QUY TRÌNH HOẠT ĐỘNG CỦA HỆ THỐNG PKI

CHỨNG THỰC ĐIỆN TỬ

NỘI DUNG

- Chức năng thành phần CA
- Chức năng thành phần RA
- Chức năng người dùng/ thực thể đầu cuối
- Chức năng của các hệ thống dịch vụ chứng thực chữ ký số
- Quy trình quản lý vòng đời chứng thư số

CHỨC NĂNG THÀNH PHẦN CA

- CA (Certification Authority) là cơ quan có thẩm quyền và được tất cả người dùng khác tin cậy
- Được tin tưởng trong việc cấp phát CTS và công nhận các nội dung thông tin lưu giữ trong CTS.
- Là trái tim của hệ thống PKI,
- Là tổ chức quản lý của PKI

- Nhiệm vụ của CA là gì?

CHỨC NĂNG THÀNH PHẦN CA

- Nhiệm vụ chính:
  - Gắn một cặp khóa công khai với một định danh đã cho
  - Chứng nhận việc gắn kết này bằng cách ký số một cấu chức dữ liệu chứa biểu diễn của định danh (gọi là CTS – Chứng thư số)
  - Cấp phát, công nhận CTS
  - Phát hành các danh sách CTS bị hủy (CRL)
- Chức năng của CA
  - Cấp mới, gia hạn, thu hồi chứng thư số.
  - Phát hành CRL.
  - Quản lý vòng đời của chứng thư số sau khi phát hành

CHỨC NĂNG THÀNH PHẦN RA

- Khi số lượng thực thể cuối trong miền PKI mở rộng và phân tán thì việc đăng ký tại một CA sẽ khó giải quyết
- Cần thêm một thực thể độc lập thực hiện việc đăng ký CTS.
- => thực thể đó là Ủy quyền đăng ký (Registration Authority – RA)
- Mục đích:
  - Giảm thiểu công việc cho CA trong quá trình đăng ký

CHỨC NĂNG THÀNH PHẦN RA

- Chức năng:
  - Xác thực và kiểm tra tính hợp lệ của thông tin cá nhân chủ thể đăng ký CTS.
  - Xác nhận quyền của chủ thể đối với những thuộc tính chứng thư được yêu cầu.
  - Kiểm tra xem chủ thể có thực sự sở hữu khoá riêng đang được đăng ký không.
  - Tạo cặp khoá bí mật /công khai.
  - Phân phối bí mật được chia sẻ đến thực thể cuối.
  - Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.
  - Lưu trữ khoá riêng.
  - Khởi sinh qúa trình khôi phục khoá.
  - Phân phối thẻ bài vật lý (ví dụ như thẻ thông minh) chứa khoá riêng.

CHỨC NĂNG THÀNH PHẦN RA

- RA không có trách nhiệm sinh và ký CTS và danh sách hủy bỏ
- Lợi ích của RA:
  - Giảm chi phí, đặc biệt là đối với các tổ chức phân tán trên diện rộng, có thể phân tán các RA để quản lý giúp CA.
  - Việc giảm nhẹ công việc cho CA giúp CA có thể nghỉ ngơi nhiều hơn. Do đó sẽ giảm thiểu được các cơ hội tấn công nhằm vào CA đó.

CHỨC NĂNG NGƯỜI DÙNG/THỰC THỂ ĐẦU CUỐI

- Người dùng/thực thể đầu cuối (EE) là đối tượng của hệ thống PKI, là khách hàng của dịch vụ PKI
- Các EE bị ràng buộc bởi các CTS
- Để có CTS, cần thực hiện các bước sau:
  - Gửi một yêu cầu sinh cặp khóa bí mật – công khai
  - Sau khi cặp khóa được sinh ra, một yêu cầu được gửi tới CA để sinh chứng thư. Yêu cầu này có thể thông qua RA.
  - Sau khi client nhận chứng thư từ CA, họ có thể sử dụng chứng thư để định danh cho chính bản thân hoặc dùng để xác thực người nắm giữ chứng thư.
- Giao dịch giữa EE và CA phải được giữ an toàn
- EE phải đảm bảo an toàn cho khóa riêng của họ

CHỨC NĂNG CỦA CÁC HỆ THỐNG DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ

- Thành phần VA (Validation Authority) đóng vai trò là kho công cộng chứa CTS và các CRL
  - CTS được CA cấp phát cho người dùng, đồng thời được lưu trữ vào kho chứng thư (Certificate Repository).
  - Kho chứng thư được CA công bố và được truy cập bằng nhiều giao thức khác nhau (http, ftp...)
- Kho lưu trữ CTS thường là một thư mục, hay một cách nào đó để lưu các thông tin liên quan của PKI
- Lợi ích cơ bản của kho lưu trữ giúp các EE có thể tìm các CTS và các CRL.

CHỨC NĂNG CỦA CÁC HỆ THỐNG DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ

- Các dịch vụ chứng thực:
  - CRL:
    - Danh sách CTS bị thu hồi
    - Một CRL được tạo và phát hành định kỳ sau một khoảng thời gian nào đó do người quản trị CA chỉ định
  - OCSP:
    - Là một giao thức được dùng để kiểm tra trạng thái của CTS có chuẩn X.509
  - TimeStamp:
    - Là đối tượng dữ liệu gắn kết một dữ kiện với một mốc thời gian xác định.
    - Dịch vụ cấp dấu thời gian sẽ cấp timestamp cho EE thông qua một bên thứ 3 tin cậy gọi là Thẩm quyền cấp dấu thời gian (TSA)

QUY TRÌNH QUẢN LÝ VÒNG ĐỜI CHỨNG THƯ SỐ

- Chứng thư số là một phần của hệ thống PKI
- CTS sẽ có hiệu lực trong một khoảng thời gian, gọi là thời gian sống của CTS
- Thời gian sống được xác định bởi chính sách của CA
- CTS có thể bị vô hiệu hóa trước khi hết hạn
- Làm thế nào để chắc chắn rằng CTS còn hợp lệ?

