[Câu 1. Các nguy cơ tiềm ẩn trong môi trường điện tử và giải pháp cho từng nguy cơ 2](#_Toc359369088)

[Câu 2. Hỗ trợ ứng dụng: Mô hình đăng nhập một lần 2](#_Toc359369089)

[Câu 3: Ý nghĩa của Tem thời gian trong PKI: 3](#_Toc359369090)

[Câu 4 a, PKI có những dịch vụ cốt lõi? TRình bày hiểu biết về dịch vụ xác thực. 4](#_Toc359369091)

[Câu 6 Vẽ mô hình quản lý vòng đời khóa/ chứng chỉ. Trình bày quá trình hết hạn chứng chỉ và hủy bỏ chứng chỉ trong giai đoạn hủy bỏ. 9](#_Toc359369092)

[Câu 7 có mấy loại mô hình tin cậy trong PKI? Trình bày mô hình mạng lưới. 13](#_Toc359369093)

[Cau 7.2 có mấy loại mô hình tin cậy trong PKI ? cái nay trong slide của ong thầy (bài 4 slide5) đọc xem thế nào phản hồi. ko biết là 3 hay 7 nữa. 16](#_Toc359369094)

[Câu 7.2 Hủy bỏ chứng chỉ (làm thêm thôi) 21](#_Toc359369095)

[Câu 8 PKI trong thực tế : 23](#_Toc359369096)

[Câu 9 Tương lai của PKI: nguyên nhân và hướng phát triển 26](#_Toc359369097)

[Câu 10 Trình bày thiết kế chi tiết kiến trúc phân cấp PKI với các mức phân cấp CA 27](#_Toc359369098)

[Câu 11. Trong khuôn dạng CRL của X.509 có các trường mở rộng sau: Các trường mở rộng chung, các điểm phân tán CRL, các Delta-CRL, các CRL gián tiếp và việc treo chứng chỉ. Vậy Delta-CRL là gì? Việc sử dụng Delta-CRL có ý nghĩa như thế nào? 28](#_Toc359369099)

[Câu 12. Minh họa khuân dạng chứng chỉ X.509 ver 3. Vì sao khuân dạng X.509 v1 và v2 không đáp ứng được tất cả các yêu cầu? giải thích việc bổ sung một số trường V3) 31](#_Toc359369100)

[Câu 13: Những vấn đề có thể gặp phải khi triển khai một hệ thống PKI?Vì sao lại xảy ra những vấn đề đó? 33](#_Toc359369101)

[Câu 14 Chữ ký số: định nghĩa, thuộc tính và yêu cầu của một chữ ký số(bài 2 –52) 35](#_Toc359369102)

[Câu 15: Trình bày hiểu biết về các giao thức của PKI? 35](#_Toc359369103)

[Câu 16.Xác thực mạnh () 35](#_Toc359369104)

[Câu 17.Hiểu biết về hộ chiếu điện tử 35](#_Toc359369105)

# **Câu 1. Các nguy cơ tiềm ẩn trong môi trường điện tử và giải pháp cho từng nguy cơ**

\*\*Các nguy cơ tiềm ẩn trong môi trường giao dịch điện tử:

-Bảo mật => Nghe trộm

-Toàn vẹn => Sửa đổi dữ liệu

-Xác thực => Giả mạo

-Chống chối bỏ =>Chối bỏ trách nhiệm

\*\*Các giải pháp:

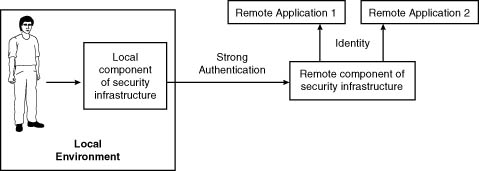
-Bảo mật => Mã hóa dữ liệu

-Toàn vẹn => Hàm băm, chữ ký số

-Xác thực => Chứng chỉ số, chữ ký số

-Chống chối bỏ => Chữ ký số, nhật ký

Câu 2. Hỗ trợ ứng dụng: Mô hình đăng nhập một lần

****

Đăng nhập một lần (SSO – single sign on) cho phép đăng nhập cùng một id/password để đăng nhập nhiều ứng dụng trong cùng một tổ chức. Sự đăng nhập này có thể kết nối tới rất nhiều các thiết bị ở xa, do đó sẽ loại bỏ được yếu tố cần phải đăng nhập nhiều lần. Tuy nhiên đăng nhập một lần cũng có thể được kết hợp với các cơ chế kiểm soát truy cập khác. Đứng trên quan điềm tiện dụng thì đăng nhập một lần rất được mong muốn vì người dùng chỉ phải nhớ một vài mật khẩu và chỉ cần phải biết thủ tục một lần để truy cập tới nhiều hệ thống. Đứng trên quan điểm an ninh thì đây là điều cũng được mong muốn bởi vì các mật khẩu được truyền qua mạng với tần suất ít hơn.

Mô hình đăng nhập một lần có những lợi điểm cho người dùng và người quản trị như sau:

-Dễ sử dụng

-Mật khẩu chỉ giới hạn trong máy nội bộ

-Việc quản lý được đơn giản hóa

-Kiểm soát truy nhập không bị ảnh hưởng

-Dể sử dụng: khách hàng có thể đăng nhập một lần và có quyền truy nhập tới mọi máy chủ mà người này được trao quyền mà không bị ngắt đoạn bởi các yêu cầu về mật khẩu.

-Mật khẩu chỉ giới hạn trong máy nội bộ: Để đăng nhập, người dùng gõ mật khẩu bảo vệ bởi cơ sở dữ liệu khóa công khai trên máy nội bộ, mật khẩu không gửi qua mạng.

-Việc quản lý được đơn giản hóa: Người quản trị có thể kiểm soát các máy chủ được phép truy nhập bằng cách kiểm soát các danh sách cơ quan chứng thực được duy trì bởi phần mềm của máy khách và máy chủ. Những danh sách này ngắn hơn những danh sách tên người dùng, mật khẩu và không thường xuyên thay đổi.

-Kiểm soát truy nhập không bị ảnh hưởng: Đăng nhập một lần liên quan đến thay thế các cơ chế xác thực máy khách mà không liên quan đến các cơ chế kiểm soát truy nhập. Người quản trị không cần thiết thay đổi những ACL hiện có mà ban đầu đã được thiết lập cho mục đích xác thực cơ bản.

# **Câu 3: Ý nghĩa của Tem thời gian trong PKI:**

* Tem 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 tem thời gian được liên kết với dữ liệu là xác thực và có tính toàn vẹn,
* Dịch vụ tem thời gian an toàn có thể sử dụng các dịch vụ cốt lõi của PKI.
* Phải có một nguồn cung cấp thời gian được tin cậy,
* Nguồn cung cấp thời gian này còn được gọi là thẩm quyền thời gian được tin cậy,
* Không yêu cầu chỉ có 1 thẩm quyền thời gian duy nhất cho dịch vụ này, có thể mỗi môi trường cục bộ có 1
* Giải pháp thường được chọn là chỉ có 1 số rất ít dịch vụ thời gian an toàn trong mạng (có thể chỉ 1),
* Dịch vụ tem thời gian an toàn sử dụng các dịch vụ cốt lõi của PKI về xác thực và toàn vẹn,
* Tem thời gian bao gồm chữ ký số trên tổ hợp của:
  + dữ liệu biểu diễn thời gian,
  + giá trị băm của chính tài liệu
* Các thực thể PKI liên quan cần biết và tin cậy bằng chứng khóa công khai của dịch vụ tem thời gian,
  + Để chữ ký trên tem thời gian có thể được kiểm tra và tin cậy;
* Tất cả các tem thời gian được ký bằng khóa không tin cậy được xem là không hợp lệ./.
* **Ý nghĩa của Tem thời gian trong PKI**
* Một phần tử quan trọng trong việc hỗ trợ cho các dịch vụ không chối bỏ là việc sử dụng của tem 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 (tức là, máy chủ tem thời gian an toàn mà chứng chỉ của nó là được kiểm tra bởi cộng đồng có liên quan những người dùng 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 tem thời gian trong nhiều môi trường
* Nhãn thời gian T phê chuẩn sự lưu hành của chứng chỉ
* Sử dụng khi khóa riêng của A bị lộ
* Đảm bảo rằng không phải thông báo cũ mà là thông báo có chứa khóa công khai hiện thời của B
* Đồng thời chỉ ra thời hạn kết thúc của chứng chỉ

# **Câu 4 a, PKI có những dịch vụ cốt lõi? TRình bày hiểu biết về dịch vụ xác thực.**

PKI được kết hợp từ 3 dịch vụ cơ bản sau

Xác thực (Authentication),

Toàn vẹn (Integrity),

Bảo mật (Confidentiality)

* **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:
* Định danh thực thể: Phục vụ cho việc định danh một thực thể xác định,
* Định danh nguồn gốc dữ liệu: Định danh một thực thể như là nguồn gốc hoặc xuất phát điểm của một mẫu dữ liệu
* Hai kiểu xác thực: Cục bộ và ở xa
  + **Xác thực cục bộ:**
* Xác thực một thực thể với môi trường cục bộ,
* Luôn đòi hỏi người dùng tham gia trực tiếp
  + **Xác thực ở xa:**
* Xác thực một thực thể với môi trường ở xa,
* Có thể không cần tới sự tham gia trực tiếp của người dùng;

=>> Khó bảo vệ dữ liệu nhạy cảm và không thuận tiện cho người dùng khi nhập vào thông tin xác thực nhiều lần

* Xác thực từ xa dựa trên PKI có 3 lợi ích:
* Giảm được sự phức tạp của việc phân phối trước khóa dùng chung,
* Dữ liệu xác thực nhạy cảm không phải truyền trên mạng,
* Khả năng đăng nhập một lần;
* Công nghệ khóa công khai được sử dụng để thực hiện việc xác thực sử dụng giao thức Yêu cầu/Đáp ứng và các thông điệp được ký
* **Toàn vẹn dữ liệu**
* Đảm bảo dữ liệu không bị thay đổi, nếu có thay đổi thì bị phát hiện,
* Cần một hệ thống có khả năng phát hiện những thay đổi dữ liệu trái phép,
* Giúp cho người nhận dữ liệu xác minh được rằng dữ liệu không bị thay đổi
* Các kỹ thuật mật mã được sử dụng trong toàn vẹn dữ liệu ,
* Thường có sự thỏa thuận về các thuật toán và khóa thích hợp giữa 2 bên,
* Dịch vụ PKI về toàn vẹn thỏa mãn lợi ích của cả 2 bên:
* Qua đó việc thỏa thuận về thuật toán và khóa được thực hiện,
* Hoàn toàn trong suốt
* **Bảo mật**
* Đảm bảo tính bí mật của dữ liệu:
* Không ai có thể đọc được nội dung của dữ liệu ngoại trừ những người dùng định trước;
* Các dữ liệu nhạy cảm đều cần được bảo mật.
* Thường được yêu cầu khi:
* Dữ liệu được lưu trên phương tiện dễ bị đọc bởi những người dùng không được quyền,
* được lưu trên thiết bị có thể bị rơi vào tay những người không được phép,
* được truyền trên các mạng không được bảo vệ.
* Để đảm bảo tính bí mật, các thuật toán thích hợp và khóa sẽ được thỏa thuận
* Dịch vụ PKI về tính bảo mật giúp cho quá trình này trở nên trong suốt với các thực thể có liên quan

**CÁC KỸ THUẬT**

* **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 3 giá trị sau:
* Dữ liệu nào đó được xác thực:
* Dùng cho xác thực nguồn gốc dữ liệu;
* Một yêu cầu nào đó mà người dùng muốn gửi đến thiết bị ở xa;
* Một yêu cầu được đưa ra bởi thi ết bị ở xa:
* Dùng cho xác thực thực thể
* **Toàn vẹn dữ liệu:**
* Dịch vụ PKI về toàn vẹn có thể áp dụng một trong hai kỹ thuật:
* Chữ ký số: Nếu dữ liệu bị thay đổi, chữ ký sẽ loại bỏ khi kiểm tra vì vậy việc mất tính toàn vẹn của dữ liệu dễ dàng bị phát hiện;
* Mã xác thực thông điệp (Message Authentication Code - MAC):Kỹ thuật này thường sử dụng một mã khối đối xứng hoặc một hàm băm mật mã
* Khi Alice muốn gửi tới Bob dữ liệu được bảo vệ tính toàn vẹn, Alice có thể thực hiện dãy các thao tác sau:

+ Tạo khoá đối xứng mới,

+ Sử dụng khoá đối xứng để sinh MAC cho dữ liệu,

+ Mã hoá khoá đối xứng bằng khoá công khai của Bob,

+ Gửi dữ liệu cho Bob cùng với khoá đã được mã hoá.

* Nếu Bob có khóa công khai (chẳng hạn khóa công khai Diffie - Hellman) Alice có thể thực hiện dãy các thao tác sau:

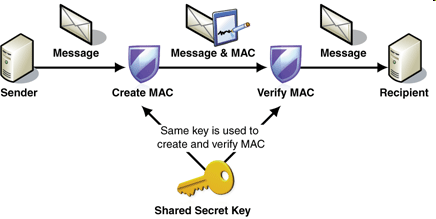
+ Tạo khoá đối xứng mới từ khóa công khai của Bob và khóa bí mật của mình,

+ Sử dụng khoá đối xứng để sinh MAC cho dữ liệu,

+ Gửi dữ liệu cho Bob cùng với chứng chỉ khoá công khai của mình.

