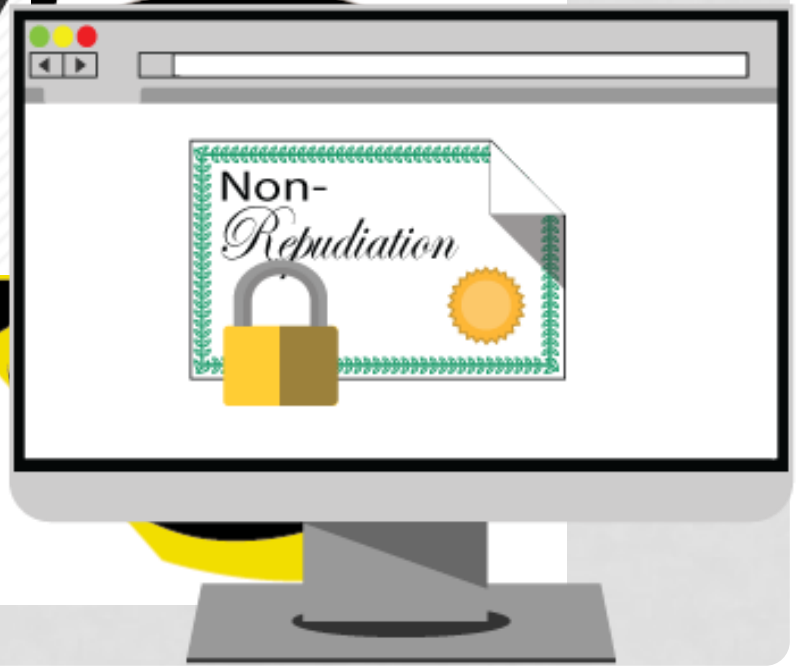
CÁC LÝ THUYẾT CƠ BẢN VỀ HỆ THỐNG PKI

CHỨNG THỰC ĐIỆN TỬ

TẠI SAO CẦN CÓ CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI

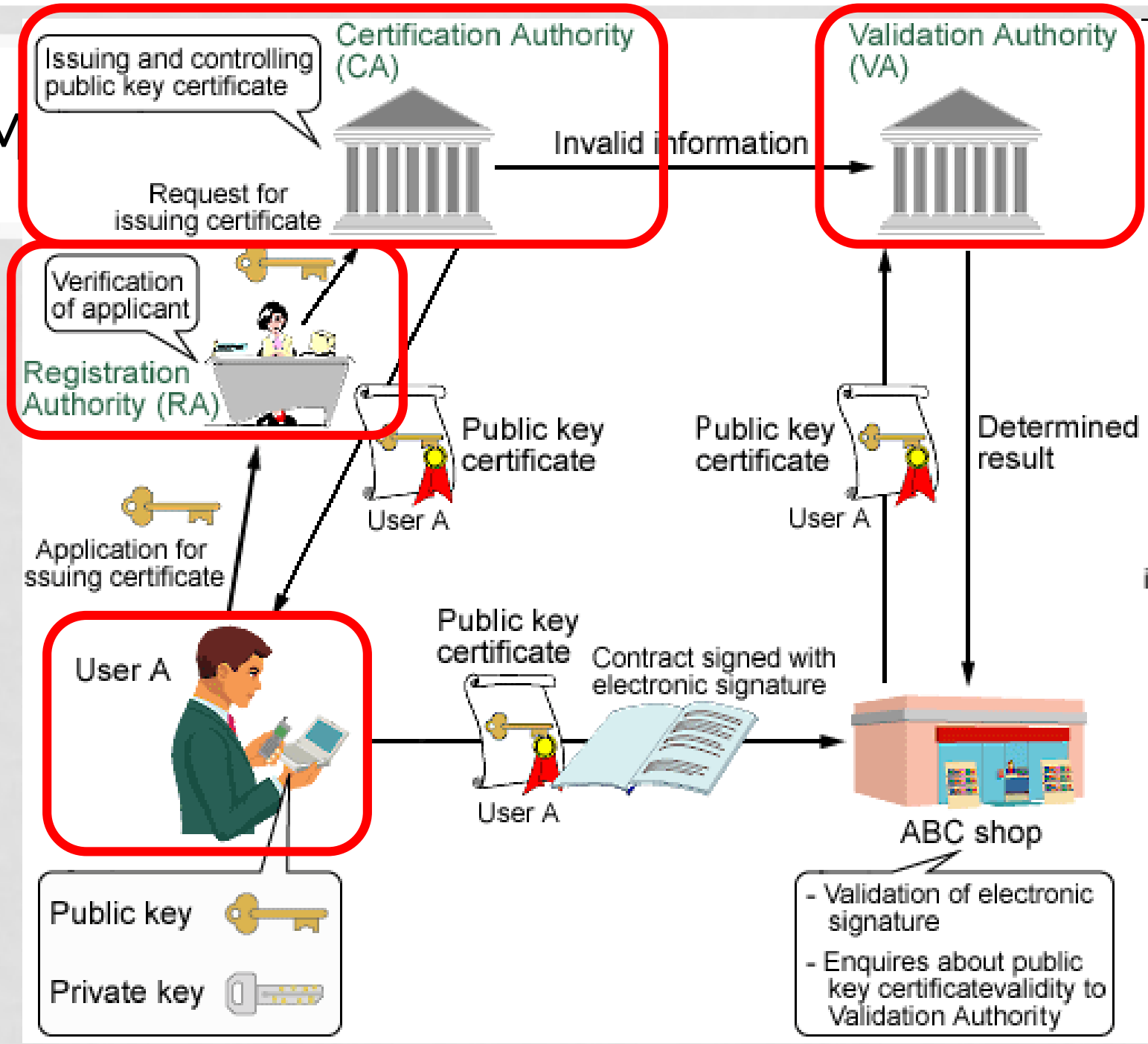


TỔNG QUAN VỀ PKI

- Cơ sở hạ tầng khóa công khai (Public Key Infrastructure – PKI)
- Mục tiêu
  - Bí mật
  - Toàn vẹn
  - Xác thực
  - Chống chối bỏ
- Nhiều định nghĩa cho PKI

TỔNG QUAN VỀ PKI

- Đ/n 1:
  - Cơ sở hạ tầng khóa công khai (PKI) là một hệ thống tập hợp bao gồm phần cứng, phần mềm, con người, chính sách và các thủ tục cần thiết để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi các chứng thư số (chứng thư điện tử).
- Đ/n 2:
  - PKI là cơ sở của một hạ tầng an ninh rộng khắp, các dịch vụ của PKI được cài đặt và thực hiện bằng cách sử dụng các khái niệm và kỹ thuật của mật mã khoá công khai (theo "Understanding PKI").
- Khái niệm hạ tầng khóa công khai thường được dùng để chỉ toàn bộ hệ thống bao gồm thẩm quyền chứng thực cùng các cơ chế liên quan đồng thời với toàn bộ việc sử dụng các thuật toán mật mã hóa khóa công khai trong trao đổi thông tin


Issuing and controlling public key certificate
Certification Authority (CA)
Validation Authority (VA)
Invalid information
Request for issuing certificate
Verification of applicant
Registration Authority (RA)
Public key certificate
User A
Public key certificate
User A
Determined result
Application for ssuing certificate
User A
Public key certificate
Contract signed with electronic signature
User A
ABC shop
Public key
Private key
- Validation of electronic signature
- Enquires about public key certificatevalidity to Validation Authority

THẨM QUYỀN CHỨNG THỰC (CA)

- A và B liên hệ với nhau, A lấy khóa công khai của B để mã hóa thông báo gửi cho B.
- Liệu khóa công khai của B được chia sẻ trên mạng có chính xác là của B hay không?
- => Một bên thứ 3 tin cậy sẽ làm nhiệm vụ gắn kết danh tính và khóa công khai của người dùng
- Bên thứ 3 này sẽ được pháp luật công nhận

THẨM QUYỀN CHỨNG THỰC (CA)

"THẨM QUYỀN CHỨNG THỰC" (Certification Authority – CA) hay là "CƠ QUAN CHỨNG THỰC"

CA là trái tim của hệ thống PKI, là tổ chức quản lý của PKI

- **Công việc của CA là chứng nhận** việc gắn kết khóa công khai và danh tính bằng cách ký số lên một cấu trúc dữ liệu biểu diễn định danh và KCK tương ứng.
- Cấu trúc dữ liệu đó là **chứng thư khóa công khai / chứng thư số**

THẨM QUYỀN ĐĂNG KÝ RA

- Registration Authority (RA) là cơ quan chịu trách nhiệm xác nhận về tính trung thực của yêu cầu sử dụng chứng thư số.
- RA không có trách nhiệm sinh và ký chứng thư.
- RA sau khi nhận yêu cầu sẽ chuyển sang CA để thực hiện
- Kết quả của CA sẽ được chuyển tới người yêu cầu thông qua RA

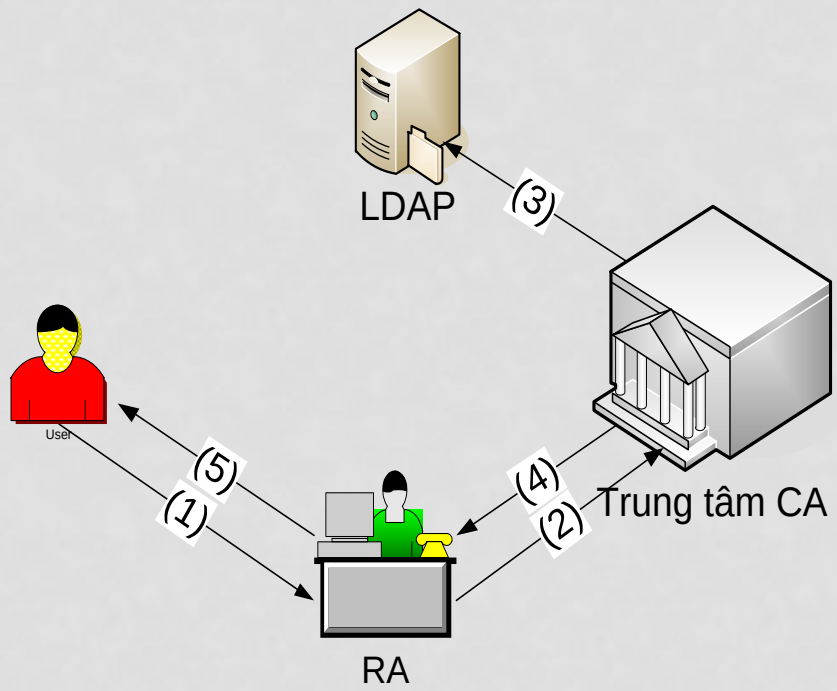
THẨM QUYỀN XÁC THỰC VA

- A và B đã có chứng thư số (CTS) được cấp bởi CA.
- A gửi một hợp đồng có chữ ký của A cho B
- B phải làm cách nào để xác định chữ ký của A trên hợp đồng là hợp lệ???

- Việc kiểm tra một CTS còn hiệu lực không rất phức tạp
- => thiết lập một dịch vụ kiểm tra chứng thư số độc lập
- => THẨM QUYỀN XÁC THỰC
- (VA – Validation Authority)

CÁC QUY TRÌNH HOẠT ĐỘNG CỦA MỘT PKI

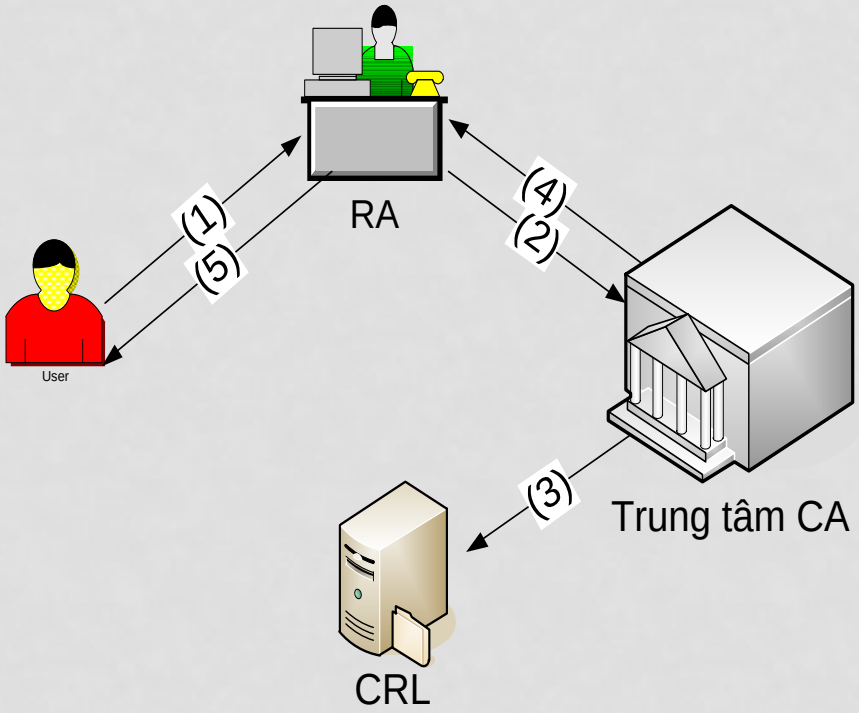
Đăng ký chứng thư số



- (1) User gửi thông tin về bản thân RA để đăng ký
- (2) RA gửi thông tin về user và ký yêu cầu được chấp thuận đến trung tâm CA
- (3) CA tạo chứng thư trên khóa công khai, ký bằng khóa bí mật của CA và cập nhật chứng thư trên thư mục LDAP
- (4) CA gửi chứng thư trở lại RA
- (5) RA cấp chứng thư cho người sử dụng

CÁC QUY TRÌNH HOẠT ĐỘNG CỦA MỘT PKI

Hủy bỏ chứng thư số



- (1) User gửi yêu cầu hủy bỏ chứng thư tới RA
- (2) RA gửi yêu cầu hủy bỏ chứng thư sau khi đã ký đến CA
- (3) Sau khi xem xét CA loại chứng thư có yêu cầu hủy bỏ và cập nhật danh sách chứng thư hủy bỏ trên thư mục các chứng thư bị hủy
- (4) CA gửi mã thông báo đã huỷ bỏ chứng thư trở lại RA
- (5) RA gửi thông báo đã hủy tới người sử dụng

KHÁI NIỆM KHÁC

- Kho chứng thư số
- Hủy bỏ chứng thư số
- Sao lưu và khôi phục khóa
- Cập nhật khóa tự động
- Lịch sử khóa
- Chứng thực chéo
- Hỗ trợ chống chối bỏ
- Dấu thời gian (time stamp)
- Phần mềm hỗ trợ tích hợp PKI

KHO LƯU TRỮ CHỨNG THƯ

- Kho lưu trữ chứng thư lưu trữ toàn bộ các chứng thư số của các cơ quan chứng thực và các chứng thư số của các thuê bao trong hệ thống, phục vụ việc tra cứu các chứng thư số. Các thông tin về danh sách hủy bỏ chứng thư số…
- X.500, LDAP, các máy chủ Web, các máy chủ FTP, DNS, các cơ sở dữ liệu

HỦY BỎ CHỨNG THƯ SỐ

- CA ký lên một chứng thư gắn một cặp khoá công khai với nhân dạng của người sử dụng. Trong các môi trường thế giới thực, sẽ cần đến việc phá bỏ gắn kết đó.
  - Ví dụ: khi người dùng bị lộ khóa bí mật, thay đổi công tác, chết, mất tích
- Cần phải có một cách nào đó để cảnh báo cho toàn bộ người dùng trong hệ thống để không tiếp tục sử dụng khóa đó để liên lạc với chủ sở hữu.
- Cơ chế cảnh báo này được gọi **là quá trình hủy bỏ chứng thư số** (certification revocation).

