Mục lục

[**Câu 1 : An toàn thông tin là gì ? Đặc điểm của an toàn thông tin ?** 2](#_Toc60607174)

[**Câu 2. Các nguy cơ tiềm ẩn trong môi trường điện tử và giải pháp cho từng nguy cơ** 2](#_Toc60607175)

[**Câu 3: So sánh chữ ký số và chứng thư số?** 2](#_Toc60607176)

[**Câu 4: Chính phủ điện tử là gì? Chức năng, mục tiêu.** 3](#_Toc60607177)

[**Câu 5: Chữ ký số là gì? Mô tả và vẽ quá trình tạo chữ ký và kiểm tra chữ ký của người A. Giải thích vì sao lại dùng chữ ký số cho việc xác thực.** 3](#_Toc60607178)

[**Câu 6: Chứng thư số là gì. Trình bày các mô hình kiến trúc tin cậy của PKI (không chắc chắn có câu cuối 7 mô hình)** 4](#_Toc60607179)

[**Câu 7: So sánh ưu và nhược điểm của hệ mật khóa công khai và hệ mật khóa bí mật, vẽ mô hình kết hợp 2 hệ này( không chắc đúng).** 7](#_Toc60607180)

[**Câu 8 : Vẽ mô hình quản lý vòng đời khóa/ chứng chỉ.** 8](#_Toc60607181)

[**Câu 9: Cơ sở hạ tầng khóa công khai PKI là gì và tại sao cần có PKI** 11](#_Toc60607182)

[**Câu 10: PKI đã và chưa làm được gì**. **Lợi ích** 11](#_Toc60607183)

[**Câu 11: CP ( chính sách chứng thư) là gì? CPS ( quy chế chứng thư) là gì? So sánh CP và CPS, đánh giá tài liệu mà chi tiết hơn và được dung để đánh giá tổ chức chính xác hơn.** 12](#_Toc60607184)

[**Câu 12: Vẽ mô hình và trình bày các bước của quy trình đăng ký và thu hồi chứng thư số và khóa của một PKI** 13](#_Toc60607185)

[**Câu 13: Trình bày các khái niệm cách thức hoạt động của OCSP. Nêu hạn chế, vẽ mô hình và quá trình thu thập thông tin** 14](#_Toc60607186)

[**Câu 14: Xác thực là gì? Trình bày dịch vụ xác thực trong PKI** 15](#_Toc60607187)

[**Câu 15: PKI triển khai bao nhiêu cặp khóa? Là những cặp khóa nào ? việc sao lưu khóa nên khuyến cáo thực hiện vơi cặp khóa nào. Vì sao?** 16](#_Toc60607188)

[**Câu 16: PKI có những dịch vụ nào? Có mấy dịch vụ cốt lõi. Trình bày** 16](#_Toc60607189)

[**Câu 17: Hỗ trợ ứng dụng: mô hình đăng nhập 1 lần** 17](#_Toc60607190)

[**Câu 18: Ý nghĩa của tem thời gian trong PKI** 17](#_Toc60607191)

[**Câu 19: Nêu định nghĩa của PKI? Vẽ mô hình tổng thể của hệ thống PKI và trình bày hiểu biết về các thành phần trong hệ thống PKI đó** 18](#_Toc60607192)

[**Câu 20: Trình bày thiết kế chi tiết kiến trúc phân cấp PKI với các mức phân cấp CA** 20](#_Toc60607193)

[**Câu 21: Nêu nhược điểm của CRL ver1? CRL VER2 khắc phục được những nhược điểm đó như thế nào. Trình bày khuôn dạng của chứng thu số X.509 VER3.** 21](#_Toc60607194)

[**Câu 22: Những vấn đề có thể gặp phải khi triển khai một hệ thống PKI? Vì sao lại xảy ra những vấn đề đó?** 22](#_Toc60607195)

[**Câu 23: Xác minh tính hợp lệ của chứng thư số gồm mấy bước, vẽ lược đồ mô tả các bước đó** 23](#_Toc60607196)

[**Câu 24: Hiểu biết về hộ chiếu điện tử** **.** 23](#_Toc60607197)

[**Câu 25: Chữ ký số?thuộc tính và yêu cầu của chữ ký số** 25](#_Toc60607198)

[**Câu 26: 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?** 26](#_Toc60607199)

[**Câu 27: 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)** 27](#_Toc60607200)

[**Câu 28: Tương lai của PKI:  nguyên nhân và hướng phát triển** 29](#_Toc60607201)

[**Câu 29: Trình bày hiểu biết về các giao thức của PKI?** 30](#_Toc60607202)

[**Câu 30: Yêu câu cần để triển khai một hệ thống PKI?** 30](#_Toc60607203)

[**Câu 31: 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.** 31](#_Toc60607204)

# **Câu 1 : An toàn thông tin là gì ? Đặc điểm của an toàn thông tin ?**

- An toàn thông tin là hành động ngăn cản, phòng ngừa sự sử dụng, truy cập, tiết lộ, chia sẻ, phát tán, ghi lại hoặc phá hủy thông tin chưa có sự cho phép.

- Đặc điểm:

+ Đảm bảo tính bảo mật

+ Đảm bảo tính toàn vẹn

+ Đảm bảo tính xác thực

+ Đảm bảo tính sẵn sàng

+ bảo vệ tài nguyên và tính riêng tư của hệ thống

# **Câu 2. 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 3: So sánh chữ ký số và chứng thư số?**

* **Chữ ký số**
* **Chữ ký số** là một dạng chữ ký điện tử. Dùng nó để cam kết lời hứa của mình và điều đó không thể rút lại được. Chữ ký số không phải sử dụng giấy mực, nó gắn đặc điểm nhận dạng của người ký vào bản cam kết.
* Chữ ký số do người sử dụng tạo ra sau khi được nhà cung cấp dịch vụ cung cấp chứng thư số.
* **Chứng thư số**
* Chứng thư số là một loại chứng thư điện tử do tổ chức dịch vụ chứng thực chữ ký số cung cấp. Có thể được xem chứng thư số như là một “chứng minh thư” của doanh nghiệp dùng trong môi trường của internet và máy tính.
* Chứng thư số được sử dụng để các đối tác của người sử dụng biết và xác định được chữ ký, chứng minh của mình là đúng. Chứng thư số sẽ bao gồm các nội dung sau:Tên của Tổ chức cung cấp dịch vụ chứng thực chữ ký số ,Tên của Thuê bao , Số hiệu chứng thư, thời hạn hiệu lực, chữ ký số của tổ chức chứng thực, phạm vi sử dụng,…
* Chứng thư số được sử dụng để xác định chắc chắn danh tính của một đối tượng, tổ chức khi tham gia vào giao dịch điện tử dựa trên máy chủ xác thực danh tính.
* Chứng thư số là cơ sở để đối tác có thể xác nhận việc ký số có đúng hay không thì chữ ký số đóng vai trò xác nhận thông tin văn bản, hoặc cam kết của cá nhân hay tổ chức. Mối quan hệ giữa chữ ký số và chứng thư số là mối quan hệ hỗ trợ.

