Chương 5

CÁC ỨNG DỤNG XÁC THỰC

Giới thiệu

- Mục đích của các ứng dụng xác thực là hỗ trợ xác thực và chữ ký số ở mức ứng dụng
- Phân làm 2 loại chính
  - Dựa trên mã hóa đối xứng
    - Dịch vụ Kerberos
    - Giao thức Needham-Schroeder
  - Dựa trên khóa công khai được chứng thực
    - Dịch vụ X.509
    - Hệ thống PGP

Kerberos

- Hệ thống dịch vụ xác thực phát triển bởi MIT
- Nhằm đối phó với các hiểm họa sau
  - Người dùng giả danh là người khác
  - Người dùng thay đổi địa chỉ mạng của client
  - Người dùng xem trộm thông tin trao đổi và thực hiện kiểu tấn công lặp lại
- Bao gồm 1 server tập trung có chức năng xác thực người dùng và các server dịch vụ phân tán
  - Tin cậy server tập trung thay vì các client
  - Giải phóng chức năng xác thực khỏi các server dịch vụ và các client

Ký hiệu

- C : Client
- AS : Server xác thực
- V : Server dịch vụ
- ID_C : Danh tính người dùng trên C
- ID_V : Danh tính của V
- P_C : Mật khẩu của người dùng trên C
- AD_C : Địa chỉ mạng của C
- K_V : Khóa bí mật chia sẻ bởi AS và V
- $\|$: Phép ghép
- TGS : Server cấp thẻ
- TS : Nhãn thời gian

Một hội thoại xác thực đơn giản

- Giao thức

  (1) C [redacted] S : $ID_C \| P_C \| ID_V$

  (2) AS [redacted] : Thẻ

  (3) C [redacted] : $ID_C \| Thẻ$

  $Thẻ = E_{K_V}[ID_C \| AD_C \| ID_V]$

- Hạn chế
  - Mật khẩu truyền từ C đến AS không được bảo mật
  - Nếu thẻ chỉ sử dụng được một lần thì phải cấp thẻ mới cho mỗi lần truy nhập cùng một dịch vụ
  - Nếu thẻ sử dụng được nhiều lần thì có thể bị lấy cắp để sử dụng trước khi hết hạn
  - Cần thẻ mới cho mỗi dịch vụ khác nhau

Hội thoại xác thực Kerberos 4

(a) Trao đổi với dịch vụ xác thực : để có thẻ cấp thẻ

(1) C [redacted] S : $ID_C \| ID_{tgs} \| TS_1$

(2) AS [redacted] : $E_{K_C}[K_{C,tgs} \| ID_{tgs} \| TS_2 \| Hạn_2 \| Thẻ_{tgs}]$

$Thẻ_{tgs} = E_{K_{tgs}}[K_{C,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Hạn_2]$