SAO LƯU VÀ PHỤC HỒI KHÓA

Trong quá trình sử dụng chứng thư số, người dùng có thể gặp một số sự cố làm mất quyền sử dụng khóa:

- Quên mật khẩu: khóa bí mật được mã hóa hoặc chứa trong một thiết bị và người dùng quên mật khẩu, không thể truy nhập khóa
- Phương tiện bị hỏng: thiết bị lưu khóa bị hỏng
- Phương tiện bị thay thế: khóa bị ghi đè,…

SAO LƯU VÀ PHỤC HỒI KHÓA

- Nếu như khoá bí mật bị mất, các tài liệu được mã hóa bởi khóa này sẽ không khôi phục được, nó có thể gây trở ngại nghiêm trọng.
- Giải pháp là sao lưu và khôi phục các khoá bí mật để giải mã (nhưng không phải các khoá bí mật để ký).
- Khi khóa bí mật bị mất, người dùng có thể đến cơ quan chứng thực để xin lại khóa (sau khi qua một số thủ tục bắt buộc)

CẬP NHẬT KHÓA TỰ ĐỘNG

- Một chứng thư có thời gian sống hữu hạn.
- Một chứng thư đã cho sẽ phải "hết hạn" và được thay bằng một chứng thư mới.
- Quá trình này được gọi là "***cập nhật khoá***"(key update) hoặc "***cập nhật chứng thư***" (certificate update).
- Đối với CTS ký, xác thực thì việc cập nhật khóa tự động sẽ khá thuận tiện cho người dùng
- Đối với CTS mã, khi thay khóa mới sẽ có nhiều vấn đề phát sinh và có thể là khe hở An ninh để khai thác chặn bắt khóa

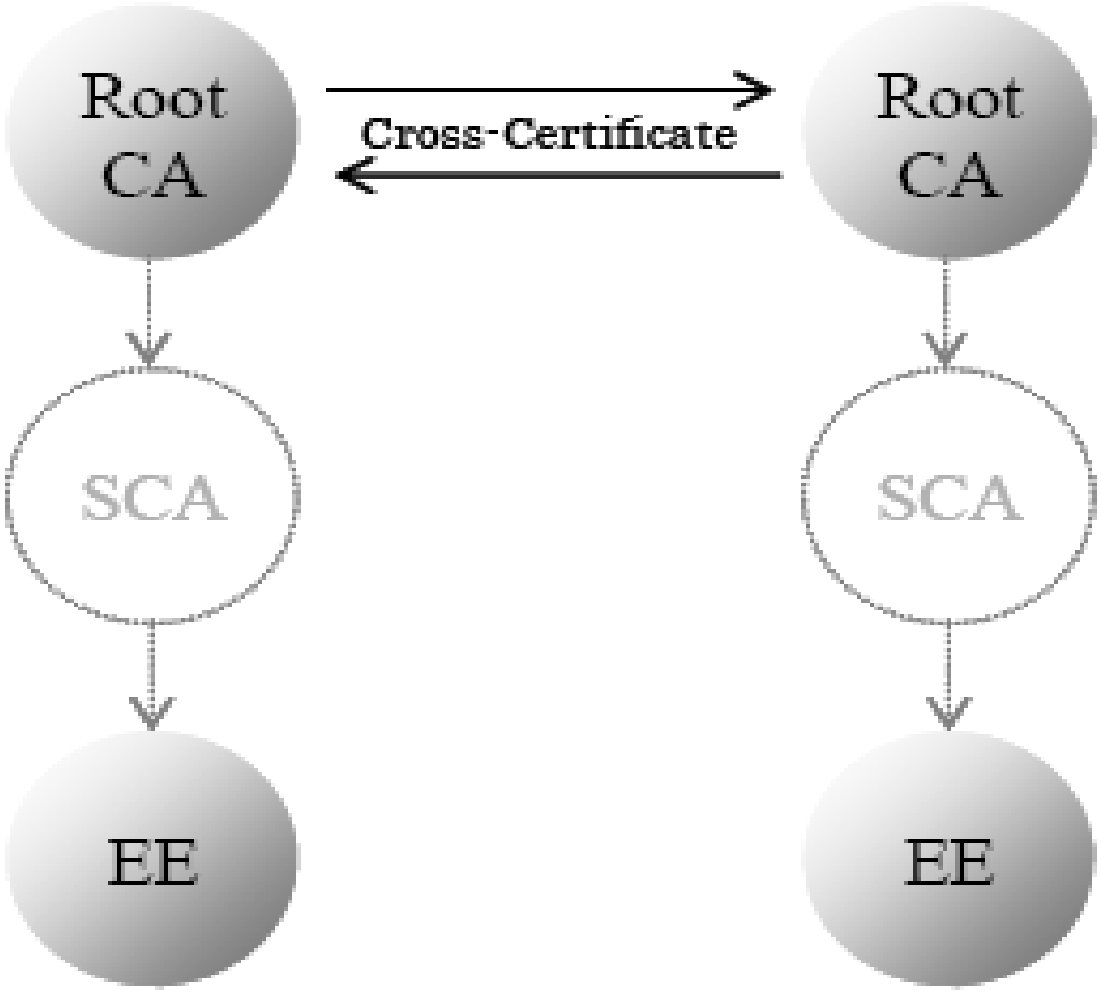
LỊCH SỬ KHÓA

- Việc cập nhật khóa trong toàn bộ quá trình sử dụng CTS, một người sử dụng đã cho có nhiều chứng thư "cũ" và ít nhất một chứng thư "hiện tại".
- Tập hợp các chứng thư này và các khoá bí mật tương ứng được biết như là "***lịch sử khoá***" (key history) của người sử dụng. (một cách đúng hơn là ***lịch sử chứng thư và khoá***).

LỊCH SỬ KHÓA

- Việc lưu giữ vết của toàn bộ lịch sử khoá này là rất quan trọng bởi vì dữ liệu mà đã mã hoá vào thời điểm 5 năm trước đây không thể giải mã được bằng khoá giải mã bí mật hiện tại.
- Do vậy cần lịch sử khóa để cho khoá giải mã đúng có thể tìm thấy nhằm giải mã dữ liệu yêu cầu. Tương tự, một số chứng thư trong lịch sử khoá này có thể cần thiết để kiểm chứng các chữ ký 5 năm trước đây.
- Việc quản trị lịch sử khóa cần tự động và hoàn toàn được duy trì bởi PKI

CHỨNG THỰC CHÉO



CHỨNG THỰC CHÉO

- Việc xây dựng một hệ thống PKI duy nhất trên toàn thế giới là điều không khả thi và không hợp lý.
- Một quốc gia có thể có nhiều hệ thống PKI
- Các PKI này hoạt động độc lập, phục vụ các môi trường và cộng đồng khác nhau
- **Chứng thực chéo** giữa các PKI để tạo ra các quan hệ tin cậy giữa các hệ thống PKI độc lập
- **Chứng thực chéo** là cơ chế cho phép người dùng ở hệ thống PKI này có thể kiểm chứng CTS của người dùng ở hệ thống PKI khác.

HỖ TRỢ CHỐNG CHỐI BỎ

- Những người dùng một PKI thường thực hiện các hành động được dự định không thể thay đổi kết hợp với danh tính của họ.
- Ví dụ:
  - một người ký số một văn bản, tức là làm khẳng định rằng anh ta chấp nhận nội dung của văn bản này.
  - Nhiều tháng sau khi ký văn bản, anh ta không thể từ chối được rằng chữ ký thực sự xuất phát từ anh ta bằng cách khẳng định rằng một ai đó có được khoá ký bí mật của anh ta và đã sử dụng nó lên văn bản mà không có sự chấp nhận của anh ta hoặc anh ta không biết.

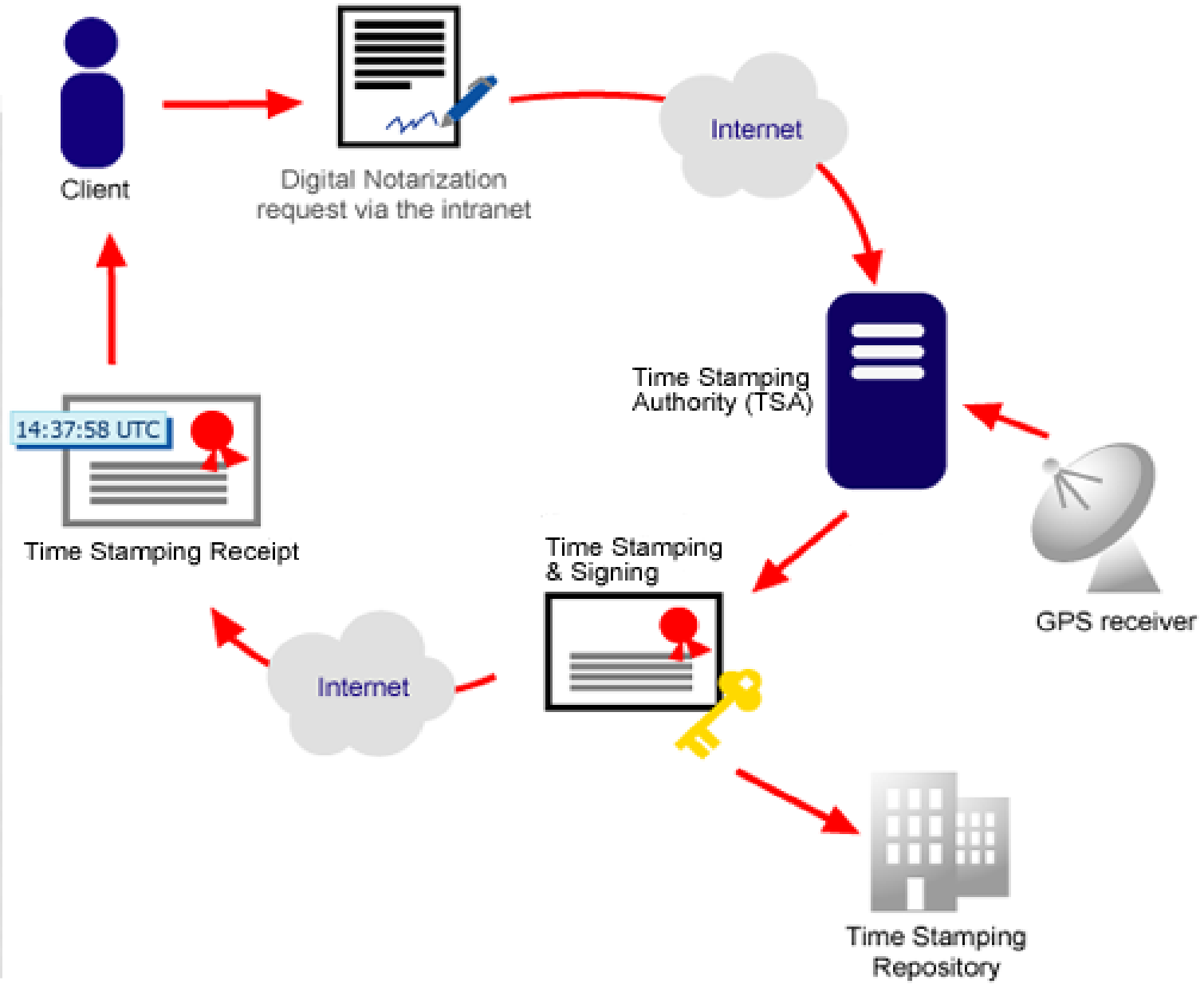
HỖ TRỢ CHỐNG CHỐI BỎ

- Một sự từ chối như vậy là sự chối bỏ của hành động, cho nên một PKI cần phải cung cấp sự hỗ trợ để tránh hoặc ngăn chặn chối bỏ- một tính chất được biết như là không chối bỏ (non-repudiation).
- Một PKI không thể tự mình cung cấp tính không chối bỏ thực sự và đầy đủ; thông thường, yếu tố con người là cần thiết để cân nhắc sự kiện và đưa ra quyết định cuối cùng.
- Tuy nhiên, PKI cần phải hỗ trợ quá trình này bằng cách cung cấp một vài bằng chứng kỹ thuật nào đó được yêu cầu, chẳng hạn như xác thực nguồn gốc dữ liệu và của thời gian mà dữ liệu đã được ký trong trường hợp xảy ra tranh chấp.

DẤU THỜI GIAN

- Một phần tử quan trọng trong việc hỗ trợ cho các dịch vụ không chối bỏ là việc sử dụng của dấu thời gian an toàn (secure time stamping) trong PKI.
- Tức là, nguồn thời gian cần được tin cậy, và giá trị thời gian cần phải được truyền nhận một cách an toàn.
- Cần phải có một nguồn có thể tin được về thời gian mà một tập hợp những người dùng PKI sẽ tin cậy.
- Nguồn có thể tin được về thời gian cho PKI không chỉ dành cho mục đích chống chối bỏ mà có thể cho nhiều mục đích khác.
- Tuy nhiên, mục đích chống chối bỏ là mục đích chính của dấu thời gian trong nhiều môi trường

GẮN DẤU THỜI GIAN



PHẦN MỀM HỖ TRỢ TÍCH HỢP PKI

- Một PKI có thể xem xét, ít nhất ở một mức nào đó, như là một tập hợp các máy chủ PKI mà sẽ "làm các việc" cho những người dùng, chẳng hạn như:
  - CA sẽ cung cấp các dịch vụ chứng thực
  - Kho sẽ lưu giữ các chứng thư và thông tin huỷ bỏ
  - Máy chủ sao lưu và khôi phục sẽ quản lý đúng các lịch sử khoá
  - Máy chủ dấu thời gian sẽ liên kết thông tin thời gian tin cậy được vào các văn bản.

