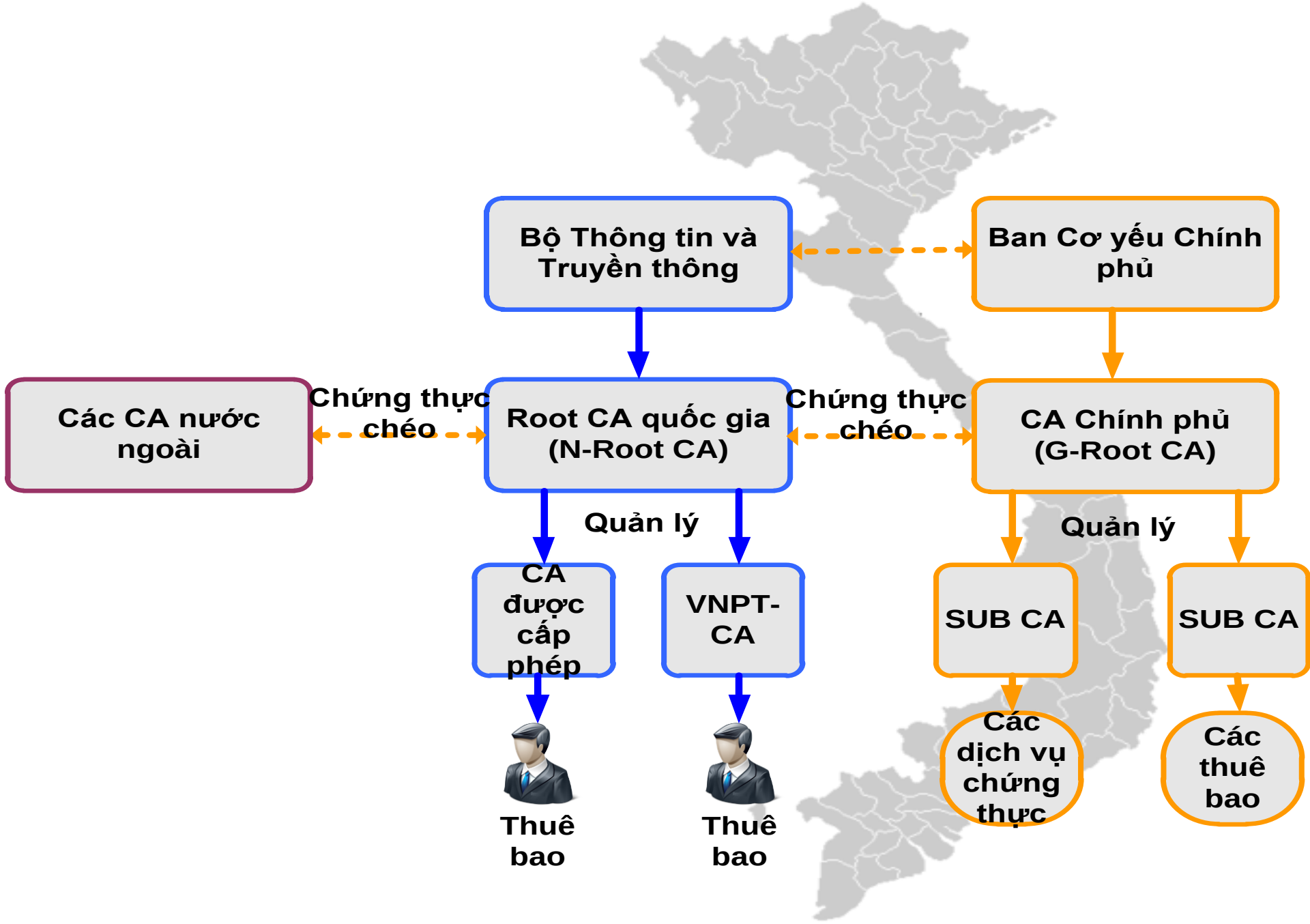
MỘT SỐ GIAO THỨC QUẢN LÝ PKI VÀ CÁC CHUẨN LIÊN QUAN

CHỨNG THỰC ĐIỆN TỬ


Bộ Thông tin và Truyền thông
Ban Cơ yếu Chính phủ
Các CA nước ngoài
Chứng thực chéo
Root CA quốc gia (N-Root CA)
Chứng thực chéo
CA Chính phủ (G-Root CA)
Quản lý
Quản lý
CA được cấp phép
VNPT-CA
SUB CA
SUB CA
Các dịch vụ chứng thực
Các thuê bao
Thuê bao
Thuê bao

NỘI DUNG

- 1. Các giao thức quản lý PKI
- 2. Nhóm chuẩn về khuôn dạng CTS và CRL
- 3. Nhóm chuẩn về giao thức hoạt động
- 4. Nhóm chuẩn về giao thức quản lý
- 5. Nhóm chuẩn về chính sách
- 6. Nhóm chuẩn về dấu thời gian và chứng thực dữ liệu

1. CÁC GIAO THỨC QUẢN LÝ PKI

- Các chuẩn PKCS
- Giao thức quản lý chứng thư số (CMP)
- Giao thức đăng ký chứng thư số đơn giản – SCEP

CÁC CHUẨN PKCS
PUBLIC KEY CRYPTOGRAPHY STANDARDS

- Vấn đề quan trọng là tích hợp các hàm nguyên thủy thực hiện các dịch vụ CTĐT. Đó là các hàm API mật mã và các hàm API liên quan đến CTS
- Xu hướng phát triển PKI là chuyên dụng hóa và chuẩn hóa các thành phần liên quan để nâng cao tính chuyên nghiệp an toàn và hiệu quả của hạ tầng PKI
- Các ứng dụng ràng buộc PKI cần phải được chuẩn hóa quốc tế

CÁC CHUẨN PKCS
PUBLIC KEY CRYPTOGRAPHY STANDARDS

- Bộ chuẩn quốc tế PKCS là một ví dụ được cung cấp bởi nhà cung cấp riêng biệt do RSA Laboratories phát triển và công bố với tên đầy đủ là Bộ chuẩn mật mã khóa công khai
- PKCS là bộ chuẩn quan trọng bậc nhất của hoạt động ứng dụng ràng buộc PKI.
- Gồm 15 chuẩn PKCS: từ PKCS#1 đến PKCS#15

CÁC CHUẨN PKCS
PUBLIC KEY CRYPTOGRAPHY STANDARDS

- Có 2 thành phần được chuẩn hóa trong bộ chuẩn này là:
  - Cú pháp thông báo – Message Syntax
  - Các thuật toán đặc trưng – Specific Algorithms
- Tập trung vào:
  - Chữ ký số: sử dụng thuật toán tóm lược thông báo trước rồi sử dụng thuật toán KCK lập mã tóm lược thông báo
  - Phong bì số: thông báo được lập mã bởi KBM và dùng KCK của người nhận để lập mã KBM.
  - Chứng thư số: yêu cầu CTS và dùng thuật toán chữ ký số để ký số
  - Thỏa thuận khóa: thuật toán thỏa thuận khóa 2 pha.

PKCS#1 – CHUẨN LẬP MÃ RSA

- Định nghĩa các cơ chế để lập mã và ký số các dữ liệu sử dụng hệ mật khóa công khai RSA
- PKCS#1-v2.1 cung cấp các chuẩn để cài đặt các lược đồ lập mã mật mã KCK và các lược đồ chữ ký số co phụ bản dựa trên thuật toán RSA.
- Định nghĩa cú pháp ASN.1 tương ứng để biểu diễn các khóa và nhận biết các lược đồ.
- Lược đồ RSA nhiều số nguyên tố được đưa ra.
  - RSA nhiều số nguyên tố có nghĩa là modulus không phải là tích của 2 số nguyên tố mà là tích của nhiều hơn 2 số nguyên tố
  - Làm tăng năng suất của các nguyên thủy mật mã RSA
  - Độ an toàn của RSA nhiều số nguyên tố cũng khác với lược đồ RSA nguyên gốc

PKCS#2 VÀ PKCS#4

- PKCS#2 và PKCS#4 được sát nhập vào PKCS#1

PKCS#3 – CHUẨN THỎA THUẬN KHÓA DIFFIE- HELLMAN

- Xác thực giao thức thỏa thuận khóa Diffie-Hellman
- PKCS#4 v1.4 mô tả phương pháp cài đặt thỏa thuận khóa Diffie-Hellman
  - 2 thực thể thỏa thuận khóa bí mật với nhau.
- Có 02 loại lược đồ thiết lập khóa
  - Lược đồ thỏa thuận khóa
    - Dữ liệu tạo khóa được thiết lập là hàm phân phối được cung cấp bởi cả 2 thực thể theo cách mà không thực thể nào có thể xác định trước được giá trị của dữ liệu tạo khóa
    - Ví dụ là lược đồ thỏa thuận khóa Diffie-Hellman
  - Lược đồ vận chuyển khóa
    - Dữ liệu tạo khóa được thiết lập được xác định hoàn toàn bởi một thực thể
    - Ví dụ: lược đồ bọc khóa, khóa phiên được mã hóa với khóa bí mật cho trước

PKCS#5
CHUẨN LẬP MÃ DỰA TRÊN MẬT KHẨU

- Vấn đề liên quan đến ứng dụng mật khẩu:
  - MK không được trực tiếp ứng dụng như là khóa cho một hệ mật thông dụng
  - Các mật khẩu thường được chọn từ một không gian tương đối hẹp.
  - => chế độ bảo vệ để chống lại các tấn công dò tìm
- PKCS#5 cung cấp cơ chế để đạt độ an toàn nâng cao đối với các nguyên thủy mật mã dựa trên mật khẩu bao gồm các hàm dẫn xuất khóa, lược đồ lập mã, lược đồ xác thực thông báo, và một số kỹ thuật trong quá trình chuẩn hóa IEEE 1363.2

PKCS#6
CHUẨN CÚ PHÁP CHỨNG THƯ SỐ MỞ RỘNG

- Khi PKCS#6 được dự thảo thì X.509 mới ở phiên bản 1.0 và chưa có các trường extensions
- Khi có X.509 v3 thì PKCS#6 đã chỉ còn là lịch sử

PKCS#7
CÚ PHÁP THÔNG BÁO MẬT MÃ CMS

- Định nghĩa cú pháp cụ thể cho các thông báo có mật mã được áp dụng vào
- Thay thế cho IEEE RFC 3369 thành CMS làm cơ sở đối với đặc tả S/MIME
- CMS xác định cú pháp được sử dụng để ký số, tóm lược, xác thực hay lập mã nội dung thông báo bất kỳ
- CMS mô tả cú pháp đóng gói để bảo vệ dữ liệu
  - Cho phép đóng gói nhiều lần
  - Ký số 1 dữ liệu đã được đóng gói trước đó
- Các thuộc tính bất kỳ có thể được ký cùng với nội dung thông báo (ví dụ dấu thời gian,...)

PKCS#8 – CHUẨN CÚ PHÁP THÔNG TIN KHÓA BÍ MẬT

- Định nghĩa phương pháp lưu trữ thông tin khóa bí mật
- Mô tả cú pháp đối với thông tin khóa bí mật bao gồm khóa bí mật đối với thuật toán khóa công khai nào đó và một tập các thuộc tính và cú pháp đối với thông tin khóa bí mật được lập mã.
- 2 đối tượng
  - PrivateKeyInfo: thông tin khóa bí mật để nhận biết thuật toán khóa bí mật
  - EncryptedPrivateKeyInfo: thông tin thuật toán lập mã và dữ liệu được lập mã. Là kết quả của việc lập mã thông tin khóa bí mật

PKCS#9 – CÁC LỚP ĐỐI TƯỢNG VÀ KIỂU THUỘC TÍNH ĐƯỢC LỰA CHỌN

- Định nghĩa 2 lớp đối tượng là pkcsEntity và naturalPerson để hỗ trợ các thuộc tính được xác định trong các hệ thống thư mục dựa trên họ giao thức LDAP và X.509
- Định nghĩa một số kiểu thuộc tính mới và các quy tắc trùng khớp có thể sử dụng trong các chuẩn PKCS khác
- Định nghĩa 2 quy tắc trùng khớp pkcs9CaseIgnoreMatch và signingTimeMatch để xác định xem 2 giá trị thuộc PKCS#9 có trùng nhau không
- Kiểu thuộc tính được định nghĩa trong PKCS#9 có thể dùng trong các chuẩn PKCS#7 và CMS, PKCS#10, PKCS#12 và PKCS#15

PKCS#10 – CHUẨN CÚ PHÁP YÊU CẦU CHỨNG THỰC

- PKCS#10 v1.7 đặc tả cú pháp yêu cầu chứng thư số
- PKCS#10 không đặc tả các dạng mà thẩm quyền chứng thực trả về CTS mới
- Các bước xây dựng yêu cầu chứng thực:
  - Xây dựng đối tượng CertificationRequestInfo chứa các trường:
    - Phiên bản, Chủ thể, thuộc tính của chủ thể
    - Thông tin KCK của chủ thể
  - Ký đối tượng CertificationRequestInfo với khóa bí mật của thực thể chủ thể
  - Xây dựng đối tượng CertificationRequest chứa các trường:
    - CertificationRequestInfo
    - SignatureAlgorithm
    - Signature

PKCS#11
CHUẨN GIAO DIỆN THẺ TOKEN MẬT MÃ

- Định nghĩa giao diện lập trình độc lập công nghệ với các thiết bị mật mã (smartcard)
- Ver2.20 đặc tả giao diện lập trình ứng dụng API gọi là Cryptoki cho các thiết bị lưu trữ thông tin mật mã và thực hiện các hàm mật mã.
- Ver 2.20 đặc tả các kiểu dữ liệu và các hàm cung cấp cho ứng dụng yêu cầu các dịch vụ mật mã sử dụng ngôn ngữ lập trình ANSI.C