# **Câu 4: Chính phủ điện tử là gì? Chức năng, mục tiêu.**

* Chính phủ điện tử là chính phủ ứng dụng công nghệ thông tin và truyền thông nhằm tăng hiệu quả hoạt động của các cơ quan chính phủ, phục vụ ngƣời dân và doanh nghiệp tốt hơn.
* **Chức năng**
* Thứ nhất, CPĐT đã đưa chính phủ tới gần dân và đưa dân tới gần chính phủ.
* Thứ hai, CPĐT làm minh bạch hóa hoạt động của chính phủ, chống tham nhũng, quan liêu, độc quyền
* Thứ ba, CPĐT giúp chính phủ hoạt động có hiệu quả trong quản lý và phục vụ dân (cải cách hành chính và nâng cao chất lƣợng dịch vụ công)
* **Mục tiêu:**

- Tạo môi trường kinh doanh tốt hơn;

- Khách hàng trực tuyến, không phải xếp hàng;

- Tăng cường sự điều hành có hiệu quả của chính phủ và sự tham gia rộng rãi của người dân;

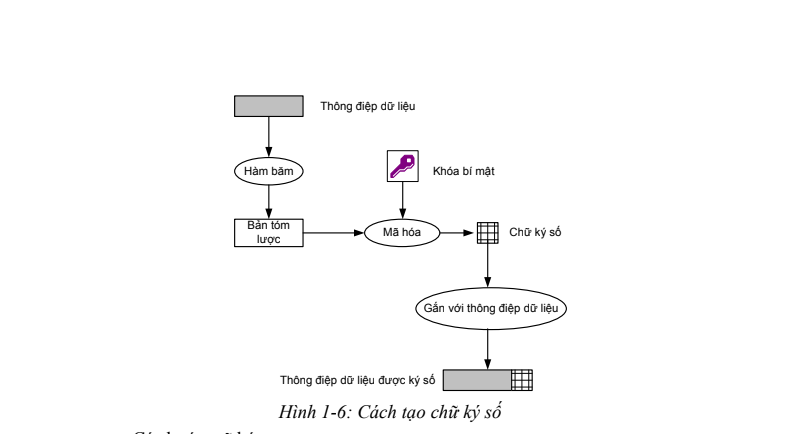
- Nâng cao năng suất và tính hiệu quả của các cơ quan chính phủ;

- Nâng cao chất lượng cuộc sống cho các cộng đồng vùng sâu vùng xa.

# **Câu 5: Chữ ký số là gì? Mô tả và vẽ quá trình tạo chữ ký và kiểm tra chữ ký của người A. Giải thích vì sao lại dùng chữ ký số cho việc xác thực.**

- **Chữ ký số** là một dạng chữ ký điện tử. Về căn bản, chữ ký số cũng giống như chữ viết tay vậy. Dùng nó để cam kết lời hứa của mình và điều đó không thể rút lại được. Chữ ký số không phải sử dụng giấy mực, nó gắn đặc điểm nhận dạng của người ký vào bản cam kết.

**- Tạo chữ ký số:**

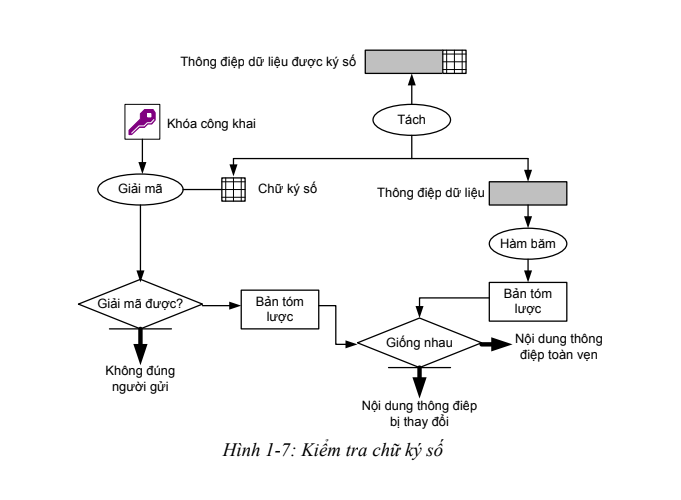


1. Dùng giải thuật băm để thay đổi thông điệp cần truyền đi. Kết quả ta được một bản tóm lược

2. Sử dụng khóa bí mật của người gửi mã để mã hóa bản tóm lược thu được ở bước 1 🡺 thu được chữ ký số

3. Ghép chữ ký số vào văn bản gốc, mọi sự thay đổi trên văn bản gốc hoặc chữ ký sẽ bị phát hiện trong giai đoạn kiểm tra. Ngoài ra, việc ký số này đảm bảo người nhận tin tưởng văn bản này xuất phát từ người gửi chứ không phải là ai khác.

* **Cách kiểm tra**



1. Dùng khóa công khai của người gửi để mã chữ ký số của văn bản
2. Dùng giải thuật băm để băm văn bản đính kèm
3. So sánh kết quả ở bước 1 và 2 nếu trùng nhau ta kết luận: dữ liệu nhận được có tính toàn vẹn ( vì kết quả băm là duy nhất và một chiều) dữ liệu nhận được do chính người gửi gửi đi vì chỉ duy nhất người gửi mới có khóa bí mật phù hợp với khóa công khai đã được sử dụng để giải mã. Vậy tính chồng chối bỏ và tính xác thực được kiểm tra và xác nhận

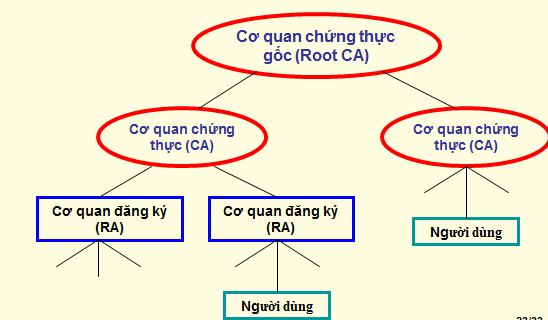
* Giải thích như trên

# **Câu 6: Chứng thư số là gì. Trình bày các mô hình kiến trúc tin cậy của PKI (không chắc chắn có câu cuối 7 mô hình)**

* Chứng thư số là một loại chứng thư điện tử do tổ chức dịch vụ chứng thực chữ ký số cung cấp. Có thể được xem chứng thư số như là một “chứng minh thư” của doanh nghiệp dùng trong môi trường của internet và máy tính.