PHẦN MỀM HỖ TRỢ TÍCH HỢP PKI

- Phần mềm hỗ trợ tích hợp PKI là một thành phần cần thiết của một hệ thống PKI có đầy đủ các tính năng và các hoạt động.
- Không có nó, nhiều dịch vụ cung cấp bởi PKI không thể được triển khai tới người dùng cuối.
- Các phần mềm hỗ trợ tích hợp PKI được chuẩn hóa để các ứng dụng khác có thể thông qua để giao tiếp với PKI.
- Ở các dạng:
  - Tương đối lớn: xử lý đường dẫn chứng thư, kiểm tra CTS, xác thực,…
  - Tương đối nhỏ: thực hiện dịch vụ PKI
  - Một Java applet được tải về
  - Thư viện liên kết động (DLL)

CÁC CHUẨN VÀ ĐẶC TẢ PKI

- PKCS (Public Key Cryptography Standards) là tập các đặc tả được đưa ra cho mục đích hỗ trợ sự phát triển của mật mã KCK và hạ tầng PKI
- Họ chuẩn PKCS:
  - PKCS#1: Chuẩn mã hóa RSA
  - PKCS#3: Chuẩn thỏa thuận khóa Diffe-Hellman
  - PKCS#5: Chuẩn mã hóa dựa trên mật khẩu
  - PKCS#6: Chuẩn cú pháp chứng thư mở rộng
  - PKCS#7: Chuẩn cú pháp thông điệp sử dụng mật mã
  - PKCS#8: Chuẩn cú pháp thông tin khóa bí mật
  - PKCS#9: Các kiểu thuộc tính được lựa chọn
  - PKCS#10: Chuẩn cú pháp yêu cầu chứng thư
  - PKCS#11: Chuẩn giao tiếp thẻ mật mã
  - PKCS#12: Chuẩn cú pháp chuyển đổi thông tin cá nhân
  - PKCS #13: Chuẩn mật mã đường cong Elliptic: (đang phát triển)
  - PKCS #14: Chuẩn sinh số giả ngẫu nhiên
  - PKCS #15: Chuẩn khuôn dạng thông tin thẻ mật mã
- Các chuẩn hay được sử dụng là PKCS#1, 6, 7, 10, 11, 12

CÁC DỊCH VỤ CỦA PKI

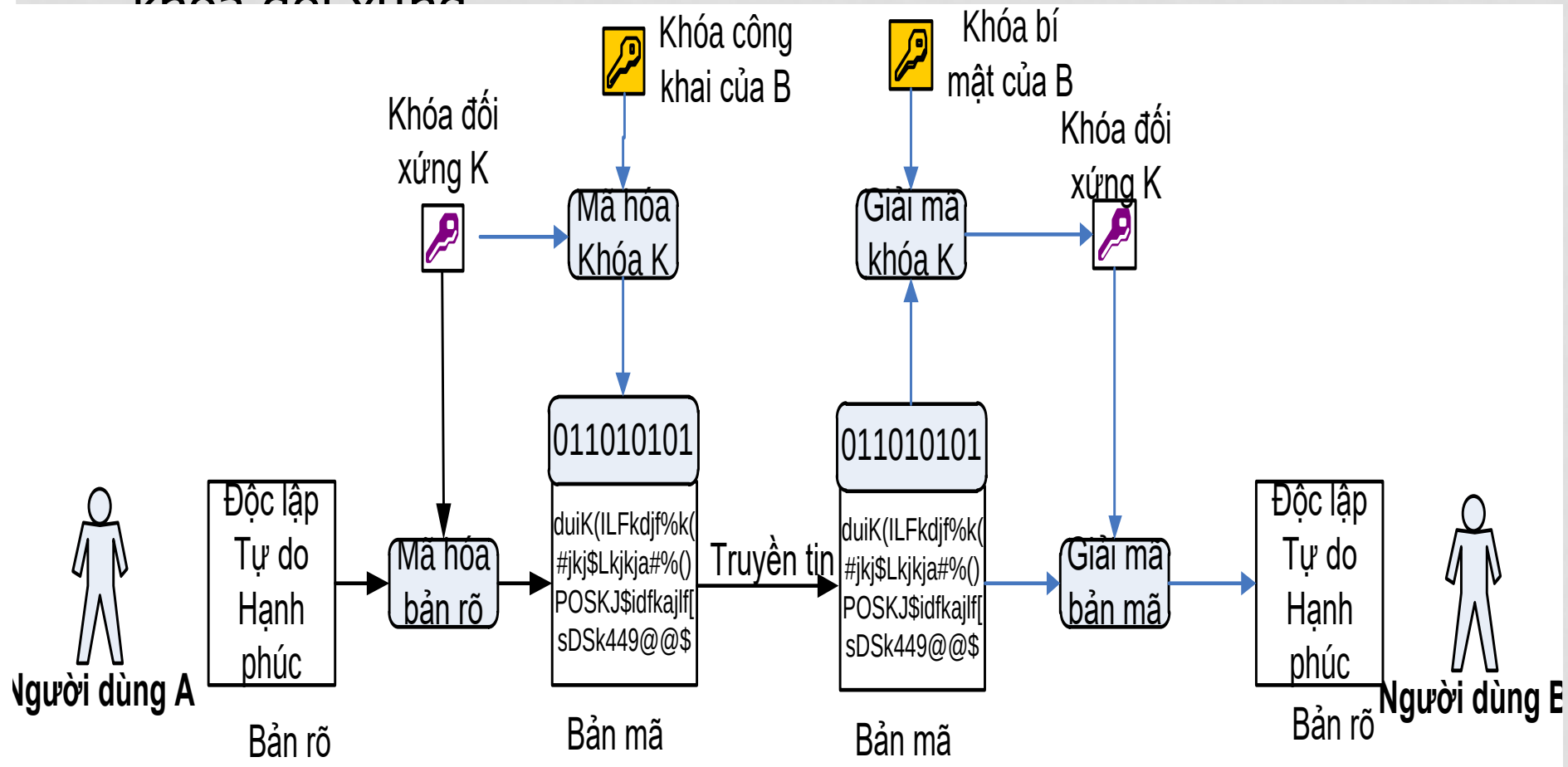
- Dịch vụ đảm bảo tính bí mật
- Dịch vụ đảm bảo tính toàn vẹn
- Dịch vụ xác thực
- Dịch vụ hỗ trợ chống chối bỏ
- Dịch vụ dấu thời gian

DỊCH VỤ ĐẢM BẢO TÍNH BÍ MẬT

- Là đảm bảo tính bí mật của dữ liệu
- Chỉ có những người có quyền mới có thể truy cập được dữ liệu và đọc nội dung dữ liệu
- Tính bí mật được cung cấp bởi các cơ chế mã hóa mật mã.
- => kết hợp mật mã KCK và mật mã khóa đối xứng
- Nhiệm vụ:
  - Đảm bảo tính bí mật của dữ liệu chống lại các tấn công đọc trộm, nghe lén dữ liệu bởi những người dùng bất hợp pháp
  - Các dữ liệu nhạy cảm hoặc những dữ liệu được quy định là mật trở lên cần được bảo mật.
  - Để đảm bảo tính bí mật, các thuật toán thích hợp và khóa sẽ được thỏa thuận giữa các bên để có thể mã hóa và giải mã chính xác dữ liệu

DỊCH VỤ ĐẢM BẢO TÍNH BÍ MẬT

- Lược đồ kết hợp mật mã khóa công khai và mật mã khóa đối xứng



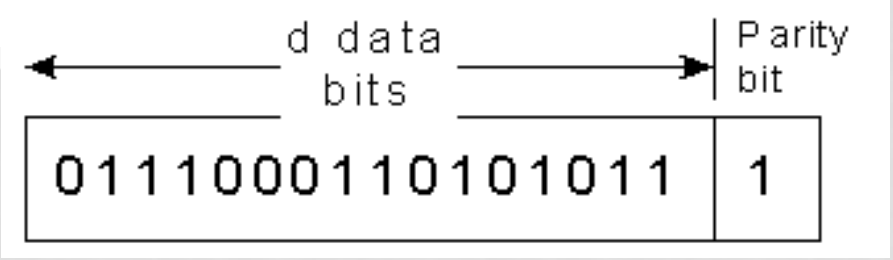
DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

- Toàn vẹn dữ liệu: đảm bảo dữ liệu không bị thay đổi thông qua quá trình truyền đi hay lưu trữ
- Có khả năng phát hiện những thay đổi trái phép, giúp người nhận dữ liệu nhận biết được dữ liệu có bị thay đổi hay không
- Các kỹ thuật mật mã:
  - Mã phát hiện lỗi
  - Mã xác thực thông điệp (MAC)
  - Chữ ký số

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

- Mã phát hiện lỗi
  - Kiểm tra tính chẵn lẻ:
    - là dạng đơn giản nhất là sử dụng một bit chẵn lẻ.
  - Phương pháp tính tổng kiểm tra (checksum)
    - Tính tổng tất cả các số nguyên k bít và sử dụng kết quả tính được làm các bít phát hiện lỗi
  - Kiểm tra dư thừa vòng (mã CRC)

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN



- Mã phát hiện lỗi
  - Kiểm tra tính chẵn lẻ
    - Nếu hệ thống sử dụng bít chẵn lẻ chẵn thì tổng số bit trong d+1 bit là số chẵn
      - Nếu tổng là số lẻ thì sẽ báo lỗi
    - Nếu hệ thống sử dụng bit chẵn lẻ lẻ thì tổng số bit là số lẻ
      - Nếu tổng là số chẵn thì sẽ báo lỗi
    - Vẫn có khả năng thay đổi số bit mà ko bị phát hiện

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

- Mã phát hiện lỗi
  - Phương pháp tính tổng kiểm tra (checksum)
    - Mỗi gói dữ liệu sẽ được tính toán để gắn 1 giá trị vào gói dữ liệu đó để truyền đi
    - Bên nhận sẽ nhận gói dữ liệu, rồi tính toán các giá trị trên gói dữ liệu nhận được
    - Nếu giá trị bên nhận tự tính = với giá trị gắn trên gói dữ liệu được gửi đến thì việc truyền dữ liệu là chính xác, và ngược lại
    - Trong giao thức TCP/IP, Internet checksum tính toán trên tất cả các trường kể cả header và dữ liệu

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

- Mã phát hiện lỗi
  - Kiểm tra dư thừa vòng – CRC (Cyclic Redundancy Check)
    - Là một loại hàm băm, sinh ra giá trị kiểm thử của một chuỗi bit có chiều dài ngắn và cố định
    - Giá trị CRC sẽ được tính toán và đính kèm với dữ liệu khi dữ liệu được truyền đi
    - Khi dữ liệu được sử dụng, dữ liệu sẽ được kiểm tra bằng cách sinh ra mã CRC và so sánh với mã CRC gắn với dữ liệu

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

- Mã phát hiện lỗi
  - Kiểm tra dư thừa vòng – CRC (Cyclic Redundancy Check)
    - Là một phương pháp phát hiện lỗi bằng cách gắn thêm một khối bit phía sau dữ liệu
    - Các bit bổ sung thêm vào gọi là các bit CRC
    - Thuật toán để tạo ra khối bit CRC là dựa trên phép cộng modulo 2 (GF(2))
    - CRC là phần dư của phép chia nhị phân không nhớ

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

- Cách xác định CRC-n:
  - Các bước thực hiện
    - Biểu diễn chuỗi bit thành đa thức nhị phân $M(x)$
    - Nhân $M(x)$ với x^n thu được $M(x) \cdot x^n$
    - Chia $M(x) \cdot x^n$ cho đa thức sinh $G(x)$ của CRC-n
    - Thu được $Q(x)$ và phần dư $R(x)$ sao cho:

$$M(x) \cdot x^n = Q(x) \cdot G(x) + R(x)$$

    - Phần dư $R(x)$ là CRC-n

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

CRC-n	G(x)	USE
CRC-1	$x+1$	Hardware (parity bit)
CRC-4	$x^4 + x + 1$	PCM-30
CRC-5 - CCITT	$x^5 + x^3 + x + 1$	ITU-G.704
CRC-5 – USB	$x^5 + x^2 + 1$	USB token packets
CRC-7	$x^7 + x^3 + 1$	Telecom systems, MMC
CRC-8	$x^8 + x^7 + x^6 + x^4 + x^2 + 1$	
CRC-12	$x^{12} + x^{11} + x^3 + x^2 + x + 1$	use: telecom systems
CRC-32 - MPEG2	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	
…		

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

- Ví dụ:
- Tìm CRC-1 của chuỗi số nhị phân sau: 1101001010101010

- Đáp án:
  - CRC-1 => n=1
  - Đa thức sinh G(x) = x+1
  - Biểu diễn chuỗi số thành đa thức nhị phân
  - $M(x) = x^{15} + x^{14} + x^{12} + x^9 + x^7 + x^5 + x^3 + x$
  - $M(x).x^n = x^{16} + x^{15} + x^{13} + x^{10} + x^8 + x^6 + x^4 + x^2$
  - Thực hiện phép chia nhị phân $M(x).x^n$ cho $G(x)$ thu được:
  - $Q(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^3 + x^2$
  - $R(x) = 0$
  - $\rightarrow$ **CRC-1 = 0**