* Sau khi nhận được dữ liệu từ Alice, Bob tạo lại khoá đối xứng, sử dụng khoá công khai của Alice, khoá bí mật của mình để kiểm tra tính toàn vẹn

**Mô hình MAC - DES-CBC-MAC**



* **Bảo mật:**
* Dịch vụ PKI về bảo mật sử dụng một cơ chế tương tự với một trong các phương án của dịch vụ toàn vẹn. Tức là:
* Alice sinh ra khóa đối xứng
* Khóa đối xứng được sử dụng để mã hóa dữ liệu
* Dữ liệu đã mã được gửi tới bob, hoặc cùng với khóa công khai của thỏa thuận khóa của Alice hoặc cùng với bản sao của khóa đối xứng đã được mã hóa bằng khóa công khai để mã của bob.

Câu 5 [**Các chứng chỉ X.509**](#_Toc163211164)**,** Khuôn dạng v3, Ý nghĩa của Các trường mở rộng

* Chứng chỉ X.509:

Gồm 3 phiên bản khác nhau:

* Phiên bản 1 được đị nh nghĩa năm 1988:

Nhược điểm là không mềm dẻo do không có trường mở rộng để hỗ trợ thêm các đặc tính;

* Phiên bản 2 được ra đời năm 1993:

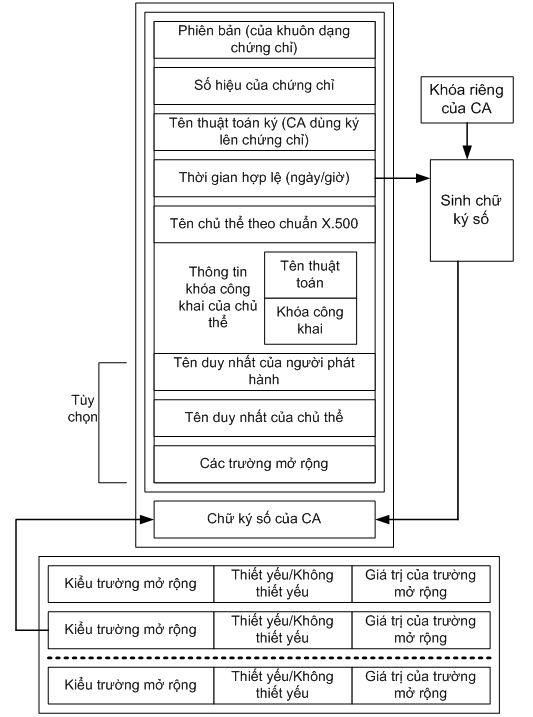
Bổ sung vào phiên bản 1 bằng việc thêm vào 2 trường lựa chọn,

Nhưng vẫn không có khả năng hỗ trợ các mở rộng khác

Phiên bản 3 được giới thiệu năm 1997:

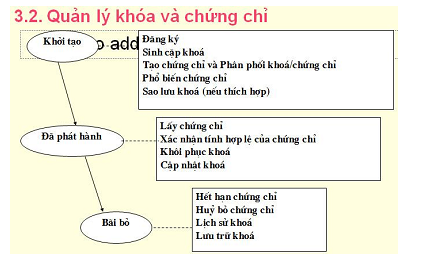
Điều chỉnh những thiếu sót trong phiên bản 1 và 2,

Bổ sung nhiều lựa chọn mở rộng, hỗ trợ đầy đủ các yêu cầu

* **Khuôn dạng v3**
* 
* Ý nghĩa của Các trường mở rộng
* Các khuôn dạng chứng chỉ trong phiên bản 1 và 2 không đáp ứng được tất cả các yêu cầu. Do đó cần phải bổ sung hem các thông tin.
* Giả thiết chủ thể của một chứng chỉ bất kỳ có các chứng chỉ khác nhau với các khóa công khai khác nhau và giả thiết rằng các cặp khóa cần được cập nhật định kỳ, do vậy cần phải có cách để phân biệt các chứng chỉ khác nhau của đối tượng một cách dễ dàng.
* Một tên trong X.500 trở thành tên duy nhất của chủ thể nhưng không có đầy đủ thông tin cho người sử dụng chứng chỉ khác nhận dạng chủ thể => 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 chỉ khác nhau có thể được phát hành theo các chính sách và các hoạt động chứng thực khác nhau. Các chính sách và các hoạt động chứng thực này thường chi phối mức tin cậy của người sử dụng đối với một chứng chỉ.
* Các đường dẫn chứng thực không được dài tùy tiện và phức tạp. Khi 1 CA (CA phát hành) chứng thực CA khác (CA của một chủ thể), CA phát hành có thể chỉ muốn chấp nhận một tập hợp con các chứng chỉ được CA của một chủ thể phát hành.

**Câu 6 Vẽ mô hình quản lý vòng đời khóa/ chứng chỉ. Trình bày quá trình hết hạn chứng chỉ và hủy bỏ chứng chỉ trong giai đoạn hủy bỏ**.

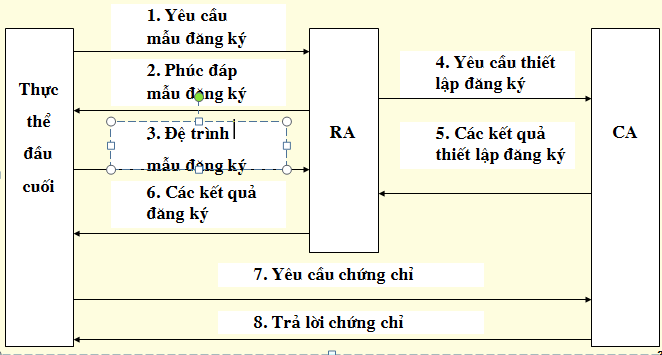
* Mô hình quản lý khóa và vòng đời khóa



**B1-Giai đoạn khởi tạo**

Trước khi các thực thể có thể tham gia vào các dịch vụ, chúng cần được khởi tạo

* Việc khởi tạo bao gồm:
  + - Đăng ký thực thể cuối,
    - Sinh cặp khóa,
    - Tạo chứng chỉ và phân phối khóa/chứng chỉ,
    - Phổ biến chứng chỉ và sao lưu khóa (nếu được áp dụng).
* ***Quá trình đăng ký***: Có thể có nhiều kịch bản khác nhau



* Là quá trình trong đó định danh của thực thể được thiết lập và kiểm tra,
* Mức độ kiểm tra tùy thuộc vào chính sách chứng chỉ
* **Qúa trình sinh cặp khóa**
* Tức là sinh cặp khóa bí mật/công khai,
* Có thể được sinh trước qtrình đăng ký hoặc trong trả lời trực tiếp cho qtrình đăng ký thực thể cuối
  + Trong mô hình PKI toàn diện, các khóa có thể được sinh tại:
* Thực thể cuối,
* Trong RA,
* Hoặc trong CA
  + Các nhân tố có thể ảnh hưởng đến việc chọn vị trí sinh khóa bao bồm:
* Khả năng,
* Hiệu suất,
* Tính đảm bảo,
* Phân nhánh pháp lý và cách sử dụng khóa định sẵn.
  + **Vị trí sinh cặp khóa là quan trọng:**
* Và trong tất cả các trường hợp người sử dụng phải có trách nhiệm lưu giữ và đảm bảo sự an toàn, bí mật cho khóa riêng của mình,
* Trường hợp do CA tạo ra, CA phải có cơ chế, phương tiện đặc biệt và trách nhiệm đảm bảo bí mật tuyệt đối khóa riêng của.
* **Tạo chứng chỉ và phân phối khóa/chứng chỉ**
* Trách nhiệm tạo chứng chỉ chỉ thuộc về CA được cấp phép,
* Nếu khóa công khai được sinh bởi thành phần khác CA thì khóa công khai đó phải được chuyển đến CA một cách an toàn
* Khi khóa và chứng chỉ liên quan đã được sinh ra, nó cần được phân phối hợp lý.
* Các yêu cầu phân phối khóa và chứng chỉ cụ thể phụ thuộc vào nhiều yếu tố. Bao gồm
* Nơi mà các khóa được sinh ra,
* Mục đích sử dụng của chứng chỉ,
* Các ràng buộc về chính sách
* **Phổ biến chứng chỉ**
* Khi khóa bí mật và chứng chỉ khóa công khai tương ứng đã được phân phối, chứng chỉ được phổ biến,
* Các phương pháp phổ biến**:**
* Phân phối thủ công,
* Lưu chứng chỉ trong kho công cộng để hỗ trợ việc tải về trực tuyến theo yêu cầu
* **Sao lưu khóa (key backup)**
* Nếu cặp khóa bí mật/công khai được dùng cho việc đảm bảo tính bí mật, giai đoạn khởi tạo có thể bao gồm cả việc sao lưu khóa và chứng chỉ bởi bên thứ 3 tin cậy,
* Việc sao lưu khóa còn tùy thuộc vào chính sách trong từng môi trường cụ

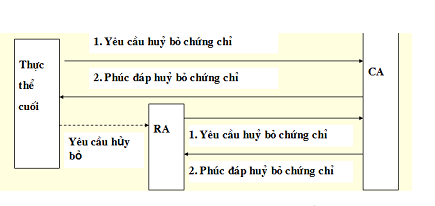
**B2- Giai đoạn sau phát hành**

* Khi khóa bí mật và chứng chỉ đã được phân phối, giai đoạn sau phát hành của việc quản lý khóa/chứng chỉ được bắt đầu
* Giai đoạn này bao gồm:
* Tải chứng chỉ từ một kho ở xa (khi được yêu cầu),
* Kiểm tra tính hợp lệ của chứng chỉ,
* Khôi phục khóa khi cần thiết,
* Cập nhật khóa tự động.
* **Tải chứng chỉ**
* Thực thể cuối yêu cầu lấy chứng chỉ để dùng,
* Có thể xuất phát từ 2 yêu cầu sử dụng riêng biệt
  + - * Để mã hóa dữ liệu được gửi tới một thực thể cuối khác,
        + Thường là mã khóa khóa đối xứng để gửi cho người nhận;
      * Để kiểm tra chữ ký số từ một thực thể cuối khác;
* Liên quan đến tính sẵn sàng truy cập chứng chỉ của thực thể đầu cuối
* **Xác nhận tính hợp lệ của chứng chỉ**
* Tính toàn vẹn của chứng chỉ được kiểm tra bởi vì chứng chỉ được ký số bởi CA phát hành,
* Tính toàn vẹn chỉ là một trong số những phép kiểm tra cần thực hiện trước khi chứng chỉ được coi là hợp lệ.
* Bao gồm:
* Chứng chỉ đã được phát hành bởi nơi tin cậy được xác nhận,
* Tính toàn vẹn được đảm bảo,
* Chứng chỉ vẫn trong thời gian hợp lệ,
* Chứng chỉ chưa bị hủy bỏ,
* Chứng chỉ phù hợp với chính sách
* **Khôi phục khóa (Key Recovery)**
* Như ta đã biết, việc sao lưu và khôi phục khóa trong PKI là rất cần thiết,
* Sao lưu và khôi phục khóa thường gắn liền với quá trình quản lý vòng đời của chứng chỉ
* **Cập nhật khóa (Key Update)**
* Các chứng chỉ được gán một thời gian sống cố định khi phát hành,
* Khi một chứng chỉ gần hết hạn, cần phải phát hành cặp khóa mới và chứng chỉ mới tương ứng:Đó là cập nhật khóa;
* Thực chất là chạy lại quá trình khởi tạo,
* Cập nhật khóa cần phải được tự động

**B3- Giai đoạn hủy bỏ**

* Quản lý vòng đời của khóa/chứng chỉ kết thúc bằng giai đoạn hủy bỏ,
* Giai đoạn này bao gồm:
  + Hết hạn chứng chỉ,
  + Hủy bỏ chứng chỉ,
  + Lịch sử khóa,
* Lưu trữ khóa
* **Hết hạn chứng chỉ**
* Các chứng chỉ được gán một khoảng thời gian sống cố định
* Khi chứng chỉ hết hạn, có 3 khả năng có thể xẩy ra với thực thể cuối**:**
* Không ảnh hưởng gì nếu thực thể cuối không tiếp tục tham gia vào PKI,
* Việc đổi mới chứng chỉ được thực hiện (đặt lại thời gian hợp lệ mới)
* Việc cập nhập chứng chỉ được thực hiện
* **Hủy bỏ chứng chỉ**
* Hủy bỏ đúng lúc chứng chỉ trước khi nó hết hạn về thời gian,
* Việc hủy bỏ xuất phát từ một số nhân tố:
  + - * Khóa bí mật bị nghi ngờ,
      * Sự thay đổi trong trạng thái công việc hoặc kết thúc thuê bao PKI.