(b) Trao đổi với dịch vụ cấp thẻ : để có thẻ dịch vụ

(3) C [redacted] GS : $ID_V \| Thẻ_{tgs} \| Dấu_C$

(4) TGS [redacted] : $E_{K_{C,tgs}}[K_{C,V} \| ID_V \| TS_4 \| Thẻ_V]$

$Thẻ_V = E_{K_V}[K_{C,V} \| ID_C \| AD_C \| ID_V \| TS_4 \| Hạn_4]$

$Dấu_C = E_{K_{C,tgs}}[ID_C \| AD_C \|$ [redacted] TS_3

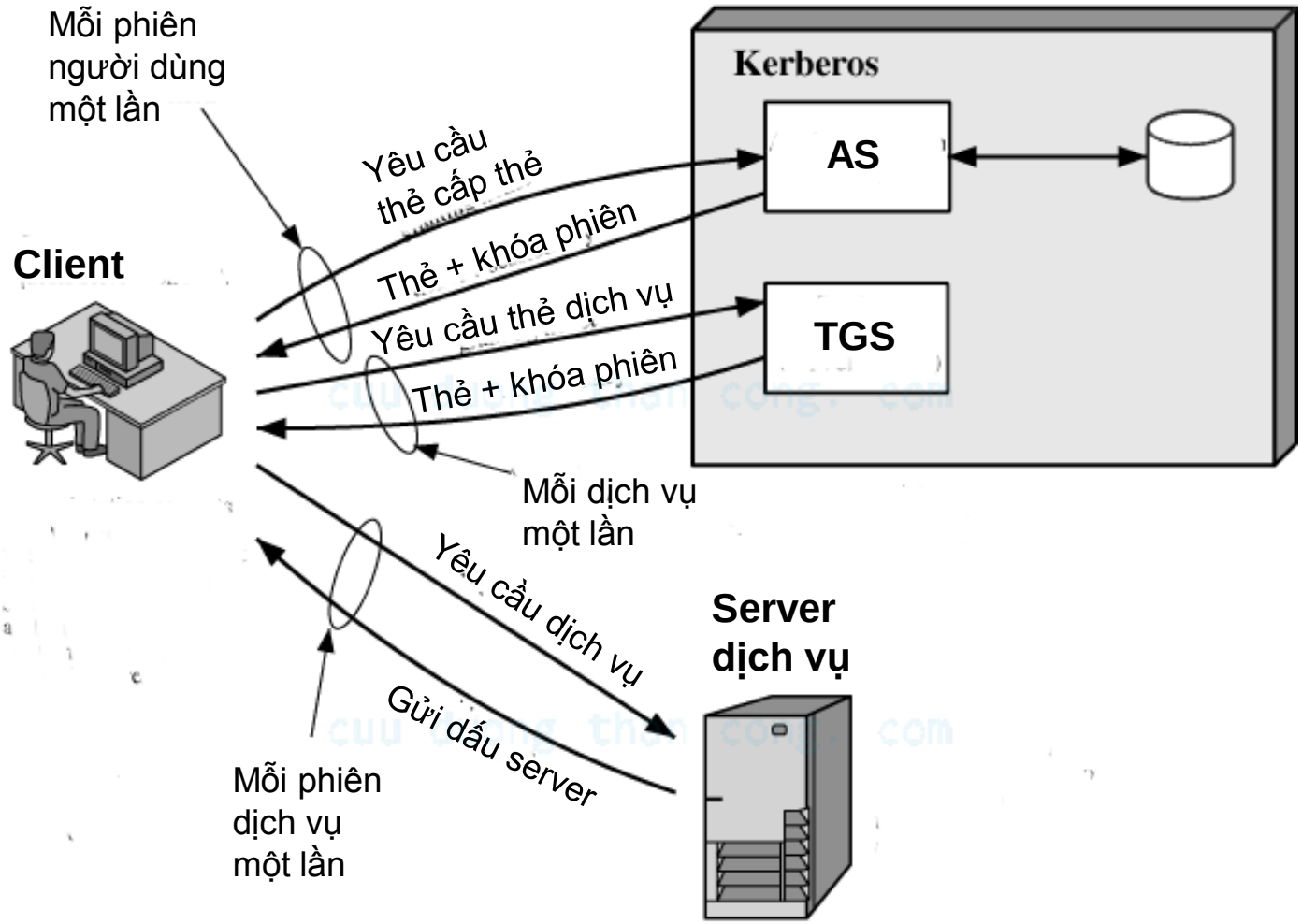
(c) Trao đổi xác thực client/server : để có dịch vụ

