MỞ ĐẦU

1. Lý do chọn đề tài

Chúng ta đã biết rằng hiện này Nhà nước ta đang tiến hành cải cách hành chính, trong đó việc xây dựng một chính phủ điện tử đóng một vai trò trọng tâm. Nói đến chính phủ điện tử là nói đến những vấn đề như về hạ tầng máy tính, về con người, về tổ chức, về chính sách, về an toàn – an ninh thông tin….

Trong đó đảm bảo an toàn – an ninh thông tin cho các dịch vụ đóng một vai trò quan trọng vì nếu thông tin mà không đảm bảo an ninh – an toàn, đặc biệt là những thông tin nhạy cảm thì việc xây dựng chính phủ điện tử, thương mại điện tự trở nên vô nghĩa vì lợi bất cập hại. Xây dựng một chính sách, đảm bảo an ninh – an toàn thông tin liên quan chặt chẽ đến việc xây dựng một hệ thống cơ sở hạ tầng mật mã khoá công khai, viết tắt là PKI (Public Key Infrastrueture).

Trong thời đại công nghệ thông tin thì giấy tờ không phải là cách duy nhất chứng nhận thoả thuận giữa các bên. Ở nhiều nước tiên tiến, các thoả thuận thông qua hệ thống thông tin điện tử giữa các bên đã được hợp pháp hoá và có giá trị tương đương với các thoả thuận thông thường về mặt pháp lý. Sự kiện này đánh dấu một bước nhảy quan trọng trong việc phát triển chính phủ điện tử, thương mại điện tử. Tuy nhiên cho đến nay các dự án vẫn chưa được triển khai rộng rãi, do nhiều nguyên nhân khác nhau. Một trong những nguyên nhân quan trọng đó là người dùng vẫn luôn cảm thấy không an tâm khi sử dụng hệ thống. Chẳng hạn khi gửi mẫu tin có thể là văn bản, hình ảnh, video….người nhận có quyền nghi ngờ: Thông tin đó có phải là của đối tác không, nó có bị xâm phạm và những người khác có thể giải mã nó được không…. Những vấn đề đặt ra này thu hút sự chú ý của nhiều nhà khoa học trong lĩnh vực nghiên cứu bảo mật thông tin. Đây cũng chính là nguyên nhân giải thích tại sao PKI ngày càng được chú trọng nghiên cứu, phát triển.

Đến nay các nước tiên tiến trên thế giới đã ứng dụng thành công PKI. Ở châu Á nhiều nước cũng đã có những ứng dụng tuy mức độ khác nhau như ở Singapore, Hàn Quốc, Trung Quốc, Thái Lan… Trong đó Sigapore, Hàn Quốc sẵn sàng tài trợ

chính, kỹ thuật, chuyên gia trong lĩnh vực mật mã sang giúp Việt Nam xây dựng hệ thống PKI.

Do đây là một vấn đề mới, nhạy cảm, gắn liền với bảo mật thông tin nên chúng ta cần những tìm hiểu sâu sắc và thận trọng về vấn đề này. Đây là vấn đề cấp thiết nên chúng ta không thể không tiến hành nghiên cứu.

Là những kỹ sư công nghệ thông tin trong tương lai, chúng ta có nhiệm vụ nghiên cứu, tìm hiểu sâu sắc hơn vấn đề quan trọng và cấp bách này nhằm góp phần đảm bảo an ninh – an toàn thông tin, điều này càng có ý nghĩa khi chúng ta hội nhập WTO, làm chủ được công nghệ này giúp giữ vững an ninh quốc gia, thúc đẩy phát triển kinh tế - xã hội.

Xuất phát từ lý do trên, được sự nhất trí của nhà trường và thầy giáo hướng dẫn, em đã chọn đề tài **"Tìm hiểu cơ sở hạ tầng mật mã khoá công khai và ứng dụng"** làm đề tài khoá luận tốt nghiệp của mình.

2. Mục đích nghiên cứu.

- Nghiên cứu, đánh giá, phân tích các giải thuật mật mã điển hình.
- Nghiên cứu các thành phần của PKI và những ứng dụng của nó.

3. Đối tượng, phạm vi nghiên cứu.

- Các giải thuật mã đối xứng, phi đối xứng, hàm băm, chữ ký số.

4. Phương pháp nghiên cứu.

- Nghiên cứu các lý thuyết cơ bản liên quan đến mã hoá, mật mã.
- Tham khảo tài liệu, tổng hợp, đánh giá.