- Tìm CRC-7 của chuỗi số nhị phân sau: 1101001010101010

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

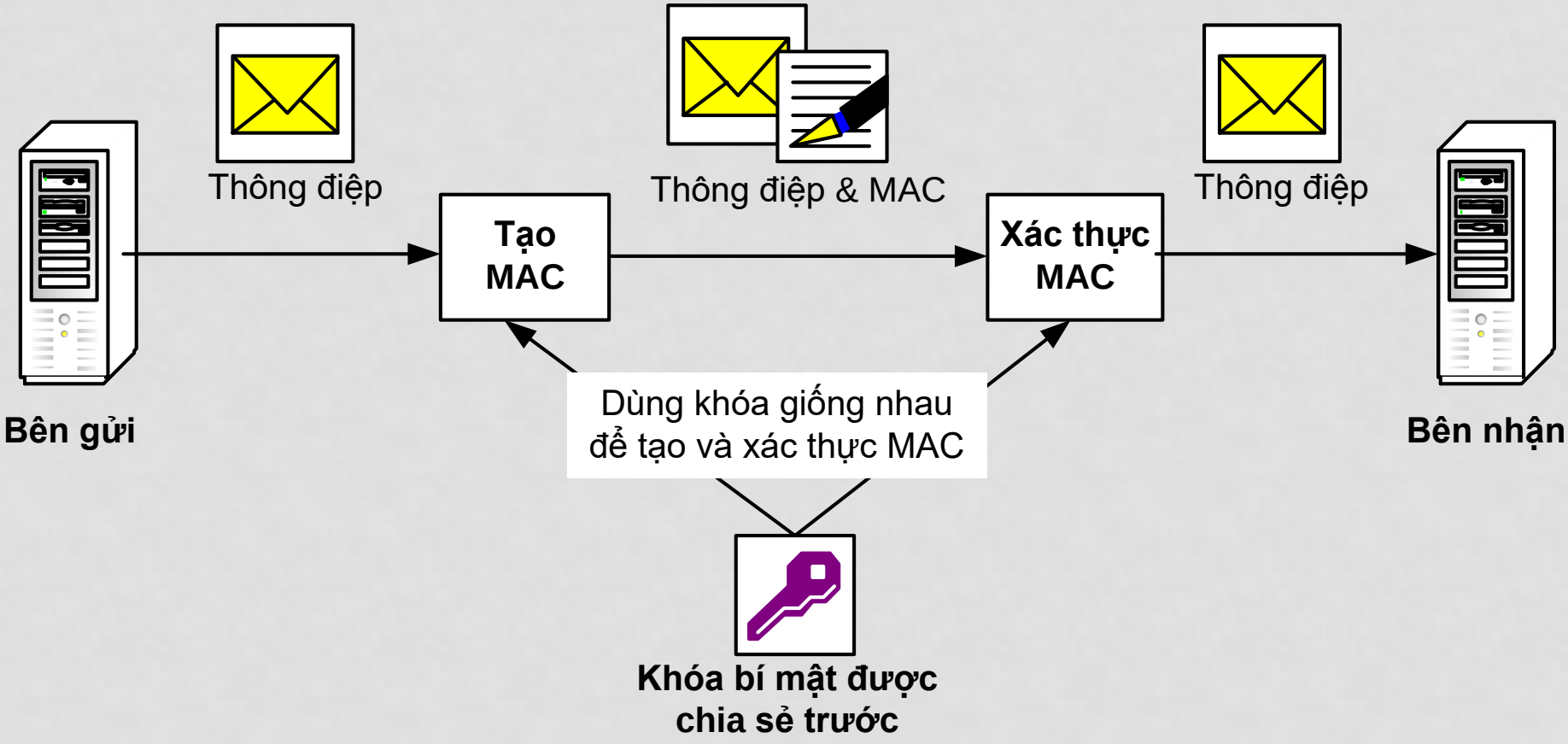
- Mã xác thực thông điệp (MAC)
  - Tạo ra một khối thông tin nhỏ có kích thước cố định, phụ thuộc vào thông điệp và khóa nào đó
  - Không cần giải mã
  - Gắn kèm với thông điệp gốc để giúp xác thực
  - Nhược điểm: MAC phụ thuộc vào cả thông điệp và người gửi
  - MAC không phải là chữ ký điện tử

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

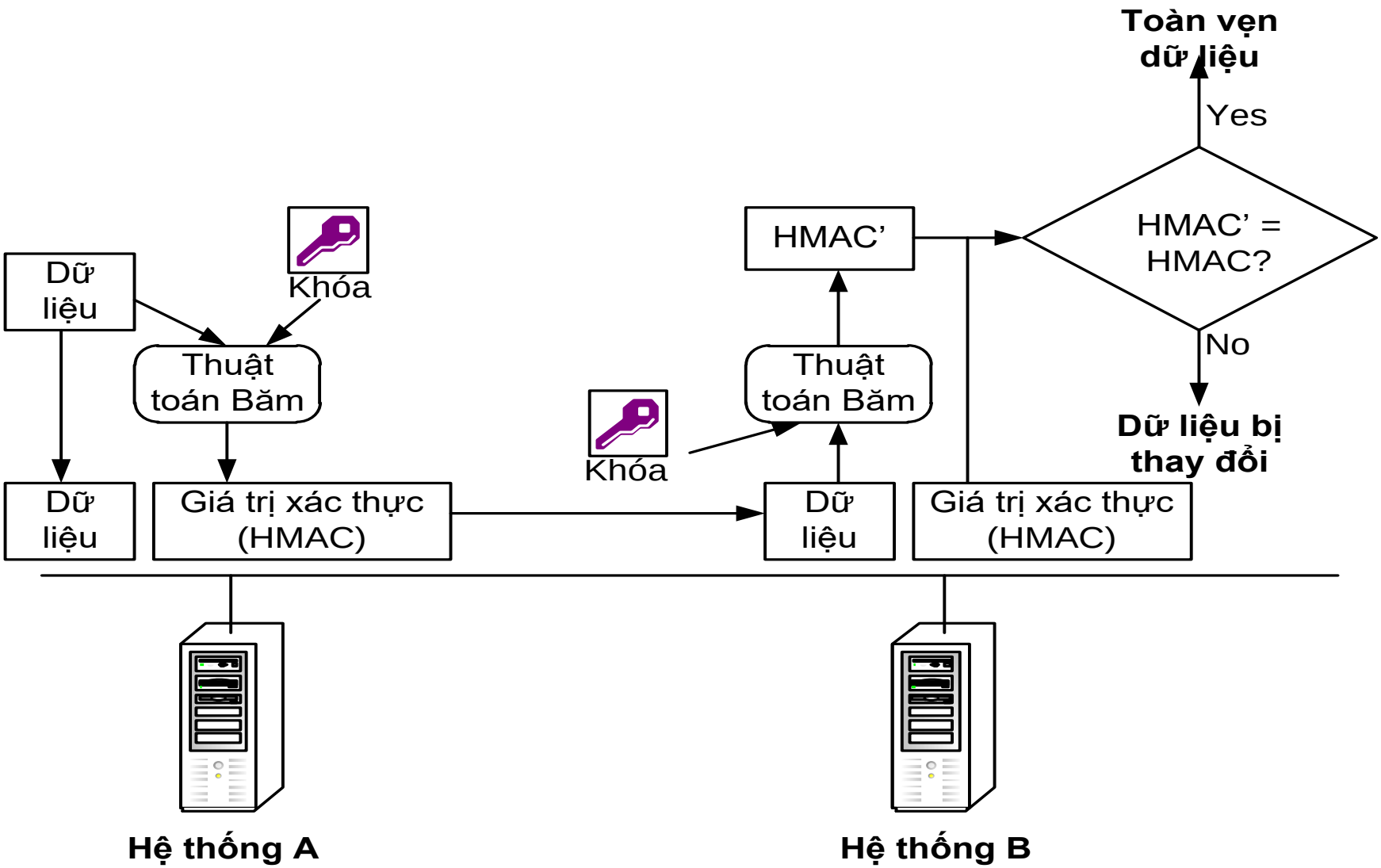
- Mã xác thực thông điệp – MAC
  - Tính chất của MAC
    - MAC là thông tin nén của thông điệp kết hợp với khoá MAC = $C_K(M)$
    - Nén bản tin M có độ dài tùy ý
    - Sử dụng khoá mật K
    - Tạo nên dấu xác thực có độ dài cố định
    - Là hàm nhiều - một
  - Yêu cầu đối với MAC
    - Biết thông điệp và MAC, không thể tìm được thông điệp khác có cùng MAC.
    - Các MAC cần phải phân bố đều
    - MAC phải phụ thuộc như nhau vào tất cả các bit trong thông điệp

DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN

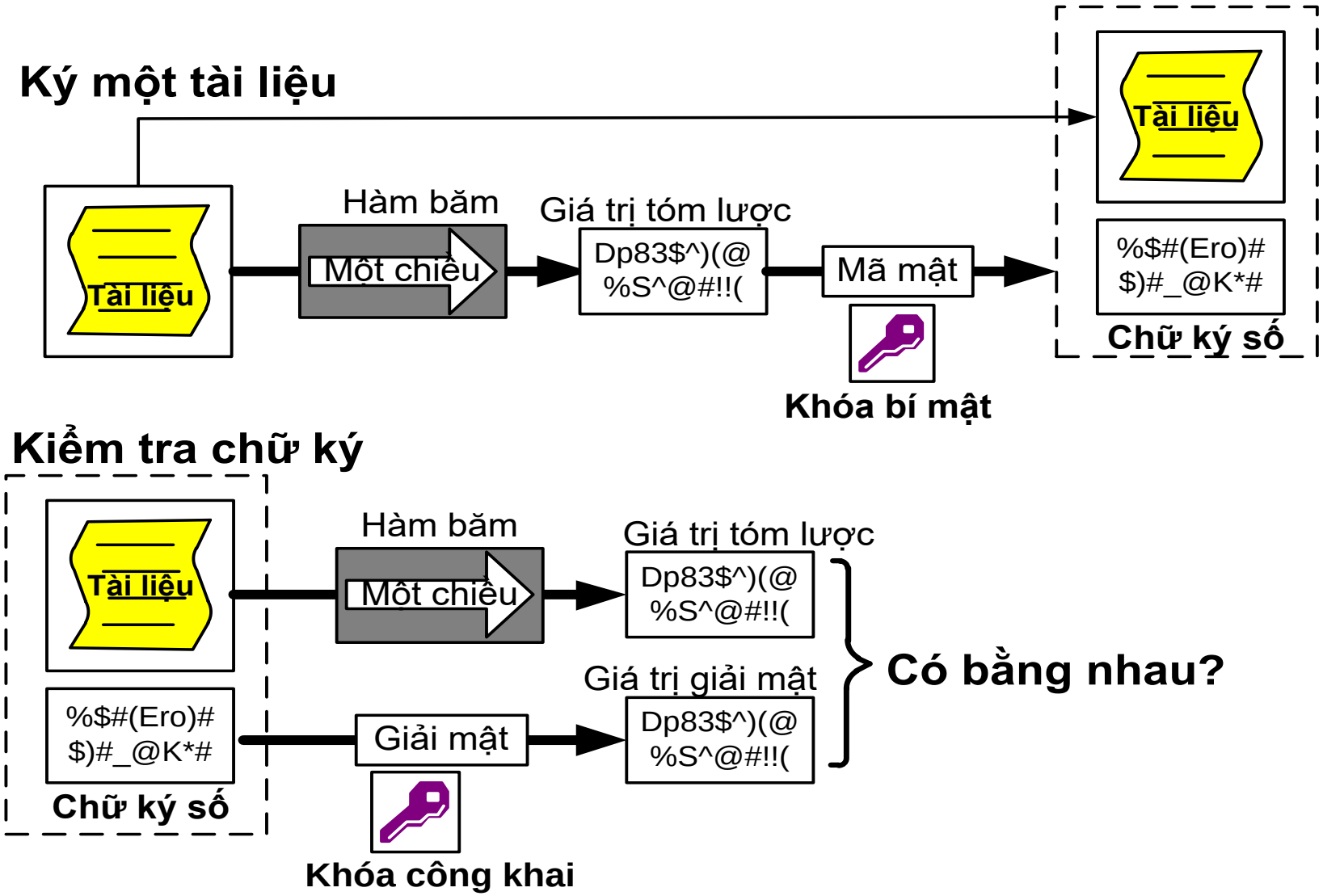
- Sử dụng mã khối đối xứng DES-CBC-MAC



DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN



DỊCH VỤ ĐẢM BẢO TÍNH TOÀN VẸN



DỊCH VỤ XÁC THỰC

- Đảm bảo cho một người dùng rằng một thực thể nào đó đúng là đối tượng mà họ đang cần khẳng định,
- Hai ngữ cảnh ứng dụng chính:
  - Xác minh định danh thực thể
  - Xác minh nguồn gốc dữ liệu
- Hai kiểu xác thực
  - Xác thực cục bộ
  - Xác thực từ xa

DỊCH VỤ XÁC THỰC

- Xác minh thực thể:
  - Hoạt động này tách khỏi các hoạt động khác của thực thể
  - Xác minh thực thể sinh ra một kết quả, sử dụng kết quả này cho các hoạt động khác
- Xác minh nguồn gốc dữ liệu:
  - Xác minh dữ liệu được gắn kết với một thực thể nào đó
  - Hỗ trợ chống chối bỏ nguồn gốc dữ liệu

DỊCH VỤ XÁC THỰC

- Hai kiểu xác thực
  - Xác minh thực thể trong môi trường cục bộ- tức là, xác minh tới thiết bị vật lý của cá nhân thực thể mà không truyền tới các thiết bị khác trong mạng.
  - Xác thực từ xa: Xác thực thực thể tới một thiết bị, thực thể hay môi trường ở xa có hoặc không có người sử dụng trực tiếp tham gia. Có thể không cần tới sự tham gia trực tiếp của người dùng: khó bảo vệ dữ liệu nhạy cảm và không thuận tiện với người dùng.

CÁC NHÂN TỐ XÁC THỰC

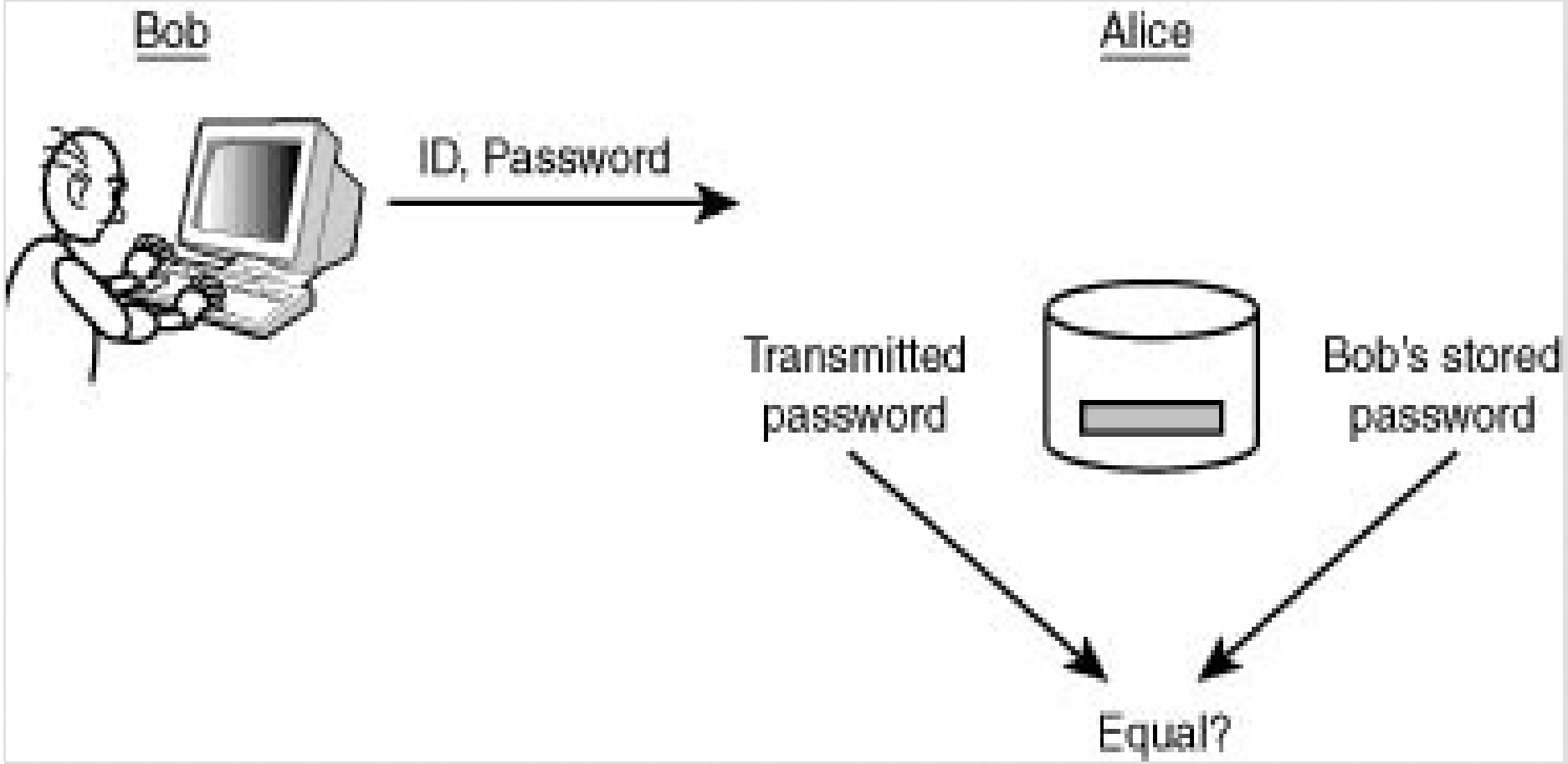
- Something you have (such as a smart card or a hardware token)
- Something you know (such as a password or a PIN)
- Something you are or something intrinsic to your body (such as a thumbprint or a retinal scan)
- Something you do (such as your typing characteristics or handwriting style)