- 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 quản chứng thực, là duy nhất. Là điểm tin cậy cho người dung trong hệ thống các CA

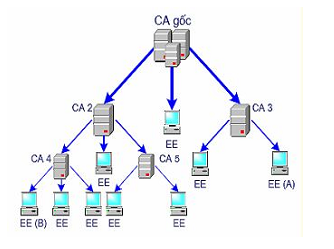
*Người dùng tin cậy vào Root CA, họ sẽ tin cậy vào CA được cấp chứng chỉ bởi Root CA*

* 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.
* ***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.

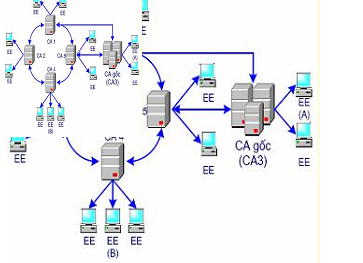
***Ưu điểm:***

* 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****:*

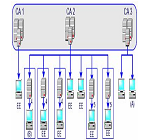
* Đây là mô hình linh động, thích hợp với các mối liên hệ - quan hệ tin cậy lẫn nhau trong thực tế của công việc kinh doanh.
* Cho phép các CA xác thực ngang hàng trực tiếp.

=> 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:**

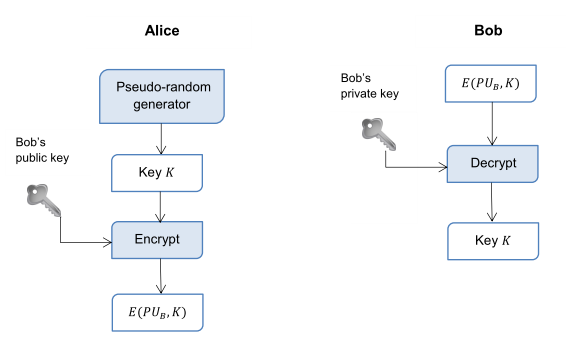
* Việc quản lý danh sách CA được tin cậy của một tổ chức là rất khó khăn.
* Cấu trúc chứng chỉ không có nhiều hỗ trợ cho việc tìm ra các nhánh xác nhận.
* Không có những hỗ  trợ  trực tiếp đối với các cặp chứng  chỉ  ngang hàng do vậy hạn chế  của CA trong việc quản lý sự tin cậy của mình với các CA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

# **Câu 7: So sánh ưu và nhược điểm của hệ mật khóa công khai và hệ mật khóa bí mật, vẽ mô hình kết hợp 2 hệ này( không chắc đúng).**

* Ưu điểm và nhược điểm :

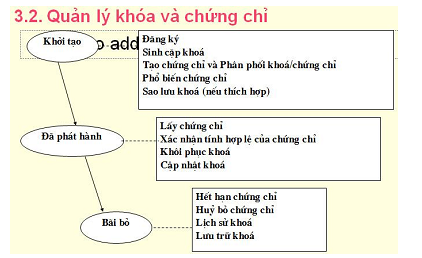
+ Các thuật toán mã hóa đối xứng có tốc độ nhanh hơn và đòi hỏi sức mạnh tính toán thấp hơn, nhưng nhược điểm khi sử dụng loại mã hóa này là cần gửi khóa. Vì phương thức này sử dụng cùng một khóa để mã hóa và giải mã thông tin, nên khóa đó phải được gửi cho bất kỳ ai cần truy cập dữ liệu, và điều này sẽ tự nhiên mở ra các nguy cơ về bảo mật.

+ Ngược lại, mã hóa bất đối xứng giải quyết vấn đề gửi khóa vì phương thức này sử dụng khóa công khai để mã hóa và khóa cá nhân để giải mã. Tuy nhiên, đổi lại, các hệ thống mã hóa bất đối xứng có tốc độ chậm hơn nhiều so với hệ thống đối xứng và đòi hỏi nhiều khả năng tính toán hơn vì khóa của chúng có độ dài lớn hơn nhiều.

* Mô hình: 

# **Câu 8 : Vẽ mô hình quản lý vòng đời khóa/ chứng chỉ.**

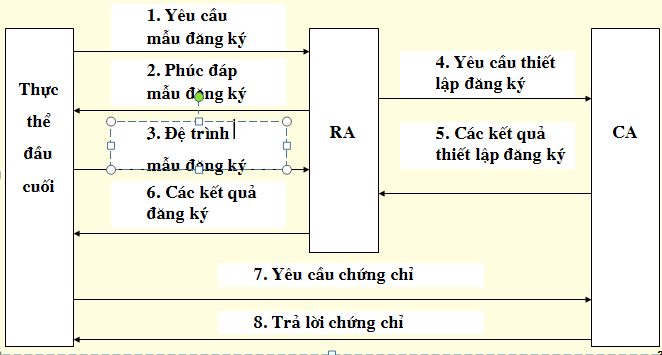
* Mô hình quản lý khóa và vòng đời khóa



**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

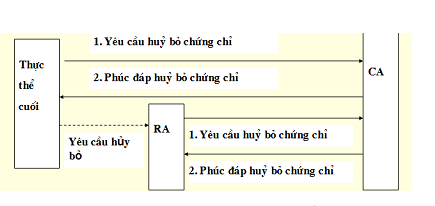
**B2- Giai đoạn sau phát hành**

* 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 9: Cơ sở hạ tầng khóa công khai PKI là gì và tại sao cần có PKI**

* Cơ sở hạ tầng khóa công khai (PKI) là một hệ thống tập hợp bao gồm phần cứng, phần mềm, con ngƣời, chính sách và các thủ tục cần thiết để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi các chứng thư số.
* PKI là cơ sở của một hạ tầng an ninh rộng khắp, các dịch vụ của PKI được cài đặt và thực hiện bằng cách sử dụng các khái niệm và kỹ thuật của mật mã khoá công khai.
* Tại sao nên dung PKI ?