(5) C [redacted] : $Thẻ_V \| Dấu_C$

(6) V [redacted] : $E_{K_{C,V}}[TS_5 + 1]$

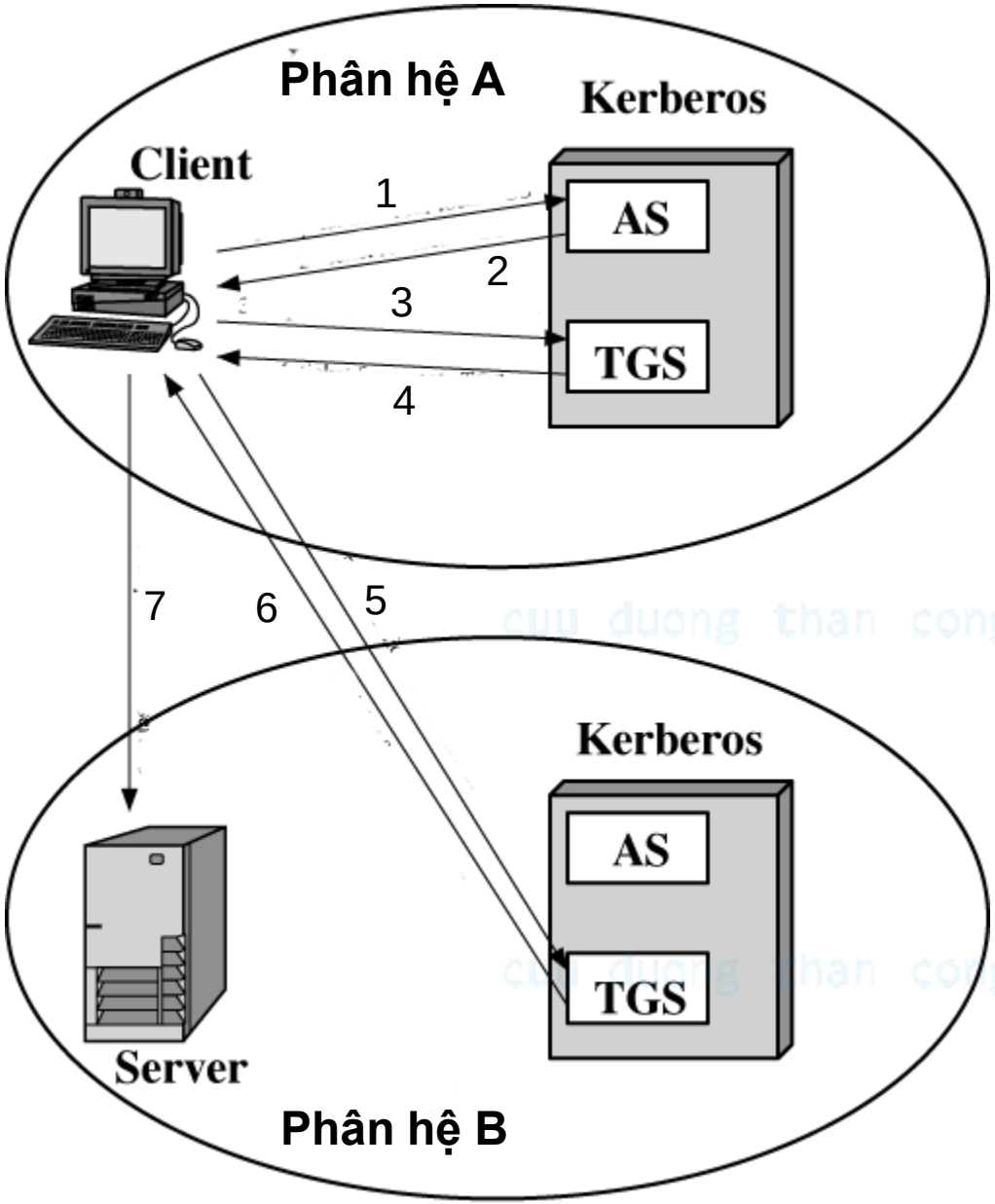
$Dấu_C = E_{K_{C,V}}[ID_C \| AD_C \| TS_5]$