5. Bố cục đề tài bao gồm:

Mục lục, danh mục từ viết tắt, danh mục hình vẽ, mở đầu, nội dung, kết luận, danh mục tài liệu tham khảo.

Phần nội dung gồm 2 phần chia làm 5 chương, trong đó phần A (chương 1, 2) là những kiến thức chung về mật mã, phần B (Chương 3, 4, 5) là về cơ sở hạ tầng mật mã khoá công khai và ứng dụng.

***Chương 1*: LÝ THUYẾT MẬT MÃ.**

Giới thiệu về lịch sử hình thành cảm mật mã; các khái niệm cơ bản trong mật mã; đồng thời trình bày về hệ mật mã đối xứng, hệ mật mã công khai, ưu nhược

điểm của các hệ mật mã này; khái niệm về hệ mật RSA, Elgamal. Đây là những kiếm thức nền tảng giúp bạn hiểu được PKI.

Chương 2: **XÁC THỰC, CHỮ KÝ SỐ VÀ HÀM BĂM.**

Trình bày các khái niệm về xác thực; khái niệm về chữ ký số, chữ ký số dựa trên RSA và Elgamal; khái niệm về hàm băm, một số hàm băm điển hình. Xác thực, chữ ký số và những ứng dụng cụ thể nhất, thường gặp khi xây dựng hệ thống PKI; hàm băm là một kỹ thuật mã hoá không thể thiếu khi nghiên cứu, xây dựng các hệ thống giúp đảm bảo an ninh – an toàn thông tin.

Chương 3: **CƠ SỞ HẠ TẦNG MẬT MÃ KHOÁ CÔNG KHAI.**

Tổng quan về PKI, cơ sở lí luận, chức năng của PKI. Chương này trình bày những kiến thức cơ bản liên quan đến PKI và giải thích tại sao chúng ta lại phải xây dựng hệ thống PKI.

Chương 4: **CHỨNG CHỈ SỐ.**

Trình bày các khái niệm liên quan, chức năng nhiệm vụ của CA, phân loại CA. Chứng chỉ số là phần đặc biệt quan trọng của PKI, chương này trình bày cụ thể về chứng chỉ số CA.

Chương 5: **ỨNG DỤNG.**

Trình bày những ứng dụng trong dịch vụ web, email.

PHẦN A: NHỮNG KIẾN THỨC BỔ TRỢ.

Chương 1: LÝ THUYẾT MẬT MÃ.

1.1. GIỚI THIỆU

Mật mã đã được con người sử dụng từ rất lâu, khi nghiên cứu về nền văn minh Ai Cập cổ đại người ta đã tìm được bằng chứng chứng minh hình thức mật mã sơ khai, nó cách đây khoảng 4 nghìn năn trước. Trải qua hàng nghìn năm mật mã vẫn được sử dụng rộng rãi ở các quốc gia khác nhau trên thế giới để giữ bí mật trong quá trình trao đổi thông tin trong nhiều lĩnh vực hoạt động giữa con người, giữa các quốc gia đặc biệt trong lĩnh vực ngoại giao, quân sự, kinh tế.

Mật mã khoá công khai (PKI) là một mảng quan trọng trong mật mã, bản chất của PKI đó là hệ thống công nghệ vừa mang tính tiêu chuẩn, vừa mang tính ứng dụng để khởi tạo, lưu trữ và quản lý các chứng chỉ số. Vào năm 1995 người ta đưa ra sáng kiến thiết lập PKI khi mà chính phủ các nước, các doanh nghiệp đang cần một chuẩn để đảm bảo dữ liệu truyền trên mạng được an toàn.

Cho đến nay, sau hơn 10 năm hình thành và phát triển, dần dần các ý tưởng hoá về PKI đã đi vào hiện thực, nhiều chuẩn đảm bảo thông tin trên mạng đã ra đời. Một số kết quả từ sáng kiến PKI như là: SSL/TLS (Secure Sockets Layer/ Transport Layer Security) hoặc như VPN (Virtual Private Network).

1.2. CÁC KHÁI NIỆM BAN ĐẦU

A muốn gửi thông điệp cho B thì có thể có nhiều cách khác nhau như thư tín, email, fax… và có thể thông qua một người trung gian, tức là thông tin này có thể bị người khác biết được. Vấn đề đặt ra là làm thế nào thông điệp A gửi cho B chỉ có B đọc được? Để làm được điều này thì A sẽ tiến hành mã hoá thông điệp đó và gửi cho B đoạn đã mã hoá, B sẽ giải mã được đoạn mã hoá này thông qua quy ước (Khoá chung) giữa hai người, do đó người C nhận được cũng không biết thông tin trong đó. Khoá chung đó được gọi là khoá mật mã, ta có một số khái niệm liên quan:

- Mã hoá: Là quá trình chuyển các thông tin thông thường (văn bản rõ) thành dạng không đọc được (văn bản mã).