+ cung cấp xác thực mạnh

+ nó gắn cặp khoá bí mật/công khai với một cái tên

+ 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 10: PKI đã và chưa làm được gì**. **Lợi ích**

* **Đã làm được**
* 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 chỉ cung cấp xác thực

**Chưa làm được**

* PKI không cung cấp việc 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
* PKI không làm cho mọi vật trở nên an toàn
* 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
* 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 11: CP ( chính sách chứng thư) là gì? CPS ( quy chế chứng thư) là gì? So sánh CP và CPS, đánh giá tài liệu mà chi tiết hơn và được dung để đánh giá tổ chức chính xác hơn.**

**Chính sách (CP)**

* Chính sách chứng thư (CP) là một tài liệu mô tả cá 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 địch dự kiến của một chứng thư
* Sự cần thiết của chính sách chứng thư:

+ Chính sách chứng thu cung cấp mức tin cậy xác định cho relying party theo quyết định có sử dụng chứng thư số hay khoogn trong TH cụ thể

+ Chính sách là cơ sở cho hoạt động điểm toán

+ xây dựng long tin hay đánh giá về một CA

**Quy chế chứng thực (CPS)**

* Quy chế chứng thực là một tài liệu mô tả các biện pháp đảm bảo an toàn cho hoạt động của CA và quản lý các chứng thu đã phát hành của CA đó
* Sự cần thiết của quy chế chứng thực:

+ Cung cấp mức độ tin cậy xác định cho replying party quyết định có sử dụng chứng thư số hay không trong TH cụ thể

+ Đưa ra đánh giá chính xác hơn về độ tin cậy của CA só với dựa vào CP vì CP có thể được viết ra và dung được cho nhiều miền PKI, CA khác nhau

+ Là tài liệu chỉ ra các biện pháp thực hiện yêu cầu của chính sách chứng thư.

**Mối quan hệ:**

* Sự giống nhau:

+ CP và CPS đều giải quyết các chủ đề về mối quan tâm của replying party đến cập độ an toàn và mực điêu của chứng thư số có nên tin cậy hay không

+ CP và CPS đều do tổ chức vận hành CA phát hành

* Sự khác nhau:

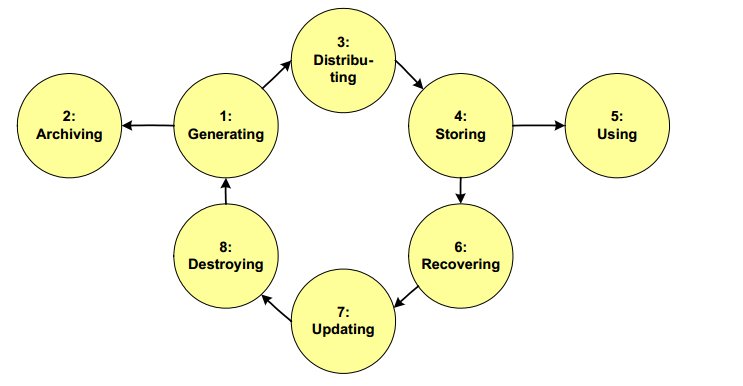
+ mục đích của CP là xác định các bên tham gia cần phải thực hiện điều gì, CPS là chỉ ra cách các bên tham gia thực hiện chức năng và thi hành quyền như thế nào

+ CP chỉ xác định các yêu cầu và chuẩn còn CPS xác định cách thức thực hiện của các bên nên nó chỉ áp dụng được với một miền PKI, CA, tổ chức cụ thể

+ CPS chỉ ra cách thực hiện còn CP chỉ ra các yêu cầu nên CPS thường chi tiết hơn CP

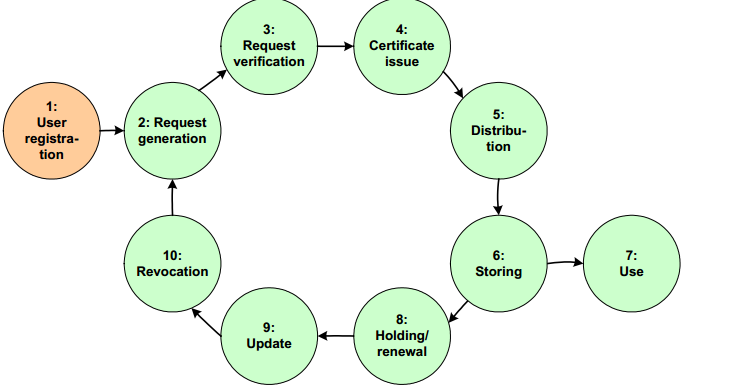
**Câu 12: Vẽ mô hình và trình bày các bước của quy trình đăng ký và thu hồi chứng thư số và khóa của một PKI**

* **Vòng đời của khóa như như thế nào?**



* 1. Tạo khóa: Là công việc quan trọng trong việc duy trì sự tin cậy, mức độ an toàn của khóa phụ thuộc vào yêu cầu tạo khóa và môi trường tạo khóa.
  2. Cất giữ khóa: Sau khi tạo, khóa sẽ lưu trữ ở tổ chức CA và được sử dụng trong dịch vụ khôi phục khóa
  3. Phân Phối: Sau khi tạo khóa, khóa được chuyển tiếp vào thiết bị lưu trữ, private key sẽ được lưu trong token – thiết bị phần cứng bảo mật, public key sẽ gửi đến cơ quan chứng nhận CA để tạo chứng thư số
  4. Lưu trữ khóa: Sau đó khóa được lưu trong một thiết bị phần cứng an toàn. Thiết bị lưu trữ có thể là Token hoặc Smart Card
  5. Sử dụng khóa: Người dùng sử dụng cặp khóa lưu trong token để kí văn bản, dữ liệu
  6. Khôi phục khóa: Do mất khóa, người dùng sẽ gửi yêu cầu lên cơ quan chứng nhận CA đề nghị yêu cầu khôi phục khóa
  7. Cập nhật khóa: Khóa tồn tại trong một khoảng thời gian dài sẽ giảm khả năng an toàn nên phải cập nhật khóa sau một khoảng thời gian
  8. Hủy khóa: Khi khóa bị lộ hoặc có nguy cơ mất an toàn sẽ thực hiện hủy khóa để đảm bảo an toàn