PKCS#11 - CRYPTOKI

- Cryptoki – viết tắt của giao diện thẻ token mật mã tuân theo cách tiếp cận dựa trên đối tượng đơn giản
- Là giao diện giữa các ứng dụng và tất cả các dạng của thiết bị mật mã di động (smartcard, PCMCIA,…)
- Giao diện lập trình bậc thấp làm bóc tách ra các chi tiết của các thiết bị và truyền đến cho ứng dụng một mô hình chung về thiết bị mật mã (thẻ token)
- Cách ly ứng dụng khỏi các chi tiết của thiết bị mật mã
  - Ứng dụng không cần thay đổi giao diện với các kiểu thiết bị hay môi trường khác -> khả chuyển

PKCS#11 - CRYPTOKI

- Cryptoki có chủ định đối với các thiết bị mật mã liên kết với chỉ một người dùng,
  - Không có phương tiện để phân biệt user
  - Chỉ tập trung lên khóa của một người dùng
- Cài đặt như một thư viện hỗ trợ các hàm trong giao diện và các ứng dụng sẽ được liên kết đến thư viện.
  - Nếu thư viện có thể thay đổi dễ dàng thì attacker có thể sử dụng một thư viện giả để chặn bắt số PIN của người dùng.
- Định nghĩa các kiểu dữ liệu tổng quát, các đối tượng và các hàm
- Nhận dạng được 3 lớp đối tượng:
  - Dữ liệu
  - Chứng thư số
  - Các khóa

PKCS#11 - CRYPTOKI

- Để hạn chế viêc truy cập thẻ token, PIN được sử dụng
  - Bảo vệ các đối tượng bí mật trên thẻ
  - Bảo vệ các khóa bí mật
  - Các khóa bí mật đối xứng
- Cung cấp các hàm để tạo, hủy, sao chép các đối tượng
- Để lấy được và sửa đổi các giá trị của các thuộc tính của chúng

PKCS#11 - CRYPTOKI

- Định nghĩa 13 loại hàm
  - Các hàm mục đích chung (4 hàm)
  - Các hàm quản lý thẻ token và khe slot : 09 hàm
  - Các hàm quản lý phiên : 08 hàm
  - Các hàm quản lý đối tượng : 09 hàm
  - Các hàm lập mã: 04 hàm
  - Các hàm giải mã : 04 hàm
  - các hàm tóm lược thông báo (5 hàm),
  - Các hàm MAC và ký số (6 hàm),
  - Các hàm kiểm tra chữ ký số và MAC (6 hàm),
  - Các hàm mật mã lưỡng mục đích (4 hàm),
  - Các hàm quản lý khóa (5 hàm),
  - Các hàm sinh khóa ngẫu nhiên (2 hàm),
  - Các hàm quản lý hàm song song (2 hàm)

PKCS#11 - CRYPTOKI

- Có 2 kiểu người dùng
  - Quản lý an toàn SO
    - Khởi hoạt thẻ token và đặt số PIN đối với người dùng thông thường
  - Người sử dụng thông thường
    - Chỉ có người dùng mới có thể truy cập đến các đối tượng bí mật trong thẻ token
- Một ứng dụng có thể mở một hay nhiều phiên với thẻ
  - Phiên đọc/viết (R/W): đọc các đối tượng thẻ và phiên
  - Phiên chỉ đọc (R/O): truy cập đến đối tượng thẻ token chứ không phải đối tượng của phiên
  - Một phiên có các loại sự kiện: Login SO, Login User, Log out, close Session, Device Removed

PKCS#12 – CHUẨN CÚ PHÁP TRAO ĐỔI THÔNG TIN CÁ NHÂN

- Mô tả định dạng di chuyển đối với lưu trữ và vận chuyển của các khóa bí mật, các CTS người dùng và các thông tin khác
- Ver 1.0 mô tả cú pháp dịch chuyển đối với thông tin định danh cá nhân: khóa bí mật, CTS, thông tin bí mật, và extensions.
- PKCS#12 có thể xem như thiết kế trong PKCS#8 bằng cách đưa vào thông tin định danh thiết yếu thông qua các thức toàn vẹ và giữ kín khóa công khai

PKCS#12

- Có 4 kết hợp của các thức giữ kín và các thức toàn vẹn
  - Các thức giữ kín sử dụng lập mã dựa trên mật khẩu hoặc khóa công khai để bảo vệ thông tin cá nhân khỏi bị lộ
  - Các thức toàn vẹn dựa trên mã xác thực thông báo có mật khẩu hay dựa trên chữ ký số khóa công khai bảo vệ thông tin cá nhân chống xâm phạm

PKCS#13 & PKCS#14

- PKCS#13 – chuẩn mật mã đường cong elliptic
- PKCS#14 – chuẩn sinh số giả ngẫu nhiên PRNG – đang được xây dựng

PKCS#15 – CHUẨN CÚ PHÁP THÔNG TIN THẺ TOKEN MẬT MÃ

- Có thể liên tác trong các thành phần chạy trên các nền tảng khác nhau mà không phụ thuộc vào nhà sản xuất và không phụ thuộc vào phần mềm, đồng thời duy trì tính phù hợp với các chuẩn liên quan.
- Ver1.1 chỉ rõ định dạng tệp và thu mục để lưu trữ thông tin liên quan đến an toàn trên các thẻ token mật mã

GIAO THỨC QUẢN LÝ CHỨNG THƯ SỐ

- Giao thức quản lý chứng thư số - Certificate Management Protocol – CMP
- Yêu cầu cho việc tương tác trực tuyến giữa các thực thể PKI khác nhau
- CMP có thể hoạt động
  - giữa 2 CA cho việc chứng thực chéo
  - Giữa 01 người dùng và 01 CA cấp phát
  - Hỗ trợ RA
- Quá trình quản lý CTS của Cryptlib được tự động hoàn toàn bằng việc dùng CMP

CMP

- CMP gồm 04 thành phần
  - Phần tiêu đề (header)
  - Phần bảo vệ (protection)
  - Các chứng thư số phụ (extra certificates)
  - Phần nội dung (Body)

CMP

- Phần tiêu đề:
  - Tên người gửi và người nhận
  - Thời gian của thông điệp
  - Thuật toán mã hóa được sử dụng
  - Các trường tùy chọn:
    - Định danh khóa
    - Định danh giao dịch
  - 2 trường khác:
    - Trường dùng cho mở rộng thông tin xử lý
    - Trường dùng cho thông tin người dùng

CMP

- Phần bảo vệ:
  - Tùy chọn
  - Chứa mã xác thực thông điệp dùng để kiểm tra tính toàn vẹn của header và body
- Các chứng thư số phụ:
  - Các chứng thư số phụ mà các thuê bao có thể yêu cầu thêm

CMP

- Phần body: chứa các loại thông điệp
  - Thông điệp yêu cầu – trả lời chứng thư số
  - Thông điệp yêu cầu – trả lời chứng thực chéo
  - Thông điệp yêu cầu – trả lời thu hồi CTS
  - Thông điệp yêu cầu – trả lời khôi phục khóa
  - Thông điệp yêu cầu – trả lời chứng minh quyền sở hữu
  - Thông điệp phân phối chứng thư số và CRL
  - Các thông điệp khác:
    - Thông điệp lỗi
    - Thông điệp xác nhận
    - Các loại tin nhắn chồng nhau

CMP

- Thông điệp yêu cầu CTS gồm 03 phần chính
  - Định dạng thông điệp yêu cầu CTS (CRMF – Certificate Request Messege Format)
    - Định danh yêu cầu
    - Một mẫu thông tin chứng thư số
    - Một số optional controls
  - Chứng minh tính sở hữu (Proof of possession – POP)
    - Cho phép thực thể liên kết với CTS để chứng minh thực thể sở hữu khóa bí mật tương ứng với KCK của CTS
    - Phụ thuộc vào loại khóa sử dụng trong CTS, để đưa ra cách thực hiện POP
  - Thông tin đăng ký
    - Một số các thông tin hỗ trợ được sử dụng trong quá trình yêu cầu CTS:
      - Thông tin liên hệ thực thể
      - Thông tin thanh toán

CMP

- Lợi ích
  - Cung cấp 1 giải pháp an toàn toàn vẹn cho giao dịch PKI
  - Hỗ trợ cho cơ quan đăng ký RA
- Hạn chế
  - Triển khai CMP là một quá trình phức tạp
  - Yêu cầu thiết lập một phần mềm mới vì CMP không được hỗ trợ bởi định dạng có sẵn

CMP

- Đặc tính của CMP
  - CMP được sử dụng ở bất kỳ mô hình giao dịch nào
  - CMP hỗ trợ công cụ cho việc khẳng định quyền sở hữu khóa bí mật trong suốt quá trình thỏa thuận khóa bằng cơ chế trả lời – thách đố.
  - CA cần luôn luôn duy trì thông tin trạng thái trong luồng giao dịch và thông điệp vì một CMP không thể chắc chắn chỉ ra được thông điệp hay giao dịch được sử dụng.
  - Việc mở rộng được thực hiện trong CMP với sự hỗ trợ của trường thông tin chung.
  - CMP sử dụng kỹ thuật mật mã để bảo vệ tất cả các thông điệp, bắt đầu từ yêu cầu chứng thư số ban đầu cho đến các phản hồi từ CA.

QUẢN LÝ CTS SỬ DỤNG CMS - CMC

- CMC - Certificate Management over CMS
- Giao thức này sử dụng cú pháp thông điệp mã hóa và chuẩn PKCS#10 và PKCS#7.
- Cung cấp các chức năng quan trọng của CMP
  - Lưu trữ khóa, cấp pháp CTS và thu hồi CTS
- CMP xác định quá nhiều thông điệp và giao dịch nhiều vòng thì giao dịch CMC hoàn toàn là 1 vòng duy nhất
- Nội dung giao dịch gồm 2 loại:
  - Dữ liệu PKI: thông điệp yêu cầu từ thực thể tới CA
  - Phản hồi PKI: thông điệp phản hồi các yêu cầu
- Không cần thiết phải giữ bí mật các thông điệp giao dịch CMC
- Có một cơ chế để đóng gói các thông điệp trong các dữ liệu được ký số CMS

GIAO THỨC ĐĂNG KÝ CHỨNG THƯ SỐ - SCEP

- Giao thức đăng ký chứng thư số đơn giản – Simple Certificate Enrollment Protocol – SCEP
- Thiết kế cho việc cấp pháp CTS tới các thiết bị mạng khác
- SCEP hỗ trợ các giao dịch sau
  - Phân phối khóa công khai của CA và RA
  - Thu hồi chứng thư số
  - Đăng ký chứng thư số
  - Truy vấn chứng thư số
  - Truy vấn CRL

SCEP

- Hoạt động của SCEP:
  - Điều kiện tiên quyết để thực hiện hoạt động:
    - Tên miền tiêu chuẩn đầy đủ của CA hoặc địa chỉ IP của CA
    - Đường dẫn HTTP tập lệnh CA và thông tin proxy trong trường hợp không kết nối trực tiếp với máy chủ
    - Đường dẫn URP của CTS và CRL được truy vấn
  - Quá trình PKI bắt đầu khi cặp khóa được sinh ra
    - Các thực thể có thể sử dụng bất kỳ một thuật toán được SCEP hỗ trợ như RSA
    - Có một khóa công khai của CA sử dụng chuẩn HTTP Get operation khi thực thể tin cậy vào CA
    - Sau khi thiết lập xong định danh của CA, thực thể sử dụng PKCS#10 để cấp pháp yêu cầu CTS và PKCS#7 để gửi yêu cầu tới CA

SCEP

- Hoạt động của SCEP
  - Tại thời điểm bắt đầu đăng ký CTS, SCEP hỗ trợ 2 quá trình đăng ký:
    - Manual: xác thực thủ công, thực thể phải đợi nhận yêu cầu của CA cho tới khi CA xác thực danh tính của thực thể.
    - Challenge password: xác thực bằng mật khẩu, thực thể cung cấp mật khẩu cho CA, CA sẽ xác thực yêu cầu dựa vào mật khẩu nhận được
  - Sau khi hoàn tất việc xác thực, CA sẽ cấp phát CTS cho thực thể

SCEP

- Thu hồi chứng thư số trong SCEP
  - Quá trình thu hồi CTS trong SCEP được thực hiện thủ công
  - Khi một thực thể gửi yêu cầu thu hồi CTS, thực thể đó phải liên hệ với CA thông qua điện đàm
  - CA sẽ đề nghị thực thể đưa ra mật khẩu, nếu mật khẩu được xác thực thì CTS sẽ được thu hồi.