QUY TRÌNH QUẢN LÝ VÒNG ĐỜI CHỨNG THƯ SỐ

- Danh sách thu hồi CTS (CRL - Certificate Revocation List) giúp giải quyết việc khẳng định CTS là hợp lệ
  - CRL là một danh sách bao gồm tất cả CTS bị thu hồi cùng với lý do thu hồi CTS đó.
- Một CTS sẽ có trải qua một quá trình gồm
  - Đăng ký chứng thư số
  - Quản lý, duy trì khóa và chứng thư số
  - Công bố chứng thư số
  - Hủy bỏ.
- Quá trình này gọi là vòng đời của chứng thư số

ĐĂNG KÝ CHỨNG THƯ SỐ

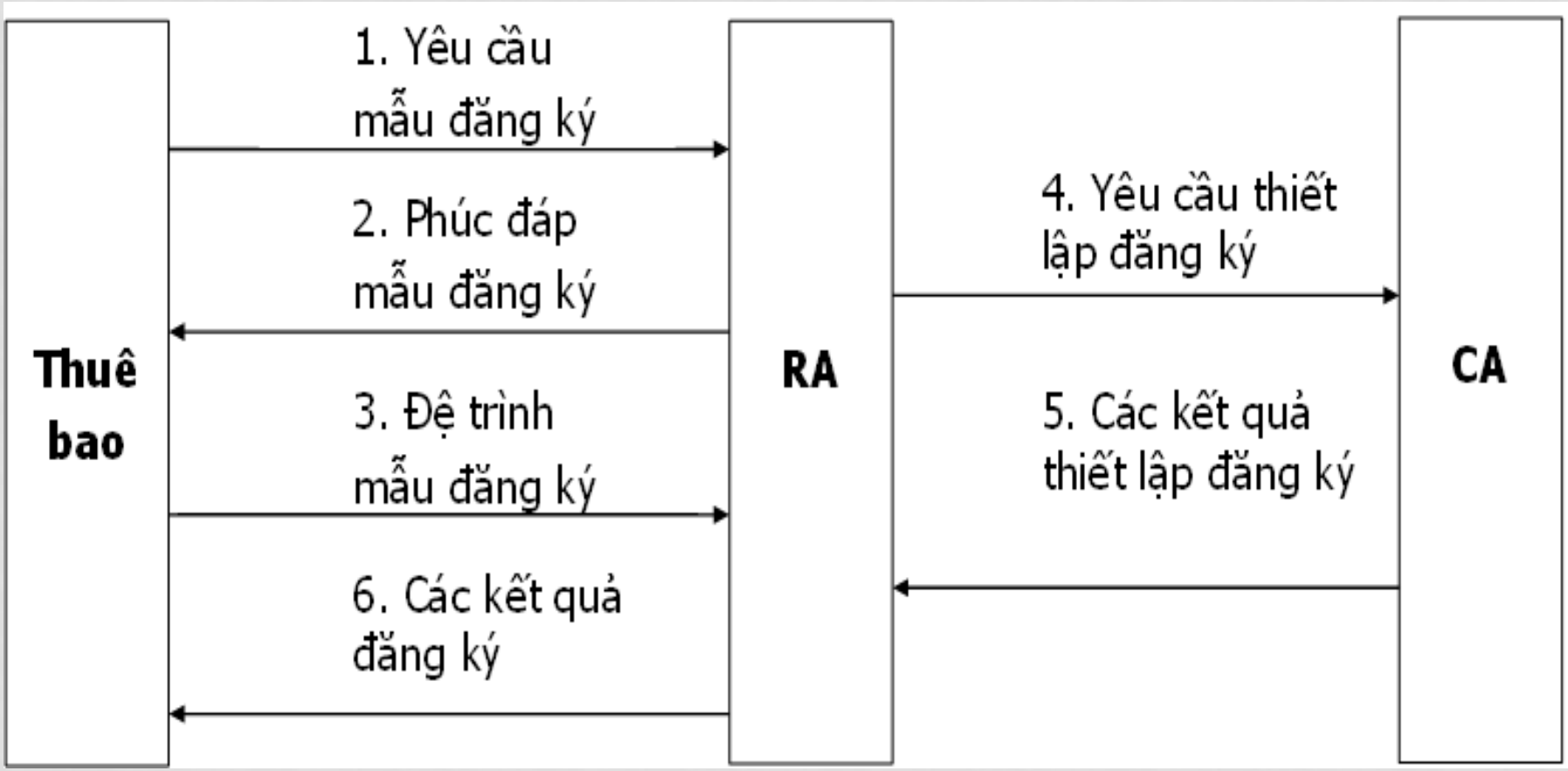
- Đăng ký chứng thư số
  - Là một quá trình người dùng gửi yêu cầu xin cấp một CTS tới CA
- Được thực hiện bởi RA, RA hỗ trợ nhiệm vụ đăng ký cho CA
- Việc đăng ký CTS gồm 3 lý do:
  - Để trở thành một PKI client và cơ quan đăng ký RA hoặc cơ quan chứng thực CA
  - Để việc cấp phát chứng thư số duy nhất và thuận lợi, giúp đảm bảo việc thu hồi chứng thư số nhanh chóng.
  - Sử dụng chuẩn chứng thư số X509

ĐĂNG KÝ CHỨNG THƯ SỐ

- RA liên quan đến 3 thành phần
  - Trình điều khiển đăng ký: là một máy chủ tiếp nhận yêu cầu đăng ký từ người dùng, và máy chủ này kết nối với máy chủ CA.
  - Nhân viên đăng ký: là một cá nhân xử lý, xác minh và chấp nhận yêu cầu đăng ký. Khi CA cấp phát chứng thư số tương ứng, thì nhân viên này sẽ phân phối chứng thư số tới người dùng
  - Người quản lý RA: là một cá nhân quản lý các nhân viên RA và đảm bảo rằng các giao dịch công bằng, trước khi nhân viên RA chuyển yêu cầu chứng thư tới CA, tất cả các yêu được được xác minh phải được sự chấp thuận của quản lý RA.

ĐĂNG KÝ CHỨNG THƯ SỐ

- Các bước thực hiện quá trình đăng ký:



ĐĂNG KÝ CHỨNG THƯ SỐ

- Sinh khóa
  - Một cặp khóa có thể được sinh tại người dùng cuối, hoặc CA cuối.
  - Vị trí sinh khóa phụ thuộc vào
    - Tính sẵn sàng của tài nguyên sinh khóa
    - Mục đích sử dụng CTS
  - Để chống chối bỏ, khuyến khích người dùng sinh cặp khóa. Vì sao?
  - Ngoài ra, CA và người dùng phải thực hiện cả việc sao lưu khóa
    - Khi khóa được sinh ra thì phải thực hiện sao lưu khóa

QUẢN LÝ, DUY TRÌ KHÓA VÀ CTS

- Việc tạo CTS của CA không liên quan đến vị trí sinh khóa
- Nếu khóa được sinh ở người dùng thì khóa công khai sẽ gửi đến CA cùng với yêu cầu sinh CTS
- Nếu CA sinh khóa thì khóa bí mật phải phân phối an toàn đến người dùng
- Một số PKI triển khai cơ chế 2 cặp khóa
  - Một cặp khóa dùng để ký và kiểm tra chữ ký
  - Một cặp khóa dùng để mã và giải mã
  - Do vậy sẽ có 2 CTS được phân phối tới người dùng