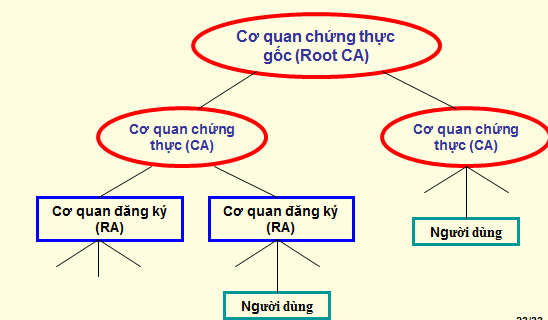
**Một số kịch bản hủy bỏ chứng chỉ**



* **Lịch sử khóa**
* Các chứng chỉ được phát hành với khoảng thời gian hợp lệ nhất định,
* Các khóa mã dần hết hạn,
* Nhưng không có nghĩa là tất cả dữ liệu đã được mã hóa bằng khóa đó sẽ không khôi phục lại được
* Vì vậy cần lưu giữ an toàn và tin cậy các khóa cần thiết để giải mã, ngay cả khi chứng chỉ tương ứng đã hết hạn,
* Tạo thành lịch sử khóa
* **Lưu trữ khóa:**
* Là cất giữ khóa một cách an toàn và tin cậy trong thời hạn lâu dài,
* Thông thường được hỗ trợ bởi CA hoặc bên tin cậy thứ 3 khác

# **Câu 7 có mấy loại mô hình tin cậy trong PKI? Trình bày mô hình mạng lưới.**

Có 3 mô hình tin cậy trong PKI là:

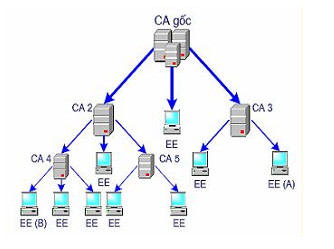
* Mô hình phân cấp
* Mô hình mạng lưới
* Mô hình danh sách tin cậy
* **Mô hình phân cấp **

Trong mô hình này:

* Cơ quan chứng thực gốc(Root CA):
* Là cơ quan cấp chứng chỉ số cho các cơ quan chứng thực,
* Duy nhất trong một hệ thống CA,
* Đây là điểm tin cậy của người dùng trong hệ thống các CA,

*Người dùng tin cậy vào Root CA, họ sẽ tin cậy vào CA được cấp chứng chỉ bởi Root CA*

* Cơ quan chứng thực(CA):
* Là cơ quan cấp chứng chỉ số cho người sử dụng**.**
* Cơ quan đăng ký (RA – Registration Authority):
* Là các đơn vị được CA uỷ quyền thực hiện các nhiệm vụ cấp chứng chỉ. Bao gồm
* Tiếp nhận hồ sơ đăng ký,
* Kiểm tra tính chính xác và hợp lệ về các thông tin đăng ký, Chuyển hồ sơ lên CA
* Người dùng:
* Là người được cấp chứng chỉ để sử dụng cho các ứng dụng của mình.
* ***(Hoặc )Mô hình phân cấp***



Có dạng hình cây với RootCA ở mức cao nhất và các nhánh được mở rộng xuống dưới.

* RootCA là gốc của tin cậy cho toàn bộ các thực thể bên dưới nó.
* Dưới RootCA là thực thể hoặc một số CA trung gian tạo thành các đỉnh trong của cây.
* Các đỉnh lá của cây là các thực thể không phải là CA.

**Trong mô hình này**

* RootCA cung cấp chứng chỉ cho các CA hoặc thực thể ngay dưới nó.
* Các CA này lại cung cấp chứng chỉ cho thực thể hoặc nhiều CA khác ngay dưới nó
* Tất cả các đối tượng đều phải biết khóa công khai của RootCA.
* Tất cả các chứng chỉ đều có thể kiểm chứng bằng cách kiểm tra đường dẫn của chứng chỉ đó tới RootCA.

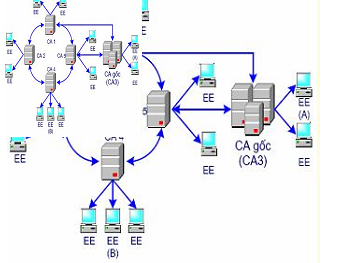
***Ưu điểm:***

* Tương đồng với cấu trúc phân cấp của hệ thống quản lý trong các tổ chức.
* Gần giống với hình thức phân cấp trong việc tổ chức thư mục nên dễ làm quen hơn.
* Cách thức tìm ra một nhánh x/thực là theo một hướng nhất định, không có hiện tượng vòng lặp.

=>Do đó đơn giản và nhanh chóng hơn.

***Nhược điểm***

* Trong một phạm vi rộng, một CA duy nhất không thể đảm nhận được tất cả quá trình xác thực.
* Các quan hệ kinh doanh thương mại không phải bao giờ cũ ng có dạng phân cấp.
* Khi khóa riêng của RootCA bị lộ thì toàn bộ hệ thống bị nguy hiểm.
* **Mô hình mạng lưới**



**Trong mô hình này**

* Các CA xác thực ngang hàng tạo nên một mạng lưới tin cậy lẫn nhau.
* Các CA kề nhau cấp chứng chỉ cho nhau.
* A có thể xác thực B theo nhiều nhánh khác nhau.

***Ưu điểm****:*

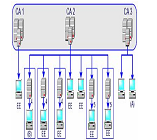
* Đây là mô hình linh động, thích hợp với các mối liên hệ - quan hệ tin cậy lẫn nhau trong thực tế của công việc kinh doanh.
* Cho phép các CA xác thực ngang hàng trực tiếp.

=> Điều này đặc biệt có lợi khi các đối tượng sử dụng của các CA làm việc với nhau thường xuyên

* Giúp giảm tải lượng đường truyền và thao tác xử lý.
* Khi một CA bị lộ khóa chỉ cần cấp phát chứng chỉ của CA tới các đối tượng có thiết lập quan hệ tin cậy với CA này.

***Nhược điểm***

* Do cấu trúc của mạng có thể phức tạp nên việc tìm kiếm các đối tượng có thể khó khăn.
* Một đối tượng không thể đưa ra một nhánh xác thực duy nhất có thể đảm bảo rằng tất cả các đối tượng trong hệ thống có thể tin cậy được.
* **Mô hình danh sách tin cậy**



* Trong mô hình này các ứng dụng duy trì một danh sách các RootCA được tin cậy.
* Đây là kiến được áp dụng rộng rãi với các dịch vụWeb.
* Các trình duyệt và các máy chủ là những đối tượng sử dụng tiêu biểu nhất.

**Ưu điểm:**

* Đây là kiến trúc đơn giản, dễ dàng triển khai,
* Các đối tượng sử dụng có toàn quyền với danh sách các CA mà mình tin cậy.
* Các đối tượng làm việc trực tiếp với CA trong danh sách các CA được tin cậy.

**Nhược điểm:**

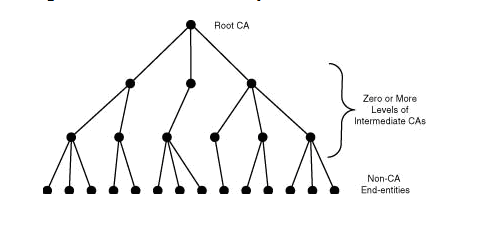
* Việc quản lý danh sách CA được tin cậy của một tổ chức là rất khó khăn.
* Cấu trúc chứng chỉ không có nhiều hỗ trợ cho việc tìm ra các nhánh xác nhận.
* Không có những hỗ trợ trực tiếp đối với các cặp chứng chỉ ngang hàng do vậy hạn chế của CA trong việc quản lý sự tin cậy của mình với các CA khác.
* Nhiều ứng dụng không hỗ trợ tính năng tự động lấy thông tin trạng thái hoặc hủy bỏ của chứng chỉ.

**Cau 7.2 có mấy loại mô hình tin cậy trong PKI ? cái nay trong slide của ong thầy (bài 4 slide5) đọc xem thế nào phản hồi. ko biết là 3 hay 7 nữa.**

* Phân cấp chặt chẽ của các CA (strict hierarchy of CAs)
* Phân cấp lỏng của các CA (loose hierarchy of CAs)
* Các phân cấp dựa trên chính sách (policy-based hierarchies)
* Kiến trúc tin cậy phân tán (distributed trust architecture)
* Mô hình 4 góc (four-corner model)
* Mô hình Web (Web model)
* Tin cậy lấy người sử dụng là trung tâm (user-centric trust).
* **Mô hình phân cấp CA chặt chẽ (strict hierarchy of CAs)**

Trong mô hình này, có 1 CA đóng vai trò là CA gốc ở trên cùng, phía dưới là các nhánh mở rộng và các lá ở cuối cùng.

RootCA đóng vai trò như là gốc tin cậy (hay còn gọi là “nguồn tin cậy”) cho toàn bộ miền của các thực thể PKI dưới nó. Ở dưới root CA có thể không có hoặc có một vài lớp intermediate CA (hay còn gọi là subCA).



Hình 9: Mô hình phân cấp CA chặt chẽ

RootCA không đơn giản là điểm khởi đầu của một mạng, hay các kết nối, nó còn là điểm khởi đầu của sự tin cậy. Tất cả các thực thể trong miền đều nắm giữ khoá công khai của CA.

Trong mô hình này, tất cả các thực thể trong kiến trúc tin cậy rootCA. Sự phân cấp được thiết lập như sau:

* RootCA được xây dựng, và tự cấp chứng chỉ cho mình (hay tự ký cho mình).
* RootCA sẽ chứng thực (tạo và ký chứng chỉ) cho các CA trực tiếp dưới nó.
* Mỗi một CA như trên lại chứng thực cho CA trực tiếp dưới nó.
* Tại mức gần cuối cùng, CA sẽ chứng thực thực thể cuối.
* Mỗi thực thể trong phân cấp phải được cung cấp bản sao khoá công khai của root CA. Quá trình tạo khoá công khai này là cơ sở cho quá trình chứng thực tất cả các kết nối sau đó, do đó, quá trình này phải được thực hiện trên một cách an toàn.

Chú ý rằng trong mô hình phân cấp chặt chẽ đa mức (multilevel strict hierarchy), các thực thể cuối được chứng thực (nghĩa là được cấp chứng chỉ) bởi CA trực tiếp ngay trên nó, nhưng gốc tin cậy thì lại là rootCA.

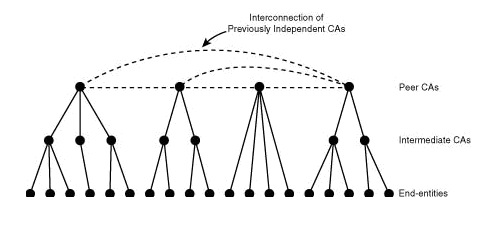
* **Mô hình phân cấp CA không chặt chẽ (loose hierarchy of CAs)**

Trong mô hình phân cấp CA không chặt chẽ các bên được chứng thực bởi cùng một CA để giải quyết vấn đề đường dẫn tin cậy mà không liên quan tới bất kỳ CA mức cao hơn, bao gồm cả root CA. Nghĩa là nếu hai thực thể (ví dụ thực thể A và thực thể B) được chứng thực bởi cùng một CA, thì thực thể A và thực thể B có thể kiếm tra tính hợp lệ của nhau mà không cần phải tạo một đường dẫn chứng thực tới root CA. Về cơ bản, thực thể A và thực thể B cùng thuộc về phân cấp chủ thể tin cậy của cả hai. Tuy nhiên, giả sử rằng có một thực thể C nào đó được chứng thực bởi một CA khác (không phải CA chứng thực cho A và B) thì thực thể A và B phải thực hiện một đường dẫn chứng thực hoàn toàn thông qua rootCA trước khi tin cậy chứng chỉ của C.

* **Mô hình kiến trúc tin cậy phân tán (distributed trust architecture)**

Kiến trúc tin cậy phân tán sẽ phân phối sự tin cậy giữa hai hay nhiều CA. Nghĩa là thực thể 1 có thể giữ bản sao khoá công khai của CA1 như nguồn tin cậy của mình, thực thể 2 có thể giữ bản sao khoá công khai của CA2 như nguồn tin cậy của mình. Bởi vì những khoá công khai của những CA này đóng vai trò như nguồn tin cậy (CA1 là gốc(root) của hệ thống phân cấp chứa thực thể 1, CA2 là gốc của hệ thống phân cấp có chứa thực thể 2).

Nếu mỗi kiến trúc phân cấp này là kiến trúc phân cấp không chặt chẽ, thì cấu hình của kiến trúc đó được gọi là kiến trúc được chia điểm (peered architeture) bởi vì tất cả các CA đều là những điểm hoàn toàn độc lập (Không có SubCA trong kiến trúc). Trái lại, nếu kiến trúc đó là phân cấp đa mức, thì kiến trúc đó được gọi là kiến trúc hình cây (treed architeture) (chú ý rằng các root CA là các điểm so với các CA khác nhưng mỗi root lại đóng vai trò như CA cấp cao đối với một hoặc nhiều SubCA).

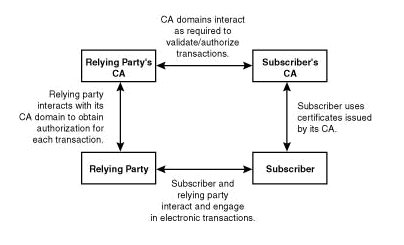


Hình 10: Mô hình kiến trúc tin cậy phân tán

Thông thường thì kiến trúc được chia điểm thường được xây dựng trong một miền của một tổ chức (ví dụ trong một công ty), trái lại, kiến trúc hình cây và kiến trúc lai (hybrid architeture) được hình thành từ các miền của các tổ chức khác nhau.