SCEP

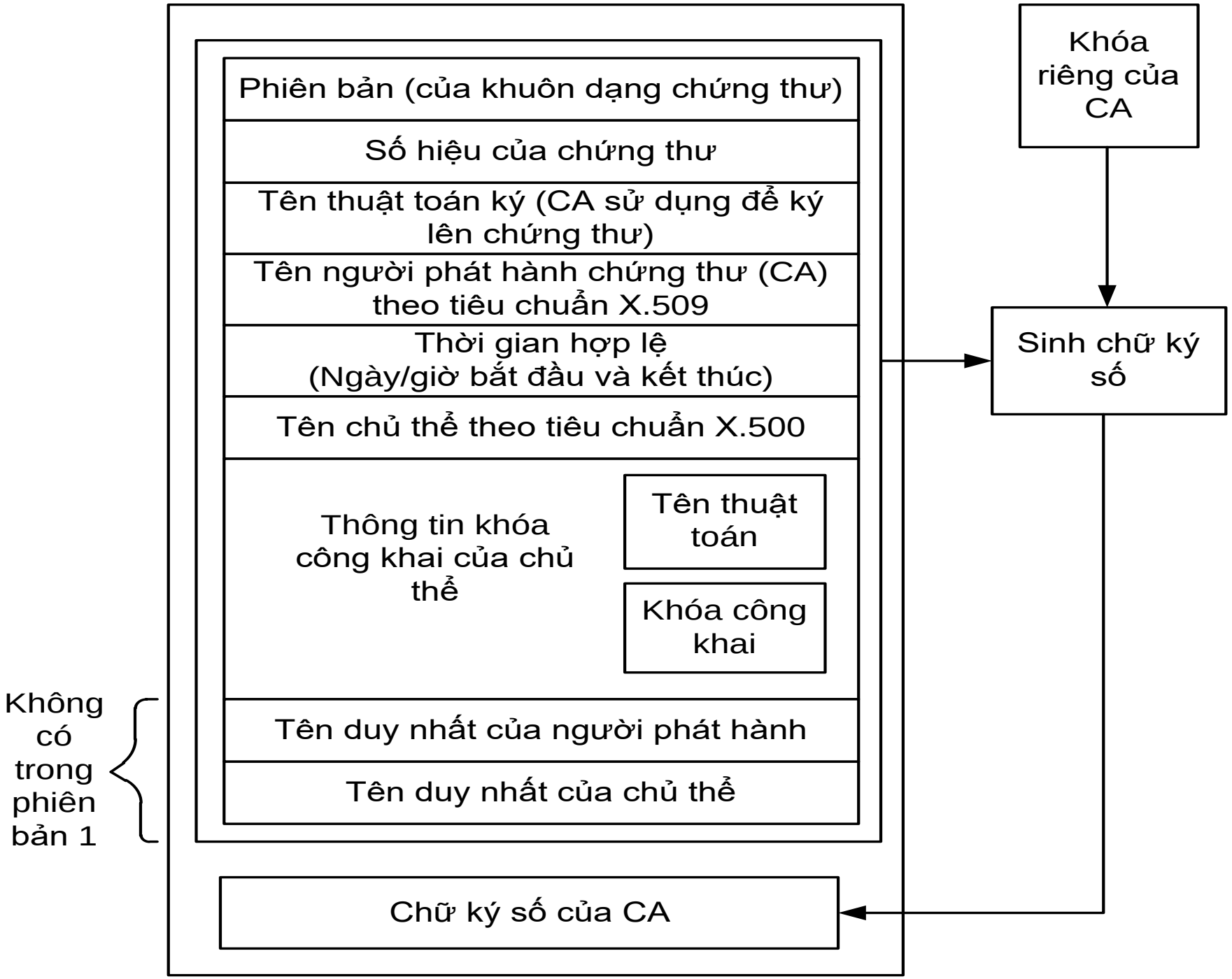
- Truy cập Chứng thư số và CRL
  - Để truy vấn CTS, thực thể có thể sử dụng LDAP hoặc thông điệp truy vấn được quy định trong SCEP
    - Thông điệp GetCertPKI
    - Thông điệp CertRepPKI
  - Để truy cập tới CRL, thực thể có thể dùng 3 phương pháp:
    - Sử dụng yêu cầu HTTP Get đơn giản
    - Sử dụng LDAP: Giả thiết máy chủ CA hỗ trợ công bố CRL LDAP và cấp phát điểm phân phối CRL trong CTS. Điểm phân phối CRL được mã hóa như một DN
    - Tạo thông điệp chứa tên CA phát hành và số serial CTS của CA
      - Phương pháp này không được khuyến cáo

SCEP

- Những hạn chế:
  - Không xác định được thông điệp yêu cầu thu hồi CTS, chỉ hỗ trợ các thông điệp yêu cầu CTS
  - Là một thuật toán đặc trưng và chỉ hỗ trợ thuật toán RSA
  - Chỉ sử dụng cho cấp phát CTS trong thiết bị mạng

2. NHÓM CHUẨN VỀ KHUÔN DẠNG CTS VÀ CRL

- Chuẩn về khuôn dạng mô tả chi tiết các trường trong cấu trúc dữ liệu CTS v3 và CRL v2.
- Giới thiệu RFC 5280– Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile 2008-05 (Định dạng X.509: danh sách chứng thư bị thu hồi và chứng thư số hạ tầng khóa công khai trong Internet)
  - Chứng thư số X.509 v3
  - Danh sách CRL và hồ sơ các trường mở rộng của CRL
  - Các trường sử dụng trong CRL
  - Các trường trong CertificateList
  - Trường trong tbsCerList
  - Các trường CRL mở rộng


Phiên bản (của khuôn dạng chứng thư)
Số hiệu của chứng thư
Tên thuật toán ký (CA sử dụng để ký lên chứng thư)
Tên người phát hành chứng thư (CA) theo tiêu chuẩn X.509
Thời gian hợp lệ (Ngày/giờ bắt đầu và kết thúc)
Tên chủ thể theo tiêu chuẩn X.500
Thông tin khóa công khai của chủ thể
Tên thuật toán
Khóa công khai
Tên duy nhất của người phát hành
Tên duy nhất của chủ thể
Không có trong phiên bản 1
Chữ ký số của CA
Khóa riêng của CA
Sinh chữ ký số

CHỨNG THƯ SỐ X.509 V3

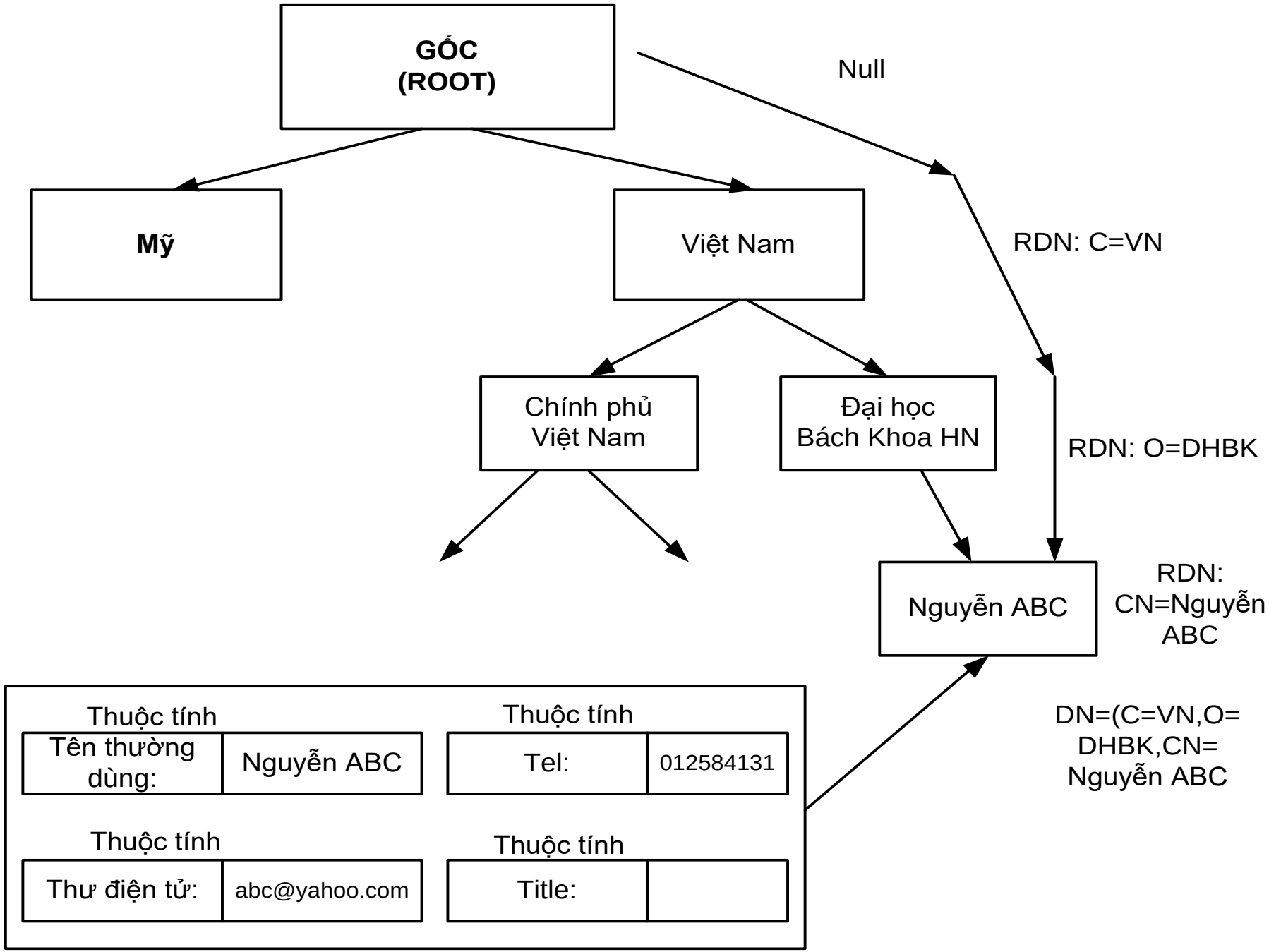
- **Phiên bản (Version)**: chỉ ra dạng phiên bản 1,2,3
- **Số hiệu (Serial Number)**: Số hiệu nhận dạng duy nhất của CTS, được CA phát hành gán cho.
- **Tên thuật toán ký (Signature)**: Tên thuật toán ký được CA sử dụng để ký CTS.
- **Người phát hành (Issuer)**: Tên theo chuẩn X.500 của CA phát hành.
- **Thời gian hợp lệ (Validity)**: Ngày/giờ có hiệu lực và hết hạn của một chứng thư.
- **Chủ thể (Subject)**: Tên X.500 của đối tượng nắm giữ khoá riêng (t/ứ với KCK)
- **Thông tin về khoá công khai của chủ thể (Subject Public key Information)**: gồm khoá công khai của chủ thể cùng với một tên thuật toán sử dụng KCK này.
- **Tên duy nhất của người phát hành**: Là một chuỗi bit tuỳ chọn, được sử dụng để chỉ ra tên rõ ràng của CA phát hành, trong trường hợp cùng một tên được gán cho các thực thể khác nhau trong cùng thời gian.
- **Tên duy nhất của chủ thể**: là một chuỗi bit tuỳ chọn, được sử dụng để chỉ ra tên rõ ràng của chủ thể, trong trường hợp cùng một tên được gán cho các thực thể khác nhau trong cùng thời gian.

TÊN TRONG X.509

- Thông tin được lưu trữ trong các thư mục X.509 gồm có một tập hợp các đầu vào liên quan đến một đối tượng thực
- Đối tượng này có một tên rõ ràng – tên phân biệt (DN)
- Tất cả các đầu vào của X.509 được tổ chức theo cấu trúc hình cây – cây thông tin thư mục
  - Một gốc có tên phân biệt là Null và không hạn chế số đỉnh
  - Mỗi đỉnh (trừ gốc) tương ứng với một đầu vào thư mục và có một tên DN

TÊN TRONG X.509

- Tên phân biệt của một đầu vào được tạo ra bằng cách kết hợp tên phân biệt của đầu vào mức trên gần nó nhất cùng với tên phân biệt liên quan (RDN – Relative Distinguished Name)
- RDN biểu diễn một hoặc nhiều thuộc tính của một thực thể.
  - Tập hợp các xác nhận về giá trị của thuộc tính
  - Các giá trị thuộc tính được cung cấp duy nhất


GỐC
(ROOT)
Null
Mỹ
Việt Nam
RDN: C=VN
Chính phủ
Việt Nam
Đại học
Bách Khoa HN
RDN: O=DHBK
Nguyễn ABC
RDN:
CN=Nguyễn
ABC
Thuộc tính
Tên thường
dùng:
Nguyễn ABC
Thuộc tính
Tel:
012584131
DN=(C=VN,O=
DHBK,CN=
Nguyễn ABC
Thuộc tính
Thư điện tử:
abc@yahoo.com
Thuộc tính
Title:

TÊN TRONG X.509

- DN không phải là giải pháp đáng tin cậy vì khó quản lý, chậm bổ sung cập nhật.
- Giải pháp khác tốt hơn:
  - Trên một RDN chỉ cần lấy một giá trị thuộc tính duy nhất trong toàn bộ thời gian
- Có một vấn đề: Với tên thường dùng (CN), có thể có nhiều tên trong cùng một tổ chức
- Tên RDN sẽ có thể có định dạng như sau:
- {CN=Nguyễn ABC, Student Number = 123456789}
  - Đây là giải pháp được nhiều tổ chức chấp nhận

ĐĂNG KÝ ĐỐI TƯỢNG

- Trong khuôn dạng CTS X.509 có các tên thuật toán, dùng để nhận dạng thuật toán ký và thuật toán sử dụng khóa công khai được chứng thực, ví dụ:
  - Chữ ký số, sử dụng DSS với hàm băm SHA.
  - Chữ ký số, sử dụng RSA với hàm băm MD5.
  - Thiết lập khoá mã hoá, sử dụng truyền khoá RSA
  - Thiết lập khoá mã hoá, sử dụng kỹ thuật Diffe-Hellman
- Đây là ví dụ cho việc gán các tên của đối tượng duy nhất