- Giải mật mã: Là quá trình ngược lại, phục hồi văn bản thường từ văn bản mã.

- Thuật toán giải mã: Ngược lại để giải mã ta cần một thuật toán và khoá bí mật tương ứng để giải mã bản mã.

1.3. HỆ MẬT MÃ

Lý thuyết mật mã là khoa học nghiên cứu cách viết bí mật, trong đó các bản rõ (plain text, clear text) được biến đổi thành các bản mã (cipher text, cryptogram). Quá trình biến đổi đó gọi là sự mã hoá (encipherment, encryption). Quá trình ngược lại biến đổi từ bản mã thành bản rõ được gọi là sự giải mã (decipherment, decryption). Cả hai quá trình nói trên đều được điều khiển bởi một (hay nhiều) khoá mật mã.

Mật mã được sử dụng để bảo vệ tính bí mật của thông tin khi thông tin được truyền trên các kênh truyền thông công cộng như các kênh bưu chính, điện thoại, mạng truyền thông máy tính, mạng internet, …. Giả sử một người gửi **A** muốn gửi đến một người nhận **B** một văn bản (chẳng hạn, một bức thư) **p**, để bảo mật **A** lập cho **p** một bản mật mã **c** và thay cho việc gửi **p**, **A** gửi cho **B** bản mật mã **c**, **B** nhận được **c** và "giải mã" **c** để lại được văn bản **p** như **A** định gửi. Để **A** biến **p** thành **c** và **B** biến ngược lại **c** thành **p, A** và **B** phải thoả thuận trước với nhau các thuật toán lập mã và giải mã và đặc biệt một khoá mật mã chung **K** để thực hiện các thuật toán đó. Người ngoài, không biết các thông tin đó (đặc biệt không biết khoá **K**), cho dù có lấy trộm được **c** trên kênh truyền thông công cộng, cũng không thể tìm được văn bản **p** mà hai người **A, B** muốn gửi cho nhau**.** Sau đây ra sẽ cho một định nghĩa hình thức về hệ thống mật mã và cách thức thực hiện để lập mã và giải mật mã.

Định nghĩa

Hệ mật mã được định nghĩa là một bộ năm (P, C, K, E, D) trong đó:

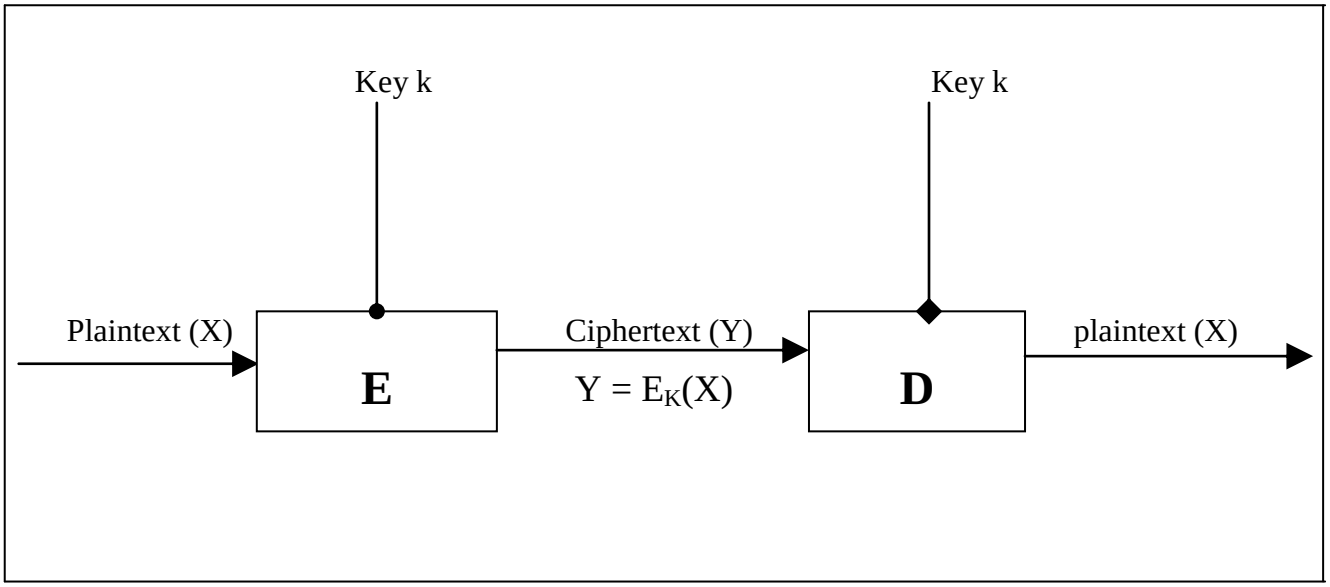
P là tập hữu hạn các bản rõ có thể.