QUẢN LÝ, DUY TRÌ KHÓA VÀ CTS

- Trong quản lý, duy trì khóa và CTS, có những công việc được thực hiện
  - Sao lưu khóa
  - Kiểm tra hết hạn và lưu trữ chứng thư số
  - Cập nhật chứng thư số
  - Tải và xác nhận tính hợp lệ của CTS

SAO LƯU KHÓA

- Việc sao lưu khóa thực hiện với cặp khóa dùng để mã hóa/giải mã.
- Khóa dùng để ký không cần thiết phải sao lưu
- CA thực hiện sao lưu khóa để nếu người dùng bị mất khóa bí mật thì dữ liệu được mã hóa bởi khóa công khai tương ứng vẫn có thể được giải mã.
- Việc sao lưu có thể được thực hiện bởi người dùng và CA

HẾT HẠN VÀ LƯU TRỮ CHỨNG THƯ SỐ

- CTS có hiệu lực trong một khoảng thời gian giới hạn
- Khi kết thúc giai đoạn này, CTS sẽ bị hết hạn
- Đôi khi CTS sẽ bị mất hiệu lực trước ngày hết hạn
- CA sẽ thu hồi các CTS hết hạn và không còn hiệu lực, và lưu thông tin vào CRL.
- CA cần phải duy trì đầy đủ thông tin lưu trữ để xác thực định danh chủ thể trong CTS và xác nhận tính hợp lệ của CTS tại thời điểm tài liệu được ký
  - Việc này được thực hiện bằng dấu thời gian mật mã

HẾT HẠN VÀ LƯU TRỮ CHỨNG THƯ SỐ

- Kho lưu trữ
  - là nơi lưu trữ thông tin lâu dài an toàn.
  - khẳng định thông tin là chính xác tại thời điểm lưu trữ, và không bị sửa đổi trong suốt quá trình lưu trữ
  - Tuy đóng vai trò thứ yếu trong hoạt động thường xuyên của PKI nhưng lại có những yêu cầu kiểm soát kỹ thuật và thủ tục nghiêm ngặt

CẬP NHẬT CHỨNG THƯ SỐ

- Khi CTS số hết hạn, một cặp khóa lại được sinh ra và khóa công khai được gắn kết với CTS => **Cập nhật khóa**.
- Cập nhật khóa được thực hiện tự động khi khóa còn 70-80% thời gian sống
- Là quá trình chuyển tiếp hợp lý cho thực thể cuối có được chứng thư số mới trong thời gian thích hợp để vẫn tiến hành các hoạt động giao dịch.
- Trong suốt với người dùng

CẬP NHẬT CHỨNG THƯ SỐ

- Để cấp phát một CTS mới, CA cũng đồng thời cấp phát một cặp khóa tái sử dụng CTS.
  - CTS đầu tiên bao gồm một KCK cũ và được ký với một KBM mới.
    - CTS tái sử dụng này cho phép thuê bao có CTS được ký với KBM để thiết lập một đường dẫn chứng thực hợp lệ tới các CTS đã ký và KBM cũ trước đó
  - CTS thứ 2 gồm KCK mới được ký với KBM cũ.
    - CTS này cho phép thuê bao có CTS được ký với KBM cũ để thiết lập đường dẫn chứng thực với CTS được ký với KBM mới
- Các thuê bao có CTS được ký bởi KBM cũ và thuê bao có CTS được ký bởi KBM mới có thể xác thực được CTS của nhau

TẢI VÀ XÁC NHẬN TÍNH HỢP LỆ CỦA CTS

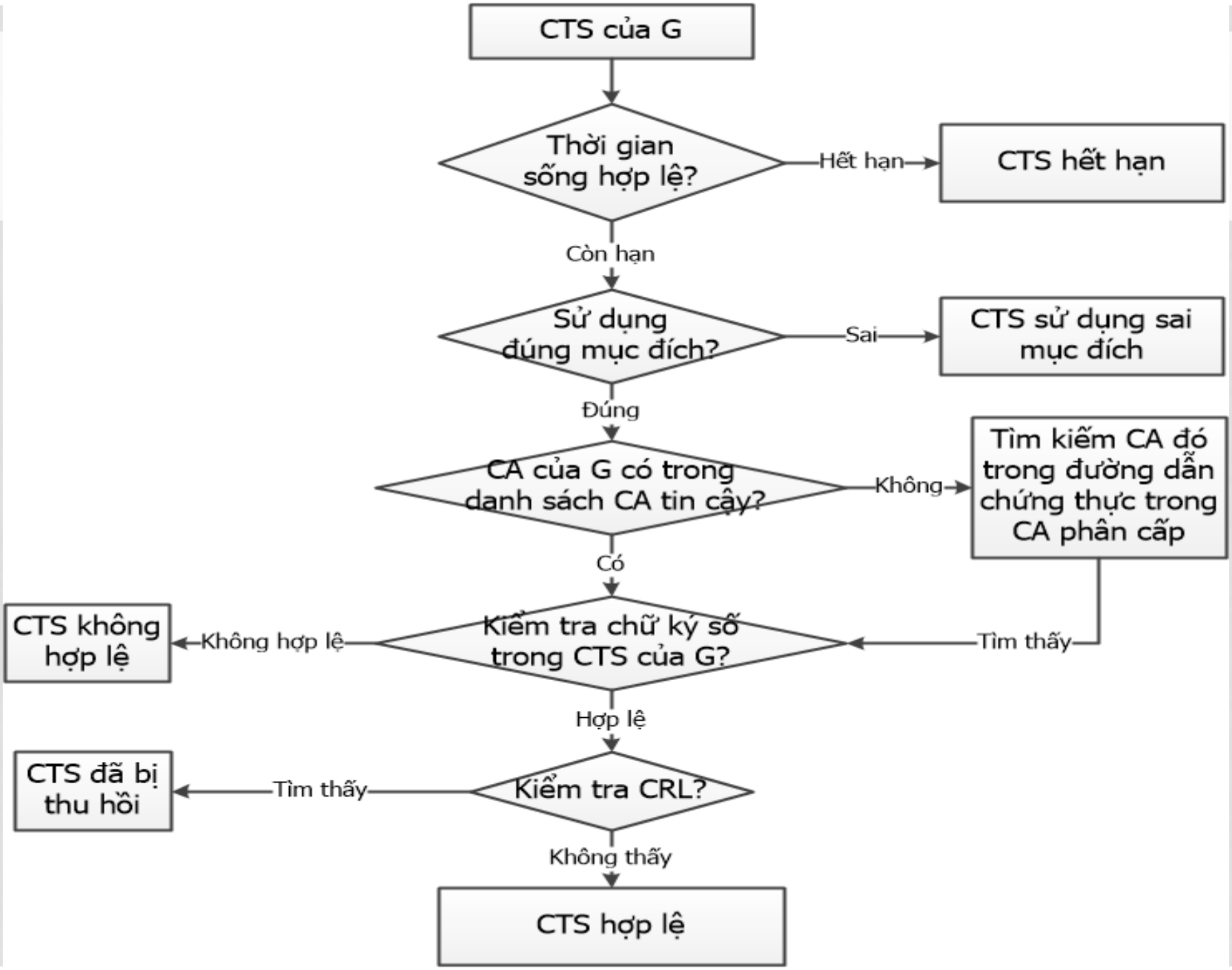
- Xác nhận độ tin cậy của CTS trước khi sử dụng là việc rất quan trọng
- Thiết lập danh tính của người dùng cho 2 nhiệm vụ
  - Tải chứng thư số
  - Xác nhận chứng thư số
    - Ví dụ, D là một người dùng của công ty Viettel., được CA cấp phát một chứng thư số.
    - C là thành viên của FPT., muốn liên lạc với D.
    - Để thực hiện được việc này, C phải đảm bảo rằng người mà anh ta giao dịch chính là D.
    - Do vậy để chứng minh danh tính của D, đầu tiên C phải có được chứng thư số của D, chứng thư số đó bao gồm thông tin liên quan đến định danh của D và được ký bởi một CA tin cậy.
    - Sau đó C sử dụng chứng thư số của CA đó để xác thực chữ ký số trên chứng thư số của D. Bằng cách đó, C xác thực được định danh của D.