ĐĂNG KÝ ĐỐI TƯỢNG

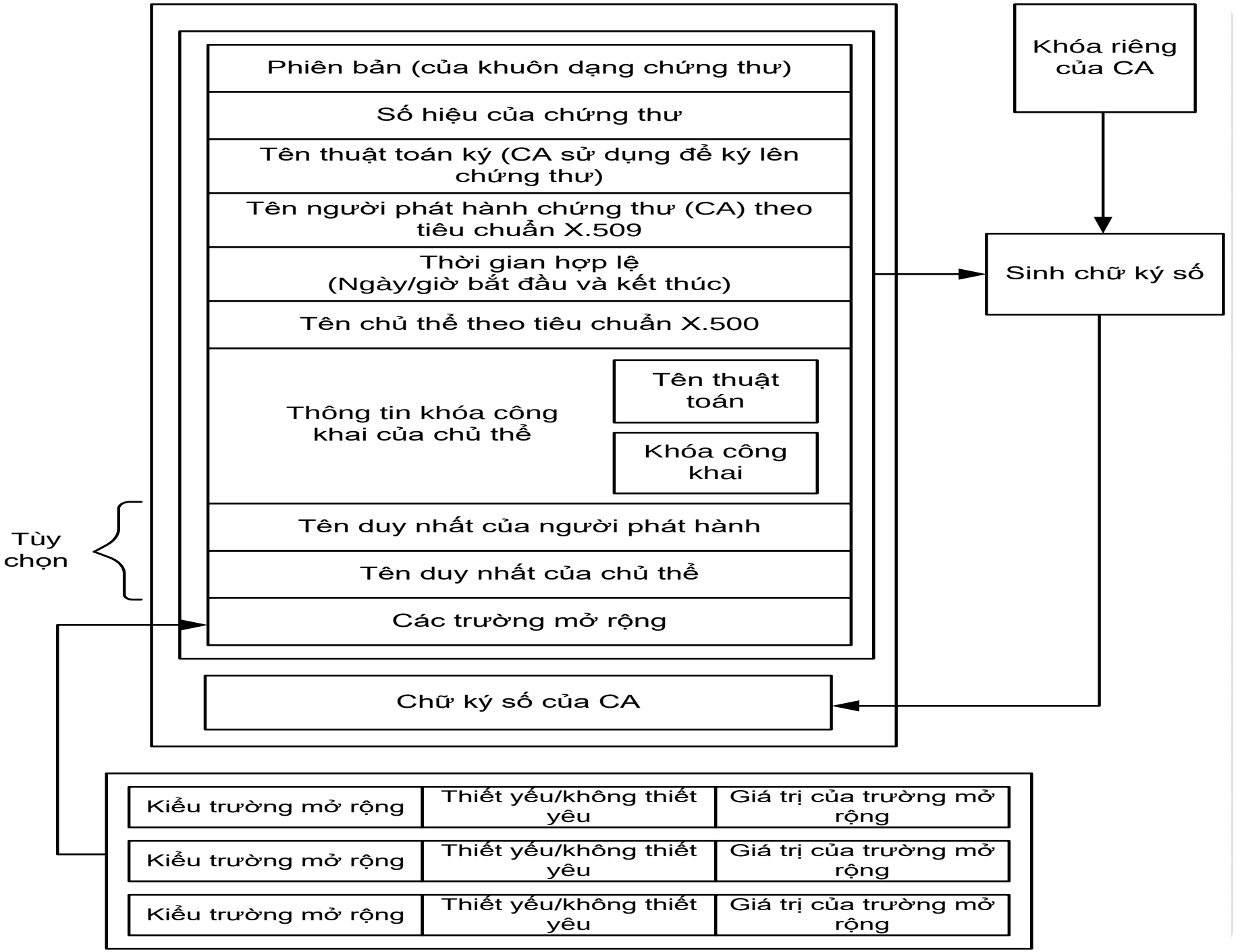
- Một hệ thống đăng ký của đối tượng sử dụng cho các tên thuật toán và cho các lớp đối tượng chính là cơ chế tên đối tượng được định rõ trong các chuẩn và được sự hỗ trợ của rất nhiều cơ quan đăng ký đối tượng
- Tên đối tượng là một giá trị, gồm một dãy các số nguyên
  - Giá trị này được gán cho một đối tượng đã đăng ký
  - Các tên đối tượng hoàn toàn khác nhau hoặc duy nhất.

KHUÔN DẠNG CHỨNG THƯ SỐ X.509 V3

- Phiên bản 1 và 2 không đáp ứng được tất cả yêu cầu nên cần phải có sự bổ sung thêm các trường thông tin
- Lý do:
  - Cần phải phân biệt được các CTS khác nhau của đối tượng một các dễ dàng.
  - Cần chuyển thêm thông tin nhận dạng chủ thể ngoài tên X.500
  - Một số các ứng dụng cần nhận dạng những người sử dụng thông qua các dạng tên xác định ứng dụng, ngoài các tên X.500
  - Các chứng thư khác nhau có thể được phát hành theo các chính sách và các hoạt động chứng thực khác nhau
  - Các đường dẫn chứng thực không được dài tùy tiện và phức tạp

KHUÔN DẠNG CHỨNG THƯ SỐ X.509 V3

- Bổ sung thêm vào CTS X.509 một cơ chế mở rộng
- => chứng thư số X.509 version 3
- Khuôn dạng như ver 1 và 2 nhưng có bổ sung thêm các trường mở rộng
  - Mỗi trường mở rộng có một kiểu (cần được đăng ký)
    - Bằng cách gán cho một tên đối tượng
    - Các kiểu của trường mở rộng được chủ thể xác định
    - Các kiểu quan trọng của trường mở rộng phải được chuẩn hóa
  - Mỗi trường chứa một giá trị tên đối tượng
    - Kiểu của trường
    - Một chỉ báo thiết yếu: xuất hiện khi trường mở rộng là thiết yếu/không thiết yếu
      - Không thiết yêu: hệ thống CTS bỏ qua trường này nếu không chấp nhận kiểu của trường
      - Thiết yếu: hệ thống sẽ không AT nếu sử dụng bất kỳ phần nào của CTS, trừ khi hệ thống chấp nhận kiểu của trường và thiết lập chức năng liên quan
    - Một giá trị


Khóa riêng của CA
Phiên bản (của khuôn dạng chứng thư)
Số hiệu của chứng thư
Tên thuật toán ký (CA sử dụng để ký lên chứng thư)
Tên người phát hành chứng thư (CA) theo tiêu chuẩn X.509
Thời gian hợp lệ (Ngày/giờ bắt đầu và kết thúc)
Tên chủ thể theo tiêu chuẩn X.500
Thông tin khóa công khai của chủ thể
Tên thuật toán
Khóa công khai
Sinh chữ ký số
Tùy chọn
Tên duy nhất của người phát hành
Tên duy nhất của chủ thể
Các trường mở rộng
Chữ ký số của CA
Kiểu trường mở rộng
Thiết yếu/không thiết yêu
Giá trị của trường mở rộng
Kiểu trường mở rộng
Thiết yếu/không thiết yêu
Giá trị của trường mở rộng
Kiểu trường mở rộng
Thiết yếu/không thiết yêu
Giá trị của trường mở rộng

CÁC TRƯỜNG MỞ RỘNG CHUẨN CỦA CTS

- Chia thành các nhóm nhỏ:
  - (1) Thông tin về khoá và chính sách
  - (2) Các thuộc tính của chủ thể và người phát hành
  - (3) Các ràng buộc đối với đường dẫn chứng thực
  - (4) Các trường mở rộng liên quan đến danh sách các chứng thư bị thu hồi (CRL)

CÁC TRƯỜNG MỞ RỘNG CHUẨN CỦA CTS

- Các trường mở rộng nhóm (1):
  - Chuyển thêm các thông tin về khóa của chủ thể và người phát hành
  - Các chỉ báo về chính sách chứng thư số
    - Thiết lập cơ sở hạ tầng KCK dễ dàng hơn
    - cho phép quản trị hạn chế các mục đích sử dụng các chứng thư và các khóa đã được chứng thực
  - Gồm các trường sau:

CÁC TRƯỜNG MỞ RỘNG CHUẨN CỦA CTS

- Các trường mở rộng nhóm (1):
  - Tên khóa của CA phát hành:
    - Phân biệt các khóa khác nhau của CA phát hành sử dụng khi ký CTS
    - Giúp cho các CA tiếp theo tìm kiếm chính xác CTS trong chuỗi CTS
  - Tên khóa của chủ thể
    - Phân biệt các khóa mà chủ thể của một CTS sử dụng
  - Sử dụng khóa:
    - Chỉ ra mục đích sử dụng khóa: Cho chữ ký số hoặc Thiết lập khóa mã
    - Thiết yếu: CA quy định chỉ được sử dụng CTS và khóa vào mục đích xác định
    - Không thiết yếu: dùng để tìm ra chứng thư số đúng

CÁC TRƯỜNG MỞ RỘNG CHUẨN CỦA CTS

- Các trường mở rộng nhóm (1):
  - Khoảng thời gian sử dụng khóa riêng
    - Chỉ ra thời hạn sử dụng một khóa riêng cho mục đích ký số.
  - Các chính sách chứng thư:
    - Chỉ ra các chính sách hoặc các hoạt động liên quan đến CTS
  - Ánh xạ chính sách
    - Chỉ sử dụng khi chủ thể CTS là một CA cho phép người phát hành xác định một hoặc nhiều chính sách có thể quan tâm ngang bằng với các chính sách khác sử dụng trong miền của CA

CÁC TRƯỜNG MỞ RỘNG CHUẨN CỦA CTS

- Các trường mở rộng của nhóm (2):
  - Chỉ ra các tên lựa chọn dành cho chủ thể và người phát hành CTS
  - Tên lựa chọn của chủ thể
    - Chỉ ra một hoặc nhiều tên lựa chọn phân biệt
    - Các chủ thể của CTS sử dụng nhiều dạng tên khác nhau
  - Tên lựa chọn của người phát hành
    - Chỉ ra một hoặc nhiều tên lựa chọn cho người phát hành CTS
  - Các thuộc tính thư mục của chủ thể
    - Chuyển thêm các giá trị thuộc tính X.500 mà chủ thể mong muốn

CÁC TRƯỜNG MỞ RỘNG CHUẨN CỦA CTS

- Các trường mở rộng của nhóm (3):
  - Giúp các tổ chức khác nhau liên kết các cơ sở hạ tầng với nhau
  - Các ràng buộc cơ bản
    - Chỉ ra chủ thể của CTS là một CA hoặc chỉ là 1 thực thể cuối
    - Ngăn chặn những người dùng cuối cạnh tranh gian lận với các CA
  - Các ràng buộc đối với tên:
    - Giới hạn không gian tên có thể chấp nhận trong các CTS có trong một đường dẫn CTS
  - Các ràng buộc đối với chính sách
    - Xác định một tập hợp các ràng buộc cho việc nhận dạng chính sách CTS và tham chiếu đến chính sách một cách tường mình.

DANH SÁCH CTS BỊ THU HỒI (CRL) VÀ HỒ SƠ CÁC TRƯỜNG MỞ RỘNG CỦA CRL

- Tổ chức cấp CRL có thể là CA hoặc là cơ quan được CA ủy quyền
- Thông báo về tình trạng các CTS đã được cấp phát
- CRL hoàn chỉnh:
  - Các CTS quá hạn trong phạm vi của CRL đã bị thu hồi
- CRL đầy đủ và hoàn chỉnh:
  - Các CTS quá hạn do CA cấp và đã bị thu hồi
- Phạm vi của CRL không bị ảnh hưởng bởi khóa sử dụng để ký vào RL hoặc khóa dùng để ký vào CTS
- Tổ chức cấp CRL có thể tạo ra các CRL Delta, để cập nhật những CTS có trạng thái thu hồi thay đổi kể từ khi phát hành CRL tham chiếu hoàn chỉnh – CRL gốc

```
CertificateList      ::=    SEQUENCE        {
   tbsCertList               TBSCertList,
   signatureAlgorithm        AlgorithmIdentifier,
   signatureValue            BIT STRING      }
    TBSCertList    ::=    SEQUENCE        {
         version   Version OPTIONAL,-- nếu hiện diện, phải là v2
         signature AlgorithmIdentifier,
         issuer    Name,
         thisUpdate       Time,
         nextUpdate       Time OPTIONAL,
         revokedCertificates   SEQUENCE OF SEQUENCE  {
               userCertificate   CertificateSerialNumber,
               revocationDate  Time,
               crlEntryExtensions      Extensions OPTIONAL
                                       -- nếu hiện diện, phải là v2
                                   }
                                   OPTIONAL,
         crlExtensions   [0]    EXPLICIT Extensions OPTIONAL
                                       -- nếu hiện diện, phải là v2
                                   }
    -- Version, Time, CertificateSerialNumber, và  AlgorithmIdentifier
```

CÁC TRƯỜNG TRONG CERTIFICATELIST

- Là một chuỗi tuần tự (SEQUENCE), có 3 trường bắt buộc:
  - Trường Danh sách chứng thư được ký – tbsCerList
    - Là một chuỗi tuần tự có tên của tổ chức phát hành, ngày phát hành, ngày phát hành tiếp theo, CRL, và các phần mở rộng CRL tùy chọn
  - Trường Thuật toán chữ ký số - signatureAlgorithm
    - Xác định thuật toán mà tổ chức cấp CRL sử dụng để ký CertificateList
    - Cùng một thuật toán với trường chữ ký trong tbsCertList
  - Trường Giá trị chữ ký – signatureValue
    - Chứa một chữ ký được tính từ tbsCertList (mã hóa theo ASN.1 DER)
    - Chữ ký được mã hóa như một chuỗi bit
    - tbsCertList mã hóa theo ASN.1 DER được sử dụng như đầu vào cho chức năng ký.

TRƯỜNG TRONG TBSCERTLIST

- Version
- Chữ ký:
  - nhận dạng thuật toán cho các thuật toán được sử dụng để ký CRL
- Tên tổ chức phát hành
  - Tên tổ chức phát hành xác định thực thể đã ký và phát hành CRL
- Ngày phát hành CRL (thisUpdate)
  - Có thể được mã hóa
- Ngày phát hành CRL tiếp theo (nextUpdate)
  - CRL có thể được phát hành trước thời gian đã chỉ định, nhưng không được chậm hơn thời gian đã chỉ định
- Các CTS bị thu hồi (revokedCertificates)
  - Các CTS bị thu hồi được liệt kê bởi các số hiệu của CTS
- Các trường mở rộng

CÁC TRƯỜNG CRL MỞ RỘNG

- Khuôn dạng của CRL X.509 ver2 cho phép xác định các trường mở rộng riêng để cung cấp thông tin cho các cộng động tương ứng
- Mỗi trường mở rộng có thể xác định:
  - Quan trọng
  - Không quan trọng
- Nếu CRL chứa 1 trường mở rộng quan trọng mà ứng dụng không thể xử lý, thì ứng dụng đó không được phép sử dụng CRL đó để xác định tình trạng của CTS.