Quá trình của việc tạo kết nối mỗi root CA thông thường được gọi là chứng thực chéo (cross-certification).

* **Mô hình 4 bên (four-corner model)**



Hình 11: Mô hình bốn bên

Trong mô hình này minh họa bốn góc của mô hình tin cậy là người thuê bao (subscriber), bên tin cậy (relying party), thuê bao của CA (subscriber’s CA) và bên tin cậy của CA (relying party’s CA).

Mô hình tin cậy 4 bên này thường được triển khai trong các giao dịch thanh toán điện tử.

Trong mô hình này , thuê bao sử dụng chứng chỉ được cấp bởi CA của nó.

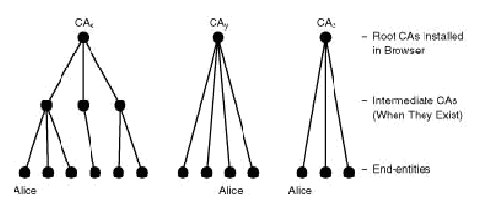
Thuê bao và bên tin cậy tương tác và ràng buộc nhau trong các giao dịch điện tử.

Bên tin cậy tương tác với miền CA (CA domain) của nó để xác thực cho mỗi phiên giao dịch.

Miền CA tương tác khi có yêu cầu xác minh tính hợp lệ/cấp quyền phiên giao dịch.

* **Mô hình Web (web model)**

Mô hình Web – đúng như tên gọi của nó, phụ thuộc vào các trình duyệt Web phổ biến như Netscape Navigator và Microsoft Internet Explorer. Trong mô hình này, số lượng khoá công khai của CA sẽ được cài đặt sẵn vào một số các trình duyệt. Các khoá này sẽ định nghĩa tập hợp các CA mà trình người dùng trình duyệt ban đầu sẽ tin tưởng và xem như các root cho việc xác minh chứng chỉ.



Hình 12: Mô hình Web

Mỗi nhà cung cấp trình duyệt đều có root của riêng mình, và nó sẽ chứng thực root CA mà được nhúng trong trình duyệt.

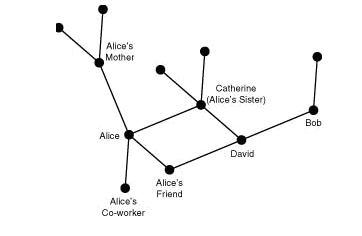
Mô hình Web có những ưu điểm rõ rệt để thuận tiện và đơn giản khả năng liên kết. Tuy nhiên, có một vài sự vấn đề an toàn cần được quan tâm trong mô hình này khi quyết định triển khai. Ví dụ, bởi vì người dùng trình duyệt tự động tin tưởng vào tập hợp các khoá đã được cài sẵn trong trình duyệt, nên an toàn sẽ có thể bị mất nếu một trong số các rootCA đó “rơi vào tình trạng nguy hiểm”.

Một vấn đề an toàn nữa cũng cần phải được quan tâm đó là trong mô hình Web, không có cơ chế thực thế nào có thể thu hồi bấy kỳ khoá của root đã được nhúng trong trình duyệt. Nếu chúng ta phát hiện ra một trong những CA “đang trong tình trạng nguy hiểm” hoặc khoá riêng tương ứng với bất kỳ khoá công khai của root bị lộ, thì hiển nhiên là không thể tiếp tục sử dụng khoá đó trong hàng triệu các trình duyệt web trên thế giới.

* **Mô hình tin cậy lấy người dùng làm trung tâm (user-centric trust)**

Trong mô hình tin cậy lấy người dùng làm trung tâm, mỗi người dùng sẽ phải chịu trách nhiệm trực tiếp và toàn bộ để quyết định xem sẽ sử dụng chứng chỉ nào và từ chối chứng chỉ nào. Mỗi người dùng sẽ giữ một vòng khoá và vòng khoá này đóng vai trò như CA của họ. Vòng khoá này chứa các khoá công khai được tin cậy của những người sử dụng khác trong cộng đồng. Mô hình này được Zimmerman phát triển để sử dụng trong chương trình phát triển phần mềm bảo mật PGP.

Quyết định này có thể chịu ảnh hưởng của một số các nhân tố, mặc dù ban đầu tập hợp các khoá được tin cậy thông thường bao gồm các nhân tố là bạn bè, gia đình, đồng nghiệp …



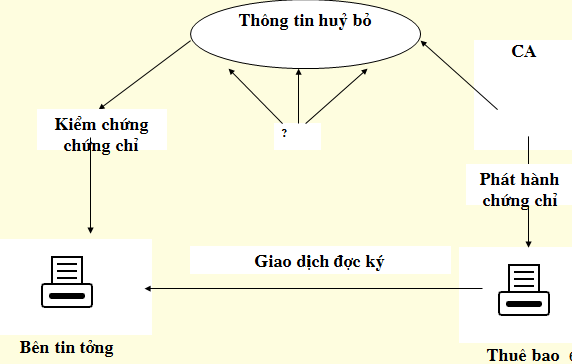
Hình 13: Mô hình tin cậy lấy người dùng làm trung tâm

Mô hình này được sử dụng rộng rãi trong phần mềm an ninh nổi tiếng là Pretty Good Privacy (PGP) [Zimm95, Garf95]. Trong PGP, người dùng xây dựng mạng lưới tín nhiệm (web of trust) đóng vai trò là CA (ký lên khoá công khai cho các thực thể khác).

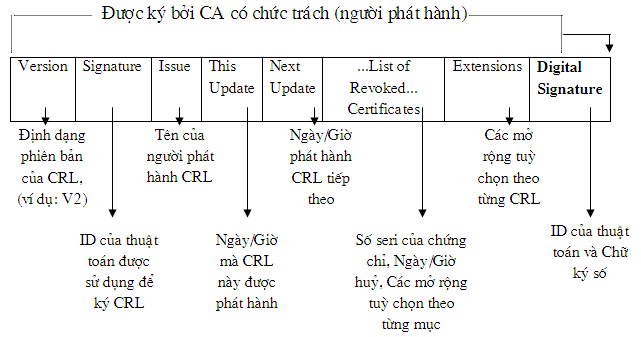
Do sự tín nhiệm của người dùng trong các họat động và các quyết định, nên mô hình tin cậy lấy người dùng làm trung tâm có thể họat động được trong cộng đồng đòi hỏi kỹ thuật và sự quan tâm cao độ, nhưng nó không thực tế đối với cộng đồng chung (cộng đồng mà trong đó nhiều người dùng chỉ có một chút hoặc không có sự hiểu biết về các khái niệm PKI hay khái niệm an toàn). Hơn nữa, một mô hình như vậy thông thường không phù hợp với các môi trường của công ty, tổ chức tài chính hoặc chính phủ.

# **Câu 7.2Hủy bỏ chứng chỉ (làm thêm thôi)**

* Bình thường chứng chỉ là hợp lệ trong toàn bộ thời gian sống của nó,
* Tuy nhiên, nhiều tình huống nảy sinh khi chứng chỉ đã được phát hành làm cho nó không còn tiếp tục được xem là hợp lệ, kể cả khi chưa hết hạn,
* Chứng chỉ không còn hợp lệ cần được hủy bỏ,
* Cần có một phương pháp hiệu quả, tin cậy cho việc hủy bỏ chứng chỉ.
* Trước khi sử dụng, chứng chỉ phải trải qua một quá trình kiểm chứng,
* **Trong đó bao gồm việc kiểm tra xem chứng chỉ đó đã bị hủy hay chưa;**
* CA có trách nhiệm niêm yết thông tin về chứng chỉ bị hủy bỏ ở một dạng nào đó,
* Bên tin cậy cần phải có cơ chế để tải được thông tin hủy bỏ chứng chỉ
  + **mô hình hủy bỏ chứng chỉ,**



* Hủy bỏ chứng chỉ có thể được cài đặt theo nhiều cách,
* Một phương pháp là CA công bố định kỳ danh sách hủy bỏ chứng chỉ (Certificate Revocation List - CRL),
* CRL là một danh sách các chứng chỉ bị hủy bỏ được gán nhãn thời gian,
* Danh sách này được CA ký và công bố
* Mỗi chứng chỉ bị hủy bỏ được CRL nhận dạng qua số hiệu của nó,
* Tần suất phát hành CRL do chính sách chứng thực quyết định.
* Định dạng tổng quát của một CRL phiên bản 2



Câu 8[PKI trong thực tế](#_Toc163211213) :

[PKI làm được những gì ?](#_Toc163211214) [PKI không làm được những gì ?](#_Toc163211215) [Lợi ích của PKI.](#_Toc163211216)

* **PKI làm được những gì**
* PKI là một công nghệ xác thực, là các phương tiện kỹ thuật để định danh các thực thể trong môi trường điện tử.
* Mật mã khoá công khai được sử dụng kết hợp với những kỹ thuật sau để tạo ra công nghệ nhằm định danh các thực thể:
* Kỹ thuật để thiết lập tin cậy theo như mô hình tin cậy được định nghĩa
* Kỹ thuật để đặt tên các thực thể sao cho mỗi thực thể được định danh một cách duy nhất trong môi trường quan tâm
* Kỹ thuật để phân phối thông tin đối với tính đúng đắn của việc gắn giữa cặp khoá cụ thể và tên cụ thể của những thực thể