DỊCH VỤ XÁC THỰC

- Dịch vụ PKI về xác thực khai thác kỹ thuật mật mã về chữ ký số
- Chữ ký số có thể được tính trên giá trị băm của một trong ba giá trị sau:
  - Dữ liệu nào đó được xác thực
  - Một yêu cầu nào đó mà người dùng dự định gửi tới thiết bị ở xa
  - Một thách thức ngẫu nhiên được phát hành bởi một thiết bị ở xa.
    - Giá trị đầu tiên hỗ trợ dịch vụ PKI về xác thực nguồn gốc dữ liệu; hai giá trị sau hỗ trợ dịch vụ PKI về xác thực thực thể.

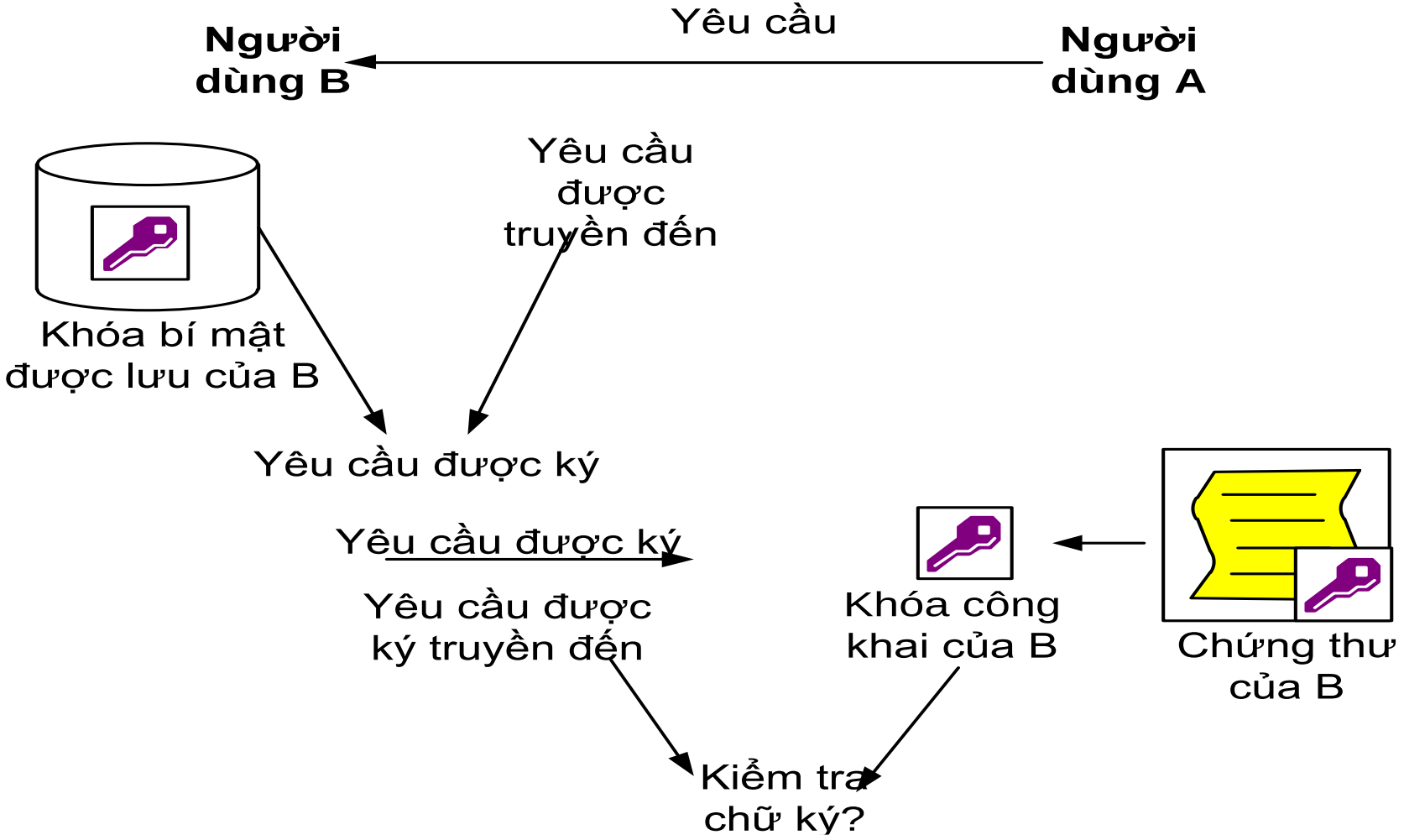
CÁC KỸ THUẬT XÁC THỰC

Xác thực dựa trên User name, password



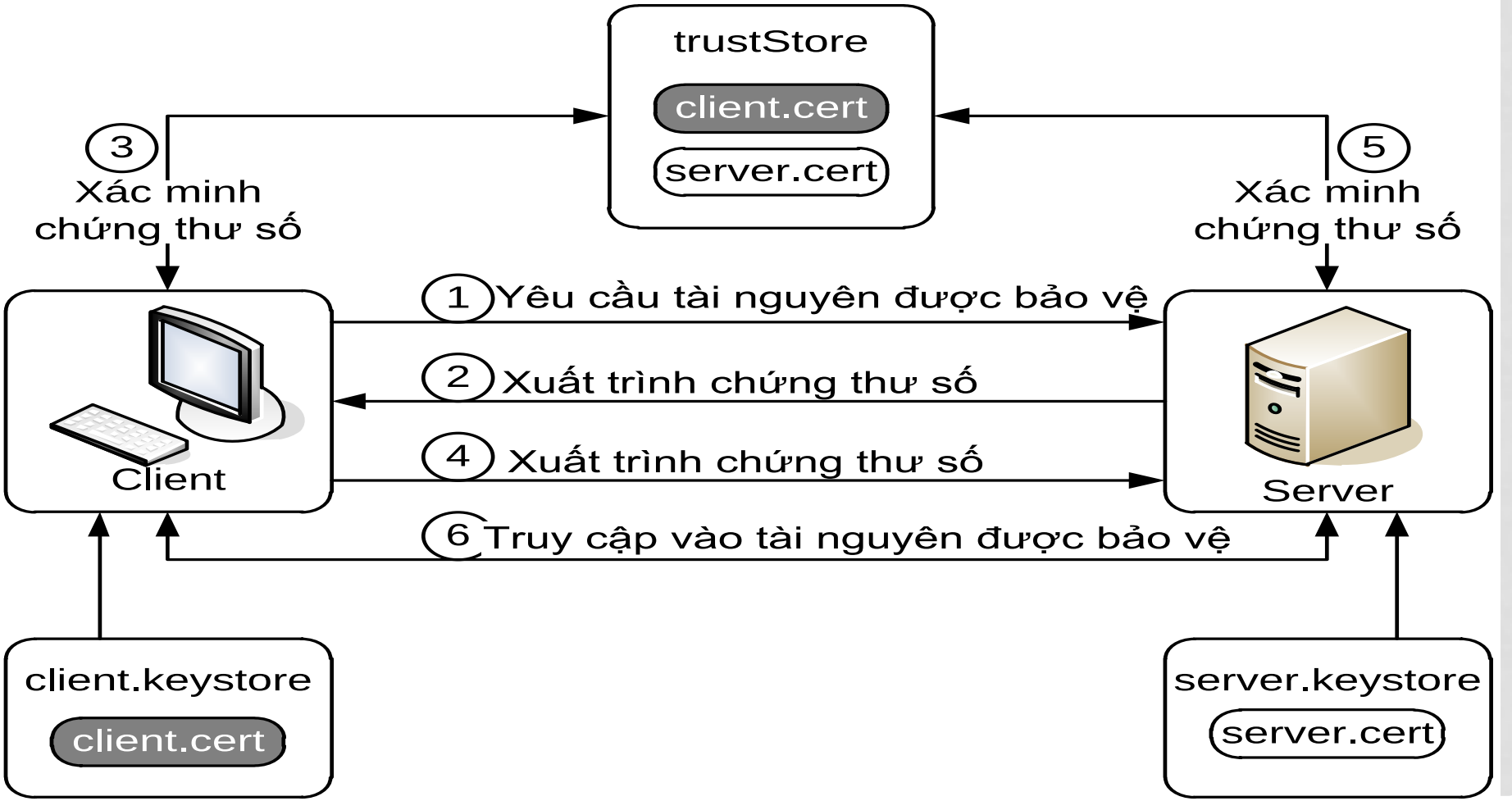
DỊCH VỤ XÁC THỰC

- Xác thực từ xa dựa trên khóa công khai



DỊCH VỤ XÁC THỰC

- Xác thực dựa trên bên thứ 3 tin cậy



DỊCH VỤ HỖ TRỢ CHỐNG CHỐI BỎ

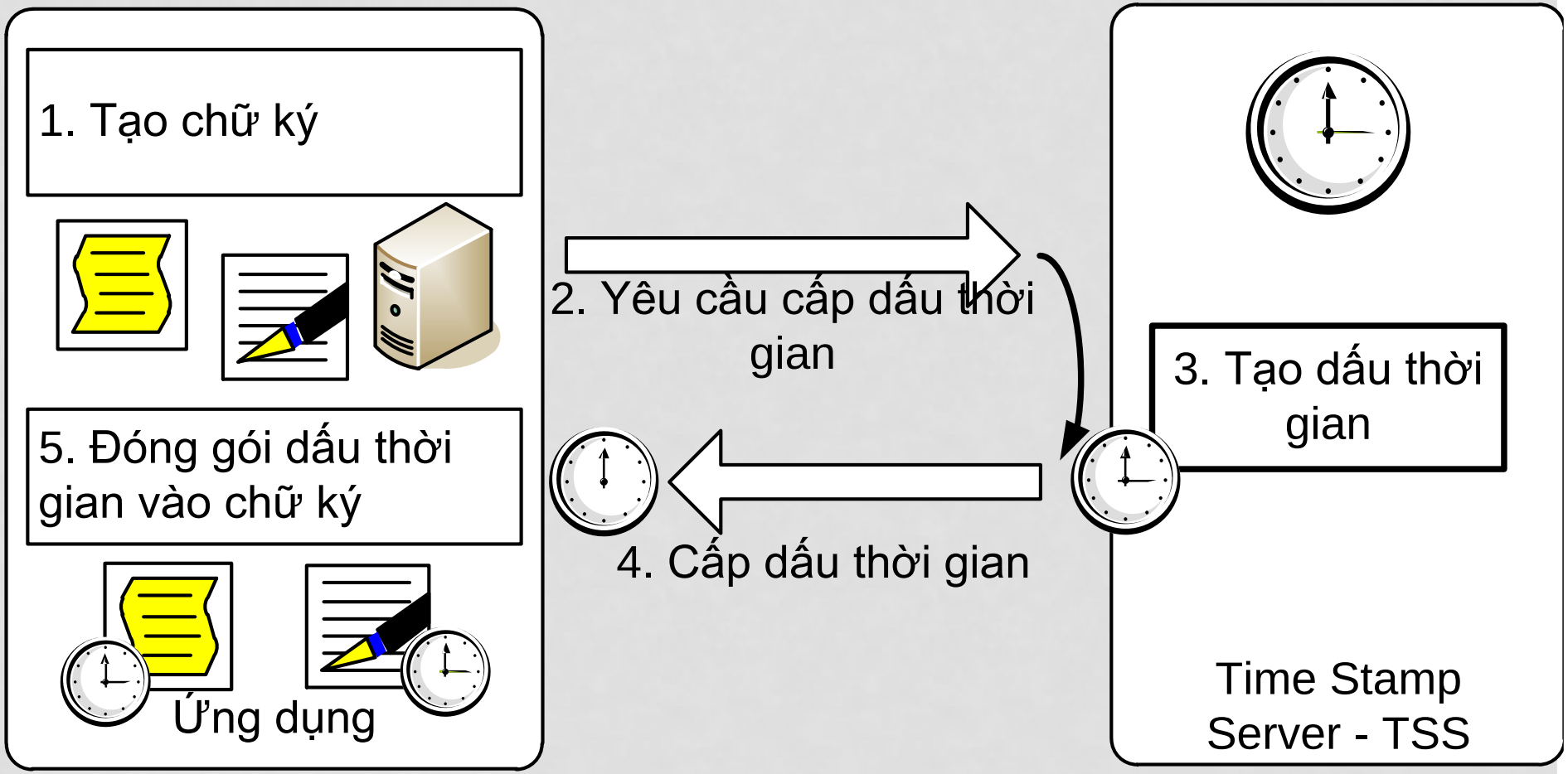
- Chối bỏ là sự không thừa nhận không tham gia một phần hoặc tất cả cuộc truyền thông
- Chống chối bỏ: Đảm bảo các thực thể phải trung thực trong việc thực hiện các hoạt động,
- Các dạng chính:
  - Không chối bỏ về nguồn gốc (non-repudiation of origin)
  - Không chối bỏ việc tiếp nhận (non-repudiation of receipt)
- Ý tưởng là gắn bằng mật mã với một hoạt động cụ thể của người dùng sao cho người dùng không thể chối bỏ được hành động của mình./.