TẢI CHỨNG THƯ SỐ

- Cần phải truy xuất vào CTS đã được cấp phát để xác định danh tính thực thể và cũng là CTS của CA cấp phát.
- Việc tải CTS phụ thuộc vào vị trí của CTS
- Có thể được phân phối bởi các phương tiện điện tử sử dụng giao thức S-MIME hoặc được công bố trong thư mục X.500
- Nếu được công bố trong X.500 thì người dùng có thể dùng LDAP để tải chứng thư số về
  - Các thông tin của CA có thể nằm trên một thư mục LDAP
  - CA có thể dùng thông tin trên thư mục LDAP này để cấp phát nhiều CTS cho các người dùng cùng một lúc với cùng một tiêu chí
- CTS cần phải được công bố dựa trên các triển khai PKI.

XÁC MINH TÍNH HỢP LỆ CỦA CTS

- Khi tải CTS cần phải kiểm tra tính hợp lệ của CTS đó
- Gồm các bước sau:
  - Kiểm tra được rằng chứng thư số còn hiệu lực
  - Xác minh được chứng thư số đó do một CA tin tưởng cấp phát
  - Đảm bảo rằng chứng thư số đó được sử dụng vào đúng mục đích
  - Kiểm tra, xác định được chứng thư số có bị thu hồi hay không


CTS của G
Thời gian sống hợp lệ?
Hết hạn
CTS hết hạn
Còn hạn
Sử dụng đúng mục đích?
Sai
CTS sử dụng sai mục đích
Đúng
CA của G có trong danh sách CA tin cậy?
Không
Tìm kiếm CA đó trong đường dẫn chứng thực trong CA phân cấp
Có
Kiểm tra chữ ký số trong CTS của G?
Không hợp lệ
CTS không hợp lệ
Tìm thấy
Hợp lệ
Kiểm tra CRL?
Tìm thấy
CTS đã bị thu hồi
Không thấy
CTS hợp lệ

THUẬT TOÁN RSA

- Chọn p và q, tính $n = p * q$
- $\phi(n) = (p-1)(q-1)$ là 1 số chẵn
- Chọn khóa e sao cho $\gcd(e, \phi(n)) = 1$
- Chọn khóa d sao cho $d = e^{-1} mod\ \phi(n)$
- (e, n) là khóa công khai
- d là khóa bí mật
- Mã hóa: $C = M^e mod\ n$
- Giải mã : $\mathrm{M} = C^d mod\ n$

VÍ DỤ

- Ví dụ:
- Cho p = 2357
- q = 2551
- Chọn e = 3674911
- Tìm d=?
- Thực hiện mã hóa và giải mã văn bản

m= 5234673

-

TẠO VÀ KIỂM TRA CHỮ KÝ SỐ

- Chữ ký số RSA
  - m là bản tin cần ký
  - Tạo chữ ký số

$$S = sig_D(m) = m^d mod\ n$$

  - Kiểm tra chữ ký số

$$Ver_E(m, S) \leftrightarrow đúng \text{ nếu } m = S^e mod\ n$$

TẠO VÀ KIỂM TRA CHỮ KÝ SỐ

- Ví dụ:
- Cho p = 31
- q = 23
- Và văn bản m cần ký là: 110110111
- Tạo chữ ký RSA trên văn bản m và kiểm tra chữ ký đó
- Ví dụ: e= 223

- ví dụ 2:
- cho p = 61,
- q= 53
- thông điệp m = 42
- thực hiện mã hóa và giải mã m
- thực hiện ký và kiểm tra chữ ký trên m
- chọn e = 17

- Ví dụ:
- Cho p = 239
- q = 251
- Và văn bản m cần ký là: 11000101
- thực hiện mã hóa và giải mã m
- Tạo chữ ký RSA trên văn bản m và kiểm tra chữ ký đó
- Ví dụ: e= 23

CÔNG BỐ CHỨNG THƯ SỐ

- Là phương pháp phân phối các CTS và thông tin thu hồi CTS phổ biến nhất
- Thông tin PKI được gửi đến những cộng đồng người dùng lớn, sẵn sàng và dễ dàng truy cập
- Thực tế là, việc công bố CTS và thông tin CRL sẽ được gửi vào một kho chứa
  - Điển hình là những máy chủ ở xa, truy cập đến qua giao thức LDAP
  - Đại lý hệ thống thư mục X.500
  - Bộ phúc đáp OCSP
  - Hệ thống tên miền
  - Các máy chủ web
  - Các cơ sở dữ liệu kết hợp
  - Các máy chủ dựa trên giao thức chuyển tệp tin FTP

CÁC PHƯƠNG PHÁP HỦY BỎ CTS

- Thu hồi CTS là quá trình loại bỏ tính hợp lệ của chứng thư số một cách sớm nhất
- Có nhiều lý do thu hồi, ví dụ:
  - Chủ sở hữu của chứng thư số đi ra khỏi tổ chức
  - Người chủ sở hữu thay đổi tên hoặc thông tin
  - Cơ quan cấp phát hoặc mối quan hệ giữa các cơ quan cấp phát và tổ chức không còn tồn tại.
  - Khóa bí mật bị nghi ngờ là bị tổn thương
- Phương thức thu hồi dựa trên chi phí, cơ sở hạ tầng và số lượng giao dịch được thực hiện

CÁC PHƯƠNG PHÁP HỦY BỎ CTS

- Các phương pháp thu hồi CTS:
  - Cơ chế công bố định kỳ
  - Cơ chế truy vấn trực tiếp

CÁC PHƯƠNG PHÁP HỦY BỎ CTS

- Cơ chế công bố định kỳ:
  - Sử dụng danh sách CRL và cây thu hồi CTS
  - CRL: danh sách gồm các CTS bị thu hồi trước khi bị hết hạn, được CA cấp phát, duy trì và cập nhật thường xuyên
  - CRT: dựa trên cấu trúc hàm băm Merkle, thể hiện toàn bộ thông tin thu hồi CTS liên quan

CÁC PHƯƠNG PHÁP HỦY BỎ CTS

- Cơ chế truy vấn trực tiếp:
  - Giao thức trạng thái CTS trực tuyến - OCSP: dùng để lấy các thông tin thu hồi CTS trực tuyến
  - Giao thức phê duyệt giao dịch trực tuyến: dùng cho việc phê duyệt trực tuyến như giao dịch qua thẻ tín dụng.

