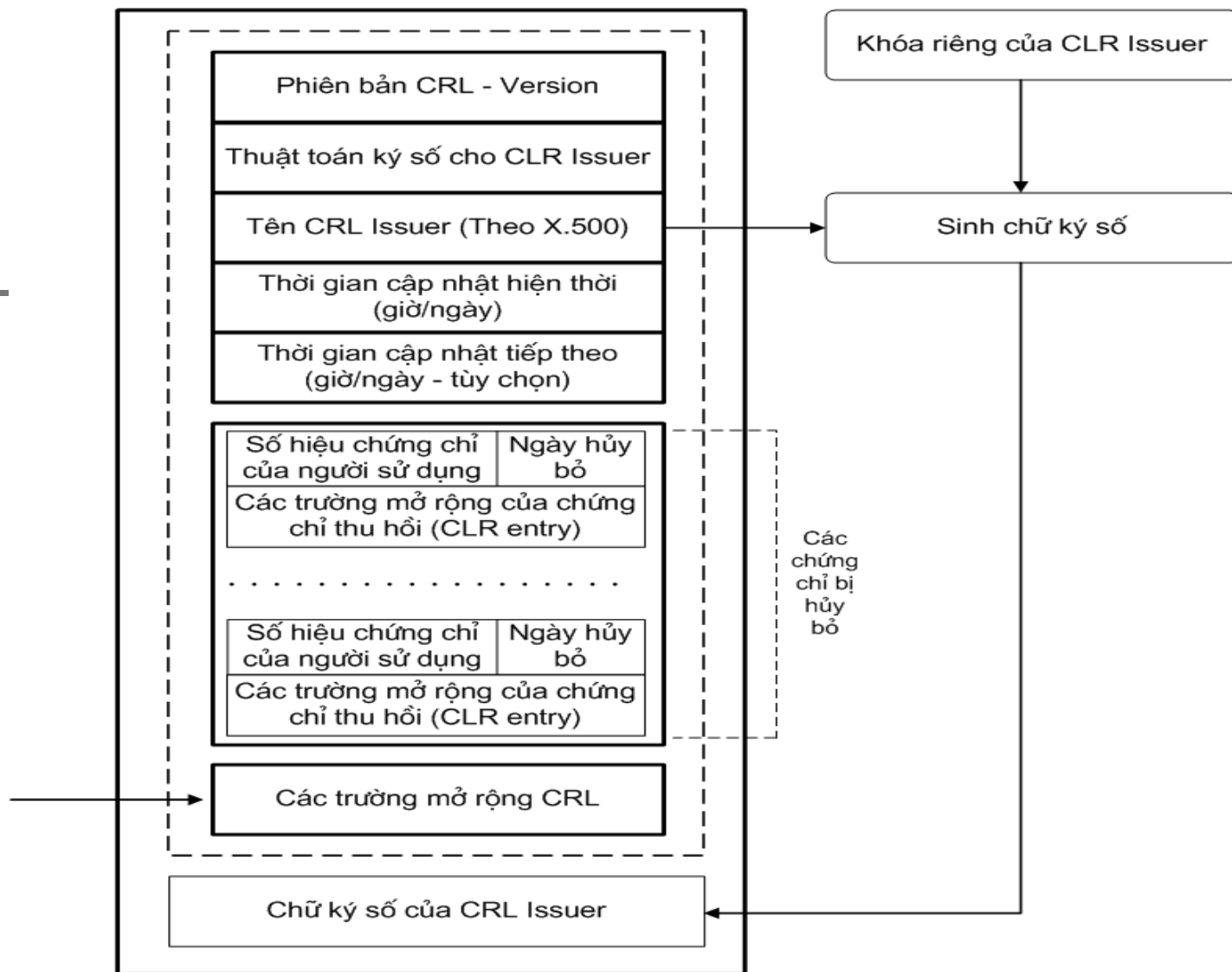
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị
.....		
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị

Thu hồi chứng thư



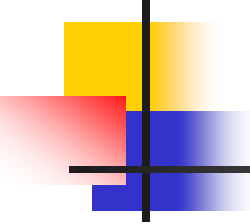


Khuôn dạng thu hồi chứng thư của X.509 v.3

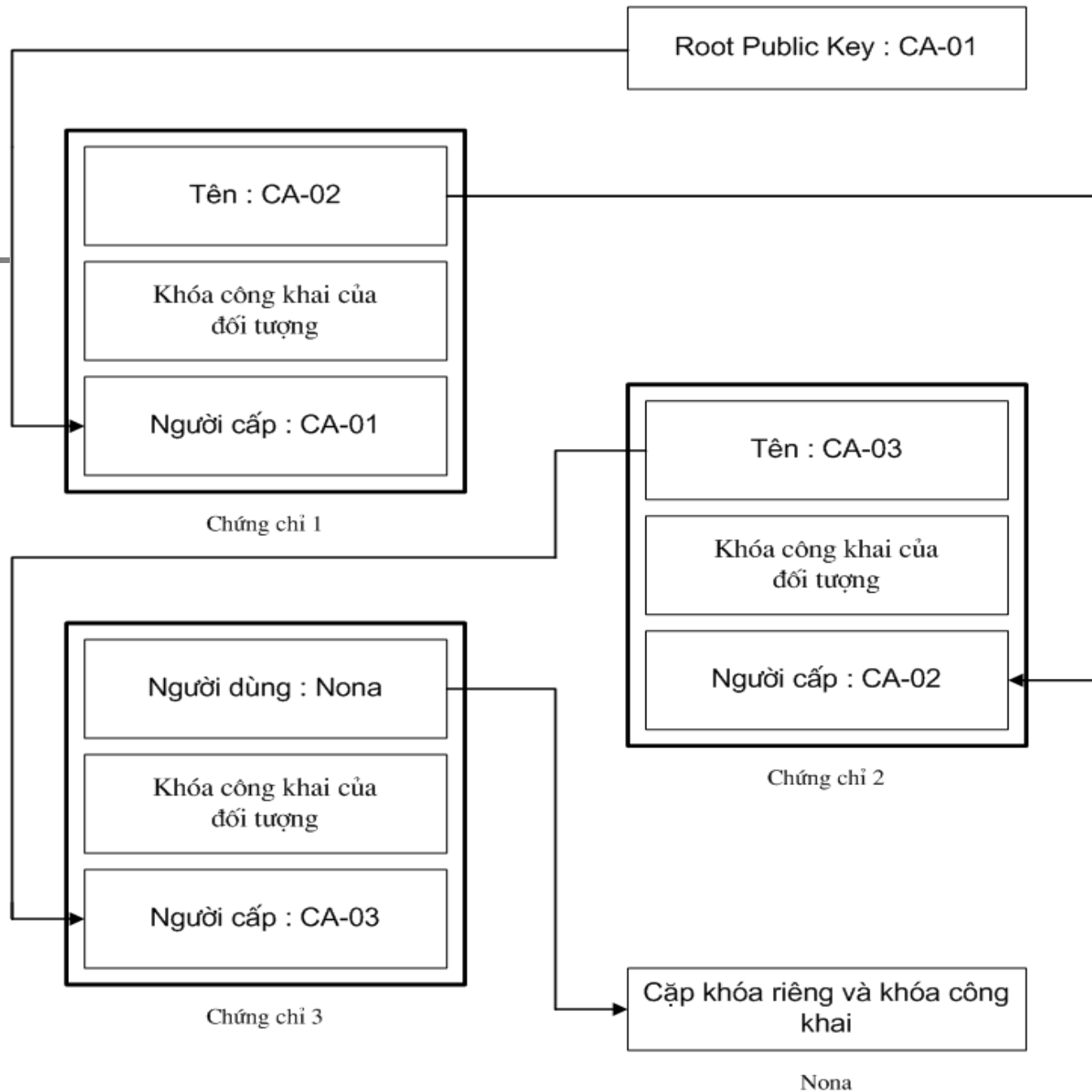


Định dạng trường mở rộng

Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị
.....		
Kiểu trường mở rộng	Cần thiết - Có/Không	Giá trị

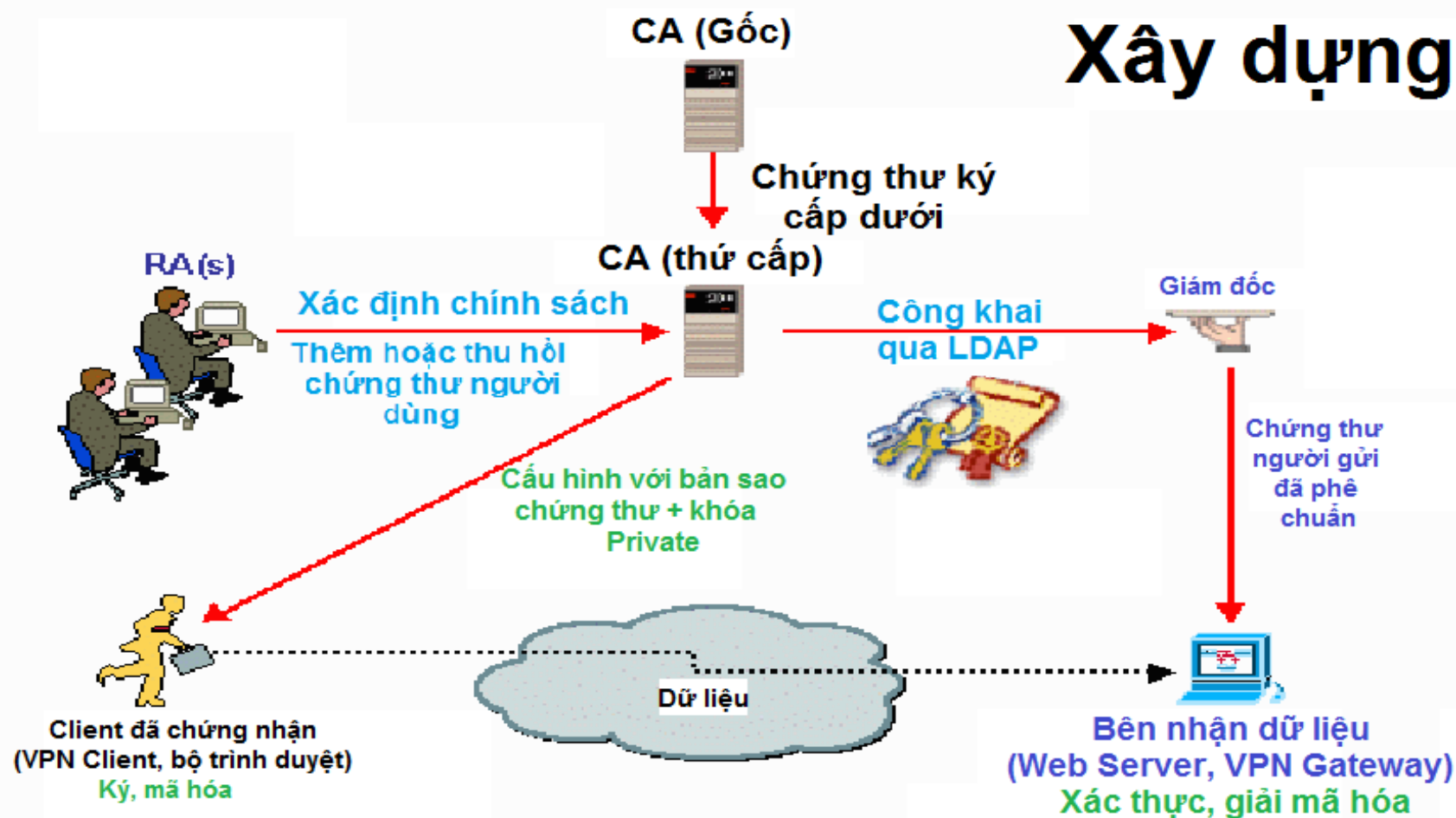


Mô hình chứng thực đệ quy



Hạ tầng PKI

Xây dựng PKI





Các thành phần PKI (1)