**Vòng đời của chứng thư số như thế nào?**

****​

1. Người dùng đăng ký: Đầu tiên người dùng sẽ làm thủ tục đăng kí chứng thư số với cơ quan đăng kí.
2. cầu tạo chứng thư số: Là một đoạn text để gửi cho CA yêu cầu tạo chứng thư số.
3. Xác minh yêu cầu chứng thư số: Tiếp theo cơ quan chứng nhận CA sẽ tiến hành xác minh thông tin trong yêu cầu chứng thư số bằng cách giải mã và so sánh thông tin, nếu thông tin chính xác sẽ phát hành chứng thư số.
4. Phát hành chứng thư số: Sau khi xác minh thông tin là chính xác thì cơ quan chứng nhận sẽ dùng private key CA kí lên chứng thư số, để chứng nhận rằng chứng thư số này do CA cấp.
5. Phân phối chứng thư số: Sau khi phát hành chứng thư số sẽ được phân phối tới cơ quan đăng ký (RA) và kho lưu trữ chứng thư số (CR).
6. Lưu trữ chứng thư số: Chứng thư số được gửi tới người dùng và lưu trong thiết bị phần cứng an toàn token.
7. Sử dụng chứng thư số: Người dùng sử dụng chứng thư số để đính kèm vào văn bản sau khi đã kí số.
8. Tạm giữ, cấp lại chứng thư số: Tạm giữ chứng thư số là việc thu hồi chứng thư số trong một khoảng thời gian xác định. Cấp lại chứng thư số là quá trình cấp lại chứng thư chỉ thay đổi hạn sử dụng.
9. Cập nhật chứng thư số: Cập nhật là quá trình ban hành chứng thư số mới với cặp khóa mới, cập nhật lại chứng thư số khi có sự thay đổi về khóa hoặc thay đổi thông tin chứng thư số.
10. Thu hồi chứng thư số: Là một trong những dịch vụ quan trọng, yêu cầu thu hồi do người dùng hoặc tổ chức có thẩm quyền yêu cầu. Một số lý do thu hồi như: Người dùng gửi yêu cầu kết thúc, thông tin trong chứng thư sai khác so với thực tế.

# **Câu 13: Trình bày các khái niệm cách thức hoạt động của OCSP. Nêu hạn chế, vẽ mô hình và quá trình thu thập thông tin**

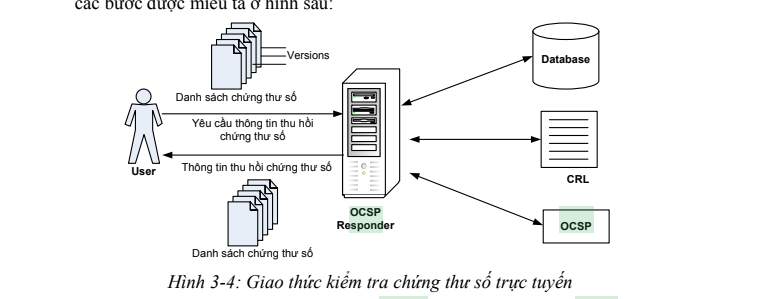
* OCSP là một giao thức được sử dụng để kiểm tra trạng thái của một chứng thư có chuẩn dưới dạng là X.509. Hoạt động theo mô hình client/server, các thông điệp của OCSP được mã hóa theo chuẩn ANS.1 và được truyền qua giao thức HTTP.
* **Các hạn chế:**

+ Mặc dù là một giao thức trực tuyến, nhưng không thể đảm bảo chắc chắn rằng việc thu hồi chứng thư số không bị chậm trễ trong khi sử dụng OCSP

+ OCSP không xác định cách thức thông tin được gọi ra từ kho lưu trữ CRL tới máy phản hồi CRL cuối.

+ Phản hối của máy phản hồi được ký số, vì thế có thể làm giảm hiệu suất hoạt động.

* **Quá trình thu thập thông tin:**



1. Người dùng gửi một yêu cầu OCSP tới máy phản hồi OCSP. Yêu

cầu này bao gồm các thông tin như: tên của CA, số serial của chứng thư số, số phiên bản giao thức

2. Khi nhận được yêu cầu, máy phản hồi OCSP xử lý các yêu cầu và trả lời các thông tin trạng thái của chứng thư số. Các thông tin trạng thái này cũng có thời gian hợp lệ của thông tin và định danh chứng thư số. Trạng thái của chứng thư số có thể có 3 giá trị: tốt, bị thu hồi hoặc không xác định.

3. Dựa vào thông tin trạng thái chứng thƣ số, người dùng có thể thực hiện các hành động thích hợp. Máy phản hồi OCSP ký số lên các phản hồi trước khi gửi tới ngườidùng để đảm bảo các phản hồi này được xác thực.

# **Câu 14: Xác thực là gì? Trình bày dịch vụ xác thực trong PKI**

* Xác thực là một hành động nhằm thiết lập hoặc chứng thực một cái gì đó (hoặc một người nào đó) đáng tin cậy, có nghĩa là, những lời khai báo do người đó đưa ra hoặc về vật đó là sự thật.
* Dịch vụ đảm bảo tính xác thực là hành động hay khẳng định điều gì đó đáng tin cậy, là một thủ tục của một thực thể xác minh các tính chất đã khẳng định về một thực thể khác.
* Có 2 kiểu xác thực là: xác thực cục bộ và xác thực ở xa.
* Dịch vụ PKI về xác thực có 04 nhân tố chính:

+ một cái gì đó người dung có ( thẻ thông minh, ATM,..)

+ một cái gì đó người dung biết (mật khẩu,..)

+ một cái gì đó gắn với người dung ( vân tay, mống mắt,..)

+ Một cái gì đó người dung thực hiện ( cách viêt tay,..)

* 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 đc xác thực

+ Một yêu cầu nào đó mà người dung dự định gửi tới thiết bị ở xa

+ Một thách thức ngẫu nhiên được phát hành bởi một thiết bị ở xa

* Các kỹ thuật xá thực:

+ Kỹ thuật xác thực độtươi của thông điệp và tính sống động của người dung

+ Kỹ thuật xác thực lẫn nhau và kỹ thuật xác thực sử dụng bên thứ 3 tin cậy

+ Kỹ thuật trao đổi khóa.

# **Câu 15: PKI triển khai bao nhiêu cặp khóa? Là những cặp khóa nào ? việc sao lưu khóa nên khuyến cáo thực hiện vơi cặp khóa nào. Vì sao?**

* PKI có thể trao đỏi thông tin một cách an toàn thông qua sử dụng một cặp khóa
* Là khóa bị mật và công khai được chứng nhận bởi một nhà cung cấp chứng nhận số CA được tín nhiệm
* Việc sao lưu sử dụng khóa công khai

# **Câu 16: PKI có những dịch vụ nào? Có mấy dịch vụ cốt lõi. Trình bày**

PKI có 5 dv: toàn vẹn, bảo mật, xác thực, chống chối bỏ, dấu thời gian

PKI được kết hợp từ 3 dịch vụ cơ bản : xác thực, toàn vẹn và bảo mật

**Toàn vẹn:**

* Toàn vẹn dữ liệu là đảm bảo dữ liệu ổn định không bị thay đổi thông qua các hoạt động như truyền đi hay lưu trữ.
* Một số kỹ thuật:

+ Mã phát hiện lỗi

+ Mã xác thực thông điệp (MAC) : Kỹ thuật này thường sử dụng một mã khối đối xứng hoặc một hàm băm mật mã