DỊCH VỤ DẤU THỜI GIAN

- Dấu thời gian biểu thị rằng một tài liệu nào đó là trước tài liệu X và sau tài liệu Y,
- Nó liên kết thời gian với dữ liệu,
- Phải có khả năng kiểm tra rằng dấu thời gian được liên kết với dữ liệu là xác thực và có tính toàn vẹn,
- Dịch vụ dấu thời gian an toàn có thể sử dụng các dịch vụ cốt lõi của PKI.
- Dấu thời gian bao gồm chữ ký số trên tổ hợp của:
  - dữ liệu biểu diễn thời gian,
  - giá trị băm của chính tài liệu

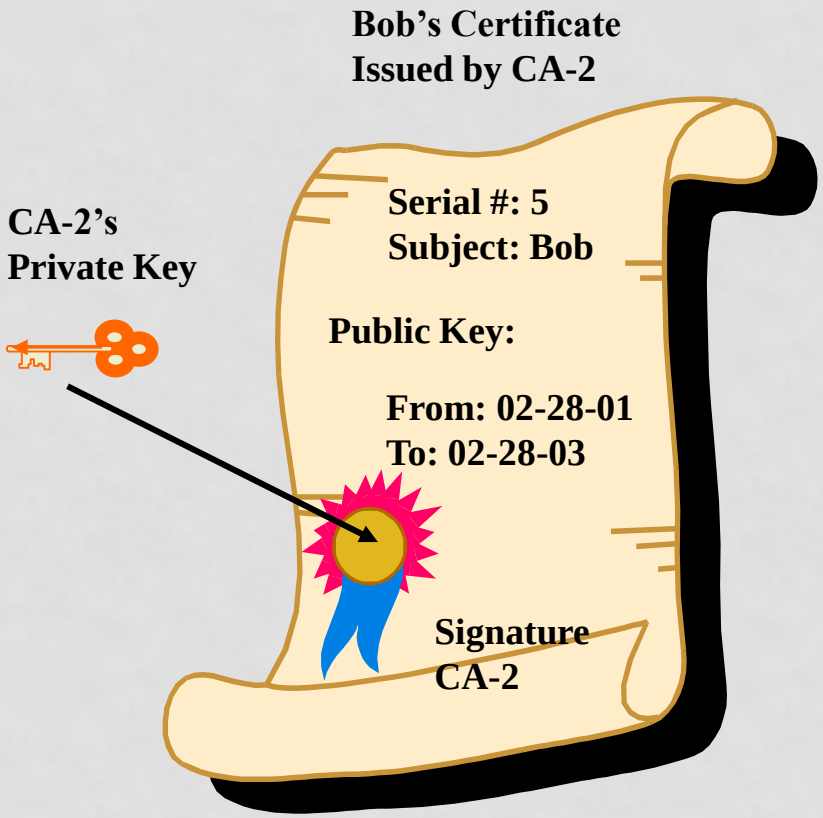
DỊCH VỤ DẤU THỜI GIAN

- Sơ đồ cấp dấu thời gian



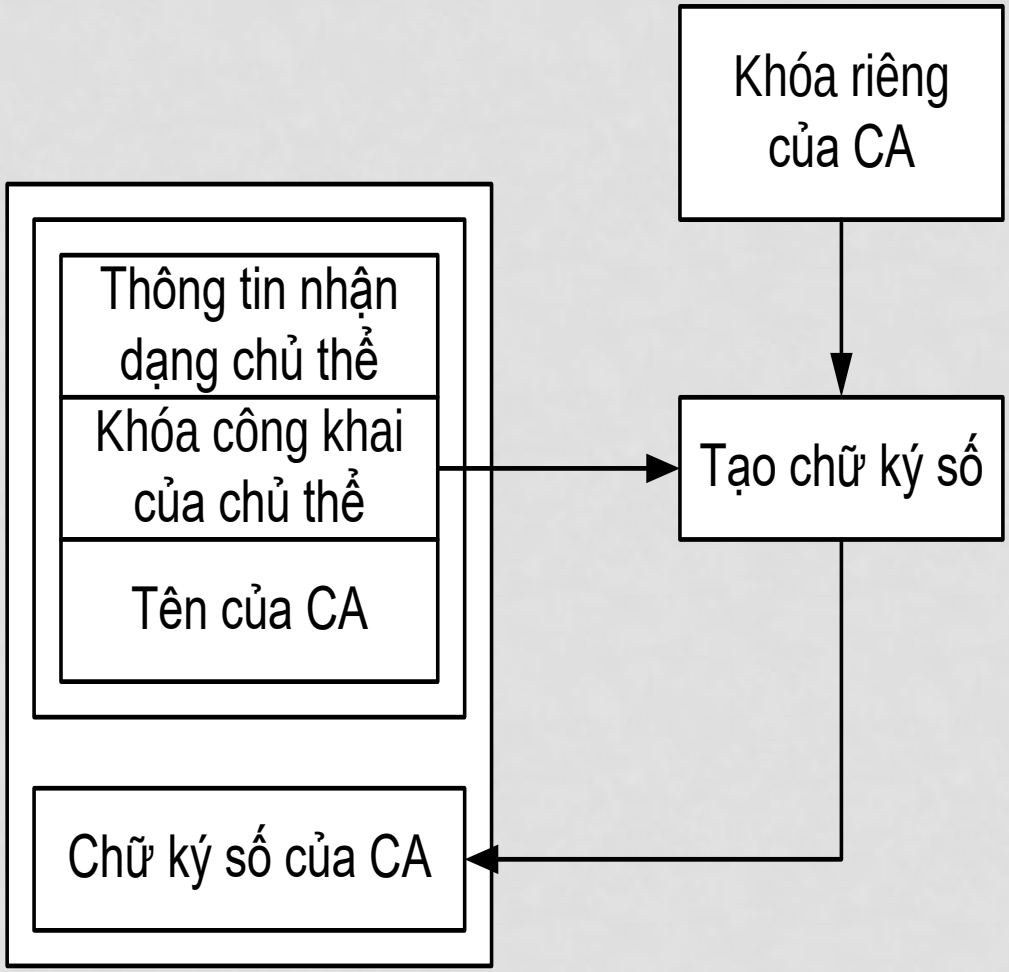
CHỨNG THƯ SỐ

- Chứng thư số là một cấu trúc dữ liệu gắn kết khoá công khai của một người với một hoặc nhiều thuộc tính để xác định người sử dụng đó
- Chứng thư số được đảm bảo bởi một đối tác tin cậy là CA
- Loại chứng thư được sử dụng phổ biến là X509 Certificate
- Một trong các kiểu chứng thư quan trọng là chứng thư khóa công khai



CHỨNG THƯ SỐ KHÓA CÔNG KHAI

- CA phát hành CTS cho những chủ thể nắm giữ cặp khóa công khai và khóa riêng. Mỗi CTS gồm có một KCK và thông tin nhận dạng duy nhất của chủ thể CTS.
- Chủ thể của CTS có thể là người, thiết bị hoặc một chủ thể khác có nắm giữ khóa riêng tương ứng.
- Các CTS đều được CA ký bằng khóa riêng của CA

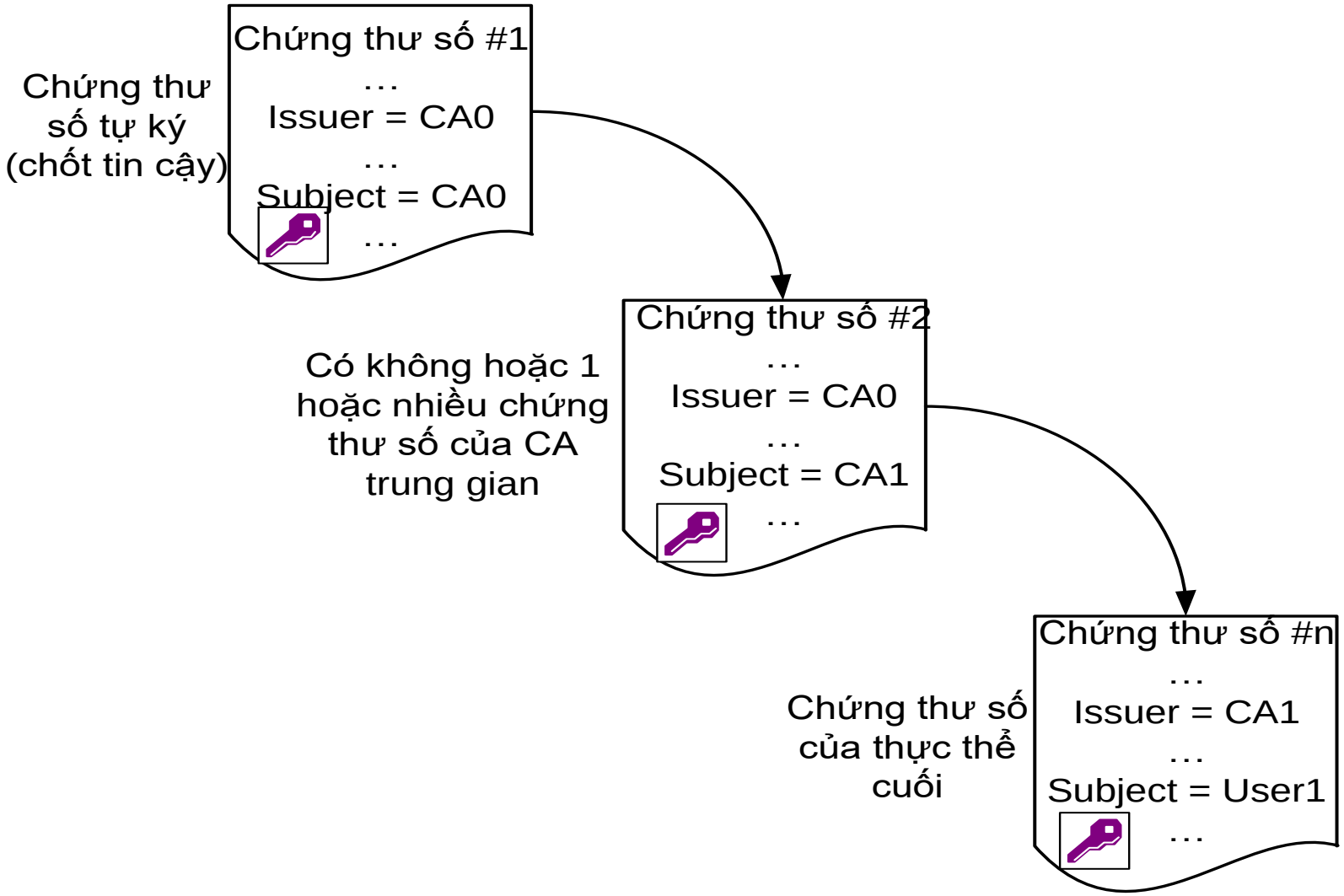


CHỨNG THƯ SỐ KHÓA CÔNG KHAI

- Lợi ích:
  - Một người dùng có thể có một số lượng lớn các khóa công khai của các thành viên khác một cách tin cậy, xuất phát từ thông tin khóa công khai của CA.
- Lưu ý, một CTS hợp lệ là khi người sử dụng khóa công khai tin tưởng rằng CA phát hành các chứng thư hợp lệ.

CHỨNG THƯ SỐ KHÓA CÔNG KHAI

- Đường dẫn chứng thực
  - Một chuỗi các chứng thư được cấp phát
  - Thực thể cấp phát CTS đầu tiên là một điểm chốt tin cậy
  - Chủ thể của CTS cuối cùng là thực thể cuối cùng nhận được CTS
  - Mục đích:
    - Tập hợp, liên kết các CTS cần thiết lại với nhau để tạo thành một đường dẫn được tin tưởng chứng thư thực thể cuối được cấp phát trực tiếp từ điểm tin tưởng của nó

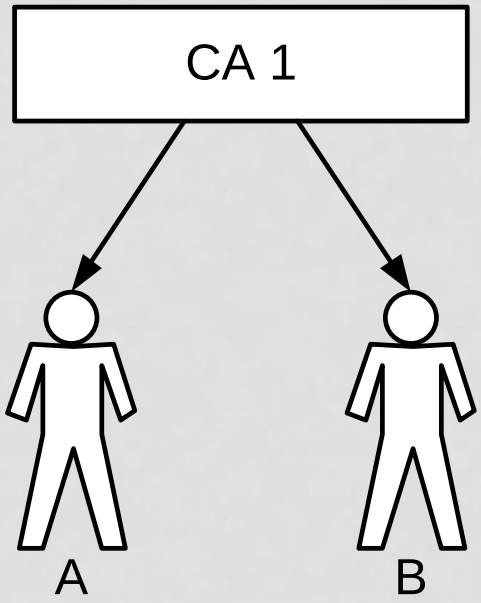

Chứng thư số #1
…
Issuer = CA0
…
Subject = CA0
…
Chứng thư số tự ký (chốt tin cậy)
Chứng thư số #2
…
Issuer = CA0
…
Subject = CA1
…
Có không hoặc 1 hoặc nhiều chứng thư số của CA trung gian
Chứng thư số #n
…
Issuer = CA1
…
Subject = User1
…
Chứng thư số của thực thể cuối

CÁC MÔ HÌNH KIẾN TRÚC TIN CẬY

- Kiến trúc hệ thống PKI được triển khai dựa vào yêu cầu của tổ chức
- Cốt lõi của mỗi kiến trúc chính là sự tin cậy
- Các loại kiến trúc đề cập:
  - Kiến trúc CA đơn
  - Kiến trúc PKI cho doanh nghiệp
    - Kiến trúc phân cấp
    - Kiến trúc mạng lưới
  - Kiến trúc PKI lai
    - Kiến trúc danh sách tin cậy mở rộng
    - Kiến trúc chứng thực chéo
    - Kiến trúc CA cầu nối

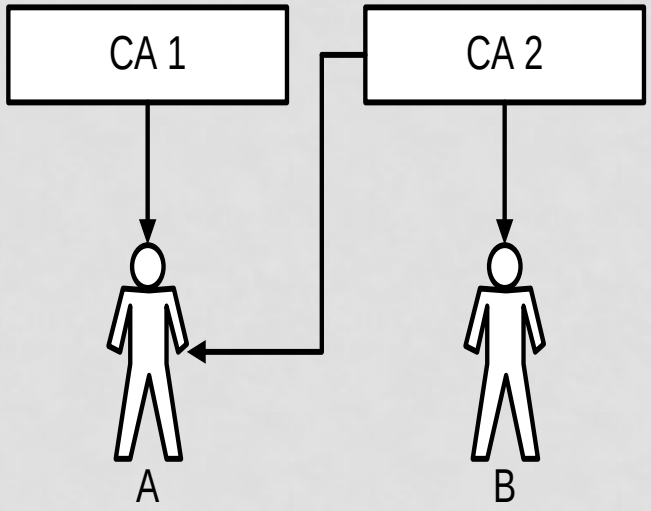
HỆ THỐNG KIẾN TRÚC CA ĐƠN

- Là mô hình cơ bản nhất của PKI
- Có duy nhất một CA cấp phát, phân phối CTS và danh sách thu hồi CTS tới các thực thể.
- Tất cả thực thể hoàn toàn tin tưởng vào CA
- Mỗi người dùng chỉ có 1 đường dẫn chứng thư duy nhất từ CA đơn
  - *Đường dẫn chứng thư cho A: [CA1 → A]*
  - *Đường dẫn chứng thư cho B: [CA1 → B]*
- Nếu khóa bí mật của CA bị lộ thì toàn bộ CTS do CA cấp sẽ bị vô hiệu hóa, và PKI bị phá vỡ hoàn toàn
- Khó mở rộng