❖ ***Tổ chức phát hành chứng thư (Certificate Authority - CA):***

là một bên thứ ba được tin cậy có trách nhiệm tạo, quản lý, phân phối, lưu trữ và thu hồi các chứng thư số. CA sẽ nhận các yêu cầu cấp chứng chỉ số và chỉ cấp cho những ai đã xác minh được nhận dạng của họ.

❖ ***Tổ chức đăng ký (Registration Authority - RA):*** đóng vai trò trung gian giữa CA và người dùng. Khi người dùng cần chứng thư số mới, họ gửi yêu cầu tới RA và RA sẽ xác nhận tất cả các thông tin nhận dạng cần thiết trước khi chuyển tiếp yêu cầu đó tới CA để CA thực hiện tạo và ký số lên chứng thư rồi gửi về cho RA hoặc gửi trực tiếp cho người dùng.



Các thành phần PKI (2)

❖ ***Kho và lưu trữ chứng thư (Certificate Repository và Archive - CRA)*** : Đầu tiên là kho lưu trữ công khai và phân phối các chứng thư và CRL (chứa danh sách các chứng thư không còn hiệu lực). Kho thứ hai là một cơ sở dữ liệu được CA dùng để sao lưu các khóa hiện đang sử dụng và lưu trữ các khóa hết hạn, kho này cần được bảo vệ an toàn như chính CA.

❖ ***Máy chủ bảo mật (Security Server - SS)*** : là một máy chủ cung cấp các dịch vụ quản lý tập trung tất cả các tài khoản người dùng, các chính sách bảo mật chứng thư số, các mối quan hệ tin cậy (trusted relationship) giữa các CA trong PKI, lập báo cáo và nhiều dịch vụ khác.



Các thành phần PKI (3)

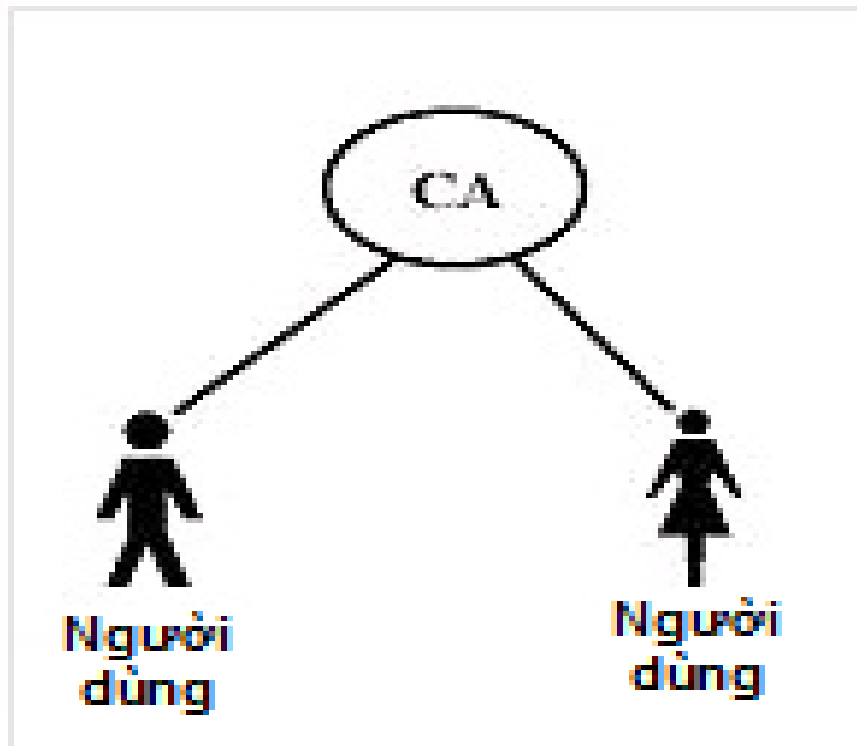
❖ ***Các ứng dụng cho phép PKI và những người sử dụng PKI (PKI-enabled applications và PKI users):*** bao gồm người dùng sử dụng các dịch vụ của PKI và các phần mềm có hỗ trợ cài đặt và sử dụng các chứng thư số như các trình duyệt web, các ứng dụng email ở phía máy khách.



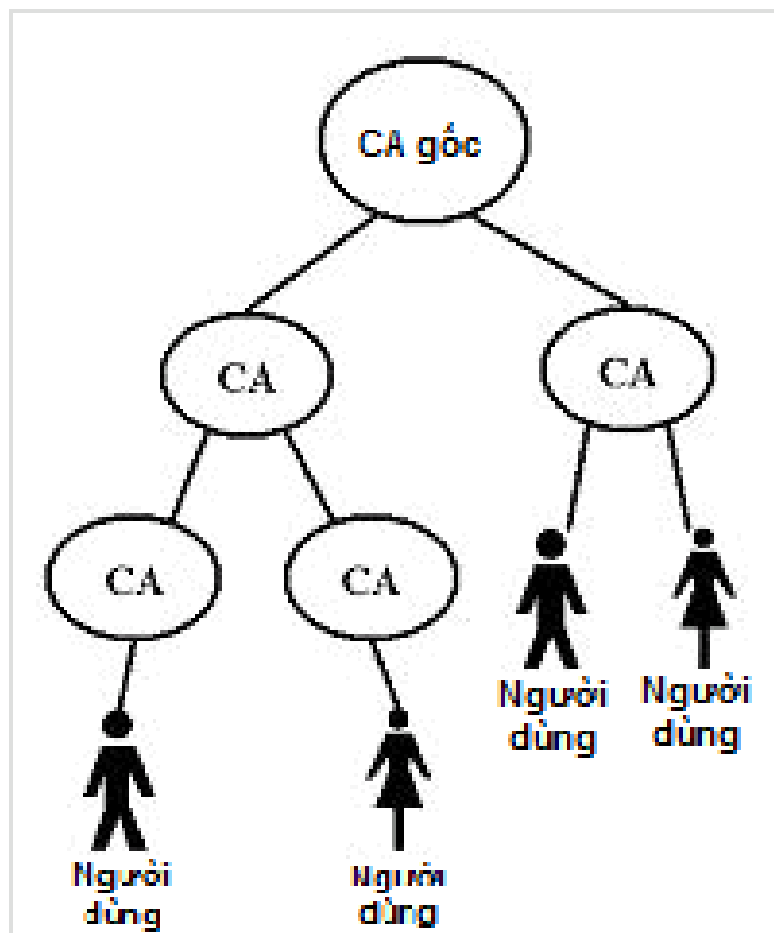
Mô hình PKI

- PKI phân cấp;
- PKI dạng lưới;
- CA đơn lẻ - Single CA.