CÁC TRƯỜNG CRL MỞ RỘNG

- Trường nhận dạng khóa của tổ chức cấp CTS (authorityKeyIdentifier)
  - Cung cấp công cụ nhận dạng các KCK đi kèm với các khóa riêng được sử dụng để ký CRL
  - Dùng hiệu quả với tổ chức phát hành có 02 chữ ký trở lên do có nhiều cặp chữ ký trùng nhau hoặc do các thay đổi
- Trường tên thay thế của tổ chức cấp chứng thư số
  - Cho phép tăng cường các đặc điểm nhận dạng của tổ chức cấp CRL
  - Các tùy chọn gồm:
    - Địa chỉ thư điện tử
    - Một tên DNS
    - Địa chỉ IP
    - Một URI

CÁC TRƯỜNG CRL MỞ RỘNG

- Số hiệu của CRL
  - Là một số theo thứ tự tăng dần
  - Là trường không quan trọng, Cho phép user xác định khi một CRL cụ thể thay thế cho một CRL khác
- Điểm phân phối phát hành
  - Là trường quan trọng giúp phân biệt điểm phân phối CRL và phạm vụ của một CRL cụ thể
- CRL mới nhất
  - Cho biết thông tin CRL Delta cho CRL hoàn chỉnh được cập nhật như thế nào
  - Là trường không quan trọng nhưng phải xuất hiện trong các CRL Delta

CÁC TRƯỜNG CRL MỞ RỘNG

- Chỉ thị CRL Delta
  - Là một trường quan trọng, gồm giá trị đơn của 01 loại số hiệu CRL gốc
  - Nhận diện CRL như là CRL Delta
  - Chứa các cập nhật về thông tin thu hồi được đưa ra trước đó
  - CRL Delta thường nhỏ hơn CRL mà chúng cập nhật nên:
    - Tiêu tốn ít độ rộng dải tầng mạng
    - Giảm gánh nặng cho mạng và thời gian xử lý trong một số môi trường
  - Sự kết hợp CRL Delta và CRL gốc tham chiếu tương đương với một CRL hoàn chỉnh trong phạm vi có thể áp dụng được tại thời điểm phát hành CRL Delta,

CÁC TRƯỜNG CRL MỞ RỘNG

- Chỉ thị CRL Delta
  - Các điều kiện có thể kết hợp CRL hoàn chỉnh và CRL Delta
    - Do cùng 1 tổ chức cấp
    - Có cùng 1 phạm vi
      - Trường mở rộng điểm phân phối trong cả CRL hoàn chỉnh và CRL delta bị bỏ qua
      - Trường mở rộng điểm phân phối CRL có trong cả CRL hoàn chỉnh và CRL Delta và giá trị mỗi trường là như nhau trong cả 2 CRL.
    - Số hiệu của CRL hoàn chỉnh ≥ số hiệu của CRL gốc trong CRL Delta
    - Số hiệu của CRL hoàn chỉnh ≤ số hiệu của CRL delta

CÁC TRƯỜNG CRL MỞ RỘNG

- Truy nhập thông tin của tổ chức cấp chứng thư số (Authority Information Access)
  - Là trường không quan trọng
  - Bao gồm ít nhất một mô tả truy nhập quy định id-ad-caIssuers như là 1 phương pháp truy cập
- Các trường mở rộng đầu mục của CRL
  - cung cấp các phương pháp để tích hợp thêm các thuộc tính vào các đầu mục CRL
  - Có thể quan trọng/không quan trọng
    - Nếu chứa đầu mục CRL quan trọng mà các ứng dụng không thể xử lý thì các ứng dụng này không được sử dụng CRL để quyết định hiện trạng của CTS
    - Các ứng dụng có thể bỏ qua các trường mở rộng đầu mục CRL không quan trọng và không được nhận dạng.

CÁC TRƯỜNG CRL MỞ RỘNG

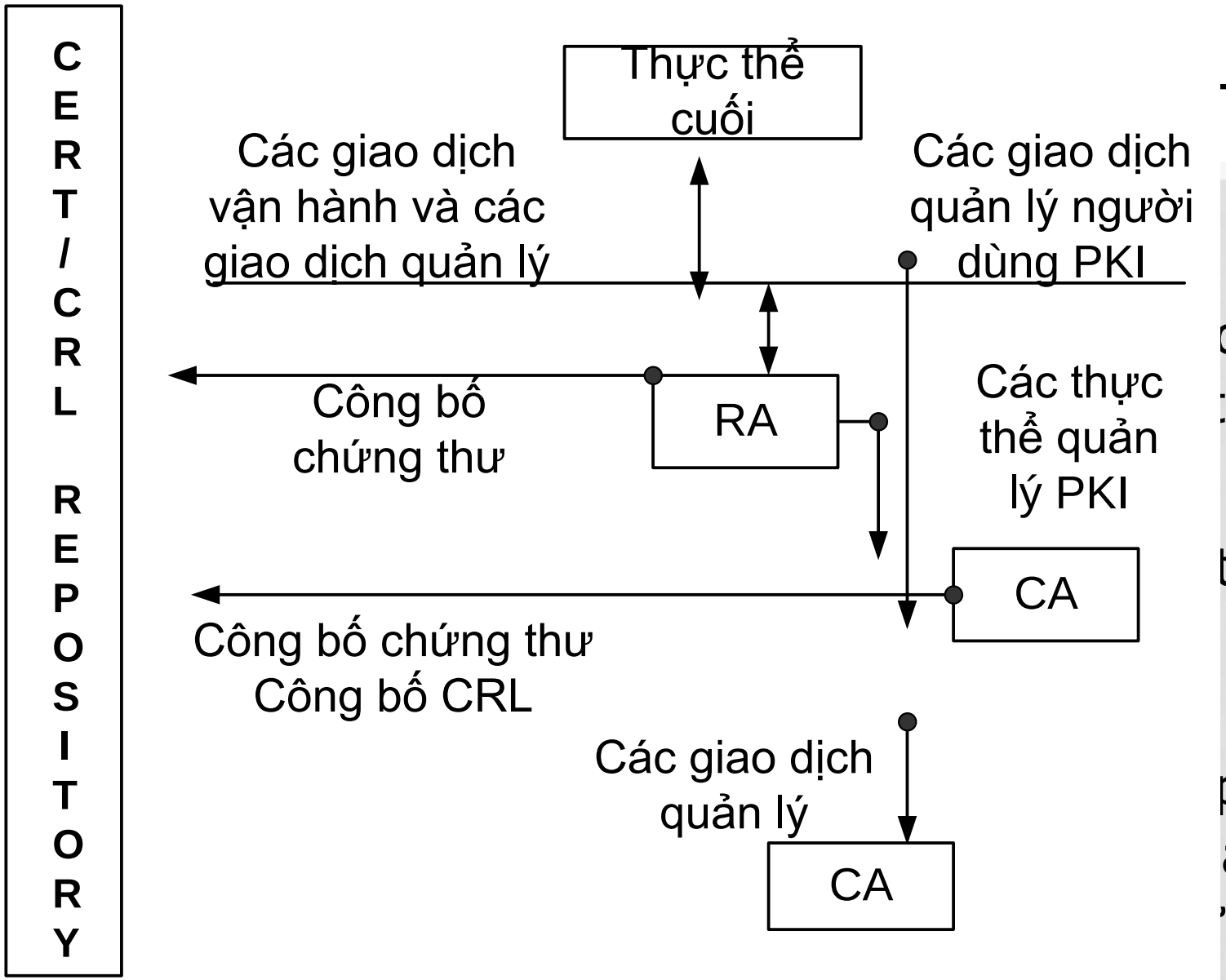
- Mã lý do thu hồi (reasonCode)
  - Là trường không quan trọng, xác định lý do thu hồi CTS
- Thời gian hết hiệu lực
  - Là trường không quan trọng, cho biết thời gian đã được biết rõ hoặc nghi rằng KBM được thỏa hiệp hay CTS hết hiệu lực
- Tổ chức cấp CTS
  - Nhận dạng tổ chức phát hành CTS gắn với một đầu mục trong CRL gián tiếp
  - Nếu hiện diện, thì tổ chức cấp CTS bao gồm một hoặc nhiều tên từ trường của tổ chức cấp CRL.
  - Nếu không xuất hiện thì tổ chức cấp CTS mặc định là tổ chức cấp CRL

3. NHÓM CHUẨN VỀ GIAO THỨC HOẠT ĐỘNG

- Nhóm chuẩn về giao thức hoạt động được quy định trong các tài liệu:
  - **RFC 2585 – Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP. 1999-05**
    - RFC 2585
    - Quy ước FTP
    - Quy ước HTTP
    - Đăng ký MIME
  - RFC 3494 - Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2. 2003-03.
  - RFC 4387 - Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP. 2006-02

RFC 2585 – INTERNET X.509 PUBLIC KEY ...S:

- M
  - ...ặc hệ ...hư;
  - ...t hệ ... quản
  - ...phân ...à ...



RFC 2585 - – INTERNET X.509 PUBLIC KEY INFRASTRUCTURE OPERATIONAL PROTOCOLS: FTP AND HTTP

- Nguồn CRL
  - Các thực thể cuối có thể có được các chứng thư và các CRL từ nguồn sử dụng FTP hoặc HTTP
  - EE công bố các CTS của họ trong nguồn FTP hoặc HTTP
  - Các RA hoặc CA công bố CTS và CRL trong nguồn FTP hoặc HTTP

QUY ƯỚC FTP

- Trong các mở rộng CTS và mở rộng CRL, dạng URI của GeneralName được dùng để xác định vị trí có thể có của CTS và CRL của người phát hành
  - ftp://ftp.netcom.com/sp/spyrus/housley.cer
  - ftp://ftp.your.org/pki/id48.cer
  - ftp://ftp.your.org/pki/id48.no42.crl
- Người dùng có thể công bố tham chiếu URI vào một tập tin có chứa các CTS
- FTP là một biện pháp thay thế cho các giao thức truy cập thư mục cho việc phân phối CTS và CRL
- Tên của các tập tin có chứa CTS phải có hậu tố ".Cer"
  - Mỗi tập tin này chứa chính xác một CTS, được mã hóa theo quy tắc mã hóa phân biệt DER
- Tương tự, tập tin CRL có hậu tố là ".Crl"

QUY ƯỚC HTTP

- Tương tự quy ước FTP:
  - Dạng URI của GeneralName được dùng để xác định vị trí
- Người dùng công bố tham chiếu URI vào một tập tin

ĐĂNG KÝ MIME

- Các loại MIME hỗ trợ cho việc chuyển các CTS và CRL:
  - application / pkix-CERT
  - application / pkix-crl

4. NHÓM CHUẨN VỀ GIAO THỨC QUẢN LÝ

- Hỗ trợ việc
  - truyền các yêu cầu và thông tin quản lý giữa các thực thể cuối với thực thể quản lý
  - Truyền thông tin giữa các thực thể quản lý
- Các nhóm chuẩn:
  - RFC 4210 - Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). 2005-09.
  - **RFC 4211 - Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF). 2005-09.**
  - RFC 5272 - Certificate Management over CMS (CMC). 2008-06.

INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE REQUEST MESSAGE FORMAT (CRMF)

- Certificate Request Message Format – CRMF định dang thông điệp yêu cầu chứng thư số
- Một yêu cầu CTS được dùng trong một giao thức truyền tải yêu cầu xin cấp CTS tới CA, có thể qua RA
  - Thông tin gồm khóa công khai và các thông tin đăng ký liên quan.
  - Các thông tin cũng được thiết kế để sử dụng được giao thức yêu cầu CTS (Certificate Request Protocol – CRP)

XÂY DỰNG YÊU CẦU CHỨNG THƯ SỐ

- Xây dựng một đối tượng CerRequest. Đối tượng này có thể là khóa công khai, toàn bộ hoặc một phần tên chủ thể (Subject name), các trường yêu cầu chứng thư số khác và các thông tin điều khiển bổ sung liên quan đến quá trình đăng ký.
- Trong trường hợp cần thiết, sự chứng minh tính sở hữu (Proof of Possession – POP) của khóa bí mật tương ứng với khóa công khai của chứng thư số sẽ được sử dụng
- Thông tin đăng ký bổ sung có thể được kết hợp với giá trị của POP và cấu trúc CertRequest từ định dạng của một CerReqMessage và được thêm vào bởi cả chủ thể và RA.
- CertReqMessage được truyền an toàn tới CA qua các phương tiện truyền thông an toàn và được xác định cụ thể bởi mỗi CRP

CẤU TRÚC CERTREQMESSAGE

- Thông điệp yêu cầu chứng thư số bao gồm yêu cầu chứng thư số, trường POP tùy chọn và trường thông tin đăng ký tùy chọn
  - CertReqMessages ::= SEQUENCE SIZE (1..MAX) OF CertReqMsg
  - CertReqMsg ::= SEQUENCE {
  - certReq CertRequest,
  - popo ProofOfPossession OPTIONAL,
  - regInfo SEQUENCE SIZE(1..MAX) of AttributeTypeAndValue OPTIONAL
  - }

CHỨNG MINH TÍNH SỞ HỮU (PROOF OF POSSESION – POP)

- Cấu trúc quản lý PKI quy định một chủ thể phải chứng minh tính sở hữu của mình đối với khóa bí mật tương ứng với KCK trong yêu cầu đăng ký CTS
  - Cho phép CA/RA kiểm tra tính hợp lệ của các ràng buộc giữa chủ thể và cặp khóa
- CRP, CA và RA được tự do lựa chọn các phương pháp POP
- CRP cần phải xác định phương pháp POP nào được yêu cầu, hay cơ chế nào cho client để tìm thấy các phương pháp POP được hỗ trợ
- *ProofOfPossession ::= CHOICE {*
- *raVerified [0] NULL,*
- *signature [1] POPOSigningKey,*
- *keyEncipherment [2] POPOPrivKey,*
- *keyAgreement [3] POPOPrivKey }*

CÚ PHÁP CERTREQ

- Cú pháp CertReq gồm:
  - Định danh yêu cầu
  - Nội dung chứng thư số mẫu (CertTemplate)
  - Chuỗi tùy chọn của thông tin điều khiển