MÔ HÌNH DANH SÁCH TIN CẬY CƠ BẢN

- Là mô hình nâng cấp của kiến trúc CA đơn
- Dịch vụ PKI được cung cấp bởi 1 số CA
- Các CA không thành lập mối quan hệ tin cậy
- Không có đường dẫn chứng thực
- Các thực thể duy trì một danh sách các CA tin cậy
- Đơn giản thiết kế
- Cồng kềnh khi số lượng CA gia tăng
- Cập nhật thông tin của CA khó khăn
- Cần xây dựng đường dẫn chứng thực để xác thực CTS đầu tiên



XÂY DỰNG ĐƯỜNG DẪN CHỨNG THỰC CHO KIẾN TRÚC CA ĐƠN VÀ DANH SÁCH TIN CẬY

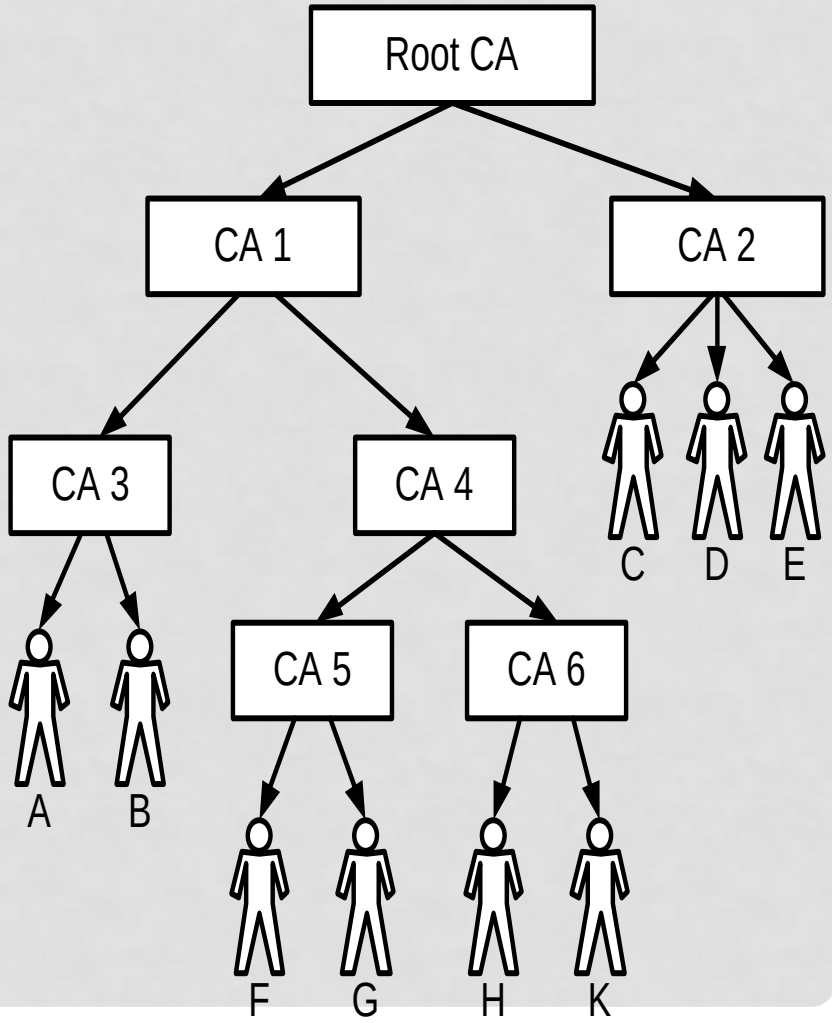
- Xây dựng đường dẫn chứng thực trong CA đơn
  - A và B tin cậy vào CA-1
  - [CA-1→A]
  - [CA-1→B]
- Xây dựng đường dẫn chứng thực cho danh sách tin cậy
  - A có CA-1 và CA-2 trong danh sách tin cậy
  - B có CA-2, CA-3, CA-4 trong danh sách tin cậy
  - Đường dẫn chứng thực cho A có thể là 1 trong 2 đường dẫn
    - [CA-1→A]
    - [CA-2→A]
  - Đường dẫn chứng thực cho B có thể là 1 trong những đường dẫn
    - [CA-2→B]
    - [CA-3→B]
    - [CA-4→B]

HỆ THỐNG KIẾN TRÚC CHO DOANH NGHIỆP

- Kiến trúc phân cấp
- Kiến trúc mạng lưới

KIẾN TRÚC PHÂN CẤP

- Là kiến trúc PKI phổ biến
- Nhiều CA tham gia
- Mối quan hệ tin cậy lẫn nhau – quan hệ thứ bậc
- Hình cây ngược
- Một gốc: CA gốc (Root CA)
- Các nhánh hoặc các nút
  - Các nút: các CA cấp dưới của Root CA
  - Nút lá cuối cùng: thực thể cuối
- Ngoài trừ Root CA, tất cả các CA đều có một CA cấp trên duy nhất

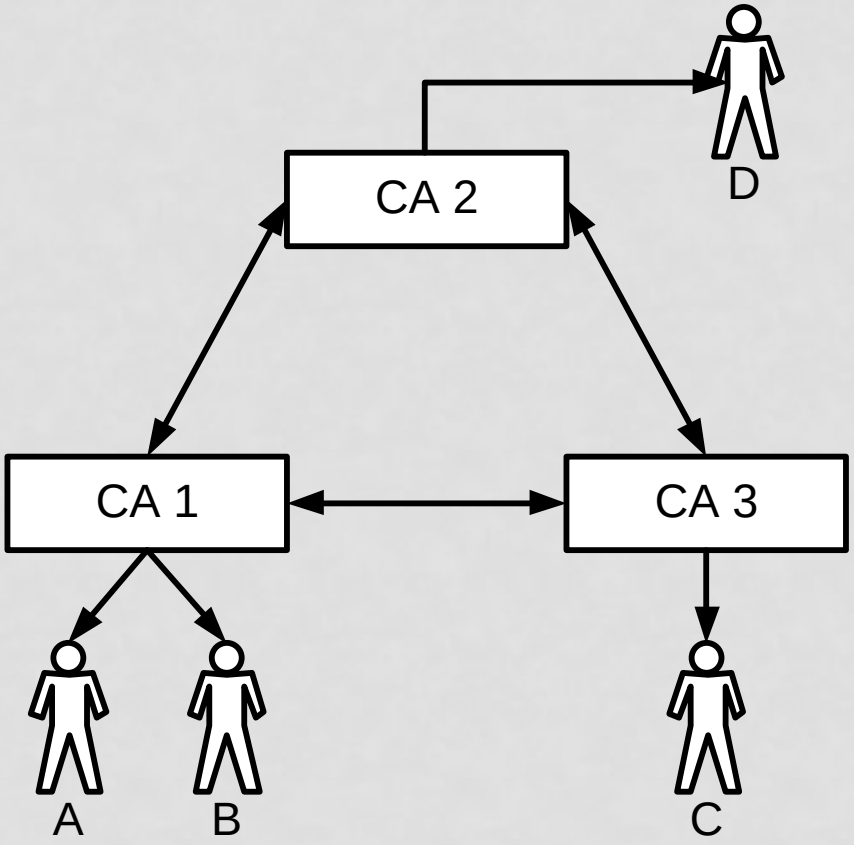


KIẾN TRÚC PHÂN CẤP

- Root CA cấp phát CTS cho các CA cấp dưới, không phát hành cho người dùng cuối
- Các CA cấp dưới có thể cấp phát CTS cho:
  - Các CA ở mức thấp hơn
  - Người dùng cuối
- Root CA tự phát, ký chứng nhận (self-signed) và mọi thực thể đều tin tưởng Root CA
- Ưu điểm:
  - Dễ triển khai
  - Đường dẫn chứng thực ngắn gọn, có nhánh xác thực rõ ràng, không có hiện tượng vòng lặp
  - Ví dụ, đường dẫn chứng thực cho G:
  - [RootCA → CA-1]:[CA-1 → CA-4]:[CA-4 → CA-5]:[CA-5 → G]
- Nhược điểm
  - Chỉ có duy nhất một điểm tin cậy kiểm soát hoàn toàn kiến trúc PKI

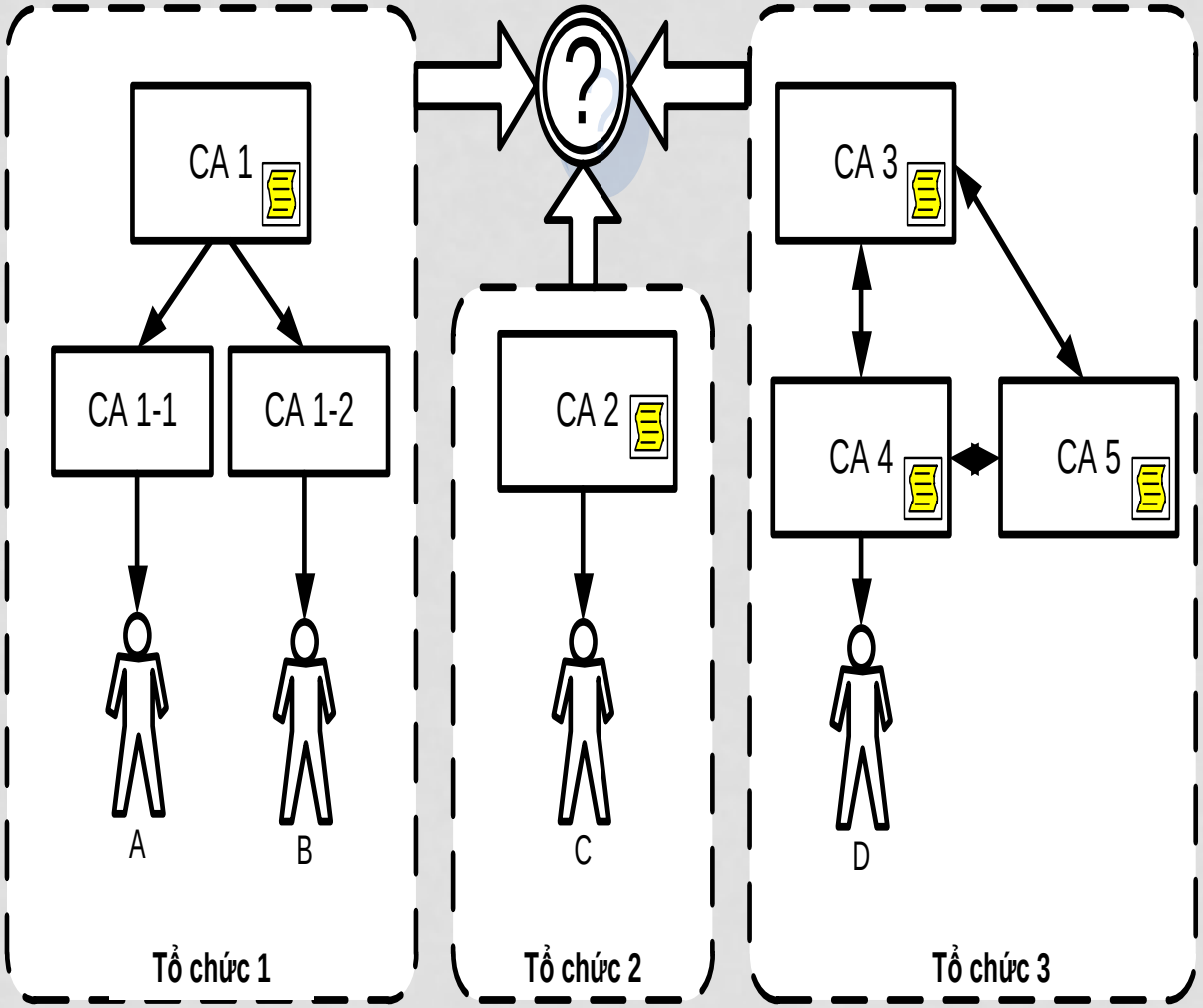
KIẾN TRÚC MẠNG LƯỚI

- Các CA có quan hệ ngang hàng với nhau, và cấp phát CTS cho nhau
- Các CA đều là các điểm tin cậy, có sự tin tưởng 2 chiều
- Có sự chứng thực chéo lẫn nhau
- Một CA đơn bị tổn thương sẽ không phá vỡ toàn bộ kiến trúc PKI
- Dễ dàng bổ sung các CA mới
- Mỗi CA kết nối với các CA khác tạo thành một đồ thị đầy đủ
- Đường dẫn chứng thực không đáng tin cậy



HỆ THỐNG LAI

- Mỗi tổ chức có nhu cầu xây dựng kiến trúc PKI khác nhau.
- Cần phải cung cấp một giải pháp tối ưu cho phép các tổ chức có thể tương tác với nhau trong một môi trường tin cậy
- Kiến trúc lai cho phép quá trình tương tác giữa các tổ chức thành công.