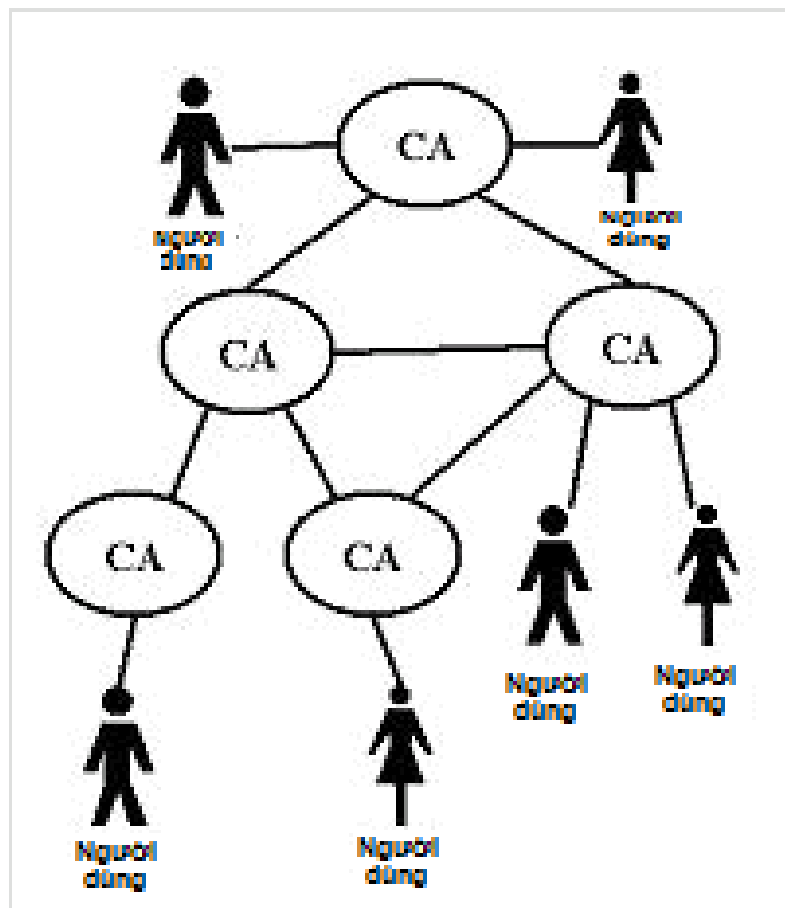
Mô hình CA đơn lẻ



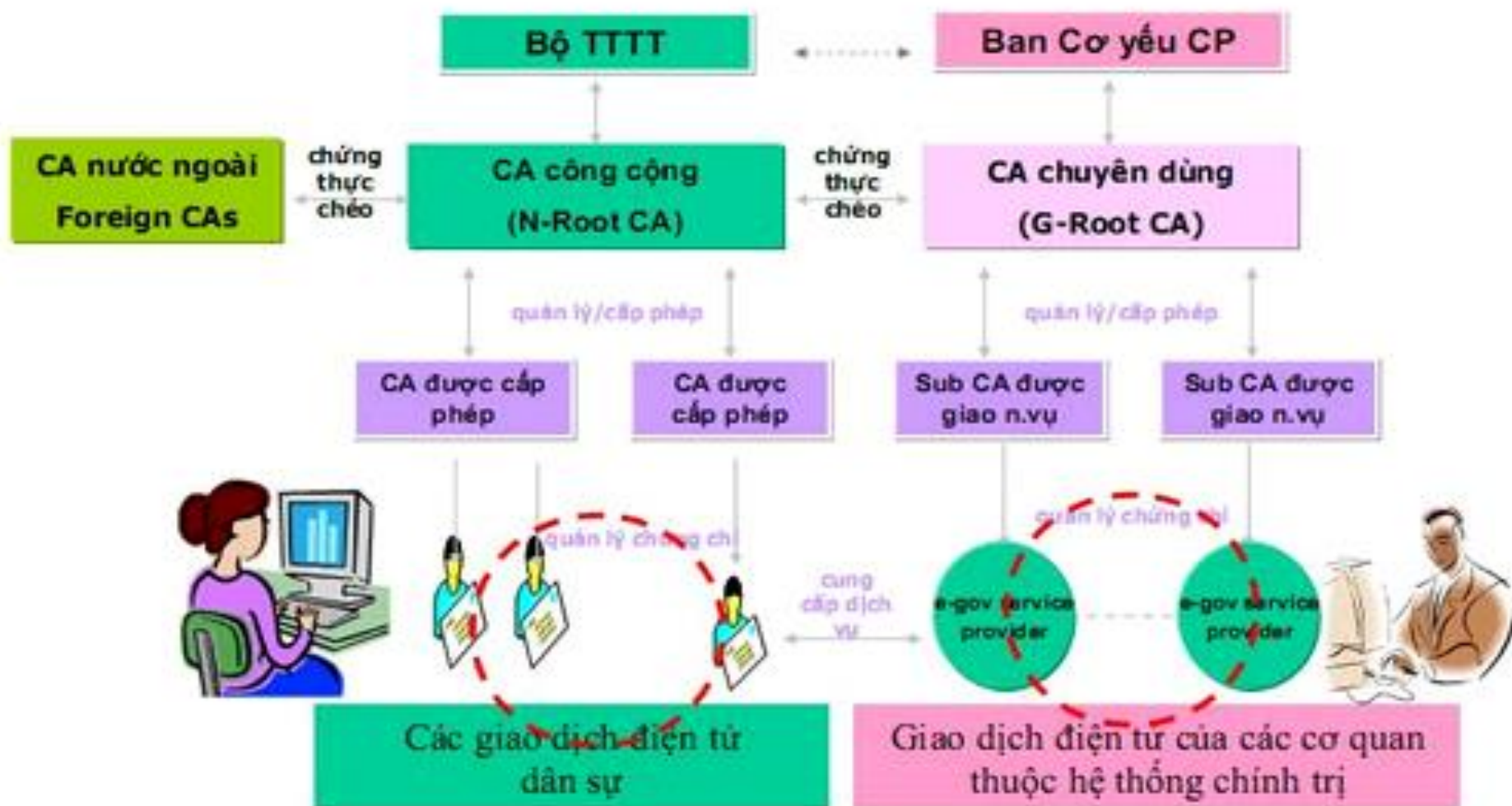
Mô hình CA phân cấp



Mô hình CA hình lưới



Mô hình CA tại Việt nam





Chương 5: Xác thực

5.1 Quản lý và phân phối khóa

5.2 Xác thực người sử dụng



Xác thực người sử dụng

- Các bước trong điều khiển truy cập

Định danh (Identification):

Người dùng cung cấp danh định (identity)



Xác thực (Authentication):

Người dùng chứng minh danh định đó là đúng



Ủy quyền (Authorization):

Xác định quyền mà người dùng có



Xác thực người sử dụng

Định danh:

- Người dùng cung cấp danh định của mình cho hệ thống
- Mục đích: tìm kiếm sự **tồn tại** và **quyền hạn** cho người dùng

Xác thực người sử dụng

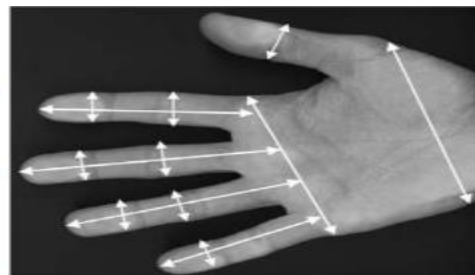
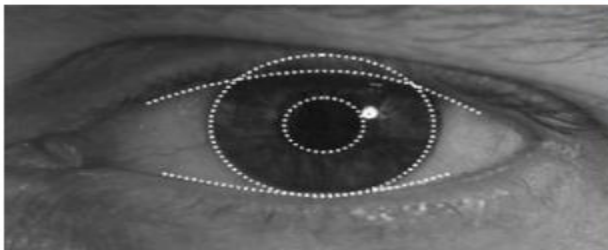
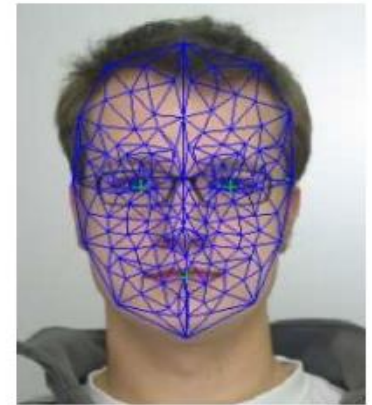
Xác thực:

- Người dùng cung cấp bằng chứng là danh định đó là đúng và phù hợp với mình.
- Mục đích:
 - Chứng minh danh định là **hợp lệ** và **phù hợp** với người dùng.
 - Quyết định có cho phép người dùng truy cập vào tài nguyên của hệ thống hay không



Xác thực người sử dụng

- ❖ Có 2 phương pháp định danh: người dùng tự nhập thông tin về định danh và định danh số hóa (có 3 dạng)
 - Người dùng tự nhập thông tin về định danh: user name, số tài khoản
 - Định danh số hóa: danh định sinh trắc
 - Nhận dạng khuôn mặt
 - Quét tròng mắt
 - Hình học bàn tay
 - Nhận dạng vân tay





Xác thực người sử dụng

❖ Có 2 phương pháp định danh:

➤ Định danh số hóa: danh định máy tính

- Tên máy tính
- Địa chỉ MAC
- Địa chỉ IP

➤ Định danh số hóa: danh định số

- Chứng chỉ số
- Thẻ thông minh



Xác thực người sử dụng

❖ Có 3 phương pháp xác thực:

- Những gì bạn biết (Something you know)
- Những gì bạn có (Something you have)
- Những gì là chính bạn (Something you are)

❖ Một phương pháp xác thực tốt là phương pháp không dễ bị đoán và bị làm giả



Xác thực người sử dụng

❖ Phương pháp xác thực: Những gì bạn biết

- Ví dụ: Password, số PIN (Personal Identification Number)
- Ưu điểm:
 - Tiện lợi
 - Chi phí thấp
- Nhược điểm:
 - Password yếu, dễ đoán
 - Mức độ bảo mật phụ thuộc vào độ phức tạp của password



Xác thực người sử dụng

❖ Phương pháp xác thực: Những gì bạn biết

- Vấn đề của password:
 - ✓ Passw yếu, dễ đoán (tên người dùng, ngày sinh,...)
- Xây dựng chính sách password:
 - ✓ Độ dài
 - ✓ Có ký tự đặc biệt, có ký tự viết hoa,...
 - ✓ Khác với username, thay đổi passw định kỳ,...
- Cần cân bằng giữa hacker khó đoán và người dùng có thể nhớ



Xác thực người sử dụng

❖ Phương pháp xác thực: Những gì bạn có

- Thẻ thông minh (smart card): có bộ nhớ nhỏ và có khả năng thực hiện 1 vài tính toán
- Trong thẻ có lưu thông tin về người dùng và password
- Địa chỉ MAC, địa chỉ IP



Xác thực người sử dụng

❖ Phương pháp xác thực: Những gì là chính bạn

- Sử dụng các yếu tố sinh trắc học để xác thực
 - Nhận dạng khuôn mặt
 - Quét tròng mắt
 - Hình học bàn tay
 - Nhận dạng vân tay
- Xác thực bằng sinh trắc học gồm 2 bước
 - Đăng ký mẫu
 - Nhận dạng



Xác thực người sử dụng

❖ Phương pháp xác thực: Những gì là chính bạn

- Ưu điểm của xác thực sinh trắc học
 - Khó tấn công
- Nhược điểm của xác thực sinh trắc học
 - Tồn kém: lưu trữ, xử lý



Xác thực người sử dụng

❖ Phương pháp xác thực: so sánh

- Phương pháp xác thực tốt thì tốn kém
- Xét về khả năng bị tấn công:
 $\text{Sinh trắc học} < \text{Smart card} < \text{Password}$
- Xét về chi phí:
 $\text{Sinh trắc học} > \text{Smart card} > \text{Password}$
- Có thể kết hợp các phương pháp xác thực với nhau



Xác thực người sử dụng

❖ Các giao thức xác thực:

- Giao thức xác thực đơn giản
- Giao thức xác thực challenge/response
- Giao thức xác thực dùng khóa đối xứng
- Giao thức xác thực dùng khóa công khai
- Giao thức xác thực Kerberos