CÚ PHÁP THUỘC TÍNH KIỂM SOÁT CONTROLS SYNTAX

- CertRequest gồm một hoặc nhiều giá trị thuộc tính kiểm soát liên quan đến việc xử lý yêu cầu
- Controls ::= SEQUENCE SIZE(1..MAX) OF AttributeTypeAndValue
  - Kiểm soát thẻ đăng ký (Registration Token Control)
  - Kiểm soát xác thực (Authenticator Control)
  - Kiểm soát thông tin công khai (Publication Information Control)
  - Kiểm soát tùy chọn lưu trữ (Archive Options Control)
  - Kiểm soát OldCert ID
  - Kiểm soát khóa mã hóa giao thức

KIỂM SOÁT THẺ ĐĂNG KÝ

- Kiểm soát regToken gồm thông tin one-time để CA xác định định danh của chủ thể trước khi cấp phát CTS
- Giá trị cho regToken có thể là:
  - Chuỗi ký tự
  - Một giá trị ngẫu nhiên
  - Các giá trị này được mã hóa như chuỗi ký tự đại diện cho giá trị nhị phân
  - id-regCtrl-regToken OBJECT IDENTIFIER ::= { id-regCtrl 1 }

KIỂM SOÁT XÁC THỰC

- Gồm thông tin sử dụng liên tục cho việc thiết lập kiểm tra định danh không được mã hóa trong liên lạc với CA
- Các giá trị này được sinh bởi CA hoặc thuê bao
- Giá trị cho việc xác thực có thể là
  - Chuỗi ký tự
  - Một giá trị ngẫu nhiên
  - id-regCtrl-authenticator OBJECT IDENTIFIER ::= { id-regCtrl 2 }

KIỂM SOÁT THÔNG TIN CÔNG KHAI

- Kiểm soát pkiPublicationInfo cho phép thuê bao tác động đến việc công bố công khai CTS của CA và RA
- Kiểm soát này được xác định bằng OID
- Cú pháp
  - id-regCtrl-pkiPublicationInfo OBJECT IDENTIFIER::={id-regCtrl 3 }
  - PKIPublicationInfo ::= SEQUENCE {
  - action INTEGER {
  - dontPublish (0),
  - pleasePublish (1) },
  - pubInfos SEQUENCE SIZE (1..MAX) OF SinglePubInfo OPTIONAL }
  - SinglePubInfo ::= SEQUENCE {
  - pubMethod INTEGER {
  - dontCare (0),
  - x500 (1),
  - web (2),
  - ldap (3) },
  - pubLocation GeneralName OPTIONAL }

KIỂM SOÁT TÙY CHỌN LƯU TRỮ

- Tùy chọn pikArchiveOptions cho phép thuê bao được hỗ trợ thông tin cần thiết lập để lưu trữ khóa bí mật tương ứng với khóa công khai của yêu cầu CTS

KIỂM SOÁT OLDCERT ID

- OldCertID xác định chứng thư số được cập nhật bởi yêu cầu chứng thư số hiện tại
- OID và cú pháp của kiểm soát này là:
- id-regCtrl-oldCertID OBJECT IDENTIFIER ::= { id-regCtrl 5 }
- CertId ::= SEQUENCE {
- issuer GeneralName,
- serialNumber INTEGER
- }

KIỂM SOÁT KHÓA MÃ HÓA GIAO THỨC

- Kiểm soát protocolEncryKey xác định một khóa mà CA sử dụng để mã hóa phản hồi tới CertReqMessage
- OID cho kiểm soát này là id-regCtrl-protocolEncrKey
- Cấu trúc tham số cho trường này là SubjectPublicKeyInfo
  - id-regCtrl-protocolEncrKey OBJECT IDENTIFIER ::= { id-regCtrl 6 }
- Kiểm soát này được sử dụng khi CA có thông tin cần được mã hóa gửi tới thuê bao.
- Thông tin này có thể gồm khóa bí mật được sinh ra bởi CA sử dụng cho thuê bao.

KIỂM SOÁT REGINFO (REGINFO CONTROLS)

- Miêu tả trường regInfo trong cấu trúc CertReqMsg:
  - uft8Pairs
    - Kiểm soát này được dùng để truyền tải thông tin ký tự (text-based information) từ chủ thể tới RA tới CA cấp phát chứng thư số
    - OID cho cấu trúc id-regInfo-utf8Pairs và có kiểu UTF8String.
    - id-regInfo-utf8Pairs OBJECT IDENTIFIER ::= { id-regInfo 1 }
  - certReq
    - Được thiết kế để giải quyết vấn đề khi RA cần thay đổi mẫu CTS mà chủ thể đề xuất, nhưng chủ thể sử dụng mẫu CTS như một phần của kết quả tính toán POP.
    - một OID id-regInfo-certReq và cấu trúc CerRequest, và thuộc tính này chỉ nhìn thấy trong chuỗi regInfo
    - id-regInfo-certReq OBJECT IDENTIFIER ::= { id-regInfo 2 }

OBJECT IDENTIFIERS

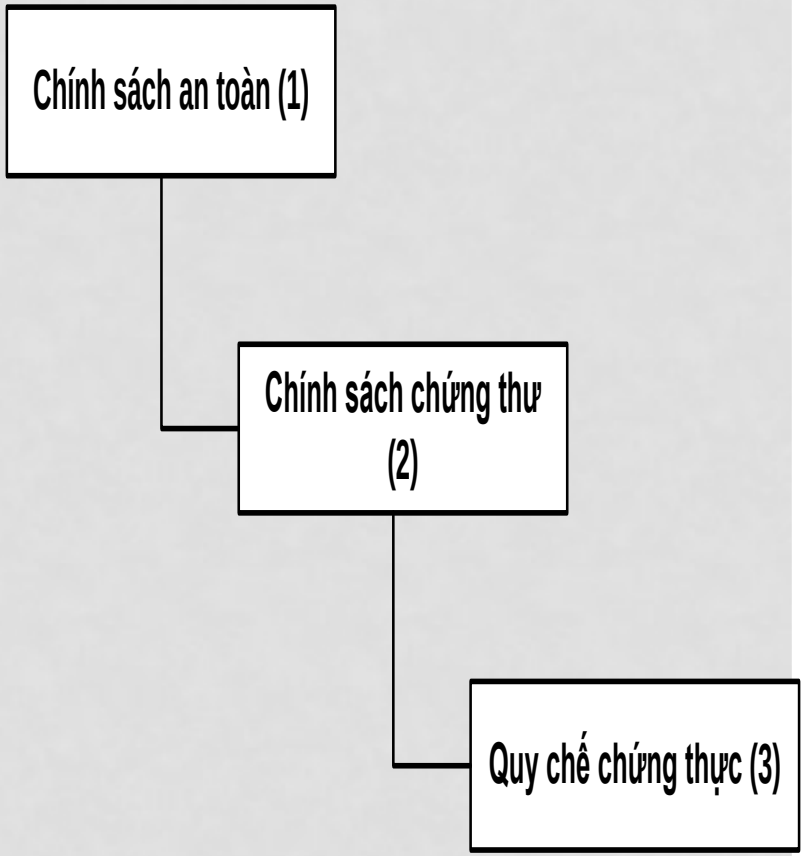
- OID id-pkix có giá trị:
- id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
- dod(6) internet(1) security(5) mechanisms(5) pkix(7) }
- -- arc cho giao thức PKI X509 và các thành phần
- id-pkip OBJECT IDENTIFIER :: { id-pkix pkip(5) }
- -- arc cho kiểm soát đăng ký trong CRMF
- id-regCtrl OBJECT IDENTIFIER ::= { id-pkip regCtrl(1) }
- -- arc cho thông tin đăng ký trong CRMF
- id-regInfo OBJECT IDENTIFIER ::= { id-pkip id-regInfo(2) }

5. NHÓM CHUẨN VỀ CHÍNH SÁCH

- Quy định 2 loại chính sách CP và CPS được mô tả trong RFC3647 – khung thực hành chứng thực và chính sách của PKI 2003-11
- Có 3 loại chính sách ảnh hưởng trực tiếp:
  - Chính sách an toàn
  - Chính sách chứng thư
  - Quy chế chứng thực

5. NHÓM CHUẨN VỀ CHÍNH SÁCH

- Mối quan hệ giữa các chính sách
  - Một tổ chức xây dựng chính sách an toàn để định nghĩa chuẩn an toàn cho tổ chức đó.
  - Chính sách chứng thư được phác thảo tuân thủ và phản ánh chính sách an toàn của tổ chức đó.
  - Quy chế chứng thực định nghĩa các thủ tục quản lý CA tuân thủ chính sách chứng thư



5. NHÓM CHUẨN VỀ CHÍNH SÁCH

- Chính sách chứng thư
- Quy chế chứng thực
- Mối quan hệ giữa chính sách chứng thư và quy chế chứng thực

CHÍNH SÁCH CHỨNG THƯ

- Chính sách chứng thư: là một tài liệu mô tả các biện pháp mà một tổ chức chứng thực sẽ sử dụng để kiểm tra danh tính của chủ thể chứng thư trước khi phát hành chứng thư và mục đích dự kiến của một chứng thư.
- Chính sách chứng thư (CP): là một tập các quy tắc xác định khả năng áp dụng của chứng thư cho một lĩnh vực nhất định hay cho một lớp các ứng dụng với các yêu cầu bảo mật chung

CHÍNH SÁCH CHỨNG THƯ

- Về mặt bản chất CP là một tài liệu mô tả (xác định) các yêu cầu cho các bên tham gia trong một miền PKI và xác định những gì các bên tham gia đó phải thực hiện.
- Chính sách được biểu diễn trong chứng thư số bằng một giá trị định danh đối tượng – OID kèm theo một con trỏ tới vị trí mô tả chính sách, trong trường Certificate Policies Extension. Mỗi chứng thư có thể được phát hành với một hay nhiều chính sách khác nhau.

CHÍNH SÁCH CHỨNG THƯ

- Sự cần thiết của chính sách chứng thư
  - Chính sách chứng thư cung cấp mức tin cậy xác định cho relying party quyết định có sử dụng chứng thư số hay không trong trường hợp cụ thể.
  - Chính sách chứng thư cũng là cơ sở cho hoạt động kiểm toán.
  - Xây dựng dựng lòng tin hay đánh giá về một CA

CHÍNH SÁCH CHỨNG THƯ

- Phân loại chính sách chứng thư:
  - Loại thứ nhất xác định khả năng áp dụng của chứng thư đối với một cộng đồng, khu vực nhất định.
  - Loại thứ hai xác định khả năng áp dụng của chứng thư đối với một lớp các ứng dụng với các mức yêu cầu bảo mật nhất định.

CHÍNH SÁCH CHỨNG THƯ

- Loại thứ nhất:
  - Loại chính sách này quy định trước các yêu cầu về việc sử dụng chứng thư và các yêu cầu về các thành viên của cộng đồng.
  - Ví dụ:
    - Yêu cầu về sử dụng chứng thư: ký, mã, xác thực…
    - Yêu cầu về thành viên: áp dụng cho một cộng đồng cùng chung một vùng địa lý (quốc gia), hoặc chính sách áp dụng cho các thành viên thực hiện dịch vụ tài chính.

CHÍNH SÁCH CHỨNG THƯ

- Loại thứ 2:
  - Loại chính sách này xác định trước một tập các ứng dụng hoặc mục đích (khả năng) sử dụng của chứng thư cần có một mức an toàn xác định. Sau đó xác định các yêu cầu phù hợp với ứng dụng hay mục đích sử dụng đó. CP thuộc
  - Loại này thường đưa ra tập các yêu cầu phù hợp với mức an toàn nhất định được cung cấp bởi CTS(lớp, loại).
  - Ví dụ chính sách xác định các mức an toàn cho chứng thư số từ thấp đến cao kèm theo các yêu cầu cụ thể cho từng mức (rudimentary, basic, medium, or high).

CHÍNH SÁCH CHỨNG THƯ - CP

- Nội dung của chính sách chứng thư (Certificate Policy)
  - Cách kiểm tra định danh (danh tính) người dùng trong quá trình đăng ký: form mẫu điền thông tin, gặp trực tiếp hay không, cách xác thực thông tin…
  - Mục đích dự kiến của chứng thư: xác thực, ký số (giá trị ?)
  - Yêu cầu của thiết bị lưu khóa bí mật: HSM hay file, phương thức bảo vệ truy nhập tới khóa…
  - Trách nhiệm của chủ thể sở hữu khóa bí mật khi khóa bí mật bị lộ hay mất: có lưu khóa bí mật của người dùng?.
  - Trách nhiệm, chính sách, thủ tục thu hồi chứng thư: Trường hợp thu hồi, quy trình, mẫu biểu

QUY CHẾ CHỨNG THỰC
CPS

- Là một tài liệu mô tả các biện pháp đảm bảo an toàn cho hoạt động của CA và quản lý các chứng thư đã phát hành của CA đó
- là bản tuyên bố chi tiết của thẩm quyền chứng thực (CA) về sự tin cậy trong hệ thống của nó và các quy trình hoạt động của CA và quản lý chứng thư (tạo, phát hành, thu hồi …)
- định nghĩa các biện pháp được thực hiện để đảm bảo an toàn cho vận hành CA, quản lý các chứng thư đã phát hành.
- Về bản chất CPS là một tài liệu định nghĩa cách thức các bên tham gia thực hiện chức năng của mình. Nó cũng được xem như là một bản giao ước giữa tổ chức quản lý CA và người dùng tin vào các chứng thư được phát hành bởi CA đó.