+ 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;

**Bảo mật**

* Dịch vụ đảm bảo tính bí mật là đảm bảo tính bí mật của dữ liệu: dữ liệu chỉ có thể truy nhập bởi những ngƣời có quyền, không ai đọc được nội dung của dữ liệu ngoại trừ những người dùng có quyền được đọc.
* Nhiệm vụ: đảm bảo tính bí mật của dữ liệu chống lại các tấn công đọc trộm, nghe lén, bảo mật dữ liệu nhạy cảm, mã hóa và giải mã chính xác thữ liệu
* Kỹ thuật:

+ sinh khóa đối xứng -> thực hiện mã hóa dữ liệu bằng khóa đối xưng -> đóng gói -> giải mã

**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 các lợi ích:

+ Giảm được sự phức tạp của việc phân phối trước khóa dùng chung,

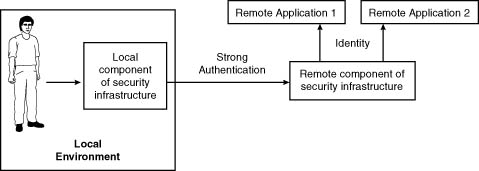
+ Dữ liệu xác thực nhạy cảm không phải truyền trên mạng,

+ 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

**Các kỹ thuật**

* 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.

# **Câu 17: Hỗ trợ ứng dụng: mô hình đăng nhập 1 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.
* Mô hình đăng nhập một lần có những lợi điểm cho người dùng và người quản trị như sau:

+ 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.

+ Quản lý đơn giản: 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.

+ 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.

# **Câu 18: Ý nghĩa của tem thời gian trong PKI**

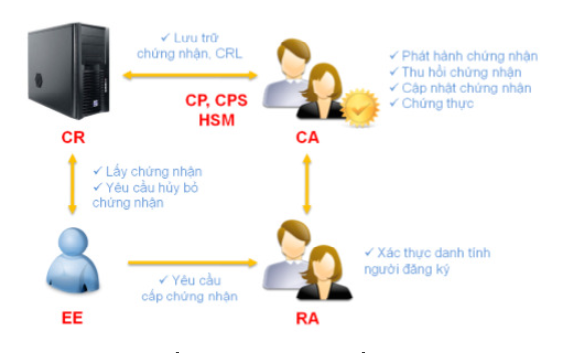
* Tem thời gian biểu thị rằng một tài liệu nào đó là trước tài liệu X và sau tài liệu Y
* Nó liên kết thời gian với dữ liệu,
* Phải có khả năng kiểm tra rằng tem thời gian được liên kết với dữ liệu là xác thực và có tính toàn vẹn,
* Dịch vụ tem thời gian an toàn có thể sử dụng các dịch vụ cốt lõi của 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**

* Hỗ trợ cho các dịch vụ không chối bỏ là việc sử dụng của tem thời gian an toàn (secure time stamping) trong PKI.
* Cần phải có một nguồn có thể tin được về thời gian mà một tập hợp những người dùng PKI sẽ tin cậy.
* Nguồn có thể tin được về thời gian cho PKI không chỉ dành cho mục đích chống chối bỏ mà có thể cho nhiều mục đích khác; Tuy nhiên, mục đích chống chối bỏ là mục đích chính của 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 19: Nêu định nghĩa của PKI? Vẽ mô hình tổng thể của hệ thống PKI và trình bày hiểu biết về các thành phần trong hệ thống PKI đó**

* PKI là hệ thống vừa mang tính tiêu chuẩn, vừa mang tính công nghệ cho phép người dùng trong một mạng công cộng không bảo mật (như Internet), có thể trao đổi thông tin một cách an toàn thông qua việc sử dụng một cặp khóa bí mật và công khai được chứng nhận bởi một nhà cung cấp chứng nhận số CA được tín nhiệm.
* Mô hình PKI:

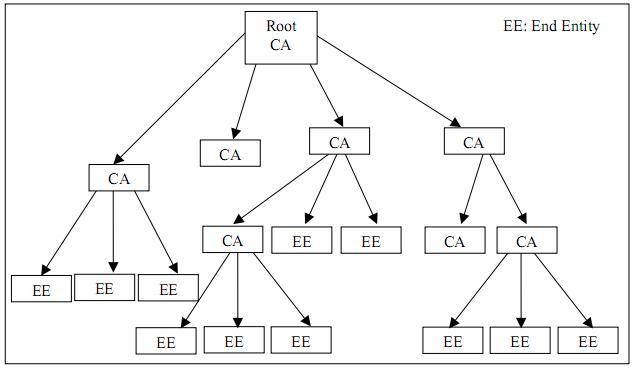


PKI gồm các thành phần chính sau:

* ***Thực thể cuối (End Entity – EE):***
  + Đối tượng sử dụng chứng nhận (chứng thư số): có thể là một tổ chức, một người cụ thể hay một dịch vụ trên máy chủ, …
* ***Tổ chức chứng nhận(Certificate Authority – CA):***
  + Có nhiệm vụ phát hành, quản lý và hủy bỏ các chứng thư số
  + Là thực thể quan trọng trong một PKI mà được thực thể cuối tín nhiệm
  + Gồm tập hợp các con người và các hệ thống máy tính có độ an toàn cao
* ***Chứng nhận khoá công khai (Public Key Certificate):***
  + Một chứng nhận khóa công khai thể hiện hay chứng nhận sự ràng buộc của danh tính và khóa công khai của thực thể cuối
  + Chứng nhận khóa công khai chứa đủ thông tin cho những thực thể khác có thể xác nhận hoặc kiể m tra danh tính của chủ nhận chứng nhận đó
  + Định dạng được sử dụng rộng rãi nhất của chứng nhận số dựa trên chuẩn IETF X.509.
* ***Tổ chức đăng kí chứng nhận (Registration Authority – RA):*** Mục đích chính của RA là để giảm tải công việc của CA
  + Xác thực cá nhân, chủ thể đăng ký chứng thư số.
  + Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.
  + Xác nhận quyền của chủ thể đối với những thuộc tính chứng thư số được yêu cầu.
  + Kiểm tra xem chủ thể có thực sự sở hữu khóa riêng đang được đăng ký hay không (chứng minh sở hữu).
  + Tạo cặp khóa bí mật, công khai. (nếu chủ thể yêu cầu)
  + Phân phối bí mật được chia sẻ đến thực thể cuối (ví dụ khóa công khai của CA).
  + Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.
  + Lưu trữ khóa riêng.
  + Khởi sinh quá trình khôi phục khóa
  + Phân phối thẻ bài vật lý (thẻ thông minh)
* ***Kho lưu trữ chứng nhận (Certificate Repository – CR):***
  + Hệ thống (có thể tập trung hoặc phân tán) lưu trữ chứng thư và danh sách các chứng thư bị thu hồi
  + Cung cấp cơ chế phân phối chứng thư và danh sách thu hồi chứng thư (CRLs - Certificate Revocatio Lists).