🡪PKI cung cấp xác thực- không hơn, không kém

* **Không làm được những gì?**
* Việc biết người nào đó là ai không có nghĩa là bạn biết người đó có thể làm cái gì
* nó cũng không có nghĩa rằng bạn tin cậy người đó một cách tự động
* điều đó không có nghĩa là bạn có đủ thông tin mà bạn cần để thực hiện đúng công việc của mình trong một giao dịch đã cho
* Nhiều bước giao dịch đòi hỏi cấp phép/sự được phép/dữ liệu quyền ưu tiên về một thực thể nào đó
* PKI không đề xuất sự hỗ trợ ở đây, ngoại trừ việc bảo vệ tính toàn vẹn, xác thực hoặc bí mật của thông tin như vậy
* Trước hết, như đã nhận thấy ở trên, PKI thông thường không đề cập tới các vấn đề cấp phép, cấp quyền
* Thứ hai, PKI gần như không mang niềm tin cậy vào các thực thể đầu cuối khác. PKI bắt đầu bằng một cơ chế thiết lập tin cậy, mục đích duy nhất của nó là làm cho mỗi thực thể- thông qua các biện pháp thủ công – *tin vào CA*
* PKI không làm cho Alice tin Bob; cô ta tin vào CA mà cô ta đã chọn và sau đó sử dụng PKI để đi tới tin tưởng rằng một cặp khoá đã cho là một thực thể nắm giữ được gọi là “Bob”
* Thứ ba, PKI không tạo ra tên duy nhất cho các thực thể; nó không cố gắng giải quyết bài toán đặt tên thực thể
* Công việc của CA không phải là tạo ra các tên mà là gắn các cặp khoá cho các tên
* Thứ tư, PKI không làm các ứng dụng, các hệ điều hành, hoặc các nền tảng tính toán “an toàn”
* Kỹ thuật xác thực không thể lấp các lỗi (hoặc các mã lập trình tồi) trong ứng dụng hoặc phần mềm hệ điều hành
* Nó không thể ngăn chặn các vấn đề được gây ra do tràn bộ đệm, nó không thể loại bỏ mối đe doạ của các tấn công DoS; nó không thể dừng virut, sâu khỏi việc gây ra hỏng hóc trong mạng
* 🡪 PKI không giải phóng người quản trị mạng khỏi các dạng khác của cảnh báo an ninh và đề phòng; Một cách xác thực mạnh là chưa thể đủ làm cho hệ thống trở nên an toàn
* Cuối cùng, PKI không làm cho người sử dụng (hoặc người sử dụng cuối hoặc những người quản trị) hành động tin cậy hơn hoặc đúng đắn hơn. Người sử dụng đầu cuối sẽ vẫn phải viết một khẩu của mình ra và gắn tờ giấy vào máy tính; người quản trị vẫn có thể làm quyết định cấu hình kém. PKI không dừng con người khỏi việc mắc các sai lầm hoặc biến “người xấu” thành “người tốt”.
* **Tóm lại pki không làm được ( đề đóng chép mỗi chỗ này)**
* PKI không cung cấp việc cấp phép (mặc dù nó có thể được sử dụng để bảo vệ thông tin cấp phép)
* PKI không tạo ra tin cậy trong các thực thể khác (mặc dù, bắt đầu bằng mô hình tin cậy, nó có thể dẫn tới niềm tin rằng một khoá đã cho ứng với một tên đã cho).
* PKI không đặt tên các thực thể (ngay cả nếu không có PKI, tôi cũng vẫn cần có thể quyết định xem thư điện tử này là từ “Fred” mà tôi biết hoặc “Fred” mà tôi không biết).
* PKI không làm cho mọi vật trở nên an toàn (ngay cả nếu nó có thể được sử dụng như là cơ sở cho một số khía cạnh của an toàn, tất cả các công cụ và kỹ thuật mạng/hệ thống khác có liên quan tới an toàn vẫn cần phải được sử dụng.
* PKI không làm thay đổi hành vi của người xấu (con người cần phải được đào tạo để không làm các việc “xấu”; những người sử dụng ác ý- đặc biệt những người quản trị ác ý – vẫn có thể tồn tại)
* **Lợi ích**
* cung cấp xác thực mạnh
* nó gắn cặp khoá bí mật/công khai với một cái tên
* Một cách tổng quát hơn, PKI là có lợi theo ít nhất 4 cách:
* Thứ nhất, người sử dụng đầu cuối thấy lợi ích bởi vì đăng nhập một lần (hoặc, tối thiểu, đăng nhập được rút gọn) là đạt được về mặt lý thuyết.
* Thứ hai, tổ chức mà khai thác PKI thấy lợi ích bởi vì lượng dữ liệu mà cần phải giữ bí mật để duy trì hoạt động của toàn hệ thống là nhỏ: khoá ký chứng thư và CRL bí mật của CA.
* Các thực thể chịu trách nhiệm giữ các khoá bí mật của họ, nhưng bất kỳ lỗi lộ khóa cũng không huỷ diệt khả năng sử dụng của cả hệ thống nói chung.
* Các khoá gốc (Public key của Rootca) cần phải được bảo vệ tại tất cả các máy, nhưng chỉ cho tính toàn vẹn (chứ không phải bí mật), nó dễ được đảm bảo hơn (vì bạn có thể nói chắc chắn rằng dữ liệu có thể bị thay đổi hay không, nhưng rất khó để bạn biết rằng một dữ liệu nào đó đã bị đọc?)
* Thứ ba, các ứng dụng và các phần tử hệ thống khác đòi hỏi xác thực thấy lợi ích bởi vì PKI cung cấp một kỹ thuật mạnh, không giả mạo được để xác thực các thực thể.
* Các ứng dụng như vậy được bảo vệ chống lại kẻ mạo danh và sự mạo danh.
* Nó không hoàn thiện: nếu ai đó có thể giành được truy cập tới máy của Alice và yêu cầu bản sao của khóa được mã bằng mật khẩu, tấn công thử-và- sai đối với mật khẩu của Alice có thể được dựng lên để mở khoá.
* Nhưng một tấn công như vậy là luôn có thể chống lại các công nghệ mà lưu trữ bí mật xác thực nào đó trên máy của người sử dụng, và nó luôn có thể giảm một cách đáng kể mối nguy hiểm bằng cách lưu các uỷ nhiệm lên thẻ cứng (hardware token), cái này không bao giờ làm lộ bí mật của nó.
* Tách khỏi việc truy cập máy của Alice, tuy nhiên, kẻ giả mạo bị ngăn trở: khoá bí mật của Alice không bao giờ di chuyển trên mạng như một phần của giao dịch xác thực, và giá trị của nó không thể bị đoán hoặc tính được từ khoá công khai của cô ta.
* Việc giả mạo chữ ký của cô ta thực ra là không thể, cho nên không có người sử dụng nào, bao gồm cả thực thể mà Alice đã xác thực với họ trong quá khứ, có thể giả mạo thành công Alice khi xác thực với thực thể khác.
* Cuối cùng, các ứng dụng và các phần tử hệ thống khác yêu cầu cấp phép, cấp quyền thấy lợi ích bởi vì PKI cung cấp một kết nối mật mã giữa các quyền ưu tiên và người khởi tạo giao dịch.
* Đặc biệt hơn, các quyền ưu tiên có thể được mang trong một cấu trúc dữ liệu được ký bởi thẩm quyền thuộc tính, thẩm quyền này mang cả khoá công khai của Alice hoặc chứng thư của cô ta trong trường Holder/Owner/Subject.
* Cho nên, thực thể bất kỳ mà có thể xác thực sử dụng khoá bí mật tương ứng khoá công khai đó là người chủ/người giữ được chủ định của các quyền ưu tiên đó.
* Một cách khác, cấu trúc dữ liệu đã được ký có thể giữ các quyền ưu tiên và giá trị băm của dữ liệu nào đó; dữ liệu bất kỳ mà băm thành giá trị đã chỉ ra là người chủ/người giữ có chủ ý của các quyền ưu tiên này.
* Cho nên, mặc dù PKI chỉ là cơ chế xác thực, nó cung cấp một số các lợi ích quan trọng, bao gồm:
* Dễ sử dụng cho thực thể đầu cuối
* Hoạt động hiệu quả cho tổ chức khai thác chi phí thấp
* Bảo vệ chống lại việc mạo danh cho các thành phần cần xác thực
* Trách nhiệm giải trình cho các thành phần được cấp phép.

Câu 9[Tương lai của PKI](#_Toc163211217): nguyên nhân và hướng phát triển

* Một số khẳng định rằng PKI sẽ không tồn tại lâu, những người khác lại nói rằng nó chỉ tạm lắng xuống
* những người khác cảm thấy rằng nó đang sống và thực ra đang phồn vinh
* Tuy nhiên, chúng ta có thể đề xuất rằng có 2 nguyên nhân là chủ yếu
* **Nguyên nhân**
* Thứ nhất, với PKI có thể có một lỗ hổng tương đối lớn trong nhiều tình huống giữa cái được “bán” và cái được “mua”. Đặc biệt, trong những ngày đầu, môi trường thương mại, các nhà phân tích, những người bán hàng quá tích cực thường miêu tả PKI như là một cài đặt đơn giản và sẽ giải quyết tất cả các vấn đề an toàn.
* Trong thực tế, nhiều nhà quản trị tìm thấy rằng công nghệ mà họ yêu cầu là tương đối khó hoặc phức tạp để cài đặt và chỉ giải quyết một số vấn đề về an ninh an toàn.
* Sự không đúng so với quảng cáo này thông thường dẫn tới sự không hài lòng, tiếp theo là vỡ mộng, sau đó là giận dữ, sau đó là phê phán.
  + Kết quả là PKI đã sai khi thực ra về bản chất và giá trị của công nghệ – nó là cái gì và nó có thể làm được gì- đã được tuyên truyền và hiểu không đúng.
* Một số người ủng hộ PKI nhấn mạnh khía cạnh hạ tầng cơ sở của công nghệ này, rằng nó là nền tảng an toàn cơ bản sao cho nhiều dịch vụ khác nhau có thể xây dựng lên trên và nhiều ứng dụng khác nhau có thể tích hợp với nó.
* Nhưng phần lớn, những người ủng hộ này không hình dung được rằng đôi khi một hạ tầng cơ sở cũng cần một hạ tầng cơ sở. Điều đó đúng cho PKI. Khó có thể được xây dựng và khai thác công nghệ này trên cơ sở không có gì cả và làm cho nó hoạt động; một hạ tầng cơ sở khác cần phải tồn tại trước đó.
* **Hướng phát triển**

Khi chúng ta nghĩ về PKI, chúng ta phát hiện ra rằng, nó cũng cần một cơ sở hạ tầng xung quanh nó để nó có thể sống được. Nó cần:

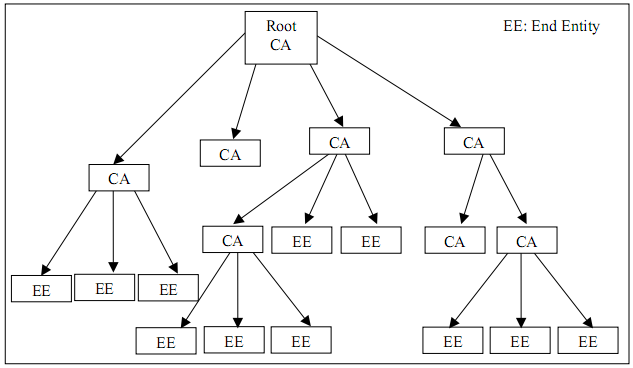
* *Một tổ chức có quyền lực được công nhận*
* *Động lực*
* *Những người sử dụng*

# **Câu 10Trình bày thiết kế chi tiết kiến trúc phân cấp PKI với các mức phân cấp CA**

Thiết kế chi tiết bao gồm 1 root CA được sự tin tưởng của toàn bộ hệ thống

Các CA con trong hệ thống, mỗi CA con thường thuộc quản lý của một công ty con hay một tổ chức thành viên, tầng CA con này có thể có nhiều tầng hoặc cũng không xuất hiện ở những công ty hoặc tổ chức quy mô nhỏ

Các người dùng cuối

****

* Mô hình CA phân cấp có thể dùng được trực tiếp cho những doanh nghiệp phân cấp và độc lập, cũng như những tổ chức chính phủ, quân đội... Nó cho phép thực thi chính sách và các chuẩn thông qua hạ tầng cơ sở. Đây là mô hình dễ vận hành giữa các tổ chức khác nhau. Tuy nhiên, mô hình này có một số nhược điểm sau:
* Có thể không thích hợp đối với môi trường mà mỗi miền khác nhau cần có chính sách và giải pháp PKI khác nhau.
* Các tổ chức có thể không tự nguyện tin vào một tổ chức khác.
* Chỉ có một CA gốc nên có thể gây ra một số vấn đề như thiếu khả năng hoạt động. Hơn nữa, trong trường hợp khóa bí mật của CA bị xâm phạm, khóa công khai mới của CA gốc phải được phân phối đến tất cả các thực thể cuối trong hệ thống theo một số cơ chế khác nhau.

# **Câu 11. Trong khuôn dạng CRL của X.509 có các trường mở rộng sau: Các trường mở rộng chung, các điểm phân tán CRL, các Delta-CRL, các CRL gián tiếp và việc treo chứng chỉ. Vậy Delta-CRL là gì? Việc sử dụng Delta-CRL có ý nghĩa như thế nào?**