CPS

- Sự cần thiết của quy chế chứng thực
  - CPS cung cấp mức tin cậy xác định cho relying party quyết định có sử dụng chứng thư số hay không.
  - Vì CPS bản chất là tài liệu chỉ ra các biện pháp thực hiện yêu cầu của CP, mỗi tổ chức chứng thực khác nhau thì lại có các biện pháp thực hiện khác nhau do đó CPS thường được viết dùng riêng cho mỗi tổ chức nên đây chính là cơ sở để so sánh độ tin cậy giữa chứng thư của các tổ chứng chứng thực khác nhau.
  - Dựa vào CPS có thể đưa ra đánh giá chính xác hơn về độ tin cậy của CA so với dựa vào CP vì CP có thể được viết ra và dùng được cho nhiều miền PKI, CA khác nhau.

CPS

- Nội dung quy chế chứng thực gồm:
  - Một danh sách các CP mà nó hỗ trợ.
  - Với mỗi CP mà nó hỗ trợ, một tập các điều khoản được thiết lập chứa các quy trình tương ứng nhằm chỉ ra cách CPS này thực hiện các yêu cầu trong mỗi CP.
  - Một tập các quy định chứa quy trình liên quan đến vận hành CA không liên quan đến CP.

CP & CPS

- Mối quan hệ giữa chính sách chứng thư và quy chế chứng thực:
  - Sự giống nhau:
    - CP và CPS đều giải quyết các chủ đề về mối quan tâm của RP (relying party) đến cấp độ an toàn và mục tiêu của chứng thư số có nên tin cậy hay không.
    - CP và CPS đều do tổ chức vận hành CA ban hành.

CP & CPS

- Sự khác nhau:
  - Mục đích tài liệu: Mục đích của CP là xác định các bên tham gia cần phải thực hiện điều gì. Mục đích của CPS là chỉ ra cách các bên tham gia thực hiện chức năng và thi hành quyền của mình như thế nào.
  - Phạm vi của hai loại tài liệu: CP chỉ xác định các yêu cầu và chuẩn nên nó có thể được coi như một hướng dẫn hoạt động và thích hợp, áp dụng được với nhiều miền PKI, tổ chức, CA khác nhau. CPS xác định cách thức thực hiện của các bên tham gia nên nó chỉ áp dụng được với một miền PKI, tổ chức, CA cụ thể.
  - Mức chi tiết của các điều khoản: CPS chỉ ra cách thức thực hiện còn CP chỉ ra các yêu cầu nên CPS thường chi tiết hơn CP.

6. NHÓM CHUẨN VỀ DẤU THỜI GIAN VÀ CHỨNG THỰC DỮ LIỆU

- Các dịch vụ dấu thời gian và chứng thực dữ liệu được xây dựng bên trên các dịch vụ cơ bản của PKI. Dịch vụ chứng thực dữ liệu kiểm tra tính chính xác của dữ liệu gửi tới nó. Dịch vụ này gần giống như dịch vụ công chứng.
  - RFC 3161 – Giao thức dấu thời gian (TSP). 2001-08
  - RFC 3628 – Các yêu cầu chính sách cho Ủy quyền cấp dấu thời gian (TSAs). 2003-11.
  - RFC 5816 - ESSCertIDv2 bản cập nhật cho RFC 3161.2010-04.
- Phần này sẽ trình bày về các yêu cầu chính sách cho ủy quyền cấp dấu thời gian (TSAs)

6. NHÓM CHUẨN VỀ DẤU THỜI GIAN VÀ CHỨNG THỰC DỮ LIỆU

- Giới thiệu
- Khái niệm chung
- Các chính sách gắn dấu thời gian
- Nghĩa vụ và trách nhiệm
- Các yêu cầu về nghiệp vụ TSA
- Những xem xét đến an ninh

GIỚI THIỆU

- Để tạo ra bằng chứng số đáng tin cậy và có thể quản lý, cần thiết phải thoả thuận phương pháp liên kết dữ liệu thời gian và giao dịch để có thể so sánh với nhau về sau.
- Một giao dịch điển hình là một tài liệu kỹ thuật số đã ký, mà cần thiết để chứng minh rằng chữ ký số của người ký được áp dụng khi chứng nhận cho người ký là hợp lệ
- Dấu thời gian hoặc đánh dấu thời gian
  - Đó là một hồ sơ kiểm tra được lưu giữ trong một biên bản kiểm tra an toàn từ một bên thứ ba đáng tin cậy
  - Được áp dụng đối với giá trị chữ ký số, chứng tỏ rằng chữ ký số được tạo ra trước ngày in trong dấu thời gian.

GIỚI THIỆU

- Để chứng tỏ chữ ký số được tạo ra khi Giấy chứng nhận của người ký là hợp lệ, chữ ký số phải được kiểm tra, thẩm định và thỏa mãn các điều kiện sau đây:
  - Dấu thời gian được áp dụng trước khi kết thúc hiệu lực giấy chứng nhận của người ký.
  - Dấu thời gian được áp dụng hoặc khi Giấy chứng nhận của người ký không bị thu hồi hoặc trước ngày thu hồi giấy chứng nhận.
- Vì vậy, một dấu thời gian được áp dụng theo cách này chứng tỏ rằng chữ ký số được tạo ra khi giấy chứng nhận (CTS) của người ký là hợp lệ. Điều này chứng tỏ tính hợp lệ của một chữ ký số trong toàn bộ bất kể chuỗi chứng nhận nào.

KHÁI NIỆM CHUNG

- Các dịch vụ gắn dấu thời gian
- Cơ quan gắn đấu thời gian –TSA
- Thuê bao
- Chính sách gắn dấu thời gian và nội dung nghiệp vụ TSA

KHÁI NIỆM CHUNG

- Các dịch vụ gắn dấu thời gian:
  - Cung cấp dịch vụ gắn dấu thời gian: dịch vụ này tạo ra mật mã dấu thời gian.
  - Quản lý gắn dấu thời gian: Các thành phần dịch vụ điều hành và kiểm soát hoạt động của các dịch vụ gắn dấu thời gian để đảm bảo rằng dịch vụ này được cung cấp theo quy định của TSA. Thành phần dịch vụ này chịu trách nhiệm cài đặt và giảm cài đặt việc cung cấp dịch vụ gắn dấu thời gian.

KHÁI NIỆM CHUNG

- Cơ quan gắn dấu thời gian (TSA - thẩm quyền dấu thời gian):
  - Được ủy thác bởi người sử dụng các dịch vụ dấu thời gian (các bên tin tưởng và thuê bao)
  - Chịu trách nhiệm tổng thể về các dịch vụ dấu thới gian
  - Có trách nhiệm với các hoạt động của một hoặc nhiều TSU (ĐƠn vị gắn dấu thời gian), tạo ra và ký thay mặt TSA
  - Chịu trách nhiệm cấp mật mã dấu thời gian có thể nhận dạng được.

KHÁI NIỆM CHUNG

- Cơ quan gắn dấu thời gian (TSA):
  - Có thể sử dụng các bên khác để cung cấp các dịch vụ gắn dấu thời gian
  - TSA luôn luôn duy trì chịu trách nhiệm tổng thể và đảm bảo rằng các yêu cầu chính sách được quy định trong phần này được đáp ứng
  - TSA có thể điều hành hoạt động của một số đơn vị gắn dấu thời gian có thể nhận dạng được. Mỗi đơn vị có một khóa khác nhau
  - khóa và các khóa bí mật (private key) được sử dụng để tạo ra mật mã dấu thời gian thuộc TSA

KHÁI NIỆM CHUNG

- Thuê bao:
  - có thể là một tổ chức, bao gồm một số người sử dụng cuối cùng hoặc cá nhân người sử dụng cuối
  - Khi thuê bao là một tổ chức, một số nghĩa vụ mà áp dụng đối với tổ chức đó cũng sẽ được áp dụng cho người sử dụng cuối cùng.
  - Khi thuê bao là người sử dụng cuối cùng, họ sẽ chịu trách nhiệm trực tiếp nếu các nghĩa vụ không được hoàn thành đầy đủ

KHÁI NIỆM CHUNG

- Chính sách gắn dấu thời gian và nội dung nghiệp vụ TSA
  - Mô tả vai trò tương đối của các chính sách gắn dấu thời gian và nội dung nghiệp vụ TSA
  - Mối quan hệ giữa chính sách gắn dấu thời gian và nội dung nghiệp vụ TSA về bản chất là tương tự như mối quan hệ của các chính sách kinh doanh khác, trong đó nêu các yêu cầu của doanh nghiệp, trong khi các đơn vị hoạt động xác định các công việc và các thủ tục để làm sao cho các chính sách này được thực hiện.

CÁC CHÍNH SÁCH GẮN DẤU THỜI GIAN

- Một chính sách gắn dấu thời gian là một "bộ các quy tắc cho biết tính khả dụng của một dấu thời gian cho một cộng đồng cụ thể và/hoặc lớp ứng dụng với những yêu cầu an ninh chung
- TSA có thể quy định chính sách riêng để tăng cường chính sách của mình được quy định.
  - Nếu độ chính xác của TSA tốt hơn 1 giây và nếu tất cả các TSUs có đặc điểm giống nhau, thì tính chính xác sẽ được quy định trong nội dung công khai của TSA, mỗi mật mã dấu thời gian được cấp với độ chính xác hơn 1 giây.

CÁC CHÍNH SÁCH GẮN DẤU THỜI GIAN

- Sự phù hợp:
  - Chính sách này có thể được sử dụng cho các dịch vụ gắn dấu thời gian công cộng hoặc các dịch vụ gắn dấu thời gian được sử dụng trong một cộng đồng khép kín
  - Các yêu cầu cho việc sử dụng định danh chính sách gắn dấu thời gian:
    - a) nếu TSA nêu ra sự phù hợp cho chính sách gắn dấu thời gian được nhận dạng và sẵn có cho thuê bao và các bên tin tưởng khi yêu cầu bằng chứng hỗ trợ về sự phù hợp;
    - b) nếu TSA đã được đánh giá phù hợp với chính sách gắn dấu thời gian bởi một bên độc lập

NGHĨA VỤ VÀ TRÁCH NHIỆM

- Các nghĩa vụ TSA
  - Đảm bảo tất cả các yêu cầu về TSA, được thực hiện phù hợp với chính sách gắn dấu thời gian ủy thác đã lựa chọn.
  - Đảm bảo sự phù hợp với các thủ tục quy định tại chính sách này.
  - Tuân thủ bất kỳ nghĩa vụ bổ sung được nêu ra trong dấu thời gian hoặc trực tiếp hoặc kết hợp bởi sự tham chiếu.
  - Cung cấp tất cả các dịch vụ gắn dấu thời gian phù hợp với nội dung nghiệp vụ TSA.
  - Đáp ứng các yêu cầu như được đưa ra trong các điều khoản và điều kiện bao gồm cả sự sẵn có và tính chính xác của dịch vụ.

NGHĨA VỤ VÀ TRÁCH NHIỆM

- Các nghĩa vụ của thuê bao
  - không quy định nghĩa vụ cụ thể cho thuê bao
- Các nghĩa vụ của bên tin tưởng
  - Các điều khoản và điều kiện cho các bên tin tưởng gồm một nghĩa vụ cho bên tin tưởng rằng, khi tin cậy vào một mật mã dấu thời gian, thì mật mã dấu thời gian sẽ:
    - a) Xác nhận rằng mật mã dấu thời gian đã được ký một cách chính xác và khóa bí mật (private key) được sử dụng để ký dấu thời gian vẫn chưa bị lộ cho đến thời điểm được kiểm tra;
    - b) Cân nhắc bất kỳ hạn chế về việc sử dụng dấu thời gian được quy định trong chính sách gắn dấu thời gian;
    - c) Cân nhắc bất kỳ biện pháp phòng ngừa nào khác theo quy định trong các thỏa thuận hoặc bất kể đâu.

NHỮNG YÊU CẦU VỀ NGHIỆP VỤ TSA

- TSA sẽ thực hiện kiểm soát đáp ứng những yêu cầu sau đây:
  - Những yêu cầu chính sách này không có nghĩa là bao hàm bất kỳ sự hạn chế nào về việc tính phí cho các dịch vụ TSA.
  - Các yêu cầu được quy định về mặt an ninh,
  - Các yêu cầu cụ thể hơn cho việc kiểm soát để đáp ứng những mục tiêu này cần thiết để tin rằng những mục tiêu này sẽ được đáp ứng.
  - Việc cung cấp một mật mã dấu thời gian đáp ứng các yêu cầu theo quyết định của TSA phụ thuộc vào bất kể thỏa thuận nào về mức độ dịch vụ nào với thuê bao

NHỮNG YÊU CẦU VỀ NGHIỆP VỤ TSA

- Nội dung nghiệp vụ và nội dung công khai TSA
- Vòng đời quản lý khóa
- Dấu thời gian
- Quản lý và hoạt động của TSA
- Tổ chức

NỘI DUNG NGHIỆP VỤ VÀ NỘI DUNG CÔNG KHAI TSA

- Nội dung nghiệp vụ TSA: TSA phải đảm bảo cho thấy được sự tin cậy cần thiết khi cung cấp dịch vụ gắn dấu thời gian.
  - a) TSA có trách nhiệm đánh giá rủi ro được thực hiện để đánh giá các tài sản kinh doanh và các mối đe dọa đến tài sản để quyết định khả năng kiểm soát an ninh cần thiết và các quy trình hoạt động.
  - b) TSA có một nội dung nghiệp vụ và các quy trình được sử dụng để giải quyết tất cả các yêu cầu được quy định trong chính sách dấu thời gian.
  - c) Nội dung nghiệp vụ TSA quy định các nghĩa vụ của tất cả các tổ chức bên ngoài hỗ trợ các dịch vụ TSA bao gồm cả các chính sách và nghiệp vụ ứng dụng.

NỘI DUNG NGHIỆP VỤ VÀ NỘI DUNG CÔNG KHAI TSA

- Nội dung nghiệp vụ TSA
  - d) Nội dung nghiệp vụ TSA sẽ sẵn có cho thuê bao và các bên tin tưởng, và các tài liệu liên quan khác cần thiết để đánh giá sự phù hợp về chính sách gắn dấu thời gian.
  - e) TSA sẽ công khai cho tất cả thuê bao và bên tin tưởng về các điều khoản và điều kiện liên quan đến việc sử dụng dấu thời gian
  - f) Các TSA phải có cơ quan quản lý cấp cao với thẩm quyền phê duyệt nội dung nghiệp vụ TSA cuối cùng.