DANH SÁCH HỦY BỎ CRL

- Các thông tin thu hồi sẽ được công bố trong CRL
- CRL được CA ký để đảm bảo tính xác thực
- Người dùng tìm kiếm trên CRL để kiểm tra liệu CTS đó có bị thu hồi hay không

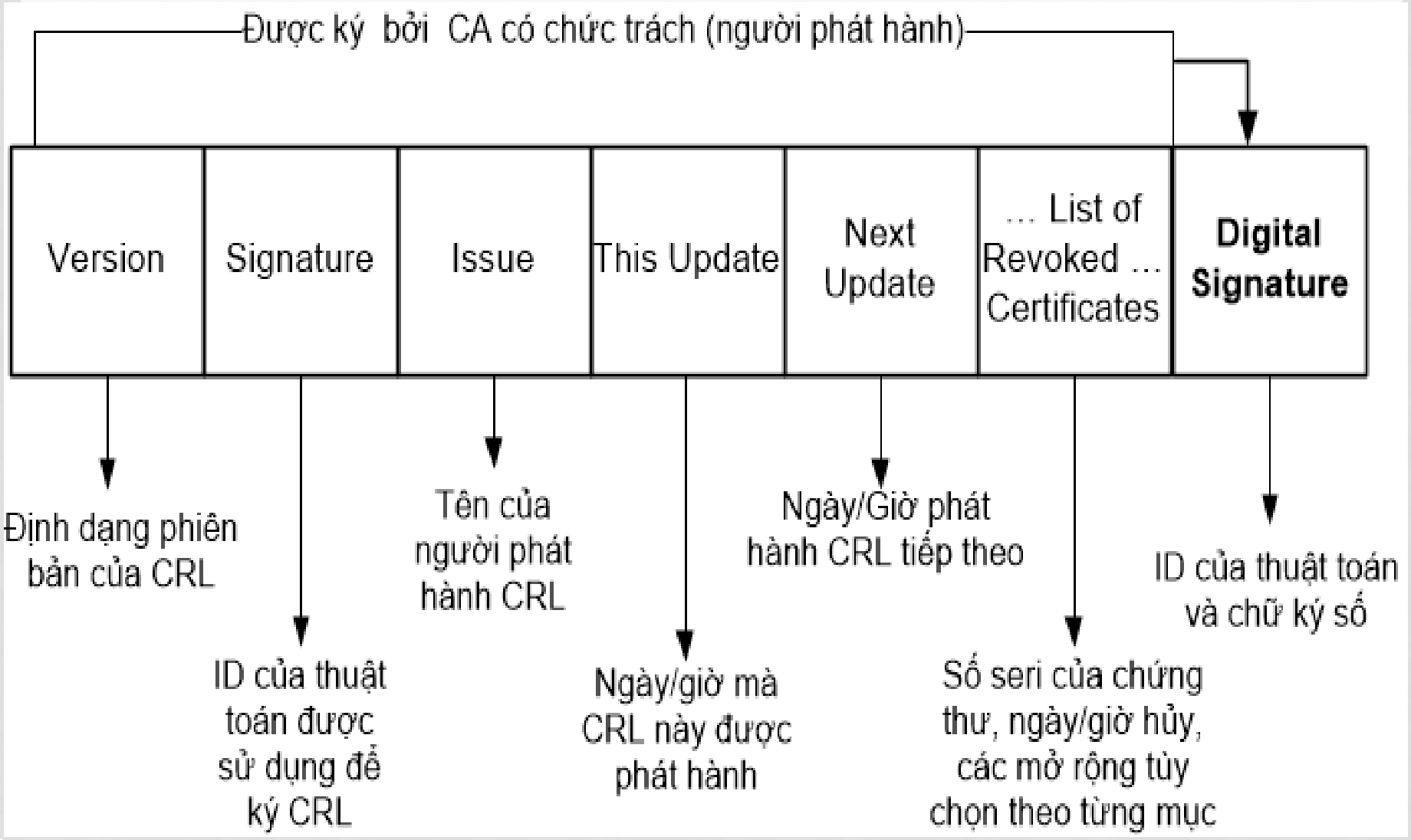
DANH SÁCH HỦY BỎ CRL

- Nếu bản CRL mới nhất không thể sử dụng để kiểm tra tính hợp lệ thì người dùng có thể sử dụng các bộ đệm CRL.
  - Các bộ đệm CRL được lưu trữ trong máy tính của user
  - Tăng tốc độ xác minh
  - Chỉ lưu những thông tin cũ nên phải thường xuyên cập nhật
- CRL bao gồm thông tin thu hồi CTS của CA được gọi là danh sách thu hồi thẩm quyền (Authority Revocation List – ARL)

DANH SÁCH HỦY BỎ CRL

- CRL tồn tại với đặc điểm kỹ thuật của CTS X.509, đặc tả X.509 sẽ quyết định các phiên bản của CRL
- Các phiên bản CRL đã phát triển
  - CRL v1: một chuẩn xác định cấu trúc dữ liệu cơ bản của một CRL
  - CRL v2: bổ sung thêm các trường mở rộng vào CRL v1 để tăng tính linh hoạt cho CRL