**Các trường mở rộng**

* *Định danh khoá thẩm quyền* (Authority Key Identifier) là định danh duy nhất của khoá mà được sử dụng để xác minh chữ ký số được tính trên cả CRL. Định danh khoá thẩm quyền chỉ sự khác biệt giữa nhiều khoá được áp dụng cho cùng một người phát hành CRL. Nhiều khoá (chưa hết hạn) có thể tồn tại cho cùng một người phát hành CRL vì một loạt các nguyên nhân, bao gồm những khoá trong các chu kỳ có giao nhau về thời gian để hỗ trợ việc đổi khoá của CA. Mở rộng này luôn được đánh dấu coi là không bắt buộc theo như X.509, nhưng việc đưa trường này vào lại là bắt buộc bởi RFC3280. FRC3280 cũng chỉ ra phương pháp định danh khoá (khác với việc sử dụng tên người phát hành/số serial) cần được sử dụng.
* *Tên khác của người phát hành* (Issue Alternative Name) là một hoặc nhiều hình thái tên khác nhau tương ứng với người phát hành CRL. Tên khác của người phát hành chỉ ra người phát hành CRL bằng cách sử dụng một cái gì đó khác với DN đã được định ra trong trường Issue Name (ví dụ, địa chỉ IP, tên DNS, địa chỉ e-mail RFC-822, ...) X.509 cho phép mở rộng này là cần thiết hoặc không, nhưng RFC3280 khuyến cáo trường này không nên coi là quan trọng.
* *Số CRL* (số CRL) truyền đạt một số seri duy nhất cho mỗi CRL đối với người phát hành CRL và thuộc tính thư mục thẩm quyền tương ứng hoặc điểm phân phối CRL (CRL Distribution Point) (xem CRL Stream Identifier ở phía sau). Đó là một số nguyên tăng đơn điệu mà cho phép phát hiện ra việc mất các CRL. Mở rộng này luôn được coi được đánh dấu là không quan trọng theo như X.509 nhưng việc đưa trường này vào là bắt buộc bởi RFC3280. RFC3280 đề xuất rằng CRL Number cần phải là duy nhất đối với người phát hành và phạm vi CRL đã định sẵn. Cái này có thể dùng để phát hiện khi một CRL đè lên một cái khác và nó định ra các CRL đầy đủ bổ sung và các CRL Delta.
* *Phạm vi CRL* (CRL Scope), một cách hình thức được chuẩn hoá trong phiên bản 2000 của X.509, cung cấp một phương pháp cực kỳ mềm dẻo để phân loại thông tin CRL. Các CRL có thể được phân loại theo nhiều cách, bao gồm bằng kiểu chứng chỉ, các mã lý do huỷ bỏ chứng chỉ, các số seri, các định danh khoá của chủ thể và các cây con về tên. Theo phiên bản năm 2000 của X.509, mở rộng này luôn được đánh dấu là quan trọng.
* *Các chỉ dẫn tới trạng thái* (Status Referrals), một cách hình thức được chuẩn hoá trong phiên bản năm 2000 của X.509, mở rộng này cung cấp hai chức năng chính. Trước hết, nó đảm bảo việc phân loại động thông tin huỷ bỏ. Mở rộng Status Referrals bao gồm CRL Scope (được bàn tới ở trên) trong cú pháp của nó, cho nên nó có thể hỗ trợ phân loại động theo nhiều cách khác nhau, bao gồm bằng kiểu chứng chỉ, các mã lý do huỷ bỏ chứng chỉ, các số seri, các định danh khoá của chủ thể và các cây con về tên. Thông tin thêm về cơ chế phân loại mềm dẻo này được cung cấp ở mục Redirect CRL ở phần sau của chương này. Thứ hai, nó cho phép CA công bố danh sách các CRL hiện tại mà có thể được sử dụng để xác định chắc chắn xem một bên tin cậy vào đã có thông tin huỷ bỏ cuối cùng hay chưa. Điều này giúp cho loại bỏ việc tải về lãng phí các CRL. Nó cũng có thể “quảng cáo” thông tin CRL mới mà có thể được công bố trước thời gian Next Update của một CRL cũ hơn (nhưng thực ra chưa hết hạn). Theo như phiên bản năm 2000 của X.509, mở rộng này luôn được đánh dấu là quan trọng.
* *Định danh dòng CRL* (CRL Stream Identifier), một cách hình thức được chuẩn hoá trong phiên bản năm 2000 của X.509, nó được sử dụng để “nhận dạng ngữ cảnh mà trong đó số CRL là duy nhất”. Ví dụ, định danh dòng duy nhất có thể được gắn vào mỗi điểm phân phối CRL. Kết hợp định danh dòng với số CRL cung cấp một định danh duy nhất cho mỗi CRL được phát hành bởi CA đã được cho, bất chấp kiểu của CRL. Theo phiên bản năm 2000 của X.509, mở rộng này luôn được đánh dấu là không quan trọng.
* *Danh sách được sắp xếp* (Ordered List), một cách hình thức đã được chuẩn hoá trong phiên bản năm 2000 của X.509, chỉ ra xem danh sách các chứng chỉ đã được huỷ bỏ là theo thứ tự tăng dựa trên số seri hay ngày tháng huỷ bỏ. Nếu mở rộng này thiếu vắng, không có thứ tự đặc biệt có thể được giả thiết trừ khi bị bắt buộc một cách khác đi bởi chính sách địa phương. Theo như phiên bản năm 2000 của X.509, mở rộng này luôn được đánh dấu là không quan trọng.
* *Thông tin Delta* (Delta Information), một cách hình thức được chuẩn hoá trong phiên bản năm 2000 của X.509, chỉ ra rằng các Delta CRLs tương ứng với CRL này là có thể. Mở rộng này cung cấp vị trí của Delta CRL (được chỉ ra như General Name) và một cách tuỳ chọn thời gian khi Delta CRL sau sẽ được phát hành. Theo như phiên bản năm 2000 của X.509, mở rộng này luôn được đánh dấu là không quan trọng.
* *Điểm phân phối phát hành* (Issuing Distribution Point) chỉ ra tên của điểm phân phối CRL (nếu có) và các kiểu của các chứng chỉ được chứa trong CRL (ví dụ, chỉ có các chứng chỉ của người sử dụng cuối, chỉ có các chứng chỉ của CA, và/hoặc chỉ có các chứng chỉ được huỷ bỏ theo một nguyên nhân đặc biệt). Khi có thể ứng dụng, nó chỉ ra rằng CRL là CRL không trực tiếp. (Thông tin thêm về các CRL không trực tiếp có ở cuối chương này). Chú ý rằng mở rộng này, nếu hiện diện, cần phải được đánh dấu là quan trọng theo như X.509. Mặc dù mở rộng này cần phải được đánh dấu là quan trọng, RFC3280 không yêu cầu các cài đặt tuân thủ để hỗ trợ mở rộng này.
* *Báo hiệu Delta CRL* (Delta CRL Indicator) chỉ ra rằng CRL này là Delta CRL so với CRL cơ sở được tham chiếu tới. Tổ hợp của CRL cơ sở và Delta CRL trình bày tất cả thông tin huỷ bỏ được biết tại thời điểm khi Delta CRL được phát hành, tương đối so với phạm vi đã được cho. Phạm vi của Delta CRL cần phải phù hợp với phạm vi của CRL cơ sở.
* *Cập nhật cơ sở* (Base Update), một cách hình thức được chuẩn hoá trong phiên bản năm 2000 của X.509, nó được sử dụng trong các Delta CRLs mà có chứa mở rộng Delta CRL Indicator để chỉ ra ngày/thời gian mà sau đó Delta CRL này cung cấp các cập nhật trạng thái huỷ bỏ. Mở rộng này là không cần thiết khi Delta CRL bao gồm mở rộng CRL Scope. Theo như phiên bản năm 2000 của X.509, mở rộng này luôn được đánh dấu là không quan trọng.
* *CRL mới nhất* (Freshest CRL), một cách hình thức đã được chuẩn hoá trong phiên bản năm 2000 của X.509, chỉ ra rằng thông tin CRL mới nhất là có thể. Trong thực tế, cái này thường là con trỏ tới Delta CRL. RFC3280 chỉ ra rằng phạm vi của Delta CRL cần phải giống như phạm vi của CRL mà chứa mở rộng này. Thêm vào đó, các Delta CRL không thể sử dụng mở rộng này (tức là không cho phép một Delta CRL trỏ tới một Delta CRL khác). Theo phiên bản năm 2000 của X.509, mở rộng này có thể được đánh dấu là quan trọng hoặc không quan trọng. Tuy nhiên, nếu nó được đánh dấu là quan trọng, thì bên tin tưởng không có lựa chọn trừ khi kiểm tra thông tin CRL mới nhất trước khi sử dụng chứng chỉ cần đánh giá.
* *Delta-CRL là một CRL bổ xung được cung cấp vào các thời điểm nhất định bao gồm các Cert đã hủy trong thời gian từ delta-CRl trước tới khi phát hành Delta CRL này.*
* *Khi đó nếu không sử dụng delta CRL thì nhà phát hành buộc phải phát hành một CRL bao gồm danh sách đầy đủ tất cả các Cert đã hủy từ trước tới nay khi đó CRL này sẽ vô cùng cồng kềnh và khiến Cert của nhà phát hành yếu đi một cách nhanh chóng*
* *Còn nếu sử dụng Delta CRL tương ứng với việc chỉ cần cung cấp các cert đã hủy bỏ giữa hai Distribution Point, để cập nhật vào bản CRL đầy đủ đang có trong tay của người dùng, tất nhiên nếu là người dùng lần đầu tiên sử dụng thì buộc phải tải về bản CRL đầy đủ tại địa chỉ mà nhà phát hành cung cấp.*

# **Câu 12. Minh họa khuân dạng chứng chỉ X.509 ver 3. Vì sao khuân dạng X.509 v1 và v2 không đáp ứng được tất cả các yêu cầu? giải thích việc bổ sung một số trường V3)**

**Khuân dạng táng câu 5 vào.**

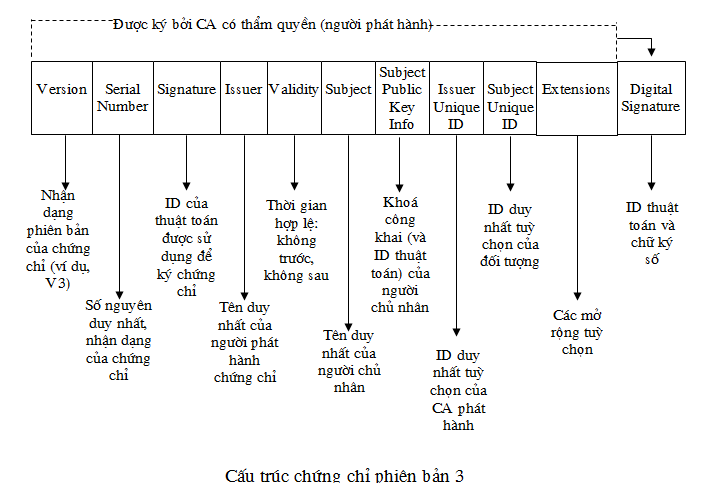
Chứng chỉ khoá công khai phiên bản 1 ban đầu được định nghĩa trong Khuyến cáo X.509 năm 1988, nó thiếu sót do tính không mềm dẻo cố hữu, bởi vì phiên bản này không thể được mở rộng để hỗ trợ các đặc tính thêm

Chứng chỉ khoá công khai phiên bản 2 đã sửa chữa nhỏ khuyết điểm này bởi vì nó đơn giản gia cố phiên bản 1 với việc thêm 2 trường lựa chọn. Bởi vì nhu cầu cho các trường này là không đáng kể và vẫn không có khả năng hỗ trợ các mở rộng khác, chứng chỉ khoá công khai phiên bản 2 đã không nhận được sự chấp nhận rộng rãi.

như đã được chỉ ra trong Khuyến cáo X.509 năm 1997, đã được giới thiệu để điều chỉnh những thiếu sót tương ứng với các định nghĩa phiên bản 1 và phiên bản 2. Đặc biệt, phiên bản 3 đề nghị những cải tiến đáng kể đối với phiên bản 1 và phiên bản 2 thông qua việc thêm các lựa chọn mở rộng.

Gần đây nhất (trong tháng 6 năm 2000), bản Khuyến cáo X.509 năm 2000 đã được hoàn thành. Phiên bản năm 2000 bao gồm nhiều thay đổi so với phiên bản trước, bao gồm định nghĩa của hai mở rộng thêm so với chứng chỉ khoá công khai phiên bản 3

* *Version* (phiên bản) chỉ ra phiên bản của chứng chỉ (hoặc là 1, 2 hoặc 3).
* *Serial Number* (Số xeri) là định danh duy nhất cho chứng chỉ này tương đối với người phát hành chứng chỉ
* *Signature* (chữ ký) chỉ ra định danh thuật toán (tức là, định danh đối tượng (Object Identifier – OID), cộng với các tham số tương ứng bất kỳ) của thuật toán được sử dụng để tính chữ ký số trên chứng chỉ. OID đơn giản là biểu diễn duy nhất cho đối tượng đã cho. Khi được biểu diễn bằng lời hoặc trong cách viết giữa những con người, OID được biểu diễn như là một dãy các số nguyên mà được phân tách bởi các dấu chấm (giống như các địa chỉ IP được biểu diễn trong ký hiệu thập phân với các dấu chấm quen thuộc). Các OID là có cấu trúc hình cây về bản chất, và chúng được đăng ký với các thẩm quyền đăng ký của một tổ chức, quốc gia, hoặc quốc tế để đảm bảo rằng OID được định vị cho một đối tượng đã cho là duy nhất. Như một ví dụ, OID cho SHA-1 với RSA (nó có thể được biểu diễn trong trường Signature của một chứng chỉ) là 1.2.840.113549.1.1.5.
* *Issuer* (người phát hành) là một tên phân biệt (Distinguised Name- DN) của CA mà phát hành chứng chỉ và luôn phải được trình bày. DN là một quy ước tên có cấu trúc hình cây được định nghĩa trong Khuyến cáo X.509. Các DN được thiết kế để giúp đảm đảo các tên thực thể là duy nhất. Không quá đi sâu vào chi tiết đối với các thư mục (Directories) và các cây thông tin thư mục (Directory Information Trees), các DN được biểu diễn như là một kết nối của các tên phân biệt tương đối (Relative Distinguished Names- RDNs) từ đỉnh mức gốc xuống tới đỉnh cuối cùng của DN. Ví dụ, “C = CA, O = ADGA, OU = AEPOS Technologies, CN = Steve Lloyd” là một ví dụ về DN. Chú ý rằng mỗi RDN ( C = CA là một RDN, O = ADGA là một RDN, và ...) cần là duy nhất tại mỗi mức, ngược lại thì tính duy nhất của DN về tổng thể không được bảo đảm.
* *Validity* (Tính hợp lệ) chỉ ra cửa sổ của thời gian mà chứng chỉ này cần được xem là hợp lệ trừ khi nó được huỷ theo một cách khác. Trường này là tổ hợp của các thời gian/ngày tháng mà chứng chỉ là Không hợp lệ trước (Not Valid Before) và Không hợp lệ sau (Not Valid After), chúng có thể được biểu diễn theo thời gian UTC hoặc theo Generalized Time (tuy nhiên, RFC3280 có các qui tắc cụ thể tương ứng với việc dùng các biểu diễn thời gian này).
* *Subject* (chủ thể) chỉ ra DN của người chủ chứng chỉ và phải khác null trừ khi một dạng tên thay thế được sử dụng (xem các trường mở rộng sau này).
* *Subject Public Key Info* (thông tin khoá công khai của chủ thể) là khoá công khai (và định danh thuật toán) tương ứng với chủ thể và luôn cần được biểu diễn.
* *Issuer Unique ID* (Định danh duy nhất của người phát hành) là định danh duy nhất không bắt buộc của người phát hành chứng chỉ chỉ được biểu diễn trong phiên bản 2 và phiên bản 3; trường này ít được sử dụng trong cài đặt thực tế, và nó không được khuyến cáo để sử dụng bởi RFC3280.
* *Subject Unique ID* (Định danh duy nhất của chủ thể) là định danh duy nhất không bắt buộc của người chủ chứng chỉ chỉ được biểu diễn trong phiên bản 2 và phiên bản 3; trường này ít được sử dụng trong cài đặt thực tế, và nó không được khuyến cáo để sử dụng bởi RFC3280.



# Câu 13: Những vấn đề có thể gặp phải khi triển khai một hệ thống PKI?Vì sao lại xảy ra những vấn đề đó?

* Mô hình tin cậy:Thứ bậc hay phân tán?

Các triển khai PKI cần dựa vào một trong các mô hình tin cậy. Trong thực tế một số các triển khai doanh nghiệp qui mô lớn nhìn thấy rõ hơn là dựa vào các thứ bậc.

* Tự làm lấy hay đi thuê?