# **Câu 20: Trình 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.
* 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.

# **Câu 21: Nêu nhược điểm của CRL ver1? CRL VER2 khắc phục được những nhược điểm đó như thế nào. Trình bày khuôn dạng của chứng thu số X.509 VER3.**

* **Nhược điểm của CRL ver 1:**

+ Độ an toàn: thông tin trong CRL ver1 được thay thế không cần sự am hiểu của CA hoặc người dung nên có thể truyền tới người dung những thông tin không chính xác.

+ Kích thước: CRL v1 không có cơ chế để kiểm soát hay giới hạn kích thước.

+ Tính mềm dẻo: CRL v1 không cho phép mở rộng liên kết với CRL thêm bất kỳ một thông tin bổ sung nào

* Các vấn đề trên đều được giải quyết ở CRL phiên bản 2. CRL v2 thay đổi lớn nhất là các trường mở rộng giúp cho CRL linh hoạt và khả năng mở rộng hơn phiên bản 1. Các trường được mô tả như sau:

+version: 2

+ chữ ký: gồm định danh thuận toán được CA cấp phát

+ người phát hành: chứa tên phân biệt X.500 (DN) của CA cấp phát

+ This update: trường này bao gồm ngày mà CRL được phát hành

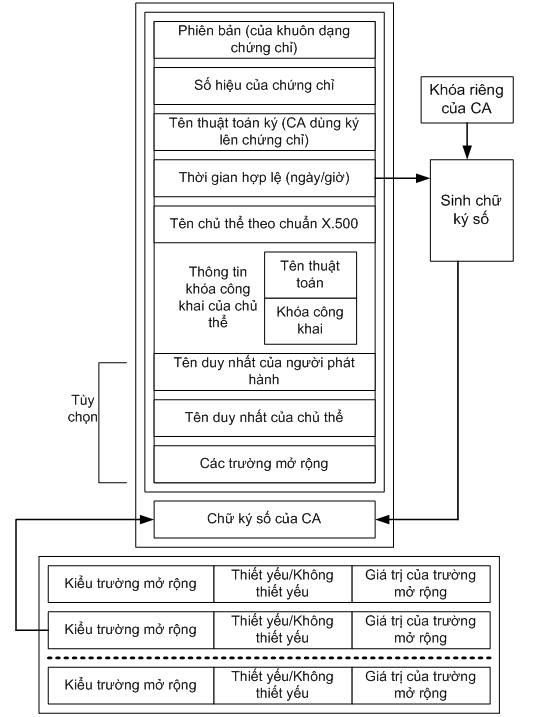
+ Next update: chứa thông tin ngày CRL tiếp theo sẽ được phát hành hoặc CRL bị hết hạn

+ List of Revoked certificate: gồm các chứng thư bị thu hồi

+ Extendsions: bao gồm các thông tin bổ sung

+ Digital Signature: ID của thuật toán và chữ ký số.

* **Khuôn dạng v3**



+ 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 22: 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.

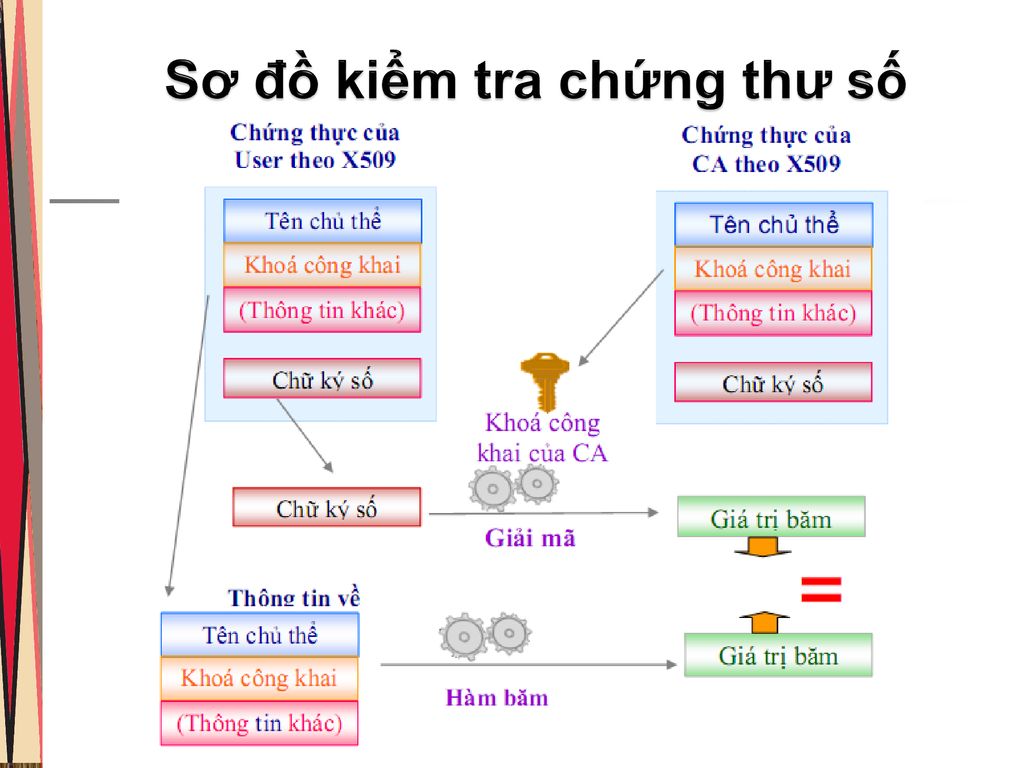
+ Môi trường mở là môi trường mà ở đó truyền thông giữa các miền được đòi hỏi hỗ trợ.

* 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?
* Các yêu cầu về thiết bị: các thành phần được bảo vệ đúng mực
* Các yêu cầu về nhân viên: nhân viên có trình độ cao
* 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: cần bao nhiêu phần cứng, quy mô bao nhiêu, giá trị phần mềm, công cụ hỗ trợ, cơ sở hạ tầng đã có gì khai thác được,…

# **Câu 23: Xác minh tính hợp lệ của chứng thư số gồm mấy bước, vẽ lược đồ mô tả các bước đó**

* Bước 1: Kiểm tra rằng chứng thư số còn hiệu lực hay không
* Bước 2: Xác minh được chứng thư đó do một CA tin tưởng cấp phát
* Bước 3: Đảm bảo rằng chứng thư số đó được sử dụng vào đúng mực đích
* Bước 4: Kiểm tra, xác định được chứng thu số có bị thu hồi hay không

**Sơ đồ**



# **Câu 24: 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 người 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 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.