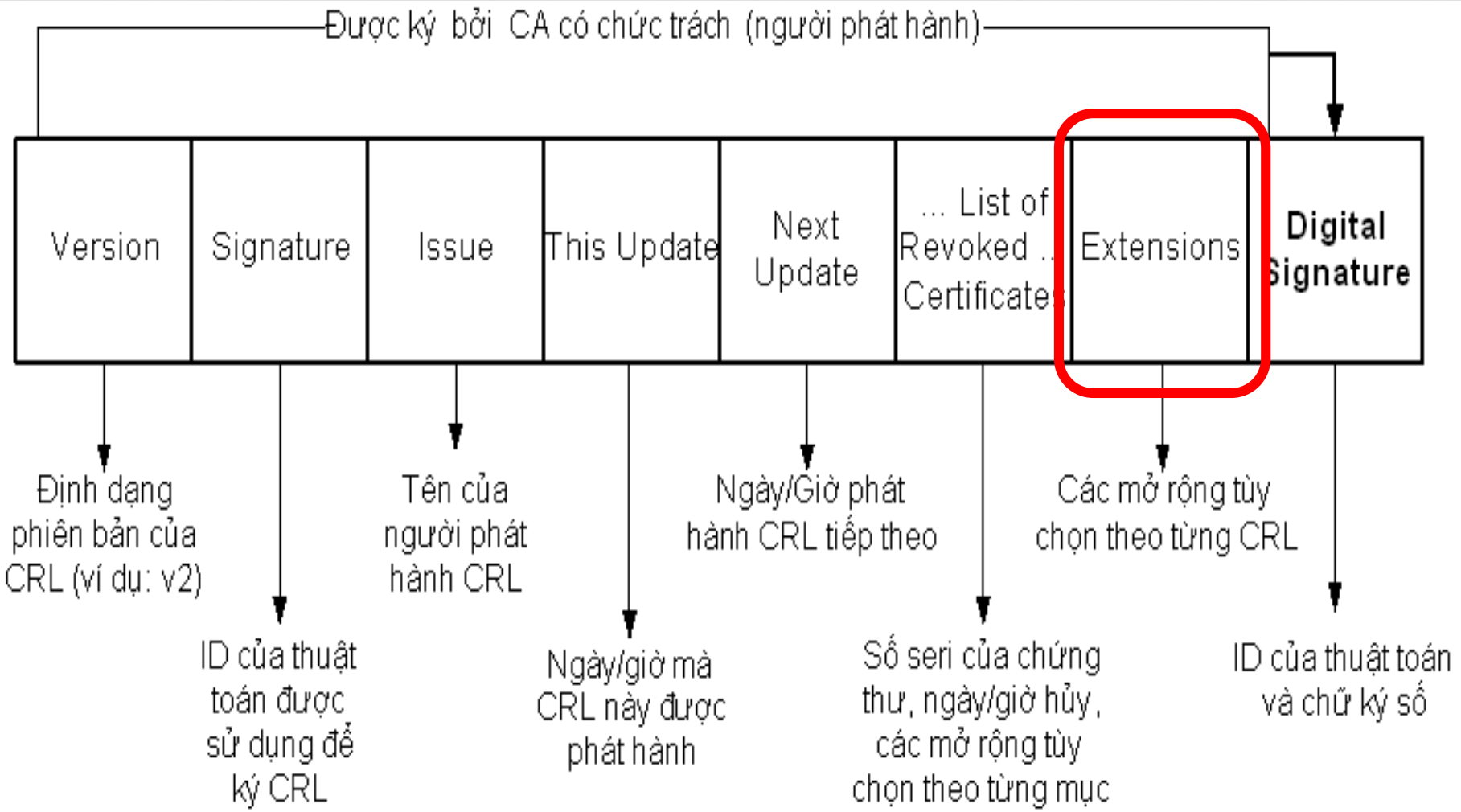
CRL V1


Được ký bởi CA có chức trách (người phát hành)
Version
Signature
Issue
This Update
Next Update
… List of Revoked … Certificates
Digital Signature
Định dạng phiên bản của CRL
ID của thuật toán được sử dụng để ký CRL
Tên của người phát hành CRL
Ngày/giờ mà CRL này được phát hành
Ngày/Giờ phát hành CRL tiếp theo
Số seri của chứng thư, ngày/giờ hủy, các mở rộng tùy chọn theo từng mục
ID của thuật toán và chữ ký số

CRL V1

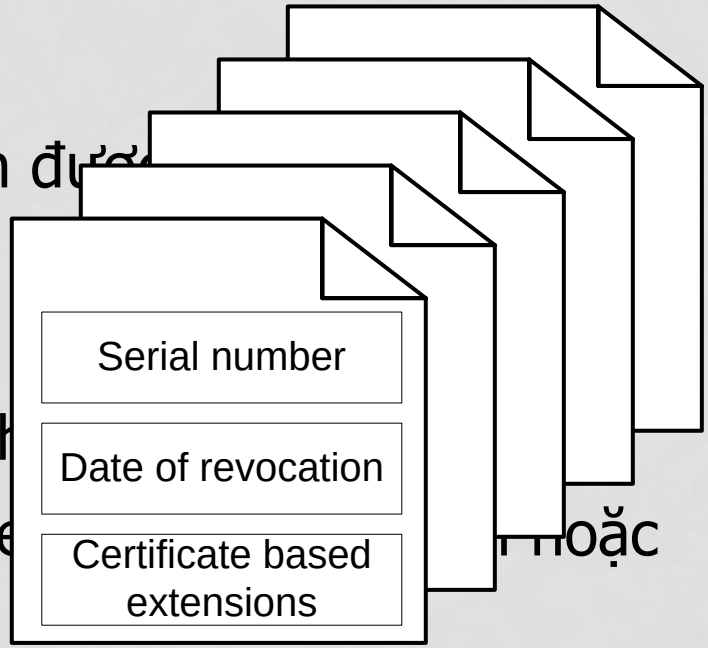
- CRL v1 trải qua một số thay đổi do:
  - Độ an toàn: thông tin trong CRL v1 được thay thế không cần sự am hiểu của CA hoặc người dùng. Do đó, các thông tin không chính xác về CRL có thể được truyền tới người dùng
  - Kích thước: CRL v1 không có cơ chế để kiểm soát hay giới hạn kích thước của nó
  - Tính mềm dẻo: CRL v1 không cho phép các trường mở rộng liên kết với CRL thêm bất kỳ một thông tin bổ sung nào
- Các vấn đề trên được giải quyết trong CRL v2

CRL V2


Được ký bởi CA có chức trách (người phát hành)
Version
Signature
Issue
This Update
Next Update
... List of Revoked .. Certificates
Extensions
Digital Signature
Định dạng phiên bản của CRL (ví dụ: v2)
ID của thuật toán được sử dụng để ký CRL
Tên của người phát hành CRL
Ngày/giờ mà CRL này được phát hành
Ngày/Giờ phát hành CRL tiếp theo
Số seri của chứng thư, ngày/giờ hủy, các mở rộng tùy chọn theo từng mục
Các mở rộng tùy chọn theo từng CRL
ID của thuật toán và chữ ký số

CRL V2

- Các trường trong CRL v2
  - Version
  - Chữ ký: gồm định danh thuật toán đ
    lên mỗi CRL
  - Người phát hành
  - This update: ngày mà CRL được ph
  - Next update: ngày mà CRL tiếp the
    CRL bị hết hạn