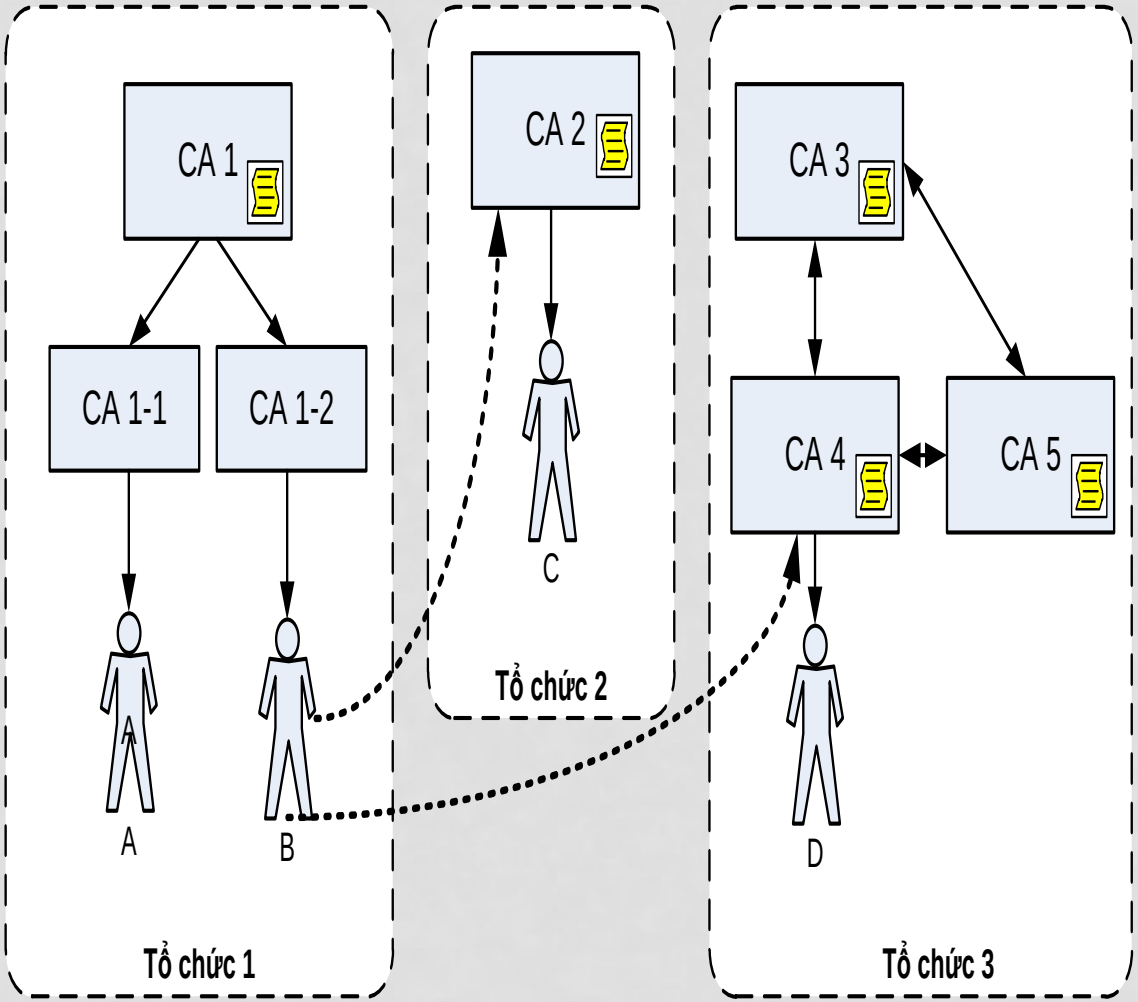


HỆ THỐNG LAI

- Một kiến trúc PKI lai sẽ liên quan đến kiến trúc đơn, kiến trúc phân cấp và kiến trúc mạng lưới.
- Các loại kiến trúc PKI lai
  - Kiến trúc danh sách tin cậy mở rộng
  - Kiến trúc PKI chứng thực chéo
  - Kiến trúc CA cầu nối

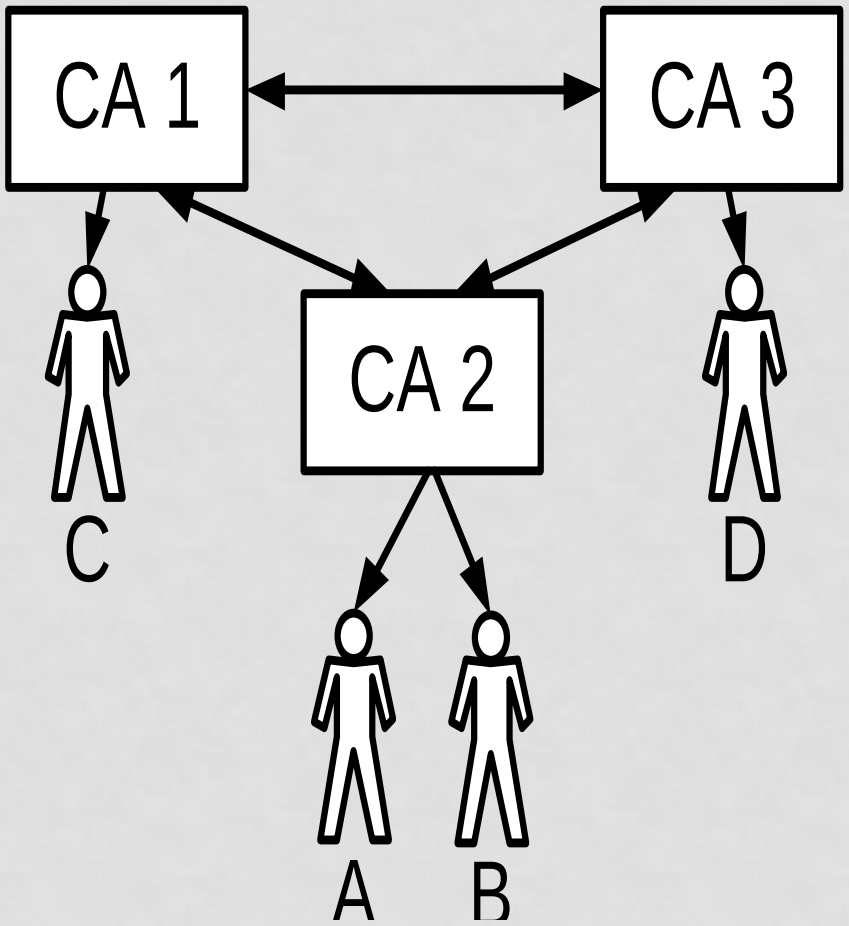
KIẾN TRÚC DANH SÁCH TIN CẬY MỞ RỘNG

- Là mạng mở rộng của kiến trúc danh sách tin cậy để hỗ trợ đường dẫn chứng thực dài hơn một CTS
- Thực thể cuối duy trì một danh sách các điểm tin cậy
- Mỗi điểm tin cậy có thể là CA đơn, PKI phân cấp, hoặc PKI mạng lưới

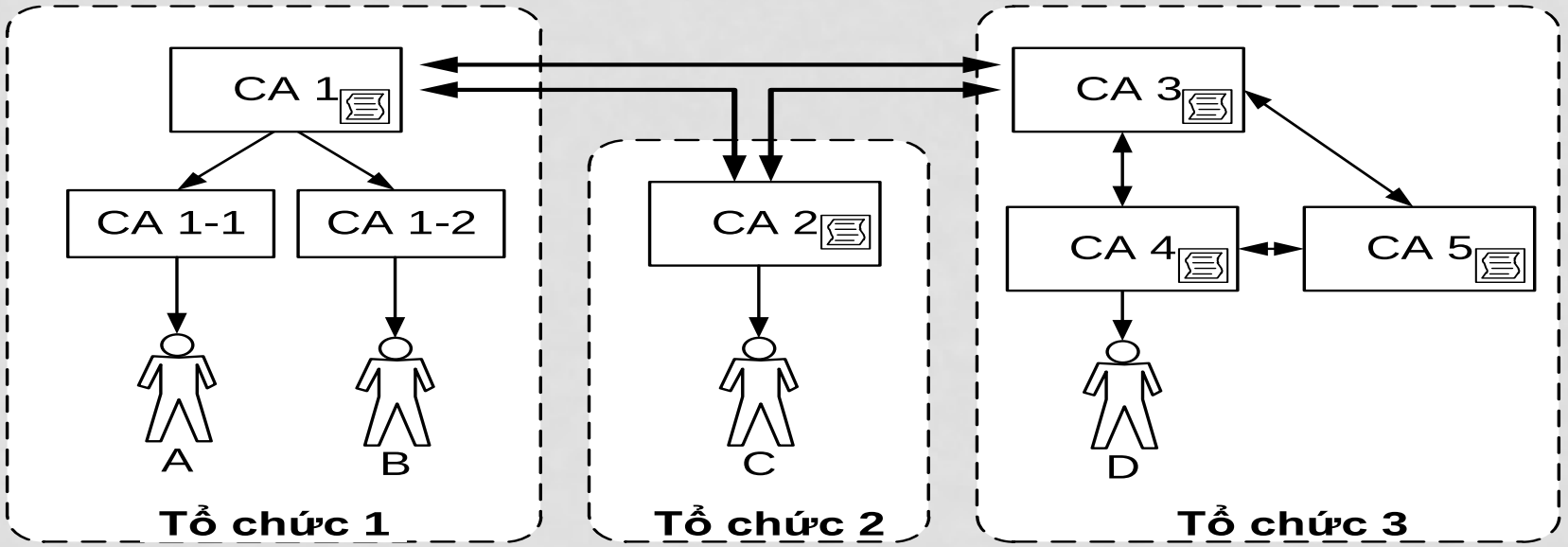


KIẾN TRÚC CHỨNG THỰC CHÉO

- Có mối quan hệ ngang hàng giữa các CA
- Các thực thể ở PKI này có thể xác thực các thực thể ở PKI khác.
- Ví dụ với 3 quan hệ ngang hàng, và 6 CTS
- => chứng thực chéo yêu cầu $\frac{(n \times n - n)}{2}$ quan hệ ngang hàng và $(n \times n - n)$ CTS, với n là số CA trong hệ thống



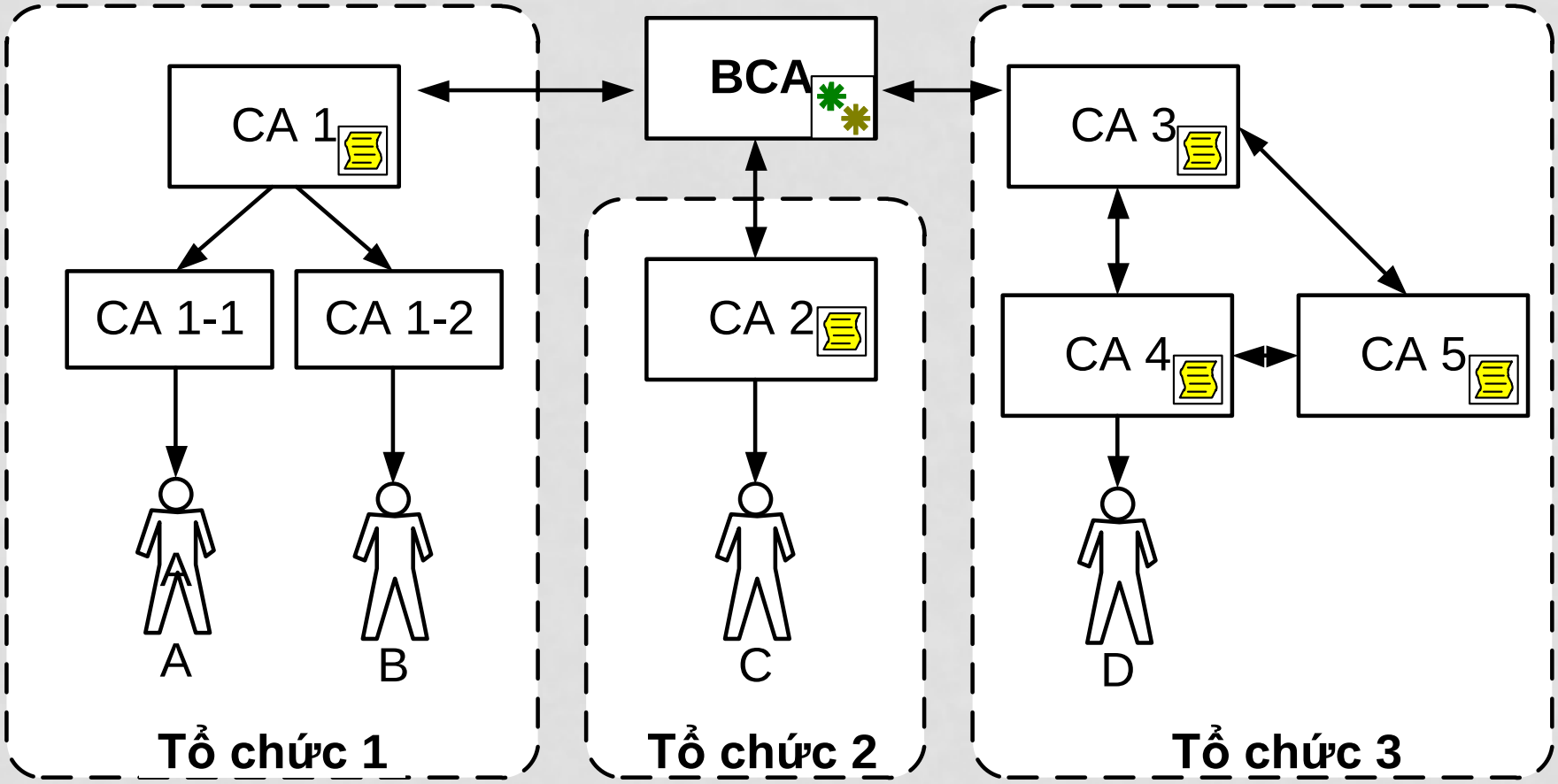
- Mô hình đường dẫn chứng thực của chứng thực chéo
  - Đường dẫn chứng thực sau được dựng lên bởi A cho B:
    - [CA–1 → CA–12] : [CA–12 → B]
  - Đường dẫn chứng thực sau được dựng lên bởi A cho C:
    - [CA–1 → CA–2] : [CA–2 → C]
  - Các đường dẫn chứng thực sau được dựng lên bởi A cho D:
    - [CA–1 → CA–3] : [CA–3 → CA–4] : [CA–4 → D]
    - [CA–1 → CA–3] : [CA–3 → CA–5] : [CA–5 → CA–4] : [CA–4 → D]



KIẾN TRÚC CẦU NỐI

- Là kiến trúc phù hợp nhất để kết nối các PKI có kiến trúc khác nhau.
- Không cấp phát CTS trực tiếp cho người dùng
- CA thiết lập mối quan hệ với CA cấu nối coi là CA chính
- Mối quan hệ giữa các CA chính và CA cầu nối là ngang hàng
- Nếu CA chính bị tổn thương thì CA cầu nối sẽ thu hồi CTS của CA này và ngược lại

KIẾN TRÚC CẦU NỐI



KIẾN TRÚC CẦU NỐI

- Đường dẫn chứng thực sau được dựng lên bởi A cho B:
  - [CA–1 → CA–12] : [CA–12 → B]
- Đường dẫn chứng thực sau được dựng lên bởi A cho C:
  - [CA–1 → BCA] : [BCA → CA–2] : [CA–2 → C]
- Các đường dẫn chứng thực sau được dựng lên bởi A cho D:
  - [CA–1 → BCA] : [BCA → CA–3] : [CA–3 → CA–4] : [CA–4 → D]
  - [CA–1 → BCA] : [BCA → CA–3] : [CA–3 → CA–5] : [CA–5 → CA–4] : [CA–4 → D]

THE END