C là tập hữu hạn các bản mã có thể.

K là tập hữu hạn các khoá có thể.

E là tập các hàm lập mã.

D là tập các hàm giải mã. Với mỗi $k \in K$, có một hàn lập mã $e_k \in E$, $e_k: P \rightarrow C$ và một hàm giải mã $d_k \in D$, $d_k: C \rightarrow P$ sao cho $d_k(e_k(x)) = x$, $\forall x \in P$



Hình 1 : Quá trình mã hóa và giải mã

1.3.1. Hệ mã hóa khóa bí mật (hay còn gọi là Hệ mật mã khóa đối xứng).

Các phương pháp cổ điển đã được biết đến từ hơn 4000 năm trước. Một số kỹ thuật đã được người Ai Cập cổ đại sử dụng từ nhiều thế kỷ trước. Những kỹ thuật chủ yếu sử dụng phương pháp thay ký tự này bằng ký tự khác hoặc dịch chuyển ký tự, các chữ cái được sắp xếp theo một trật tự nào đấy.

Hệ mật mã DES được xây dựng tại Mỹ trong những năm 70 theo yêu cầu của văn phòng quốc gia về chuẩn (NBS). DES là sự kết hợp cả 2 phương pháp thay thế và dịch chuyển. DES được thực hiện trên từng khối bản rõ là một xâu 64 bit, có khóa là một xâu 56 bít và cho ra bản mã cũng là một xâu 64 bít. Hiện nay DES và biến thể của nó là 3DES vẫn được sử dụng thành công trong nhiều lĩnh vực.

Trong hệ mật mã đối xứng chỉ có một khóa được chia sẻ giữa các bên tham gia liên lạc. Cứ mỗi lần truyền tin thì cả bên truyền và bên nhận phải thỏa thuận trước với nhau một khóa chung K, sau đó người gửi dùng e_k để lập mã cho thông báo gửi đi và người nhận sẽ dùng d_k để giải mã. Người gửi và người nhận có chung khóa K, khóa này được 2 bên giữ bí mật.

Độ an toàn của hệ mật mã bí mật phụ thuộc vào khóa K, nếu ai đó biết được khóa K thì có thể lập mã và giải mã thông điệp.

***Ưu và nhược điểm của hệ mật mã khóa đối xứng**

Ưu điểm : Ưu điểm cơ bản của hệ mật mã khóa đối xứng là tốc độ mã hóa/ giải mã rất nhanh và chính xác. Ví dụ mật mã DES có tốc độ mã/ giải mã là 35Kb/s ; của IDEA là 70 Kb/s.

Mặt khác độ an toàn của các hệ mật này được chứng minh là cao nếu không gian khóa K đủ lớn.

Nhược điểm : Tuy nhiên nhiên nhược điểm cơ bản của hệ mật mã khóa đối xứng là vấn đề phân phối khóa, trao đổi khóa rất phức tạp vì phải sử dụng đến một kênh truyền tuyệt đối bí mật. Điều này là bất lợi khi các trung tâm muốn liên lạc với nhau nhưng họ lại ở cách nhau quá xa.

1.3.2. Hệ mật mã khóa công khai.

Để khắc phục vấn đề phân phối và thỏa thuận khóa của mật mã khóa bí mật, năm 1976 Diffie và Dellman đã đưa ra khái niệm về mật mã khóa công khai và một phương pháp trao đổi khóa công khai để tạo ra một khóa bí mật chung mà tính an toàn được bảo đảm bởi độ khó của một bài toán học tính 'Logarit rời rạc'. Hệ mật mã công khai sử dụng một cặp khóa, khóa dùng để mã hóa gọi là khóa công khai (Public key), khóa dùng để giải mã gọi là khóa bí mật (Private key), về nguyên tắc thì khóa công khai và khóa bí mật là khác nhau. Một người bất kỳ có khả năng sử dụng khóa công khai để mã hóa tin nhưng chỉ có người có đúng khóa bí mật thì mới giải mã được tin đó.