  - Danh sách CTS bị thu hồi: gồm các CTS bị thu hồi (số serial, ngày thu hồi, các trường mở rộng dựa trên CTS)
  - Các trường mở rộng: bổ sung một số thông tin như lý do thu hồi, ngảy hết hiệu lực liên quan đến CRL và CTS,…

TRƯỜNG MỞ RỘNG CRL

- Được định nghĩa trong X.509 và CRL v2
- Cung cấp cơ chế bổ sung các thuộc tính cho người dùng và khóa công khai
- Dựa vào chính sách của CA, trường mở rộng có 2 lựa chọn:
  - Cần thiết: trường được xử lý bởi một ứng dụng liên quan đến xác minh CRL
  - Không cần thiết: trường không qua quá trình xác minh đó
- Các trường mở rộng được chia làm 2 loại
  - Các trường mở rộng dựa trên chứng thư số
  - Các trường mở rộng dựa trên CRL

CÁC TRƯỜNG MỞ RỘNG DỰA VÀO CTS

- Hỗ trợ việc xác định CTS bị thu hồi nhanh chóng.
- Bao gồm các thông tin định danh của CTS:
  - Số serial
  - Tên CA
  - Tên thực thể

CÁC TRƯỜNG MỞ RỘNG DỰA VÀO CTS

- Và các thông tin khác:
  - Mã lý do: xác định nguyên nhân bị thu hồi,
  - Ngày không hợp lệ: thời gian CTS bị vô hiệu hóa
  - Cơ quan phát hành CTS: giúp xác định CA đã phát hành CTS bị thu hồi
  - Mã cấu trúc lưu trữ: chứa danh sách các CTS bị đình chỉ hoạt động
    - Các CTS treo này chưa bị thu hồi, nhưng không được sử dụng cho đến khi được kích hoạt lại.
    - Trường này gồm định danh đối tượng (OID), dựa vào OID, người dùng cân nhắc có nên sử dụng CTS treo hay không

TRƯỜNG MỞ RỘNG DỰA TRÊN CRL

- Giúp CRL mềm dẻo và linh hoạt hơn,
- Giúp CA kiểm soát được kích thước của CRL
- Cụ thể:
  - Định danh thẩm quyền khóa: xác định các khóa được sử dụng để ký lên CRL
    - Định danh khóa
    - Cơ quan thẩm quyền phát hành CTS
    - Số serial CTS của cơ quan thẩm quyền cấp phát CRL
  - Tên khác của cơ quan phát hành: thông tin bổ sung để xác định chính xác được CA
  - Điểm phân phối phát hành: xác định vụ trí của CRL và loại CTS chứa trong CRL
    - Nếu trong quá trình xác minh tính hợp lệ của CTS mà không thấy trường này thì CRL bị loại bỏ

TRƯỜNG MỞ RỘNG DỰA TRÊN CRL

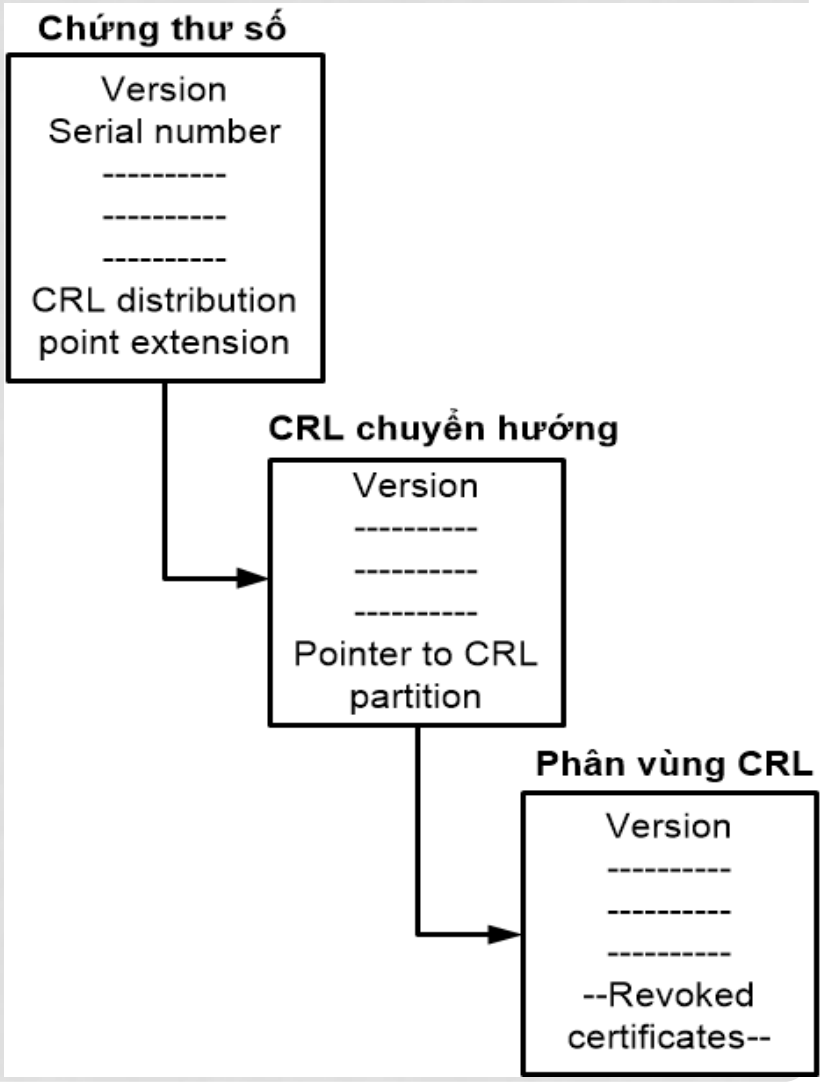
- Số CRL: số duy nhất xác định CRL, thể hiện chuỗi CRL được cấp phát bởi cơ quan thẩm quyền phát hành
- Báo hiệu Delta CRL: chưa số CRL cơ sở cho việc cập nhật được phân bổ. – trường thiết yếu
  - Các CRL được phân phối thành từng phần để có thể kiểm soát được kích thước của CRL hoặc làm đơn giản quá trình phân phối.
  - Đầu tiên, một CRL đầy đủ sẽ được phân phối – CRL cơ sở.
  - Lần tiếp theo, chỉ có bản cập nhật được phân phối. Bản cập nhật hoặc các phần CRL gọi là Delta CRL
- CRL gián tiếp
  - Khi một nhóm CA giao cho một cơ quan thẩm quyền làm nhiệm vụ cấp phát CRL tương ứng, cơ quan nảy sẽ có các thông tin thu hồi từ nhiều CA và chia sẻ cho các CA khác – cơ quan thẩm quyền CRL gián tiếp
  - CRL gián tiếp giúp hợp nhất các CRL