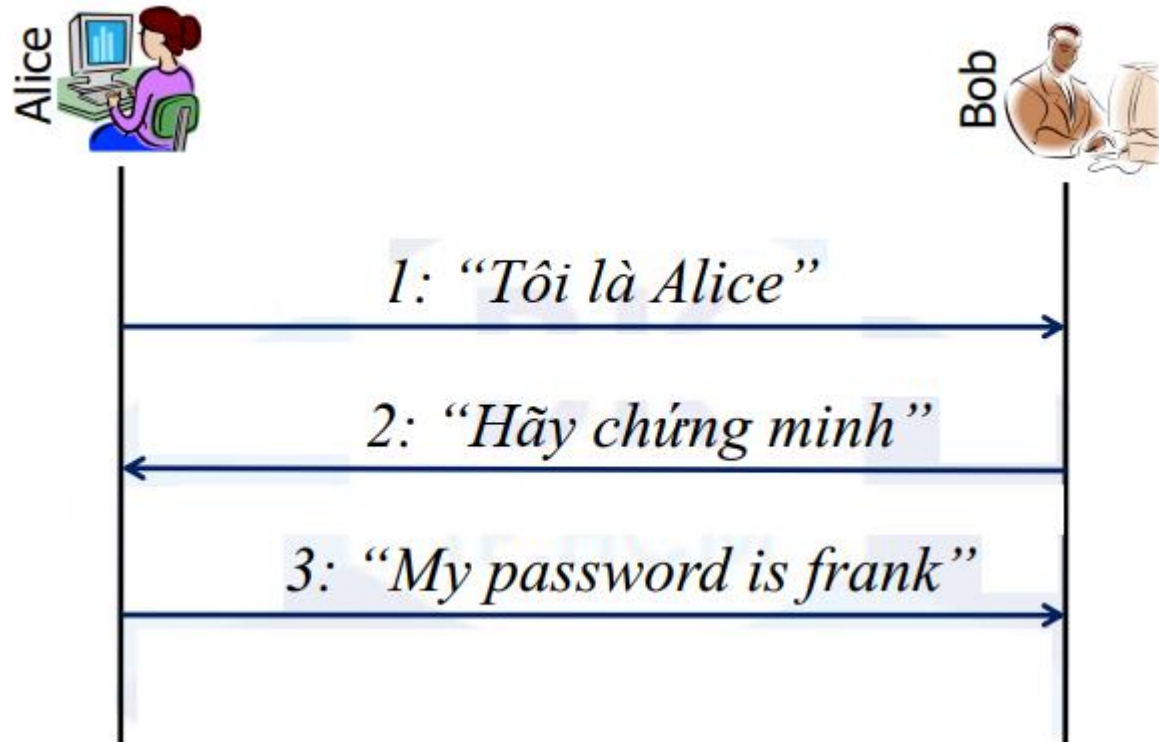
Xác thực người sử dụng

- ❖ Giả sử **Alice** muốn chứng minh với **Bob** là “**Tôi chính là Alice**”
- ❖ **Alice** cũng cần biết người mình trao đổi có đúng là **Bob** không
- ❖ **Malice** là người xấu có ý muốn phá giao thức xác thực



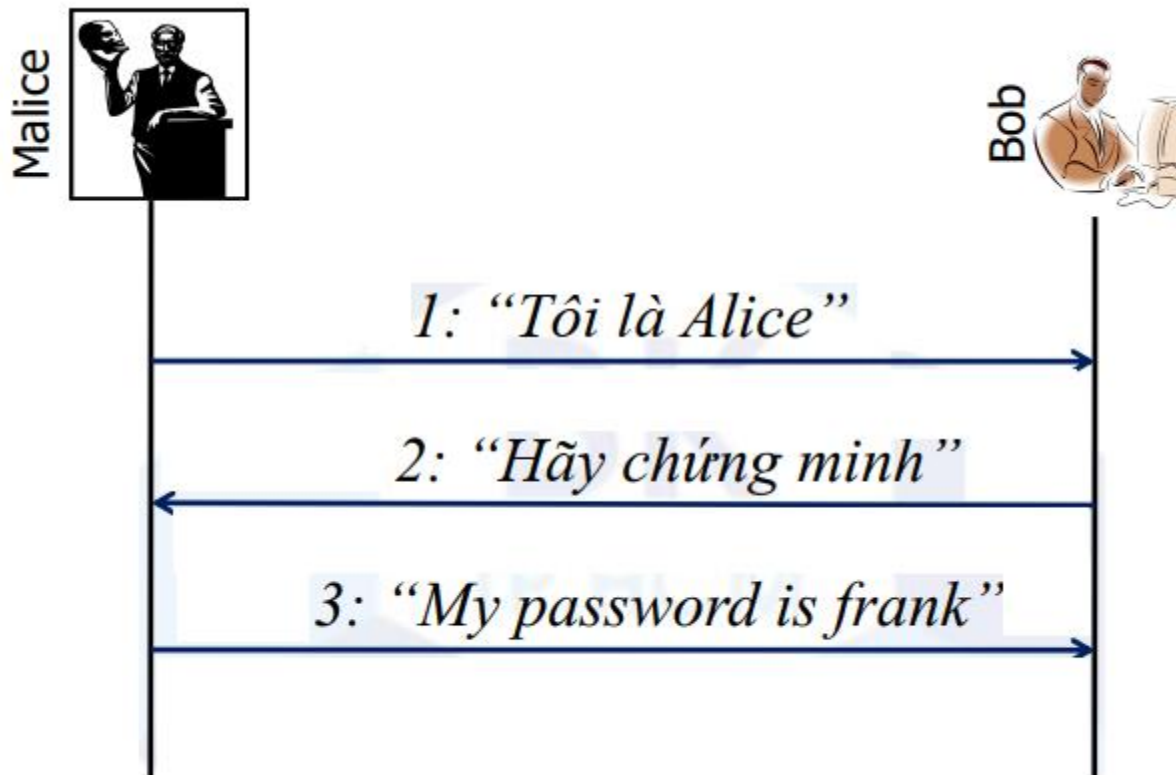
Giao thức xác thực đơn giản

❖ Alice trao đổi với Bob



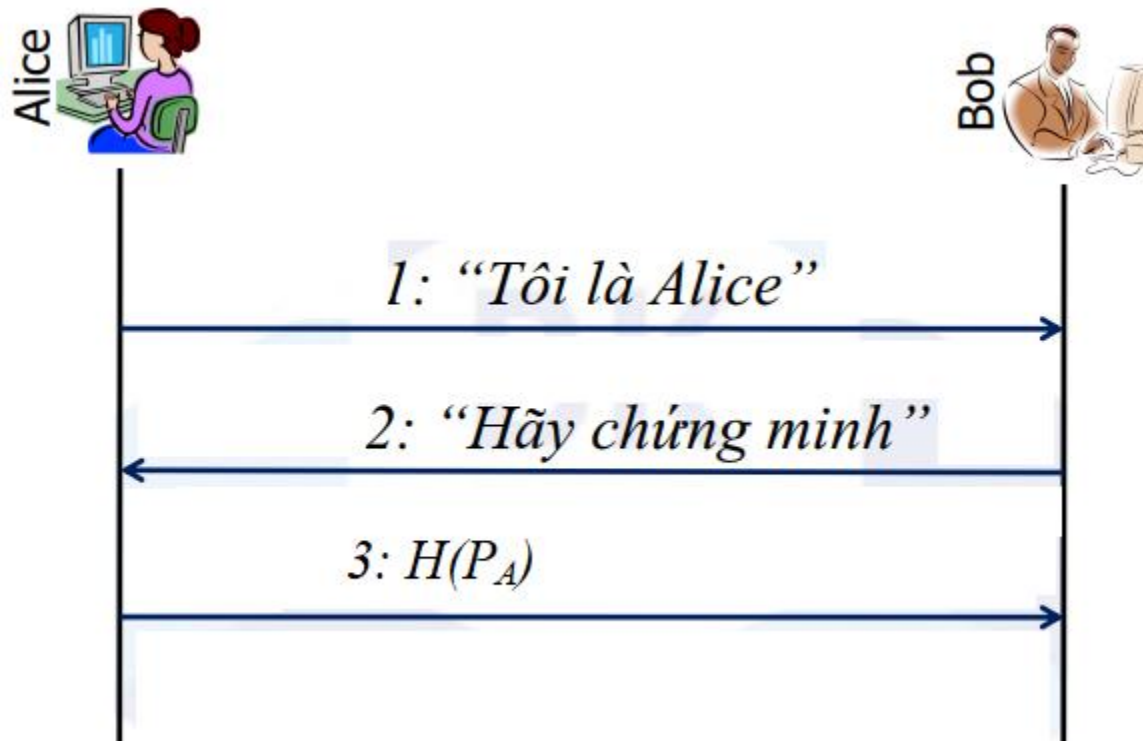
Giao thức xác thực đơn giản

- ❖ Password để ở dạng bản rõ, Malice có thể quan sát được



Giao thức xác thực đơn giản

- ❖ Alice sử dụng hàm băm của password để xác thực



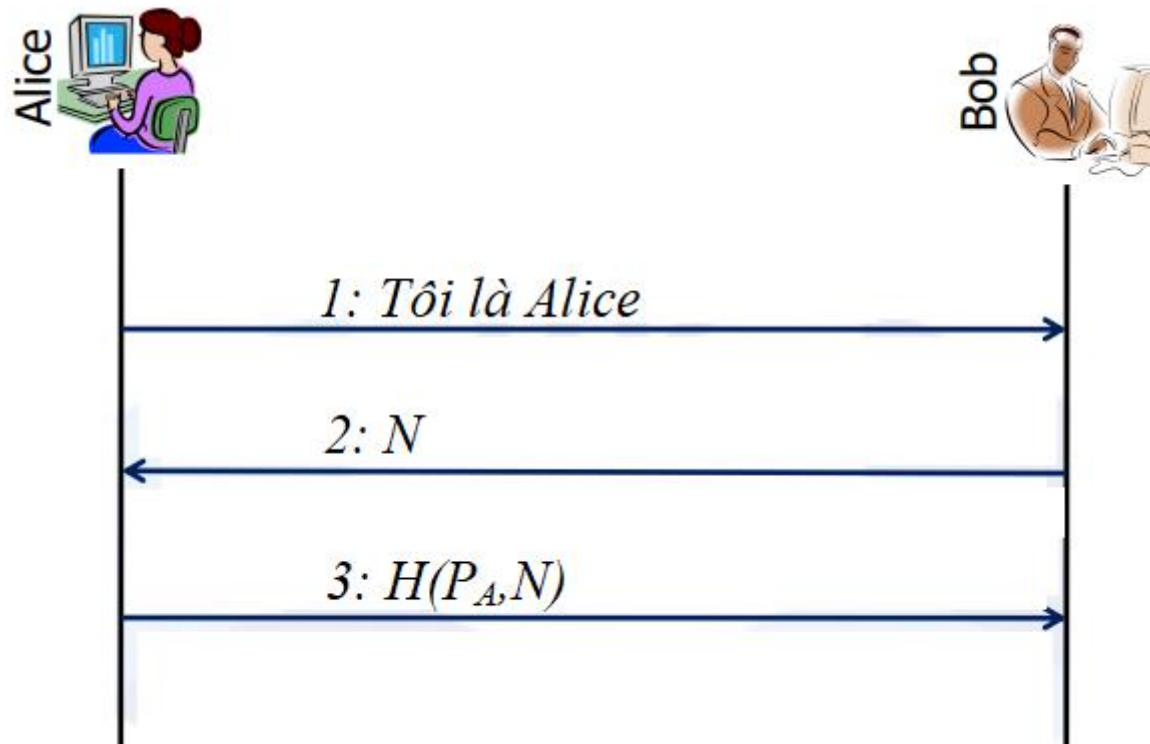
Giao thức xác thực đơn giản

- ❖ Tấn công bằng cách lặp lại thông điệp



Giao thức xác thực challenge-response

- ❖ N: số nonce (sử dụng 1 lần)