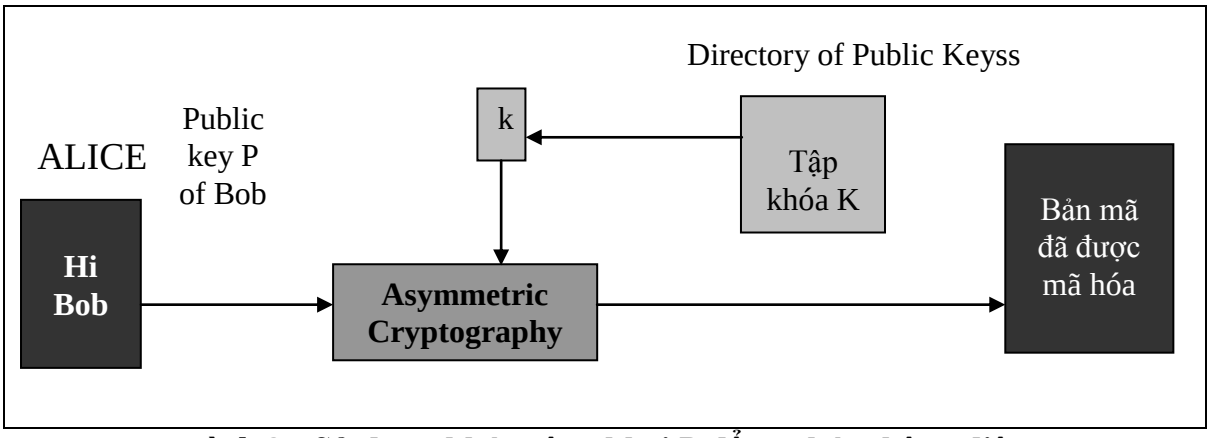
Mật mã khóa công khai (Public key) hay còn gọi là mật mã bất đối xứng là mô hình mã hóa 2 chiều sử dụng một cặp khóa là khóa riêng (Private key) và khóa công khai (Public key). Khóa công khai được dùng để mã hóa và khóa riêng được dùng để giải mã.

- Hệ thống mật mã hóa khóa công khai có thể sử dụng với các mục đích :

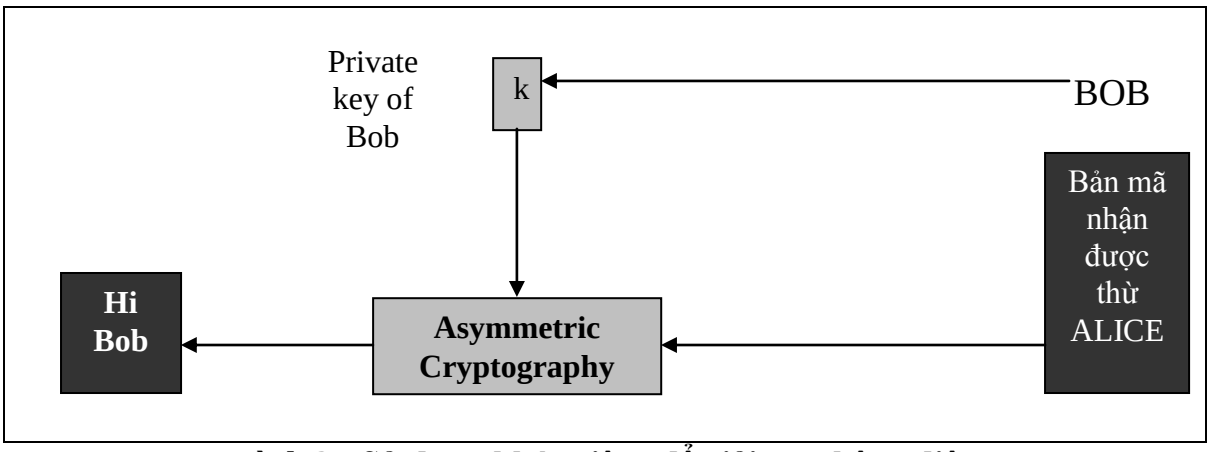
+ Mã hóa : giữ bí mật thông tin và chỉ có người có khóa bí mật mới giải mã được.