**Thành phần Gồm 2 thành phần chính :**

+ **MRZ**: 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:** 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.

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

**Clandestine scanning:** 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.

**Biometric data-leakage:** 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

**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.

**+ 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.

**+ 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.

# **Câu 25: 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.

**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 26: 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.
* *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.
* *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. 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.
* *Phạm vi CRL* (CRL Scope), 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), mở rộng 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.. 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.
* *Định danh dòng CRL* (CRL Stream Identifier), nó được sử dụng để “nhận dạng ngữ cảnh mà trong đó số CRL là duy nhất”. Mở rộng này không quan trọng
* *Danh sách được sắp xếp* (Ordered List), 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, mở rộng này luôn được đánh dấu là không quan trọng.
* *Thông tin Delta* (Delta Information),, chỉ ra rằng các Delta CRLs tương ứng với CRL này là có thể., 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. 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.
* *Cập nhật cơ sở* (Base Update), , 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 luôn được đánh dấu là không quan trọng.
* *CRL mới nhất* (Freshest CRL), 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 sung 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 27: 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)**

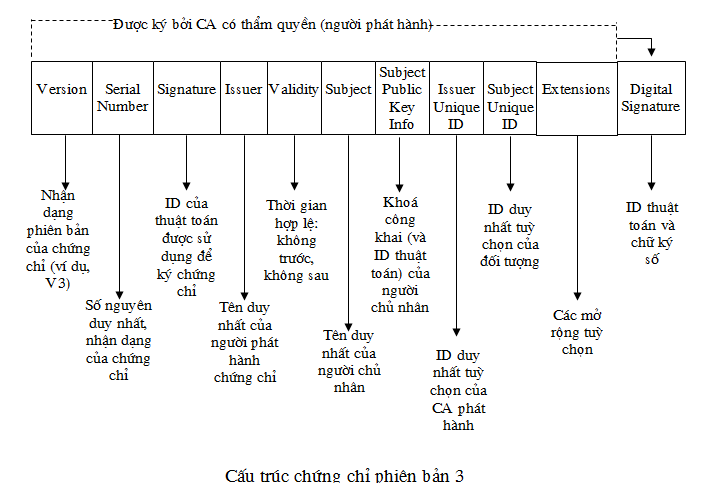
**Khuân dạng táng câu 21 vào.**

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 của thuật toán được sử dụng để tính chữ ký số trên chứng chỉ.
* *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.
* *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.
* *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; 

# **Câu 28: Tương lai của PKI:  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 29: Trình bày hiểu biết về các giao thức của PKI?**

* Giao thức trạng thái chứng thư số trực tuyến (OCSP) – cho phép tổ chức có thể xác mỉnh tính hợp lệ của chứng thư số một cách hiệu quả với chi phí hợp lý
* Giao thức quản trị
* Giao thức hoạt động

# **Câu 30: Yêu câu cần để 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.

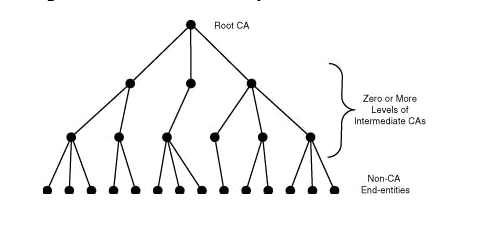
* Nếu yêu cầu được chấp thuận thì CA sẽ trả về một thông điệp trả lời yêu cầu cập nhật khóa có chứ một chứng chỉ mới cho đối tượng.

# **Câu 31: 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*

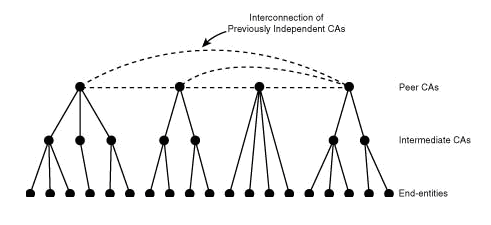
Trong mô hình này, tất cả các thực thể trong kiến trúc tin cậy rootCA. Sự phân cấp được thiết lập như sau:

* 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.
* **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.

* **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.

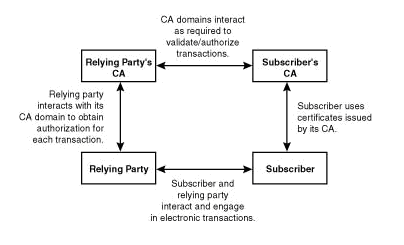


*Hình 10: Mô hình kiến trúc tin cậy phân tán*

Thông thường thì kiến trúc được chia điểm thường được xây dựng trong một miền của một tổ chức. trái lại, kiến trúc hình cây và kiến trúc lai 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)**



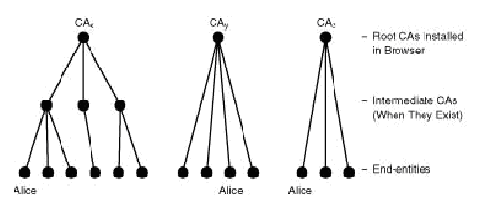
*Hình 11: Mô hình bốn bên*

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 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.

* **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.

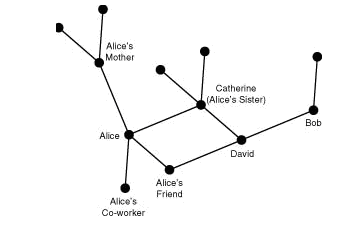
Mô hình Web có những ưu điểm rõ rệt để thuận tiện và đơn giản khả năng liên kết. Tuy nhiên, có một vài sự vấn đề an toàn cần được quan tâm trong mô hình này khi quyết định triển khai. Ví dụ, bởi vì người dùng trình duyệt tự động tin tưởng vào tập hợp các khoá đã được cài sẵn trong trình duyệt, nên an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

**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

Câu 25: Kiểm tra đường dẫn chứng thực là gì ? tại sao cần kiểm tra đường dẫn chứng thực. Nội dung kiểm tra đường dẫn chứng thực gồm những bước nào

Câu 26: Vị trí sinh cặp khóa phụ thuộc vào nhũng yếu tố nào? Để chống chối bỏ PKI khuyến khích người dung tự sinh cặp khóa vì sao

Câu 27: So sánh các kỹ thuật mật mã dùng cho đảm bảo tính toàn vẹn