- ❖ Nhược điểm: Bob phải biết trước password của Alice

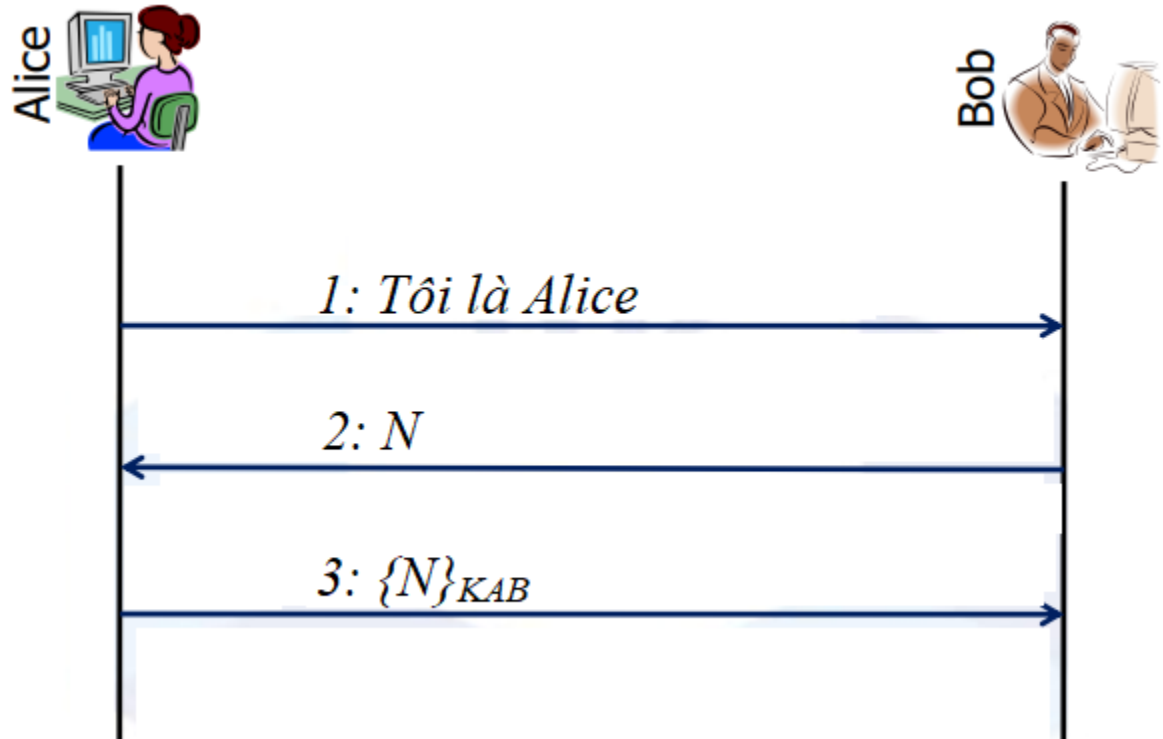


Giao thức xác thực dùng khóa đối xứng

❖ Các ký hiệu:

- M: bản rõ
- C: Bản mã
- K_A : Khóa của Alice
- $C = \{M\}_K$
- K_{AB} : Khóa chung của Alice và Bob

Giao thức xác thực dùng khóa đối xứng

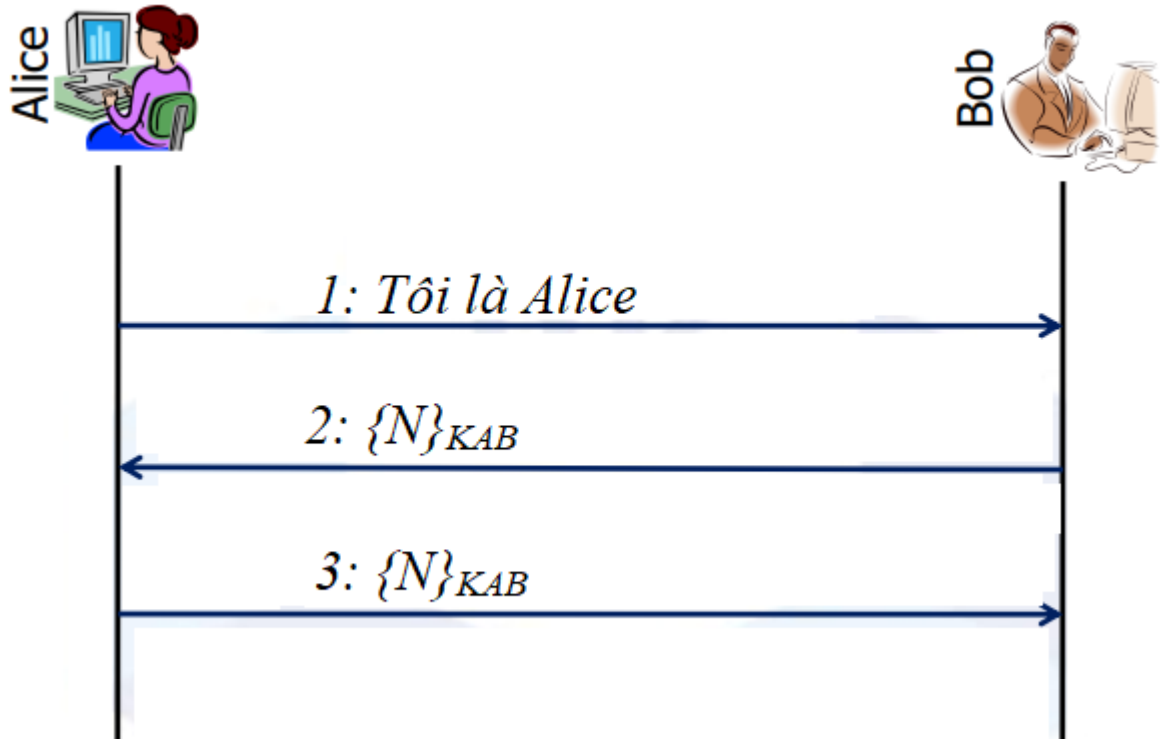


❖ Nhược điểm:

- Chỉ có Bob xác thực được Alice
- Alice không biết có đúng là Bob không

Giao thức xác thực dùng khóa đối xứng

❖ Xác thực lẫn nhau:

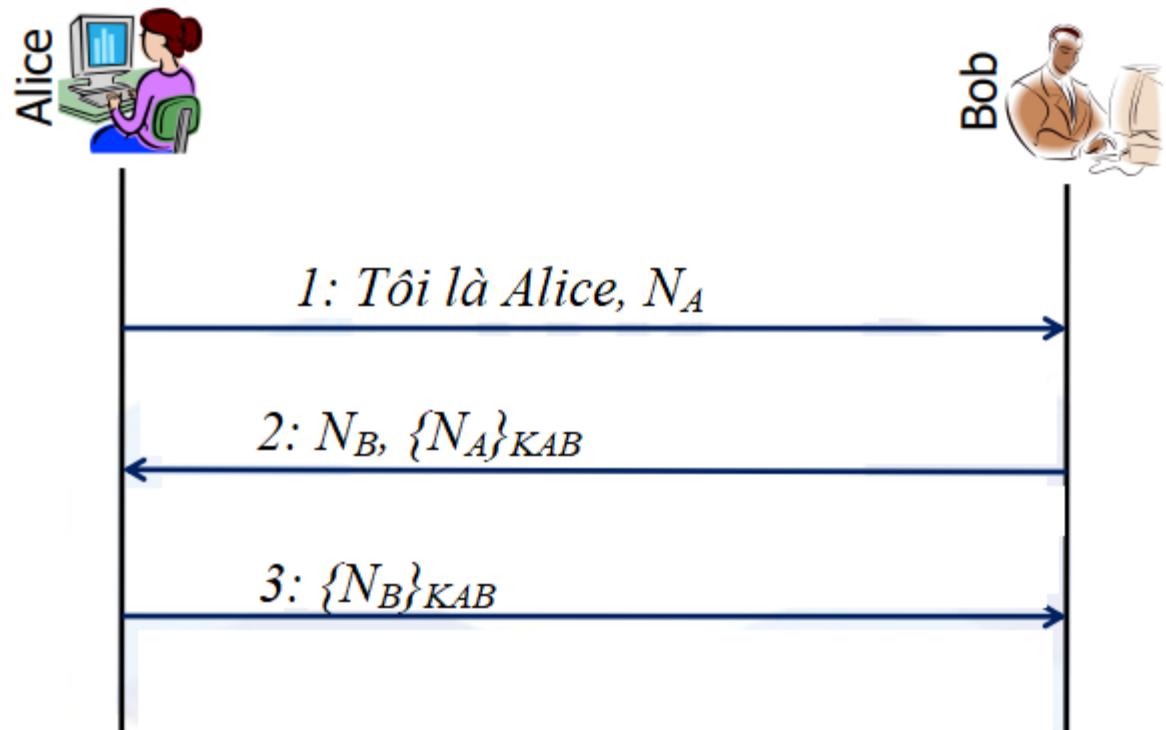


❖ Nhược điểm:

- Thông điệp ở bước 3 lặp lại ở bước 2 nên không xác thực được người gửi Alice

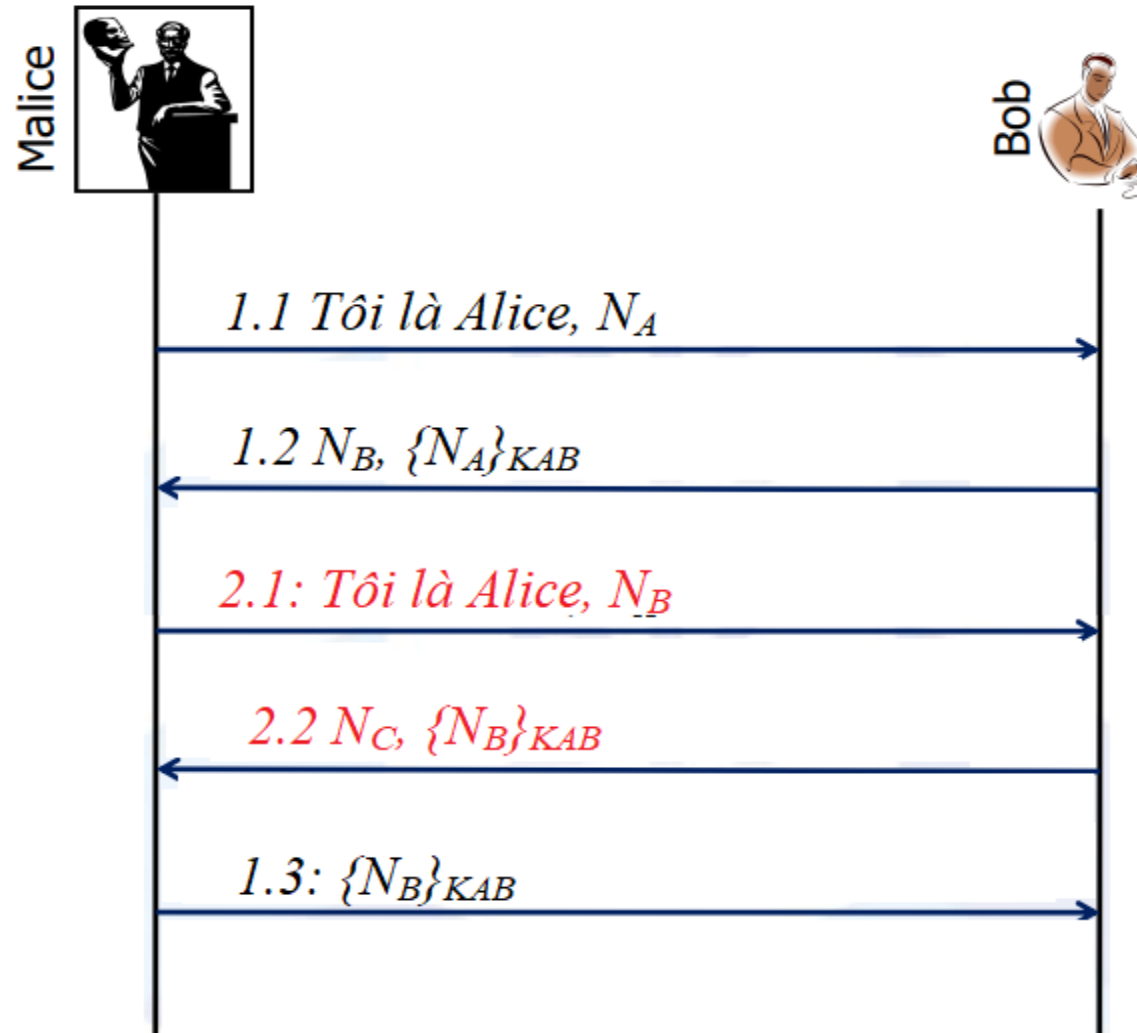
Giao thức xác thực dùng khóa đối xứng

❖ Xác thực lẫn nhau
cải tiến:



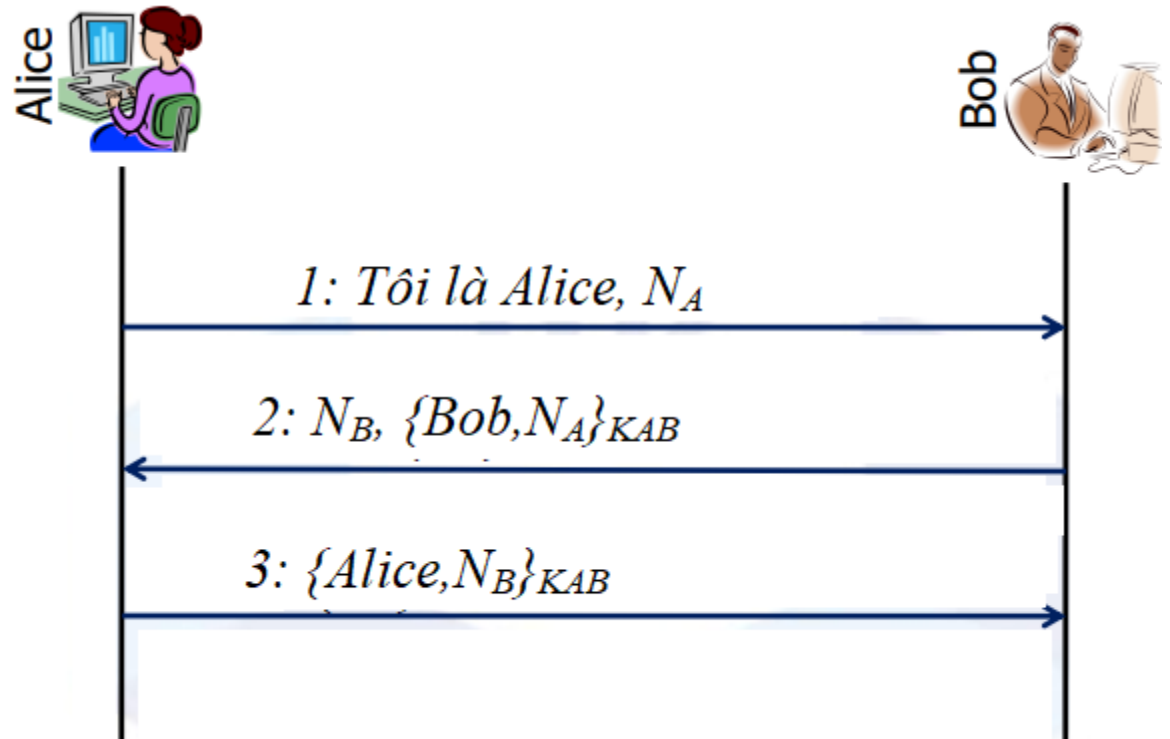
Giao thức xác thực dùng khóa đối xứng

- ❖ Tấn công giao thức xác thực lẫn nhau cải tiến:



Giao thức xác thực dùng khóa đối xứng

- ❖ Xác thực lẫn nhau cải tiến khác:





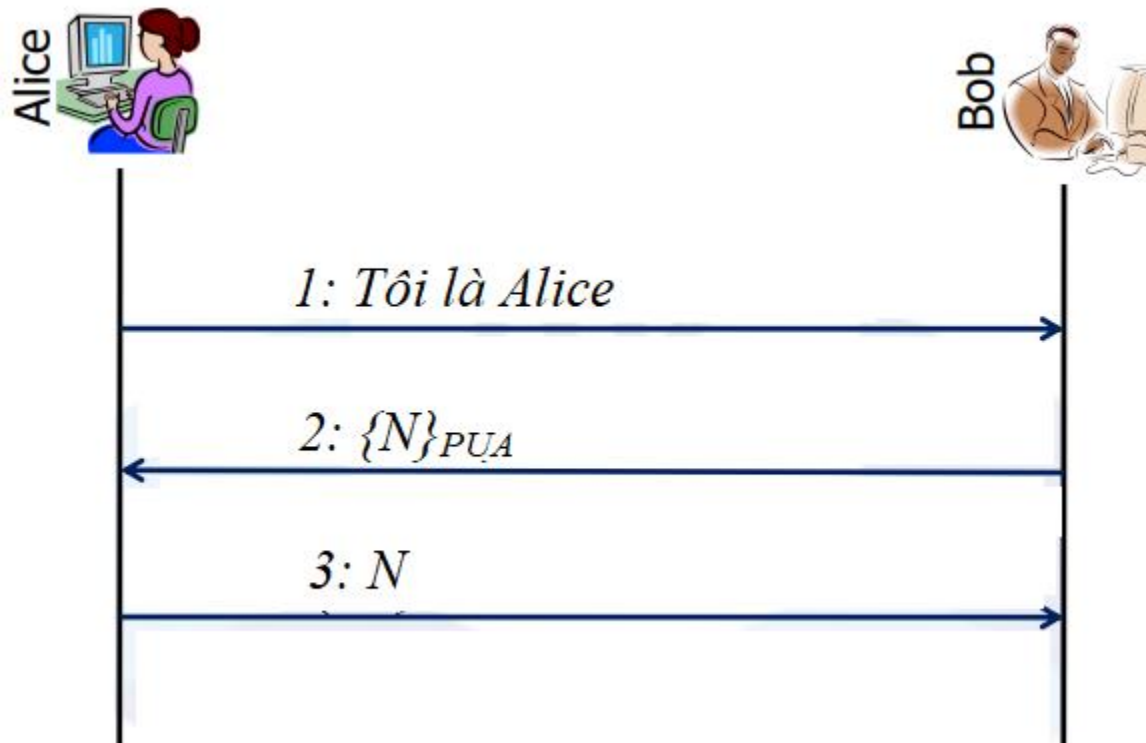
Giao thức xác thực dùng khóa công khai

❖ Các ký hiệu:

- M : bản rõ
- C : Bản mã
- PU_A, PR_A : Cặp khóa bí mật và công khai của Alice
- $C = \{M\}_{PU_A}$: Mã hóa bằng khóa công khai của Alice
- $M = [C]_{PR_A}$: Giải mã bằng khóa bí mật của Alice
- $S = [M]_{PR_A}$: Ký lên M bằng khóa bí mật của Alice