Mô hình tổng quan Kerberos



Phân hệ Kerberos

- Một phân hệ Kerberos bao gồm
  - Một server Kerberos chứa trong CSDL danh tính và mật khẩu băm của các thành viên
  - Một số người dùng đăng ký làm thành viên
  - Một số server dịch vụ, mỗi server có một khóa bí mật riêng chỉ chia sẻ với server Kerberos
- Mỗi phân hệ Kerberos thường tương ứng với một phạm vi hành chính
- Hai phân hệ có thể tương tác với nhau nếu 2 server chia sẻ 1 khóa bí mật và đăng ký với nhau
  - Điều kiện là phải tin tưởng lẫn nhau



1. Yêu cầu thẻ cho TGS cục bộ
2. Thẻ cho TGS cục bộ
3. Yêu cầu thẻ cho TGS ở xa
4. Thẻ cho TGS ở xa
5. Yêu cầu thẻ cho server ở xa
6. Thẻ cho server ở xa
7. Yêu cầu dịch vụ ở xa

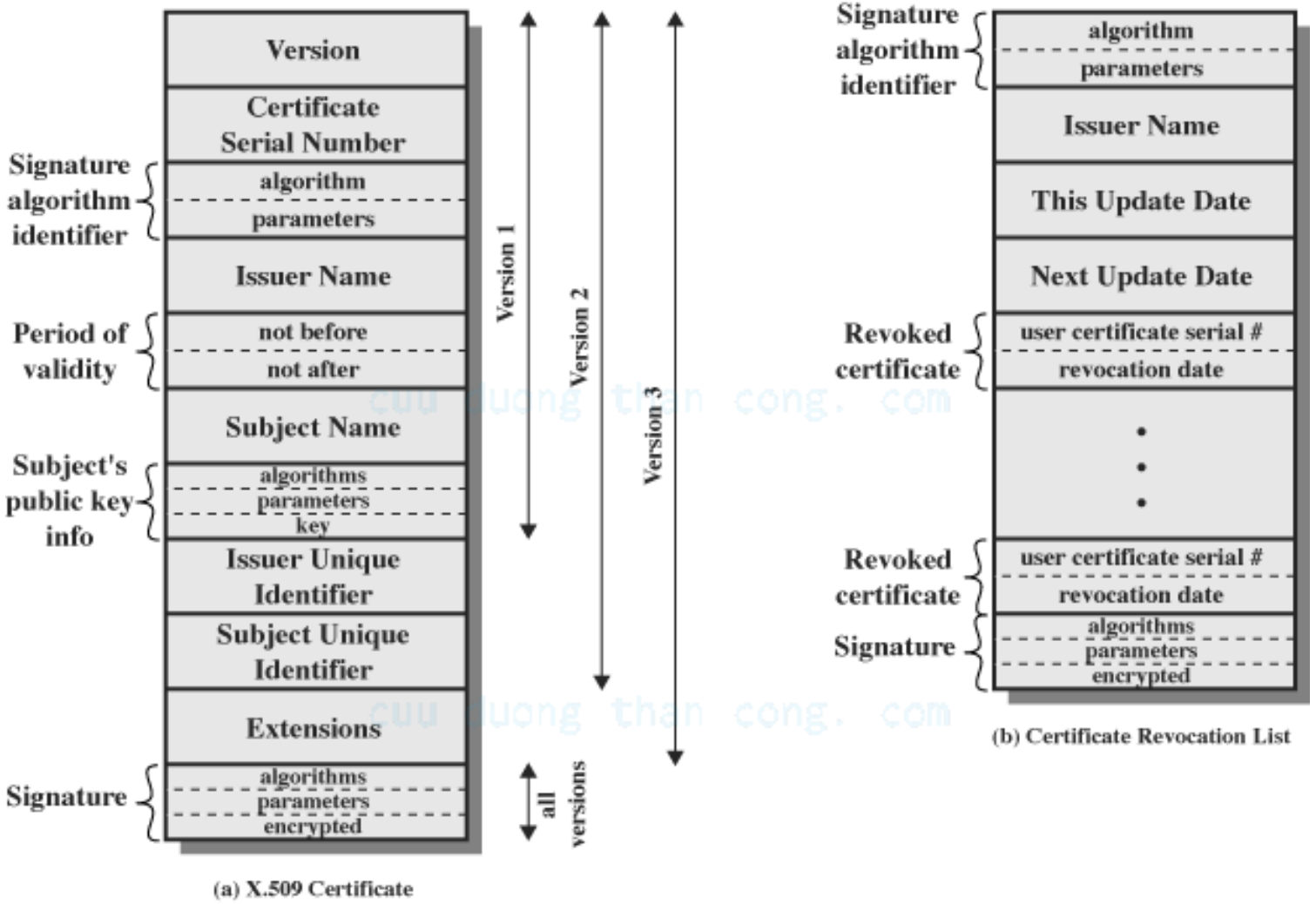
Kerberos 5

- Phát triển vào giữa những năm 1990 (sau Kerberos 4 vài năm) đặc tả trong RFC 1510
- Có một số cải tiến so với phiên bản 4
  - Khắc phục những khiếm khuyết của môi trường
    - Phụ thuộc giải thuật mã hóa, phụ thuộc giao thức mạng, trật tự byte thông báo không theo chuẩn, giá trị hạn dùng thẻ có thể quá nhỏ, không cho phép ủy nhiệm truy nhập, tương tác đa phân hệ dựa trên quá nhiều quan hệ tay đôi
  - Khắc phục những thiếu sót kỹ thuật
    - Mã hóa hai lần có một lần thừa, phương thức mã hóa PCBC để đảm bảo tính toàn vẹn không chuẩn dễ bị tấn công, khóa phiên sử dụng nhiều lần có thể bị khai thác để tấn công lặp lại, có thể bị tấn công mật khẩu