NỘI DUNG NGHIỆP VỤ VÀ NỘI DUNG CÔNG KHAI TSA

- Nội dung nghiệp vụ TSA
  - g) Việc quản lý cấp cao của TSA sẽ đảm bảo rằng các nghiệp vụ TSA được triển khai thực hiện đúng đắn.
  - h) Các TSA sẽ quy định một quá trình xem xét nghiệp vụ này bao gồm cả trách nhiệm duy trì nội dung nghiệp vụ TSA.
  - i) Các TSA phải thông báo nếu dự định thay đổi nội dung nghiệp vụ và theo phê duyệt như phần (f) ở trên, tạo cho nghiệp vụ TSA đã được sửa đổi ngay lập tức có sẵn như được yêu cầu trong phần (d) ở trên.

NỘI DUNG NGHIỆP VỤ VÀ NỘI DUNG CÔNG KHAI TSA

- Nội dung công khai TSA:
  - TSA được tiết lộ cho tất cả thuê bao và các bên tin tưởng tiềm năng các điều khoản và điều kiện về việc sử dụng các dịch vụ gắn dấu thời gian.
  - Nội dung này sẽ quy định cụ thể cho mỗi chính sách gắn dấu thời gian được hỗ trợ bởi TSA:

NỘI DUNG NGHIỆP VỤ VÀ NỘI DUNG CÔNG KHAI TSA

- Nội dung công khai TSA:
  - Các thông tin liên lạc TSA.
  - Chính sách gắn dấu thời gian được áp dụng.
  - Có ít nhất một thuật toán băm có thể được sử dụng để đại diện cho dữ liệu dấu thời gian. (Không thuật toán băm nào được uỷ quyền).
  - Thời gian tồn tại của chữ ký được sử dụng để ký mật mã dấu thời gian (phụ thuộc vào các thuật toán băm được sử dụng, thuật toán chữ ký được sử dụng và chiều dài khóa bí mật.

NỘI DUNG NGHIỆP VỤ VÀ NỘI DUNG CÔNG KHAI TSA

- Nội dung công khai TSA:
  - Độ chính xác của thời gian trong mật mã dấu thời gian đối với giờ UTC.
  - Bất kỳ hạn chế nào về việc sử dụng các dịch vụ gắn dấu thời gian.
  - Các nghĩa vụ của thuê bao và Các nghĩa vụ của bên tin tưởng dựa theo định nghĩa trong phần trên.
  - Thông tin về việc làm thế nào để thẩm định mật mã dấu thời gian, bên tin tưởng được coi là "tin tưởng một cách hợp lý" vào các mật mã dấu thời gian và bất kỳ những hạn chế có thể trong thời gian hiệu lực.

NỘI DUNG NGHIỆP VỤ VÀ NỘI DUNG CÔNG KHAI TSA

- Nội dung công khai TSA
  - Khoảng thời gian mà trong đó các bản ghi sự kiện TSA được lưu giữ lại.
  - Hệ thống pháp luật ứng dụng, bao gồm bất cứ yêu cầu bồi thường nào để đáp ứng yêu cầu của dịch vụ gắn dấu thời gian theo quy định của pháp luật nhà nước.
  - Những hạn chế về trách nhiệm.
  - Thủ tục khiếu nại và giải quyết tranh chấp.
  - Nếu TSA đã được đánh giá là tuân thủ chính sách gắn dấu thời gian, và nếu như vậy thì bởi cơ quan độc lập nào.

VÒNG ĐỜI QUẢN LÝ KHÓA

- Tạo hệ khóa TSA
  - TSA phải đảm bảo bất kỳ các khóa mật mã được tạo ra trong trường hợp được kiểm soát.
  - Việc tạo ra các khóa ký của TSU được thực hiện trong một môi trường đảm bảo an toàn của cá nhân trong vai trò đáng tin cậy
  - Việc tạo ra khóa ký của TSU được thực hiện trong một module mã hóa

VÒNG ĐỜI QUẢN LÝ KHÓA

- Bảo vệ khóa riêng TSU :
  - TSA sẽ đảm bảo rằng các private key TSU được giữ kín và duy trì tính toàn vẹn của chúng
  - Khóa ký TSU được tổ chức và sử dụng trong một module mã hóa
  - Khóa này sẽ được sao lưu, khôi phục bởi cá nhân có vai trò tin cậy
  - Bất kỳ bản sao lưu của khóa ký riêng TSU sẽ được bảo vệ để đảm bảo tính bảo mật bằng module mật mã trước khi được lưu trữ bên ngoài thiết bị đó.

VÒNG ĐỜI QUẢN LÝ KHÓA

- Phân phối khóa công cộng TSU:
  - TSA đảm bảo tính toàn vẹn và tính xác thực của khóa thẩm định chữ ký TSU và các thông số liên quan được duy trì trong quá trình phân phối.
    - a) Khóa thẩm định chữ ký TSU sẽ sẵn có cho các bên tin tưởng trong chứng thực khóa công khai.
    - b) Thẩm định chữ ký của TSU, chứng nhận khóa sẽ được cấp bởi CA hoạt động theo chính sách chứng thực cung cấp một mức độ bảo mật tương đương, hoặc cao hơn chính sách gắn dấu thời gian này.

VÒNG ĐỜI QUẢN LÝ KHÓA

- Tạo lại khóa TSU
  - Vòng đời của chứng thực khóa TSU sẽ không dài hơn khoảng thời gian mà thuật toán được lựa chọn và chiều dài khóa được công nhận là phù hợp với mục đích

VÒNG ĐỜI QUẢN LÝ KHÓA

- Kết thúc vòng đời khóa TSU:
  - TSA sẽ đảm bảo rằng các khóa ký TSU riêng không được sử dụng khi kết thúc vòng đời.
  - Các quy trình hoạt động hoặc kỹ thuật sẽ được thực hiện để đảm bảo một khóa mới được thay thế khi một khóa TSU hết hạn.
  - Các khóa ký riêng TSU, hoặc bất kể phần khóa nào, bao gồm bản sao bất kỳ phải được phá hủy để các khóa bí mật (private key) không thể được phục hồi.
  - Hệ thống tạo TST sẽ từ chối bất kỳ nỗ lực nào để cấp TSTs nếu khóa ký riêng đã hết hạn.

VÒNG ĐỜI QUẢN LÝ KHÓA

- Quản lý vòng đời của module mã hóa được dùng để ký dấu thời gian
  - TSA phải đảm bảo sự an toàn của phần cứng mã hóa trong suốt vòng đời.
  - Các yêu cầu TSA cần phải đảm bảo:
    - Phần cứng mã hóa ký dấu thời gian ko bị giả mạo khi vận chuyển;
    - Phần cứng mã hóa ký dấu thời gian không phải là giả mạo trong khi lưu trữ;
    - Cài đặt, kích hoạt và sao chép các khóa ký của TSU trong phần cứng mã hóa sẽ được thực hiện chỉ bởi các cá nhân có vai trò tin cậy.
    - Phần cứng mã hóa ký dấu thời gian đang hoạt động chính xác; và
    - Khóa ký riêng TSU được lưu trữ trên mô-đun mã hóa TSU bị xóa khi thiết bị hết hạn.

VÒNG ĐỜI QUẢN LÝ KHÓA

- Quản lý vòng đời của mô đun mã hóa
  - Các yêu cầu:
    - Phần cứng mã hóa ký dấu thời gian không bị giả mạo trong khi vận chuyển;
    - Phần cứng mã hóa ký dấu thời gian không phải là giả mạo trong khi lưu trữ;
    - Cài đặt, kích hoạt và sao chép các khóa ký của TSU trong phần cứng mã hóa chỉ được thực hiện bởi các cá nhân có vai trò tin cậy.
    - Phần cứng mã hóa ký dấu thời gian hoạt động chính xác;
    - Khóa ký riêng TSU được lưu trữ trên mô-đun mã hóa TSU bị xóa khi thiết bị hết hạn.

DẤU THỜI GIAN

- Mật mã dấu thời gian:
  - TSA sẽ đảm bảo rằng mật mã dấu thời gian được cấp một cách an toàn và bao gồm thời gian chính xác.
  - Mỗi mật mã dấu thời gian sẽ có một định danh duy nhất
- Đồng bộ hóa đồng hồ với giờ UTC:
  - TSA phải đảm bảo rằng đồng hồ được đồng bộ với giờ UTC trong phạm vi chính xác đã được tuyên bố.
  - Hồ sơ được duy trì về độ chính xác của thời gian (trong phạm vi chính xác đã được tuyên bố) khi thay đổi này xảy ra.

QUẢN LÝ VÀ HOẠT ĐỘNG CỦA TSA

- Quản lý an ninh
  - TSA phải đảm bảo rằng các thủ tục hành chính và quản lý được áp dụng là phù hợp và tương ứng với nghiệp vụ đã được công nhận.
- An ninh nhân sự
  - TSA sẽ đảm bảo rằng thông lệ tuyển dụng và nhân sự sẽ tăng cường và hỗ trợ lòng tin cho các hoạt động của TSA.
- An ninh môi trường và vật lý
  - TSA phải đảm bảo rằng việc tiếp cận về mặt vật lý với các dịch vụ quan trọng được kiểm soát và rủi ro vật lý đến các tài sản của TSA được giảm thiểu.

QUẢN LÝ VÀ HOẠT ĐỘNG CỦA TSA

- Quản lý hoạt động
  - TSA phải đảm bảo rằng các thành phần hệ thống TSA phải an toàn và hoạt động một cách chính xác, với rủi ro hỏng hóc ít nhất:
  - Các hoạt động này sẽ được quản lý bởi nhân viên TSA tin cậy, nhưng có thể thực sự được thực hiện bởi các phi chuyên gia, nhân viên hoạt động (dưới sự giám sát), như quy định trong chính sách an ninh thích hợp, các vai trò và các văn bản trách nhiệm.

QUẢN LÝ VÀ HOẠT ĐỘNG CỦA TSA

- Quản lý truy cập vào hệ thống
  - TSA đảm bảo việc truy cập vào hệ thống TSA được giới hạn đúng cho các cá nhân được ủy quyền.
- Bảo trì và triển khai các hệ thống tin cậy
  - TSA sẽ sử dụng các hệ thống và các sản phẩm tin cậy được bảo vệ để tránh bị sửa đổi.
- Tiết lộ các dịch vụ TSA.
  - TSA phải đảm bảo trong trường hợp có sự ảnh hưởng đến các dịch vụ an ninh của TSA, bao gồm cả sự thỏa hiệp khóa ký cá nhân của TSU hoặc tổn hại được phát hiện của hiệu chuẩn.

QUẢN LÝ VÀ HOẠT ĐỘNG CỦA TSA

- Chấm dứt TSA
  - TSA đảm bảo rằng sự gián đoạn tiềm ẩn cho các thuê bao và bên tin tưởng được giảm thiểu, kết quả cho sự chấm dứt dịch vụ dấu thời gian TSA, và đặc biệt là đảm bảo duy trì liên tục những thông tin cần thiết để xác minh tính đúng đắn của mật mã dấu thời gian.
- Tuân thủ các yêu cầu pháp lý
- Lưu lại các thông tin liên quan đến hoạt động của dịch vụ gắn dấu thời gian
  - TSA đảm bảo rằng tất cả các thông tin liên quan đến hoạt động của dịch vụ gắn dấu thời gian phải được lưu lại trong một khoảng thời gian xác định

TỔ CHỨC

- TSA đảm bảo rằng tổ chức là đáng tin cậy.
  - a) Chính sách và thủ tục hoạt động đồng bộ.
  - b) TSA làm cho dịch vụ của mình dễ dàng truy cập vào cho tất cả các đối tượng có các hoạt động thuộc trong lĩnh vực đã kê khai và đồng ý tuân thủ các nghĩa vụ theo quy định của các nội dung công khai TSA.
  - c) TSA là một thực thể pháp lý theo luật pháp quốc gia.

TỔ CHỨC

- TSA đảm bảo rằng tổ chức là đáng tin cậy
  - d) TSA có một hệ thống hoặc hệ thống chất lượng và quản lý bảo mật thông tin thích hợp cho các dịch vụ gắn dấu thời gian mà nó cung cấp.
  - e) TSA có sự sắp xếp đầy đủ để trang trải các khoản nợ phát sinh từ các hoạt động của nó và / hoặc hoạt động.
  - f) Có sự ổn định tài chính và nguồn lực cần thiết để hoạt động phù hợp với chính sách này.

TỔ CHỨC

- g) Thuê một số lượng đầy đủ các nhân viên có giáo dục, đào tạo, kiến thức và kinh nghiệm kỹ thuật liên quan đến loại, phạm vi và khối lượng công việc cần thiết để cung cấp dịch vụ gắn dấu thời gian.
- h) Có chính sách và thủ tục giải quyết khiếu nại và tranh chấp nhận được từ khách hàng hoặc các bên khác về việc cung cấp các dịch vụ gắn dấu thời gian hoặc bất kỳ vấn đề nào khác có liên quan.
- i) Có thỏa thuận tài liệu và mối quan hệ hợp đồng tại nơi mà việc cung cấp các dịch vụ liên quan đến hợp đồng phụ, thuê ngoài hoặc các thỏa thuận với bên thứ ba khác.

NHỮNG XEM XÉT ĐẾN AN NINH

- Khi thẩm định mật mã dấu thời gian, cần đảm bảo rằng các chứng thực TSU là đáng tin cậy và không bị thu hồi
- Khi áp dụng dấu thời gian cho các ứng dụng, cần phải xem xét cả sự an toàn của ứng dụng.
- Và đảm bảo tính toàn vẹn của dữ liệu được duy trì trược khi dấu thời gian được áp dụng