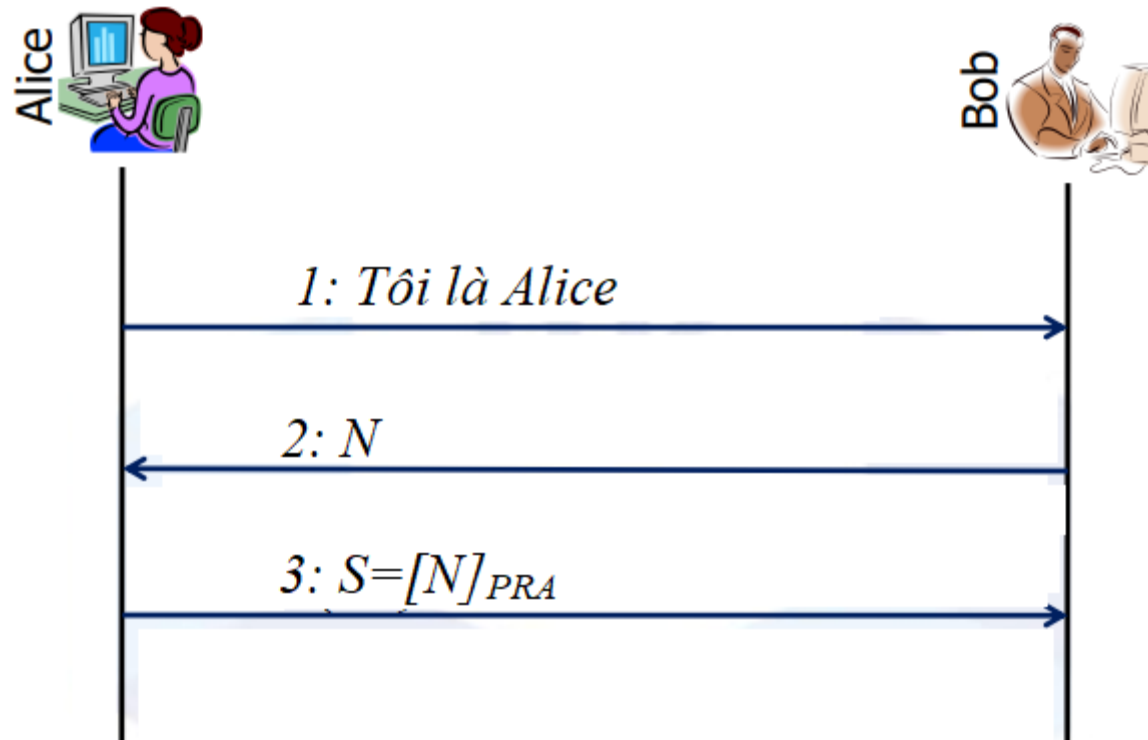
Giao thức xác thực dùng khóa công khai

❖ Dùng mã hóa công khai:



Giao thức xác thực dùng khóa công khai

❖ Dùng chữ ký số:

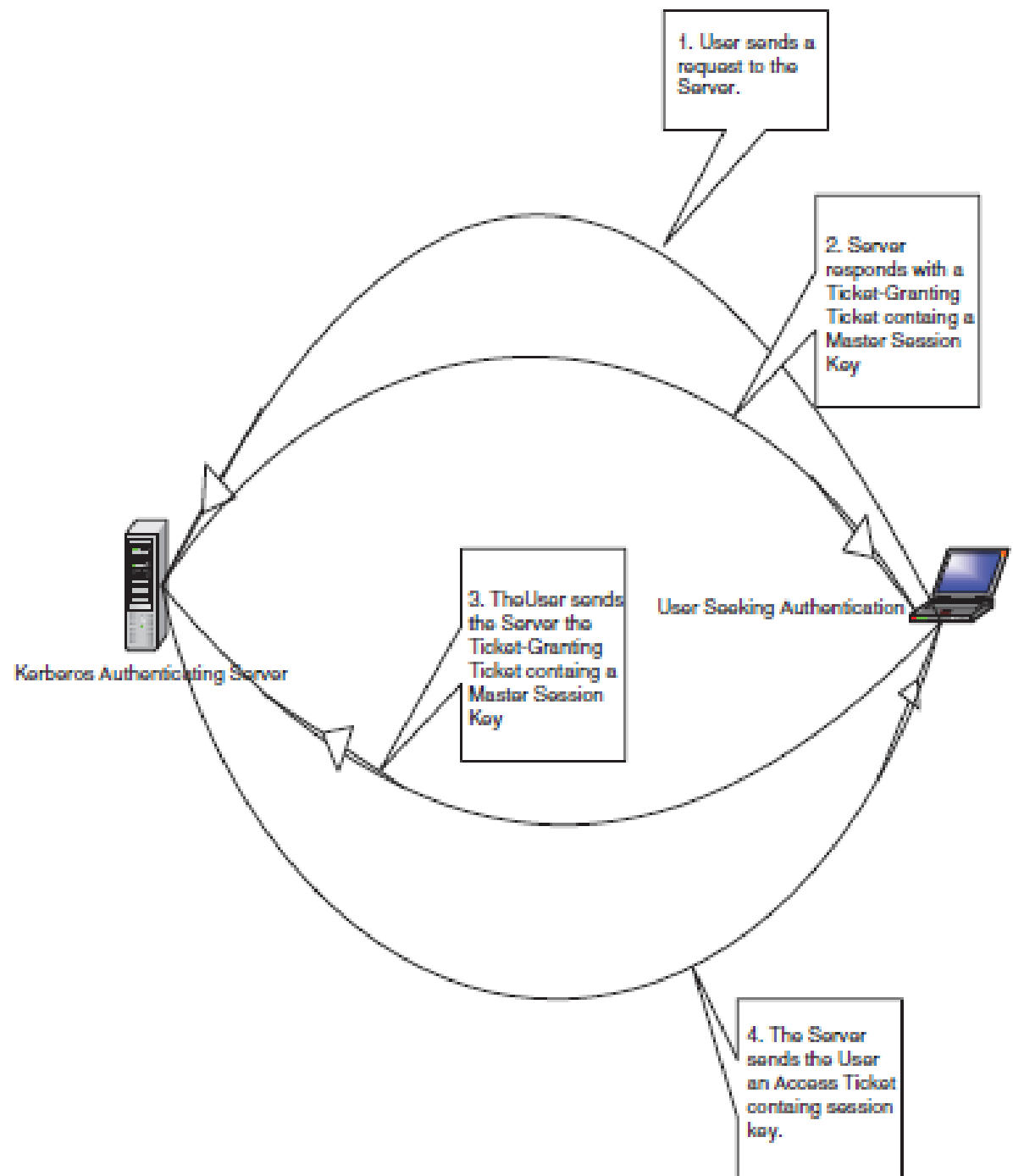




Kerberos

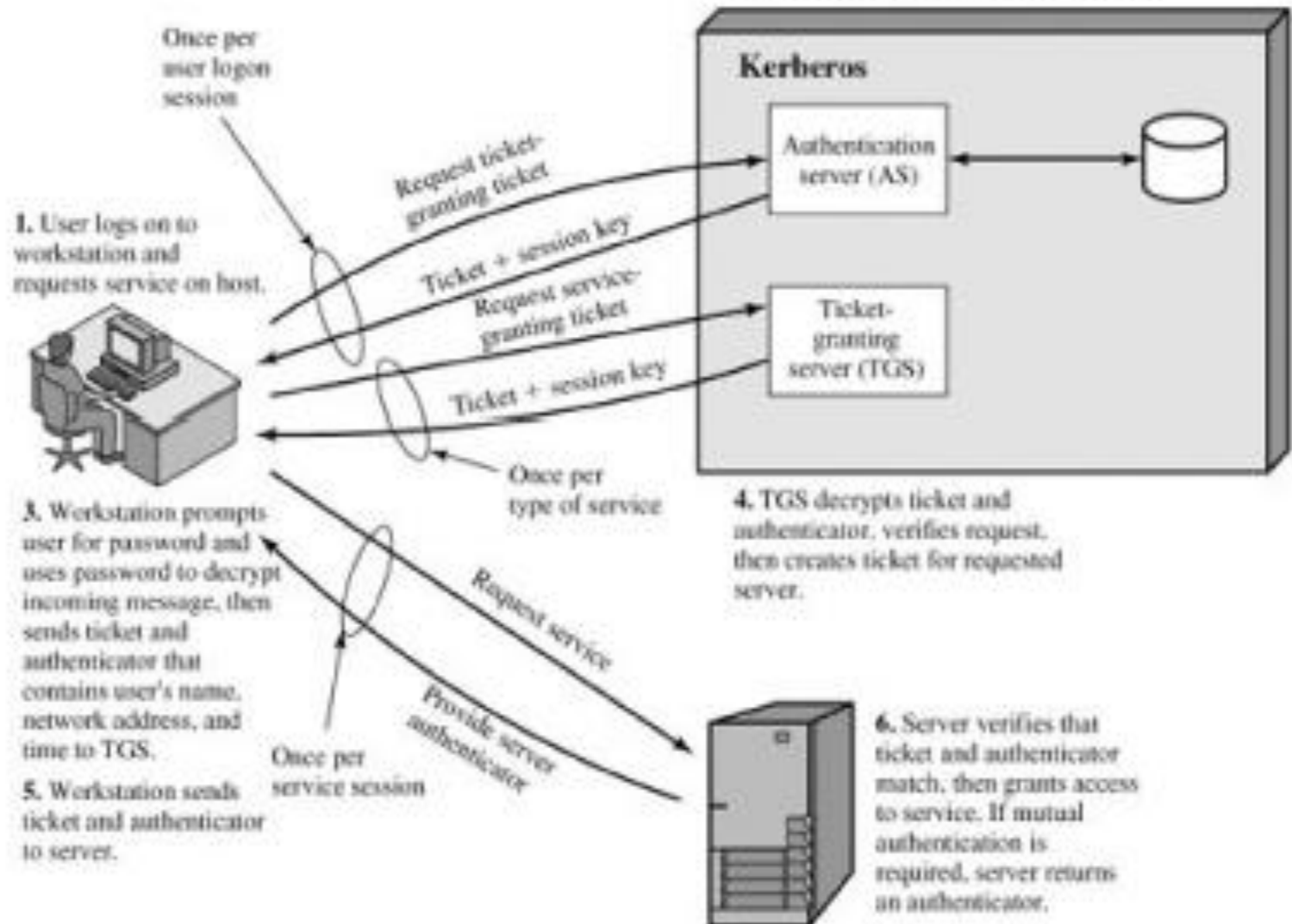
- ❖ **Giao thức xác thực mạng sử dụng mã hóa khóa bí mật.**
- ❖ **Xác thực giữa client và server.**
- ❖ **Đảm bảo tính an toàn, tính tin cậy, trong suốt, khả năng phát triển, mở rộng.**

Hệ thống xác thực Kerberos



[View full size image](#)

2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.