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 khuyến nghị RSA

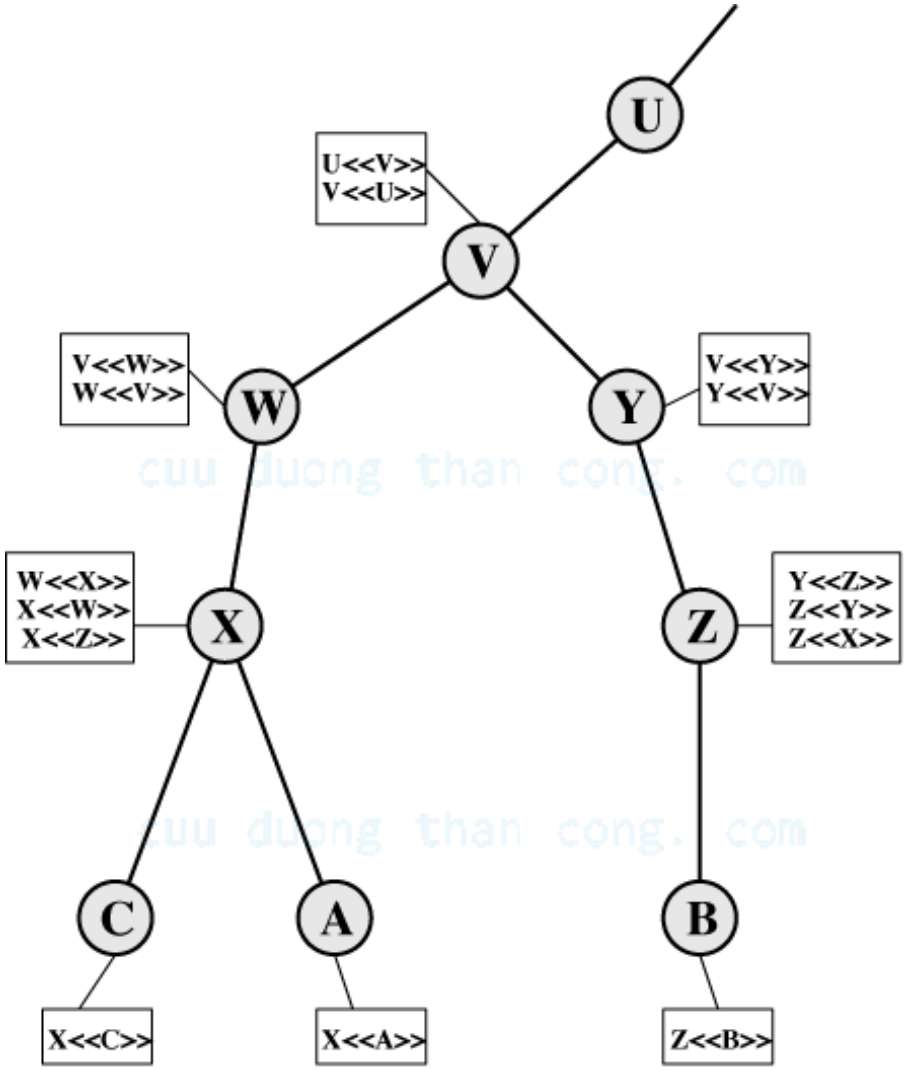
Khuôn dạng X.509



Nhận chứng thực

- 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

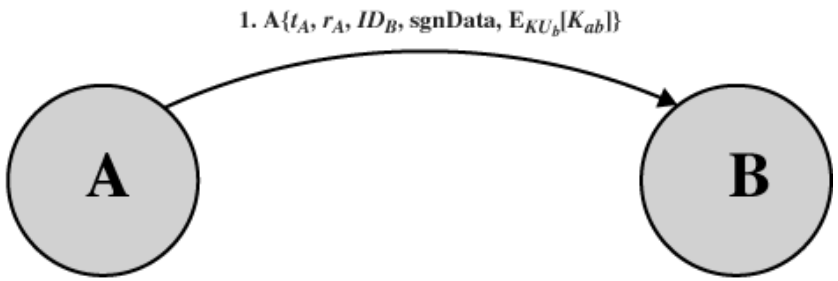
Phân cấp X.509