+ Tạo chữ ký số : cho phép kiểm tra một văn bản có phải đã được tạo với một khóa bí mật nào đó hay không.

+ Thỏa thuận khóa : Cho phép thiết lập khóa dùng để trao đổi thông tin mật giữa 2 bên.



Hình 2 : Sử dụng khóa công khai P để mã hóa thông điệp



Hình 3 : Sử dụng khóa riêng để giải mã thông điệp

Các hệ mật mã khóa công khai được biết đến nhiều là hệ RSA. Trong các hệ mật mã khóa công khai thì hệ RSA được cộng đồng quốc tế chấp nhận và ứng dụng rộng rãi nhất.

***Ưu nhược điểm của hệ mật mã khóa công khai.**

Ưu điểm : Ưu điểm chính của hệ mật mã khóa công khai là đã giải quyết được vấn đề phân phối khóa và trao đổi khóa cực kỳ thuận lợi. Một số ứng dụng quan trọng và phổ biến là xác thực và chữ ký số, cái mà hệ mật mã khóa đối xứng chưa giải quyết được.

Nhược điểm : Nhược điểm cơ bản của hệ mật khóa công khai là tốc độ mã hóa/ giải mã khá chậm (chậm hơn khoảng một ngàn lần so với mật mã khóa đối, như mã DES chẳng hạn) do phải sử dụng đến các số nguyên tố rất lớn trên trường hữu hạn. Mặt khác, người ta tin rằng nếu tuân thủ theo chuẩn (của Mỹ) thì hệ mật

khóa công khai như RSA, Elgamal… sẽ có độ an toàn mật mã cao nhưng cũng chưa có tác giả nào chứng minh được điều đó. Vì các khóa công khai được công bố một cách rộng khắp nên ta không biết nó có phải là khóa ta cần không và vâbs đề này đã được giải quyết bằng các thủ tục xác thực như X.509, Kerberos… một ưu điểm nữa của hệ mật mã khóa công khai là các ứng dụng của nó trong lĩnh vực chữ ký số, cùng với các kết quả về hàm băm, thủ tục ký để đảm bảo tính toàn vẹn của văn bản được giải quyết.

1.4. HỆ RSA

Hệ mật mã RSA, do Rivest, Shamir, Adleman tìm ra, được công bố lần đầu tiên vào tháng 8 năm 1977 trên tạp chí Scientific American. Hệ mật mã RSA được sử dụng rộng rãi trong thực tiễn đặc biệt trong lĩnh vực bảo mật và xác thực dữ liệu số. Tính bảo mật và an toàn của chúng được đảm bảo bằng bài toán phân tích số nguyên thành các thừa số nguyên tố.

1.4.1. Định nghĩa

Giả sử n=p.q trong đó p, q là hai số nguyên tố lẻ khác nhau và Φ(n) là hàm Ơle. Hệ RSA được định nghĩa như sau :

Cho $P=C=Z_n$; $K= \{(n,p,q,a,b) : ab \equiv 1 \bmod \Phi(n)\}$

Với mỗi k=(n,p,q,a,b) xác định :

$y= e_k(x)=x^b \bmod n$

và $d_k(y)=y^a \bmod n$ (x,y ỉ Z_n)

các giá trị n, b là công khai và p, q, a là bí mật.

1.4.2. Kiểm tra quy tắc giải mã

Do $ab \equiv 1 \bmod \Phi(n)$, $\Phi(n)= (p-1)(q-1)= \Phi(p)\,\Phi(q)$ nên $ab=1+t\,\Phi(n)$, với t là số nguyên khác 0. Chú ý rằng $0 \le x < n$.

*Giả sử (x,n)=1 ta có

$y^a \bmod n \equiv (x^b)^a \bmod n \equiv x.1 \bmod n=x$

** Nếu (x,n) > 1 thì d=p hoặc d=n

Nếu d=n thì x=0 và đương nhiên y=0. Do đó $y^a \bmod n=0$

Giả sử d=p khi đó $0 \le x < n$ nên x=p

Ta có $y^a \bmod n = x^{ab} \bmod n \equiv p^{ab} \bmod n$

Ký hiệu $u=p^{ab} \bmod n$

Thế thì $u+kn=p^{ab}$, $0 \le x < n$ hay $u+kpq=p^{ab}$

Do đó $u=p(p^{ab} - kq)$

Vế phải chia hết cho p nên vế trái chia hết cho p, nghĩa là u phải chia hết cho p. Nhưng $0 \le u < n$ nên hoặc u=0 hoặc u=p. Nếu u=0 thì p^{ab-1} chia hết cho q. Suy ra p chia hết cho q. Vô lý vì p,q là hai số nguyên tố khác nhau. Thế thì u=p=x, tức là $y^a \bmod n=x$.