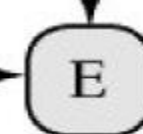
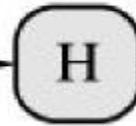
Kerberos

Xác thực sử dụng chứng thư khóa công khai

Unsigned certificate:
contains user ID,
user's public key



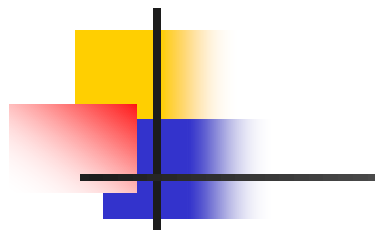
Generate hash
code of unsigned
certificate



Encrypt hash code
with CA's private key
to form signature

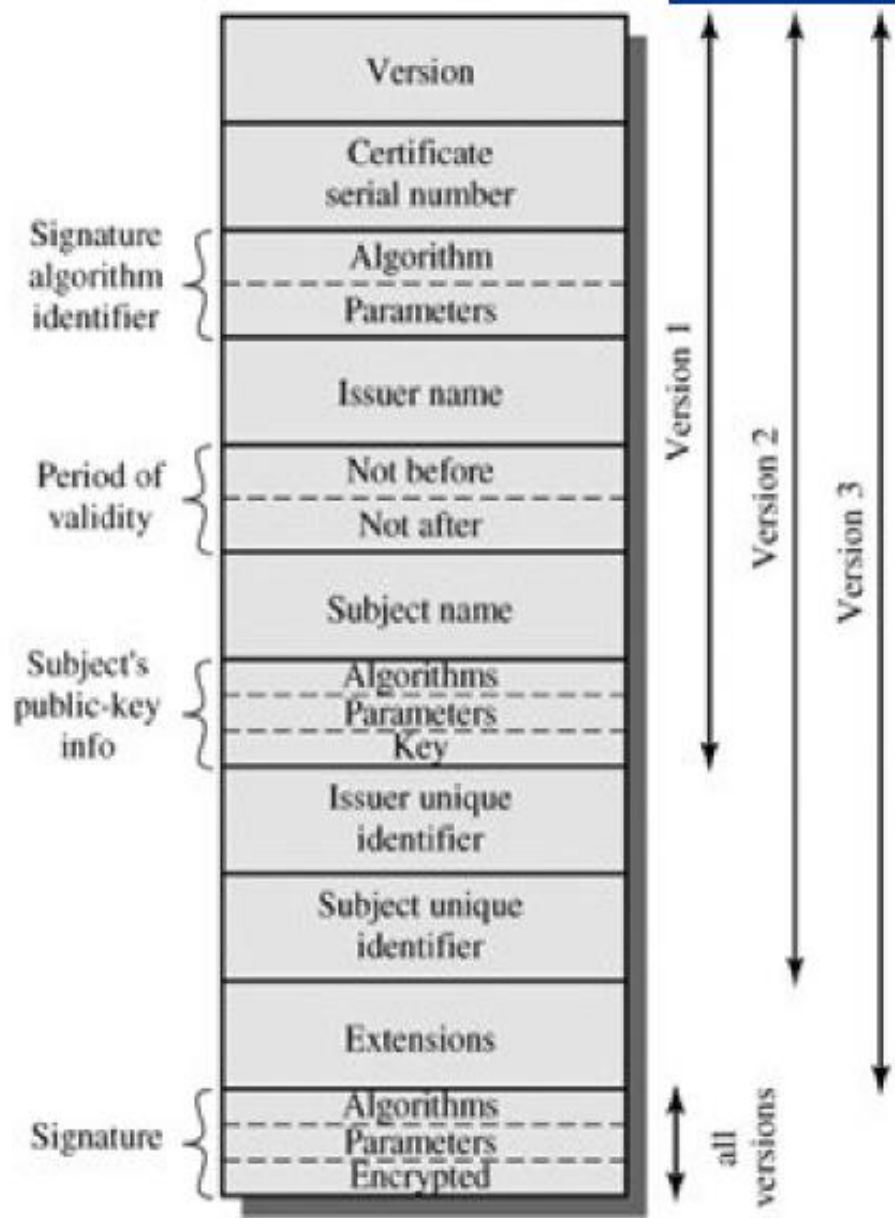


Signed certificate:
Recipient can verify
signature using CA's
public key.

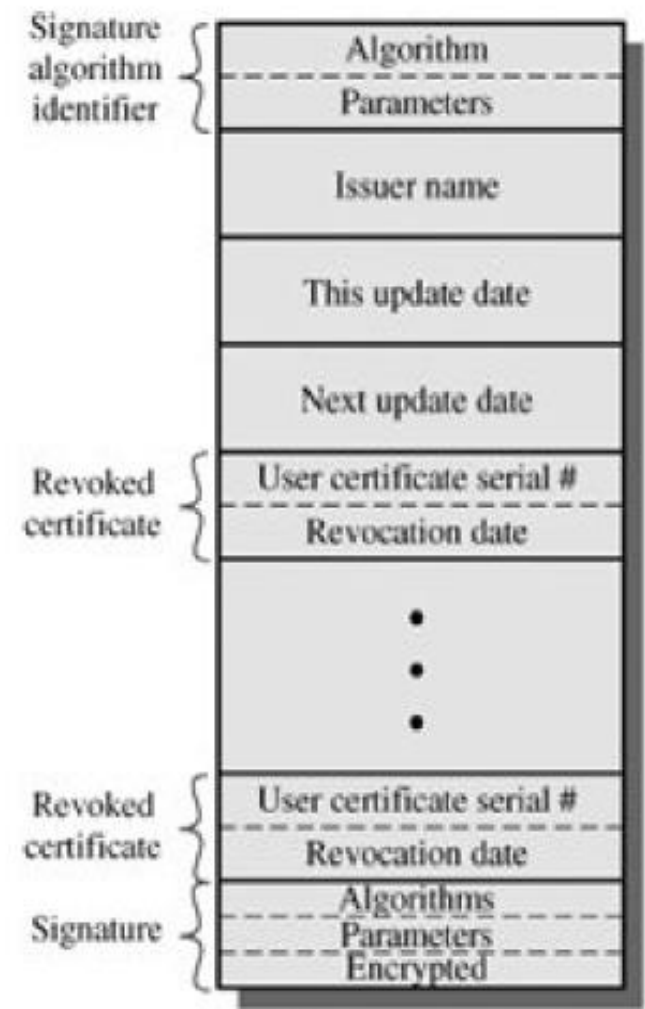


Khuôn dạng chứng thư X.509

[\[View full size image\]](#)

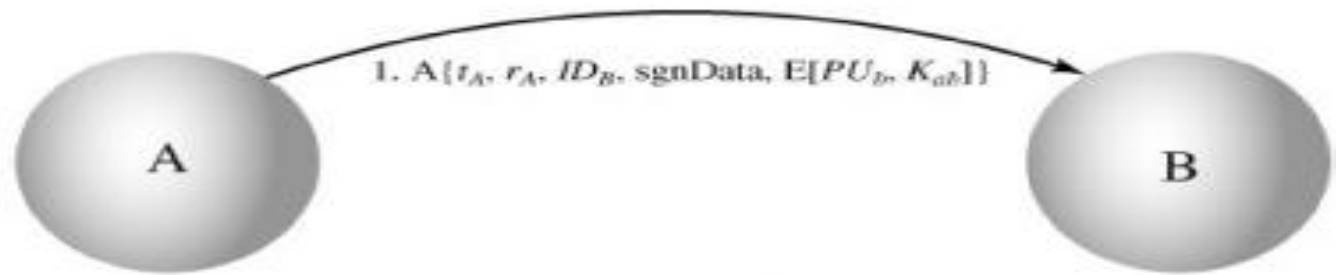


(a) X.509 certificate

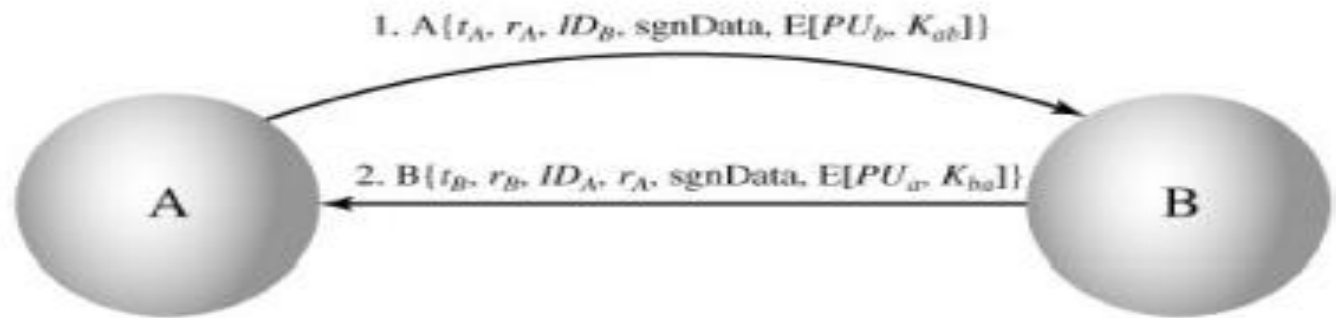


(b) Certificate revocation list

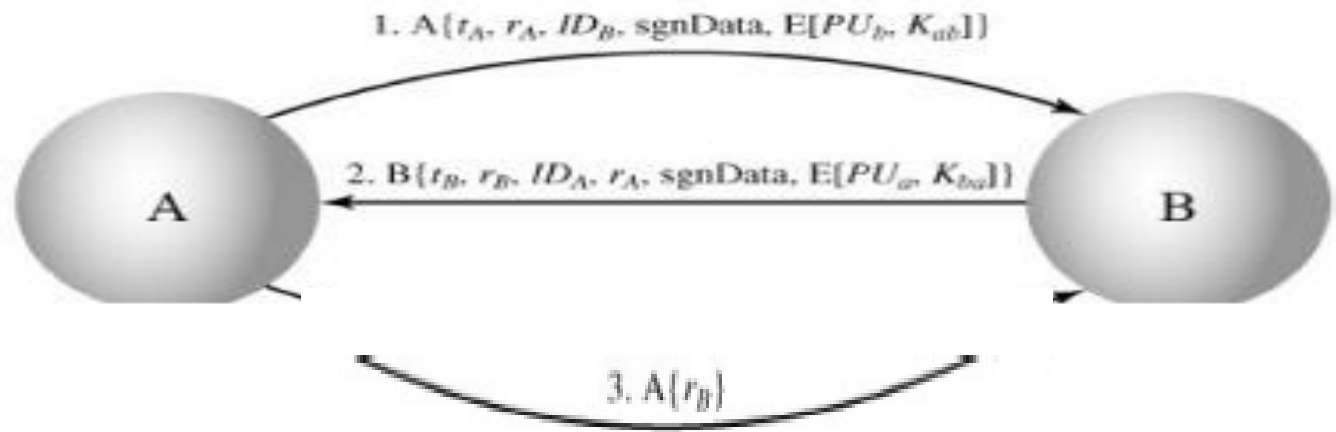
Figure 14.6. X.509 Strong Authentication Procedures



(a) One-way authentication



(b) Two-way authentication



(c) Three-way authentication

Thủ
tục
xác
thực
X.509