Tự làm khi mà doanh nghiệp quyết định triển khai PKI trong của riêng mình: Tận dụng các tài nguyên của họ, và /hoặc thuê các tài nguyên bên ngoài để trợ giúp với bất kỳ hoặc tất cả các hoạt động bên trong PKI.Đi thuê là khi cơ quan cho phép một bên ở ngoài cung cấp và vận hành một số khía cạnh.

* Tự phát triển sản phẩm hay là đi mua?

Lựa chọn “Tự phát triển” kéo theo việc cơ quan sẵn sàng đầu tư phát triển công nghệ PKI. Lựa chọn “mua” đơn giản có nghĩa rằng cơ quan sẽ mua các sản phẩm và dịch vụ PKI,nhưng lại có thể tự làm hay đi thuê.

* Môi trường áp dụng đóng hay mở?
* Môi trường đóng là một môi trường ở đó chỉ có các truyền thông ở trong miền là được xem xét tới.Miền có thể là một doanh nghiệp, hoặc một tập các doanh nghiệp.
* Môi trường mở là môi trường mà ở đó truyền thông giữa các miền được đòi hỏi hỗ trợ.
* Khuôn dạng chứng chỉ X.509 hay một khuôn dạng chứng chỉ khác?
* Phục vụ một số ứng dụng hay giải pháp tổng thể?
* Các hoạt động trực tuyến hay không trực tuyến?
* Hoạt động trực tuyến là tình huống trong đó các thực thể đầu cuối được kết nối trực tiếp tới mạng. Hoạt động không trực tuyến cho phép các thực thể đầu cuối tiêu thụ ít nhất một tập con của các dịch vụ PKI, mặc dù chúng không được nối trực tiếp tới mạng.
* Hỗ trợ ngoại vi:
* Cần xác định xem cso một module phần cứng amajt mã được yêu cầu tương ứng với hoạt đông CA hay không. Hơn nữa các token cứng hoặc smart-card cũng có thể cho người sử dụng đầu cuối.
* Các yêu cầu về thiết bị:
* Các thành phần nhạy cảm của PKI cần được bảo vệ đúng mức.
* Các yêu cầu về nhân viên:
* Các dạng nhân viên có trình độcao có thể được yêu cầu,bao gồm:
* Các sĩ quan an ninh chịu trách nhiệm để bắt buộc các chính sách an toàn được ra lệnh bởi doanh nghiệp.
* Những người vận hành thực heienj các cài đặt hệ thống, sao lưu, khởi động lại.
* Những người quản trị thực hiện các thao tác hàng ngày chẳng hạn như đăng ký thực thể đầu cuối.
* Thực thể cuối di động:
* Nhiều tổ chức có yêu cầu hỗ trợ những nhân viên trong khi đi công tác hay các nhân viên người mà hay dịch chuyển từ nơi này tới nơi khác trong một ngày làm việc.
* Hủy bỏ chứng chỉ:
* Có thể áp dụng một số kỹ thuật hủy bỏ chứng chỉ khác nhau
* Khôi phục khóa:
* Có thể cài đặt thiết bị khôi phục khóa như là một phần của CA hoặc cài đặt thành phần khôi phục khóa riêng biệt.
* Kho lưu trữ:
* Một số các tùy chọn có thể được cài đặt các thành phần dư thừa có thể cực tiểu hóa mạo hiểm tương ứng với nhiều nguồn gốc rủi ro,việc xem xét các kịch bản trường hợp tồi nhất và đảm bảo rằng các kế hoạch bất ngờ có thể tốt nhất có sẵn là quan trọng.
* Yếu tố giá cả:
* Để xác định giá thành việc triển PKI, không có công thức duy nhất được áp dụng cho tất cả các tổ chức,rất ít các nguồn trong khu vực công khai cung cấp xác định phẩm chất toàn diện.Trường hợp bất kỳ một số các xem xét cần được đánh giá để giúp xác định giá tổng cộng của quyền sở hữu trong một tổ chức đã cho gồm:
* Có bao nhiêu các thành phần phần cứng,tức là các RA,các CA,các máy chủ thư mục được…Số các thành phần có thể phụ thuộc vào nhiều yếu tố bao gồm qui mô của cộng đồng sử dụng, các xem xét địa lý,số các vùng tự trị được cấp cho các ban khác nhau.
* Giá trị của phần mềm và các công cụ hỗ trợ cần thiết?cả việc mua phần mềm ban đầu và giá cả bảo hành phần mềm về sau.
* Hạ tầng cơ sở CNTT đang tồn tại của công ty có thể được khai thác tới mức nào để hỗ trợ cộng đồng mục tiêu.
* Các yêu cầu về tài nguyên tương ứng với kế hoạch, triển khai,hoạt động và bảo hành về sau của hạ tầng cơ sở những gì?
* Các yêu cầu vè tài nguyên tương ứng với việc xác định chính sách và các thủ tục cần để hỗ trợ những người sử dụng/ tổ chức
* Cá thiết bị cần thiết có sẵn sàng để chứa các thành phần hạ tầng cơ sở,nếu không cái gì được yêu cầu và giá cả bao nhiêu.
* Các yêu cầu về tính sẵn sàng của các thành phần gì?giá thành đào tạo là bao nhiêu?
* Mức độ hỗ trợ quản trị cần yêu cầu là gì?
* PKI được triển khai có tương tác với các PKI khác dựa trên công nghệ của các nhà cung cấp khác hay không?Việc chấp nhận công nghệ trên các chuẩn là cần thiết.

**Cau 12:Những vấn đề khi triển khai một hệ thống PKI?**

Khi triển khai hệ thống PKI người ta cần lưu ý đến một số vấn đề sau

* Mô hình triển khai hệ thống PKI
* Các yêu cầu cần thiết, những chức năng bắt buộc của hệ thống PKI.
* **Mô hình triển khai hệ thống:**
  + Mô hình phân cấp.
  + Mô hình mạng.
  + Mô hình danh sách tin cậy.
* **Các yêu cầu của hệ thống PKI:** trong quá trình triển khai hệ thống PKI cần xác định chức năng mà hệ quản lý PKI cần phải có. Những chức năng bắt buộc phải có là:
  + *Khởi tạo CA gốc:*
    - Khi 1 CA tham gia vào hệ thống PKI, nó phải tự cấp phát chứng chỉ cho nó kiểu “tự ký” (self - signed).
    - Đồng thời với việc tạo chứng chỉ của mình, CA cũng khởi tạo CRL.
* *Cập nhật CA gốc:*
  + Các khóa của CA đều có thời gian hiệu lực nhất định nên chúng phải được cập nhật định kỳ.
  + Thời gian hiệu lực của khóa sẽ tùy thuộc vào chính sách được thiết lập đối với hệ thống PKI.
* *Khởi tạo CA thứ cấp:*
  + Nếu xét trên phương diện giao thức quản lý, viêc khởi tạo 1 CA thứ cấp cũng guioongs với việc tạo 1 EE.
  + Điều khác biệt duy nhất là các CA thứ cấp cũng phải khởi tạo 1 CRL của mình
* *Tạo lập CRL:*
  + Trước khi phát hành và gửi đi các thẻ xác nhận, 1 CA mới được khởi tạo phải tạo ra các CRL trống để chuẩn bị cho việc bổ sung các thẻ xác nhận cần hủy bỏ.
  + Các CRL này cũng sẽ được cập nhật thông tin định kỳ theo thời gian hiệu lực của các thẻ xác nhận.
* *Yêu cầu về thông tin hệ thống PKI:*
  + Khi một đối tượng trong hệ thống PKI(CA,RA hoặc EE) muốn có được thông tin trạng thái của 1 CA nào đó, đối tượng này có thể gửi cho CA một yêu cầu về các thông tin trên.
  + CA nhận được yêu cầu phải trả lời băng việc cung cấp ít nhất là các thông tin đã được yêu cầu.
  + Nếu có một số trường hợp thông tin nào đó không thể đáp ứng được thì phải có một thông điệp báo lỗi gửi về cho đối tượng yêu cầu.
* *Khởi tạo EE:*
  + Cũng giống như các CA, những EE cũng phải được khởi tạo khi tham gia vào hệ thống PKI.
* *Yêu cầu chứng chỉ:*
  + Mội EE sau khi khởi tạo nó sẽ yêu cầu 1 chứng chỉ vào bất cứ thời điểm nào.
  + Yêu cầu này được truyền tải bởi 1 thông điệp yêu cầu chứng chỉ nếu đối tượng đã có một cặp khóa để tạo chữ ký thì thông điệp yêu cầu sẽ được nó bảo vệ bằng cách thực thi chữ ký số đối với nó.
  + Nếu yêu cầu chấp nhận, CA sẽ trả về cho đối tượng sử dụng một chứng chỉ mới.
* *Cập nhật khóa:*
  + Khi cặp khóa của một EE không còn hiệu lực nữa, đối tượng này có thể yêu cầu được cập nhật khóa của mình. Yeeuc ầu này được truyền tải bởi thông điệp yeu cầu cập nhật khóa

>> Nếu EE đã có một cặp khóa tạo chữ ký thì thông điệp thì thông điệp yêu cầu này sẽ được bảo vệ qua phương thức chữ ký số.

* + Nếu yêu cầu được chấp thuận thì CA sẽ trả về một thông điệp trả lời yêu cầu cập nhật khóa có chứ một chứng chỉ mới cho đối tượng.

Câu 15 hiểu biết về hộ chiếu điện tử?

Hộ chiếu điện tử là hộ chiếu tích hợp chip điện tử ICC (Integrated Cỉcuit Chip) có chức năng mã hóa và lưu trữ thông tin cá nhân ngƣời dùng.

Thông tin cá nhân người dùng này phải được bảo vệ chống truy nhập trái phép và phải được xác thực tính chính xác, duy nhất của hộ chiếu.

Một trong những công cụ bảo vệ dữ liệu mà hiện nay trên thé giới sử dụng đó là phương pháp mã hóa dữ liệu. Chữ kí số được sử dụng để kí vào các dữ liệu cơ bản và chúng được lưu trữ trong chip.

**Hộ chiếu điện tử tích hợp 3 công nghệ:**

* Nhận dạng tần số Radio (RFID)
  + RFID (Radio Frequency IDentification) là công nghệ nhận dạng đối tượng bằng sóng vô tuyến. Công nghệ này cho phép nhận biết các đối tượng thông qua hệ thống thu phát sóng radio, từ đó có thể giám sát, quản lý hoặc lưu vết từng đối tượng
* Sinh trắc (vân tay, mống mắt)
* Cơ sở hạ tầng khóa công khai PKI (Public key infrastructure).

**+ yêu cầu đối với hộ chiếu điện tử:**

Tính chân thực: Cơ quan cấp hộ chiếu điện tử phải ghi đúng thông tin của người xin cấp hộ chiếu, đảm bảo rằng không có sự nhầm lẫn trong quá trình ghi thông tin vào hộ chiếu.

Tính không thể nhân bản: Yêu cầu này phải đảm bảo không thể tạo ra được bản sao chính xác của chip RFID lưu trong HCĐT.

Tính nguyên vẹn và xác thực: Cần chứng thực tất cả các thông tin lưu trên trang dữ liệu và trong chip RFID không bị thay đổi từ lúc lưu và các thông tin đó đều do cơ quan cấp HCĐT tạo ra.

Tính liên kết người - hộ chiếu: Cần phải đảm bảo rằng HCĐT thuộc về người mang nó, hay nói cách khác, các thông tin lưu trong HCĐT phải thực sự mô tả về người sở hữu hộ chiếu.

Tính liên kết hộ chiếu - chip: Cần phải đảm bảo booklet khớp với mạch RFID nhúng trong nó.

Kiểm soát truy cập: Đảm bảo sự truy cập các thông tin lưu trong chip HCĐT phải được sự đồng ý của chủ sở hữu, hạn chế truy cập đến các thông tin sinh trắc học nhạy cảm và tránh mất mát thông tin.

**+Gồm 2 thành phần chính :**

**MRZ**: MRZ (Machine Readable Zone) là hai dòng dữ liệu liên tục được thiết kế để đọc được bằng máy đọc quang học ở phía cuối trang dữ liệu. Mỗi dòng đều phải có 44 ký tự và được sắp xếp theo phông OCR-B in hoa gồm bốn thông tin quan trọng:

• Họ tên: Xuất hiện ở dòng đầu tiên từ ký tự thứ 6 đến ký tự thứ 44.

• Số hộ chiếu: Xuất hiện ở 9 ký tự đầu tiên của dòng thứ 2.

• Ngày tháng năm sinh: Xuất hiện từ ký tự thứ 14 đến 19 của dòng thứ 2 theo định dạng YYMMDD.

• Ngày hết hạn: Xuất hiện từ ký tự 22 đến 29 của dòng thứ 2 theo định dạng YYMMDD.

**Mạch tích hợp tần số radio RFIC:** Mạch tích hợp RFIC gồm một chip tuân theo chuẩn ISO/IEC 14443 và một ăngten vòng không những dùng để kết nối mà còn dùng để nhận biết tín hiệu từ đầu đọc. Điều này giải thích vì sao HCĐT không có nguồn điện trong, năng lượng hoạt động cho chip được thu nhận qua ăngten.

Mạch RFIC có thể được gắn vào một trong các vị trí khác nhau trong booklet, thông thường là giữa phần bìa và phần trang dữ liệu. Trong quá trình gắn, cần phải đảm bảo rằng chip không bị ăn mòn và không bị rời ra khỏi booklet.