Vậy $(x^b)^a \bmod n=x$, với mọi x ï [1,n-1]

1.4.3. Độ an toàn của hệ RSA.

Độ ăn toàn của hệ RSA dựa trên hy vọng rằng hàm mã hóa $e_k(x)=x^b \bmod n$ là một chiều, từ đó đối phương không thể tính toán giải mã được. Vấn đề mấu chốt ở đây là phân tích n=p.q (với p, q là hai số nguyên tố) vì khi biết được p,q thì có thể tính được Φ (n) sau đó tính được a nhờ hàm Ơclit mở rộng. Cho đến nay người ta thấy bài toán phân tích n=p.q là khó (n rất lớn) nên tính an toàn của RSA vẫn được đảm bảo.

1.4.4. Thực hiện RSA

Việc thiết lập RSA được Bob tiến hành theo các bước sau :

- Sinh ra hai số nguyên tố lớn p và q
- Tính n=p.q và Φ (n)=(p-1)(q-1)
- Chọn ngẫu nhiênb (0<b< Φ (n)) sao cho (b, Φ (n))=1
- Tính $a=b^{-1} \bmod \Phi(n)$ nhờ thuật toán Ơclit mở rộng
- Công bố n và b trong thư mục khóa công khai của mình.

Bất cứ ai muốn gửi thông điệp bí mật cho Bob đều có thể dùng khóa công khai của Bob để mã hóa và chuyển cho Bob bản mã trên kênh truyền công khai.

Như đã phân tích ở trên, muốn cho hệ RSA an toàn thì n=p.q phải lớn để không thể phân tích được nó về mặt tính toán. Các thuật toán phân tích hiện nay có thể phân tích số 130 chữ số thập phân, vì vậy người ta chọn p,q là các số nguyên tố có khoảng 100 chữ số. Khi đó n có khoảng 200 chữ số. Ngày này có nhiều phần cứng thực hiện RSA với modul n có 512 bít, trong lúc DES có tốc độ 1 Gbbit/giây, tức là RSA chậm hơn DES 1500 lần.

1.5. ELGAMAL

Giả sử p là số nguyên tố, α là phần tử nguyên thủy trên Z_p. Việc tính x, thỏa mãn $y= \alpha^x \bmod p$ được coi là khó nếu p được chọn cẩn thận đủ lớn, nghĩa là không có thuật toán nào có thể tính x trong thời gian thực tế cả. Trong khi đó nếu biết x thì việc tính y dễ dàng theo thuật toán tính nhanh. Đó là cơ sở của hệ Elgamal.

1/. Định nghĩa :

Cho p là số nguyên tố sao cho việc tính toán Logarit rời rạc trong Z_p là bài toán khó và α ï Z_p là phần tử nguyên thủy của Z_p, lấy a ngẫu nhiên, a ï Z_{p-1}

K={(p, a, α , β) : $\alpha^a \bmod p$}

Các giá trị p, α, β là công khai và a là bí mật.

Với k= (p, a, α , β) và một số ngẫu nhiên r ï Z_{p-1}, xác định $E_k(x,r)=(y_1,y_2)$

Trong đó $y_1= \alpha^r \bmod p$ và $y_2=x. \beta^r \bmod p$

Với y_1, y_2 xác định $d_k(y_1,y_2)=y_2(y_1^a)^{-1} \bmod p$

Rõ ràng là do r được chọn ngẫu nhiên nên vớ cùng một bản rõ x, hai lần mã cho hai kết quả nói chung là khác nhau.

2/. **Ví dụ :** Cho p=2579, α=2, a=765 vì thế $\beta=2^{765} \bmod 2579 = 949$

Giả sử Alice muốn gửi thông báo x=1299 Bob

Chọn ngẫu nhiên, chẳng hạn r=853. Alice tính

$y_1=2^{853} \bmod 2579 = 435$;

$y_2=1299x949^{853} \bmod 2579=2396$

Vậy là Bob sẽ nhận được $y=(y_1,y_2)=(435, 2396)$

Khi nhận được anh ta sẽ tính $x=2396x(435^{765})^{-1} \bmod 2579=1299$

Chương 2: XÁC THỰC, CHỮ KÍ SỐ VÀ HÀM BĂM

2.1. XÁC THỰC

2.1.1. Định nghĩa.