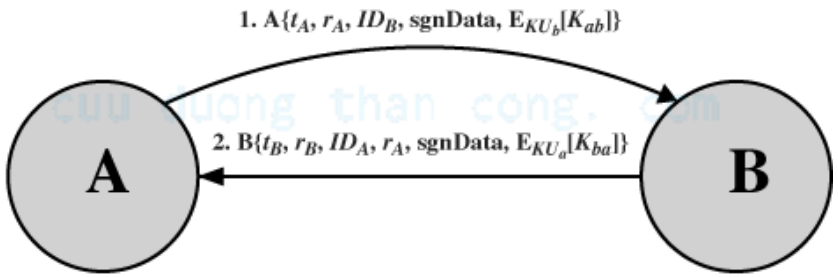
Thu hồi chứng thực

- 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

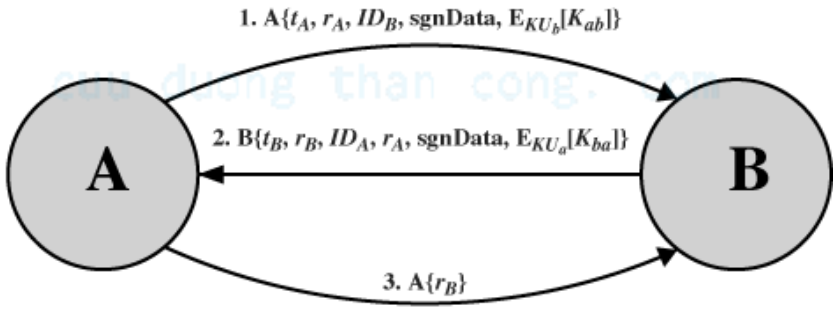
Các thủ tục xác thực



(a) One-way authentication



(b) Two-way authentication



(c) Three-way authentication