**+Tổ chức thông tin trong hộ chiếu điện tử:**tổ chức thông tin logic của hộ chiếu điện tử là tổ chức thông tin trong LDS (Logical Data Structure - LDS) thành 16 nhóm(DG). Trong đó có 2 nhóm đầu là cố đinh và không có khả năng thay đổi, 14 nhóm cuối có thể thay đổi được.

DG1: Nhóm dữ liệu chứa thông tin giống với thông tin lưu trong MRZ.

DG2: Nhóm dữ liệu lưu trữ ảnh khuôn mặt đã mã hóa của người sở hữu hộ chiếu. Ảnh này định dạng theo chuẩn JPEG hoặc JPEG2000. Kích thước ảnh khoảng từ 12 đến 20K (kilobytes). Đây là thông tin thống nhất trên toàn cầu giúp cho việc kiểm tra định danh của người sử dụng với các thông tin trong HCĐT.

**+Các nguy cơ đối với hộ chiếu điện tử là :**

**Clandestine scanning:**do không bắt buộc có kiểm soát truy cập hoặc mã hóa truyền thông giữa chip RFID và đầu đọc trong quá trình xác thực HCĐT. Nên thông tin người dùng dễ bị scanning và bị lộ.

**Clandestine tracking:** Nguy cơ này liên quan đến định danh của thẻ RFID. Việc xác định được định danh của thẻ phi tiếp xúc cho phép xác định được nguồn gốc của HCĐT, chẳng hạn như quốc tịch của người mang hộ chiếu.

**Skimming and Cloning**: Khi dữ liệu trong chip RFID bị rò rỉ, nó cho phép nhân bản chip RFID để tạo ra một HCĐT mới. Đây là một trong những nguy cơ nghiêm trọng cần phải được chú ý trong suốt quá trình phát hành và sử dụng HCĐT.

**Eavesdropping**: Nguy cơ nghe lén thông tin luôn được coi là nguy cơ có tính nguy hiểm nhất trong vấn đề bảo mật hộ chiếu điện tử. Nguy cơ này diễn ra trong quá trình đầu đọc hộ chiếu đọc dữ liệu từ chip RFID. Những thông tin được truyền giữa chip và đầu đọc có thể bị nghe lén trong một khoảng cách nhất định. Hiệu ứng lồng Faraday đối với hộ chiếu điện tử cũng không thể ngăn chặn được nguy cơ này. Tại các điểm xuất nhập cảnh, việc kiểm soát nguy cơ này có thể thực hiện được khi làm tốt việc kiểm tra tự động những thiết bị đọc thẻ RFID khác.

**Biometric data-leakage:** Cùng với các thông tin cá nhân khác, HCĐT còn chứa các dữ liệu sinh trắc học của người sở hữu hộ chiếu như ảnh khuôn mặt, dấu vân tay, mống mắt. Đây đều là những dữ liệu đặc biệt quan trọng và có nguy cơ bị lộ ra ngoài. Nguy cơ này liên quan mật thiết đến vấn đề đảm bảo an toàn đối với dữ liệu sinh trắc nói riêng và toàn bộ dữ liệu lưu trong chip nói chung.

**Cryptographic Weeknesses:** Nguy cơ này liên quan đến mô hình bảo đảm an toàn và bảo mật thông tin lưu trong chip RFID. ICAO có đưa ra một cơ chế tùy chọn cho phép xác thực và mã hóa truyền thông giữa chip và đầu đọc. Bằng cách đọc vùng dữ liệu MRZ sẽ nhận được khóa mã hóa K. Tuy nhiên, khi đầu đọc đã biết được khóa K thì không có cơ chế nào để hủy bỏ việc truy cập đến chip. Chính vì vậy cần phải sử dụng các kỹ thuật mạnh mẽ để bảo đảm an toàn bảo mật dữ liệu.

**+Các cơ chế bảo mật thông tin trong HCDT:**

**Passive Authentication (PA)**: Cơ chế xác thực bị động, là cơ chế bắt buộc đối với quá trình xác thực HCĐT, kiểm tra tính nguyên vẹn và xác thực của thông tin lưu trong chip RFID bằng cách kiểm tra chữ ký của cơ quan cấp hộ chiếu để xác thực dữ liệu được lưu trong các nhóm dữ liệu LDS trên chip RFID.

**Basic Access Control (BAC)**: Cơ chế kiểm soát truy cập cơ bản, chống lại việc nghe lén và đọc trộm thông tin trong HCĐT mà chưa có sự đồng ý của người sở hữu, ngăn chặn được nguy cơ *Skimming* và*Eavesdropping.*

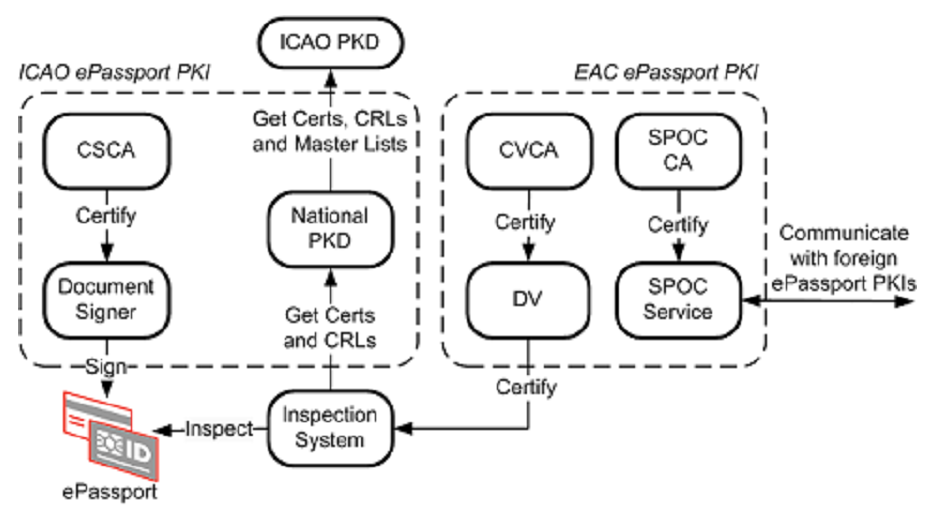
**Active Authentication (AA)**: Cơ chế xác thực chủ động, đảm bảo tính duy nhất và xác thực của chip tích hợp trong HCĐT bằng cách đưa ra một cặp khóa riêng. Khóa bí mật được lưu trữ trong nhóm dữ liệu DG15 và được bảo vệ bởi cơ chế PA. Khóa công khai tương ứng được lưu trữ trong bộ nhớ bảo mật và có thể chỉ được sử dụng trong chip RFID và không thể đọc được ở bên ngoài. Cơ chế này chỉ nên được sử dụng ở những nơi mà BAC đã được thiết lập.

**Extended Access Control (EAC):** Cơ chế kiểm soát truy cập mở rộng, tăng cường bảo vệ các thông tin sinh trắc học nhạy cảm như vân tay, mống mắt… đồng thời khắc phục hạn chế của quá trình xác thực chủ động. Cơ chế này gồm hai giai đoạn:

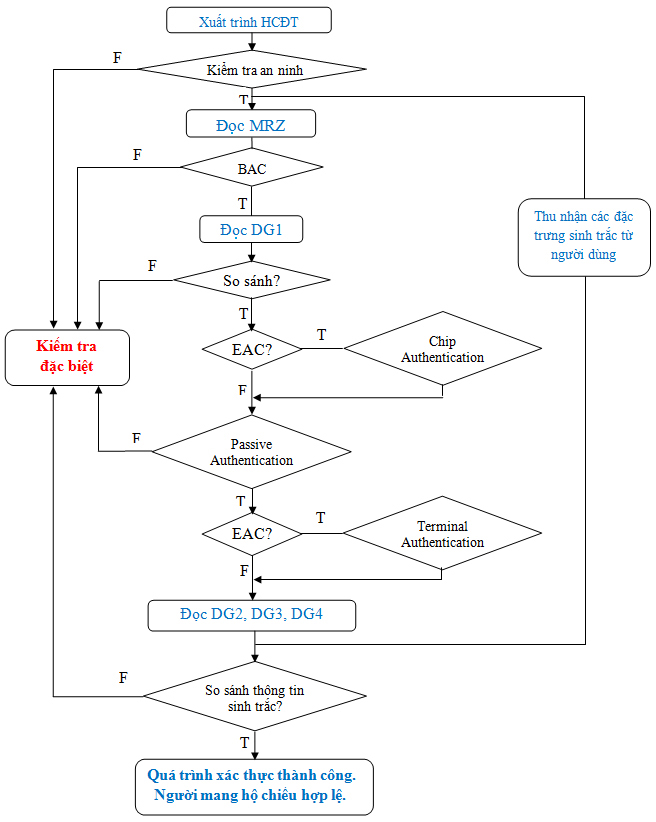
**Chip Authentication:** là một giao thức cho phép hệ thống kiểm tra xác thực tính đúng đắn của chip RFID trong HCĐT. Trước khi sử dụng giao thức này thì chip RFID cần được bảo vệ bởi giao thức BAC.

**Terminal Authentication:** là giao thức chip RFID xác minh xem hệ thống kiểm tra có được quyền truy cập đến vùng dữ liệu nhạy cảm hay không. Khi hệ thống kiểm tra có thể truy cập đến dữ liệu sinh trắc thì tất cả truyền thông phải được bảo vệ một cách phù hợp. Trước khi thực hiện giao thức này thì bắt buộc phải thực hiện thành công giao thức Chip Authentication.

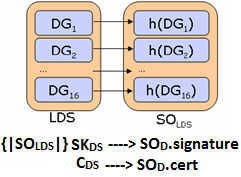
**+ mô hình**

**+** 

**+ quy trình xác thực:**

****

**+ chữ ký**

****

**Câu 11: chữ ký số?thuộc tính và yêu cầu của chữ ký số**

**ĐN:** Chữ ký số là một phần dữ liệu được đính kèm với bản tin, dùng để nhận dạng và xác thực người gửi và dữ liệu của bản tin, sử dụng mã hoá khoá công khai. Người gửi sử dụng hàm hash một chiều để tạo ra một bản mã hash có độ dài 32 bit từ dữ liệu của bản tin. Sau đó, người gửi sẽ mã hoá bản mã hash đó(hash-code) bằng khoá riêng của người gửi. Người nhận sẽ tính toán lại mã hash đó từ dữ liệu đó và giải mã bản mã hash đó bằng khoá công khai của người gửi. Nếu hai mã hash đó giống nhau, thì người nhận có thể chắc chắn rằng dữ liệu đó không bị sửa đổi và dữ liệu đó đúng là của người gửi.

**Quá trình kiểm tra chữ ký số**

Khi người nhận nhận được thông báo, để kiểm tra tính hợp lệ của nó, đầu tiên người nhận sẽ dùng khoá công khai của người gửi để giải mã chữ ký số. Kết quả của quá trình giải mã chữ ký số là bản tóm lược thông báo của người gửi tạo ra. Sau đó, người nhận dùng hàm băm một chiều để tính toán bản tóm tắt qua nội dung của thông báo một lần nữa rồi lấy kết quả đem so sánh với bản tóm lược thông báo vừa được giải mã ở trên, nếu kết quả giống nhau thì quá trình kiểm tra thành công. Ngược lại có thể kết luận đây là một thông báo đã bị giả mạo hoặc thông tin đã bị thay đổi trên quá trình gửi đi.

### Quá trình kiểm tra chữ ký số

 Khi người nhận nhận được thông báo, để kiểm tra tính hợp lệ của nó, đầu tiên người nhận sẽ dùng khoá công khai của người gửi để giải mã chữ ký số. Kết quả của quá trình giải mã chữ ký số là bản tóm lược thông báo của người gửi tạo ra. Sau đó, người nhận dùng hàm băm một chiều để tính toán bản tóm tắt qua nội dung của thông báo một lần nữa rồi lấy kết quả đem so sánh với bản tóm lược thông báo vừa được giải mã ở trên, nếu kết quả giống nhau thì quá trình kiểm tra thành công. Ngược lại có thể kết luận đây là một thông báo đã bị giả mạo hoặc thông tin đã bị thay đổi trên quá trình gửi đi.

**Các chuẩn liên quan về chữ ký số:**

Đảm bảo tính mở rộng của hệ thống,

Đảm bảo tính tương tác giữa các thành phần của PKI và giữa hệ thống PKI này với hệ thống PKI khác

Chữ ký số phải tuân theo các chuẩn của những nhà cung cấp và các tổ chức liên quan quy định đó là các chuẩn:

* + Các thuật toán mật mã,
  + Lưu trữ khóa,
  + Quản lý chứng chỉ và CRL,
  + Công bố chứng chỉ và CRL,
  + Hủy bỏ chứng chỉ,
  + Dịch vụ tem thời gian,
  + Các dịch vụ cho bên tin cậy thứ 3;
  + CP và CPS;

# **Câu 15: Trình bày hiểu biết về các giao thức của PKI?không thể tìm đâu được tài liệu**

* 1. Giao thức quản trị
  2. Giao thức hoạt động
  3. Giáo thức trạng thái chứng chỉ trực tuyến

# **Câu 16.Xác thực mạnh () như câu trên luôn, có slide ông thầy nói nhưng chẳng thấy liên quan tí nào.**

* 1. Định nghĩa
  2. Mô hình