PHÂN PHỐI CRL

- Quá trình phân phối CRL là quá trình quan trọng trong việc quản lý CRL
- CA cần xác định nhiều điểm phân phối CRL để đơn giản hóa việc phân phối CRL và giúp truy cập CRL dễ dàng hơn.
- Ví dụ:
  - Một điểm phân phối có thể cho CRL của người dùng, một điểm cho CRL của CA => giảm kích thước CRL, giảm nghẽn mạng, giảm thời gian xử lý yêu cầu.
- Hạn chế:
  - Nếu kích thước của CRL tăng thì các điểm phân phối có thể thay đổi, ảnh hưởng đến tính linh hoạt.
  - Do vậy khi quyết định các điểm phân phối, tính linh hoạt được yêu cầu và cung cấp bởi các CRL chuyển hướng

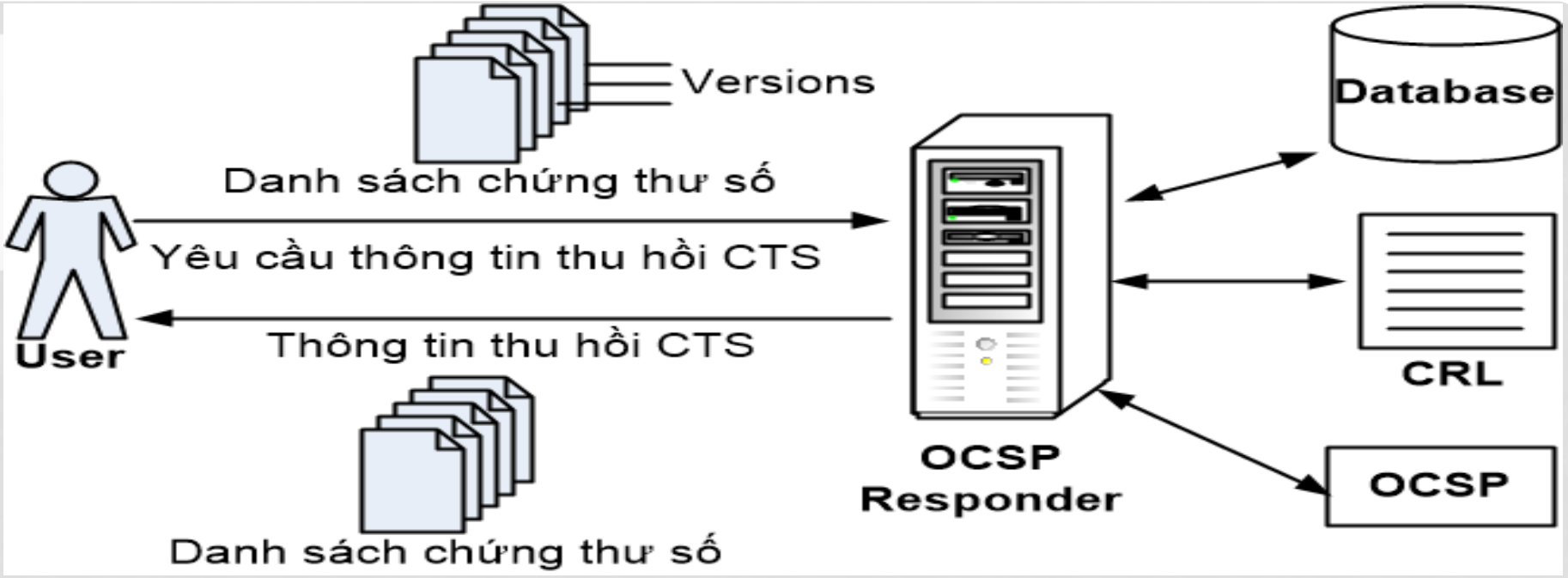
CRL CHUYỂN HƯỚNG

- Là các CRL trỏ đến nhiều điểm phân phối CRL khi CRL được xác định vị trí
- Thông tin CRL có thể bị thay đổi mà không ảnh hưởng đến trạng thái của CTS
- Cách tiếp cận này tương đối linh hoạt so với việc cố định các điểm phân phối mà không thể thay đổi được vị trí của CRL
- CRL hiệu quả ngay khi CTS được xác thực ở chế độ offline hoặc sử dụng bộ đệm CRL



GIAO THỨC TRẠNG THÁI CTS TRỰC TUYẾN ONLINE CERTIFICATE STATUS PROTOCOL - OCSP

- CRL chuyển hướng có nhiều ưu điểm nhưng nảy sinh một số các rủi ro khi CRL được cập nhật
- Một phương pháp khác được xác định để kiểm tra tình trạng CTS trực tuyến – OCSP
- Máy phản hồi OCSP dùng để xử lý các thông tin liên quan đến yêu cầu xác minh OCSP.
  - Nhận yêu cầu về thông tin hủy bỏ
  - Trả lời các yêu cầu với thông tin tình trạng CTS trực tuyến
- Quá trình thu thập thông tin thu hồi trực tuyến như sau:



- 1. User gửi yêu cầu OCSP tới máy chủ OCSP
- 2. Máy chủ OCSP xử lý yêu cầu và trả lời các thông tin trạng thái của CTS – với 3 trạng thái:
  - Tốt, Bị thu hồi và Không xác định
- 3. Dựa vào thông tin trạng thái, user có thể thực hiện các hành động thích hợp
- Máy phản hồi OCSP ký số lên các phản hồi trước khi gửi tới User

OCSP

- Tuy vậy, OCSP không cung cấp một phương thức xác thực rõ ràng, và có một số hạn chế:
  - Dù là một giao thức trực tuyến, nhưng không đảm bảo chắc chắn rằng việc thu hồi CTS không bị chậm trễ khi sử dụng OCSP
  - OCSP không xác định cách thức thông tin được gọi ra từ kho lưu trữ CRL tới máy phản hồi CRL cuối
  - Phản hồi của máy phản hồi được ký, vì thế có thể làm giảm hiệu suất hoạt động.
- OCSP vẫn cho phép xác minh tính hợp lệ của CTS một cách hiệu quả với chi phí hợp lý
- Nâng cao tính bảo mật cho giao dịch thương mại

CÁC CƠ CHẾ THU HỒI CTS KHÁC

- Ngoài CRL và OCSP còn có một số cơ chế khác
  - OCSP-X: OCSP mở rộng, có thể quyết định CTS đó có thể tin cậy hay không
  - Máy chủ CTS dữ liệu (Data Certification Server): xác minh tính chính xác của dữ liệu được gửi đến. Phương pháp được dùng để xác minh chữ ký số và trạng thái thu hồi của chứng thư số
  - Thư mục trạng thái thu hồi CTS (Certificate Revocation Status Directory): kho lưu trữ các CTS xác thực và được cấp phát mà không bị hết hạn

THE END!