Mã xác thực là một trong số những phương pháp giúp bảo vệ bí mật thông tin.Mã xác thực giúp bảo vệ tính trung thực của thông báo,tức là nó giúp trả lời hỏi 'thông tin truyền đi đã bị sửa hay chưa ?'

Định nghĩa :

Mã xác thực là một bộ (S,A,K,E) trong đó :

S là tập hữu hạn những trạng thái nguồn

A là tập hữu hạn các dấu xác thực

K (không gian khóa) là tập hữu hạn các khóa

Với $\forall$ k $\in$ K tồn tại quy tắc xác thực e_k : S$\rightarrow$ A

Tập thông báo được xác định là m=S * A : $e_k \in$ E.

Để truyền thông báo, Alice và Bob tuân thủ giao thức sau. Đầu tiên họ cùng nhau chọn khóa ngẫu nhiên k $\in$ K, điều này được thực hiện bí mật. Khi Alice muốn gửi trạng thái nguồn s $\in$ S tới Bob trên kênh truyền không an toàn, tính a=e_k(s) và gửi thông báo (s,a) cho Bob. Khi Bob nhận được (s,a) tính a'=e_k(s). Nếu a'=a, Bob chấp nhận thông báo, còn không sẽ từ trối .

2.1.2. Xác thực với trung tâm.

Thông thường khi muốn tiếp cận với một hệ thống máy tính, một chương trình có tính bảo mật thì đòi hỏi người sử dụng phải xác thực, khi đó hệ thống kiểm tra xem người đó có trong danh sách người được dùng hay không. Đơn giản và thường gặp nhất là trung tâm hay hệ thống sẽ cấp cho người được phép dùng username và password để truy nhập. Nhưng cách này không an toàn vì username và password được lưu trong cơ sở dữ liệu tại trung tâm có thể bị nhân viên hoặc ai đó lấy và truyền ra ngoài, thay đổi, sửa, xóa với mục đích xấu.

Để tăng tính an toàn, thay vì lưu trực tiếp username, password, người ta tiến hành mã hóa chúng với hàm một chiều sau đó mới lưu lại.

2.2 CHỮ KÝ SỐ

2.2.1. Giới thiệu.

Nếu người gửi A mã hóa thông điệp của riêng mình với khóa riêng thì bất kỳ ai cũng có thể giải mã thông điệp đó bằng khóa công khai. Do đó, người nhận có thể chắc chắn rằng thông điệp mình nhận chỉ có thể do A mã vì chỉ có A mới có khóa riêng của mình. Quá trình mã hóa thông điệp với khóa riêng của người gửi gọi là quá trình ‘’Ký số’’.

Trong thực tế quá trình ký số sẽ phức tạp hơn, thay việc mã hóa hóa bản thông điệp gốc với khóa riêng của người gửi thì chỉ có bản đại diện thông điệp có độ dài cố định được mã hóa với khóa riêng của người gửi và bản băm đã được mã hóa này được gắn với thông điệp gốc. Người nhận sau khi nhận được thông điệp sẽ tiến hành mã hóa với khóa công khai của người gửi sau đó băm thông điệp đi kèm với thuật toán băm tương ứng với thuật toán băm mà người gửi đã sử dụng. So sánh hai giá trị băm, nếu giống nhau thì chắc chắn thông điệp nhận được là đúng của A.

Tính toàn vẹn của thông điệp cũng được đảm bảo vì chỉ cần thay đổi giá trị một bít thì kết quả hai giá trị băm sẽ khác nhau. Tính xác thực của người gửi cũng được đảm bảo vì chỉ có người gửi mới có khóa riêng để mã hóa bản băm. Chữ ký số cũng chứng minh được tính chống chối bỏ bản gốc vì chỉ có người gửi mới có khóa riêng để ký số.

Chữ ký viết tay truyền thống dùng để ký lên văn bản hoặc một vật gì đó (thẻ rút tiền…) dùng để chỉ ra các nhân tương ứng với nó và trong nhiều trường hợp chữ ký đó phải có dấu đỏ (dấu xác nhận) mà cơ quan hay chính quyền địa phương xác thực đúng đó là chữ ký của anh ta và anh ta có trách nhiệm với nội dung mà anh ta ký, còn chữ ký số là một thuật toán dùng để gắn chữ ký với thông báo cần ký theo một cách nào đó.

Khi kiểm tra : Đối với chữ ký truyền thống sẽ so sánh chữ ký đó với bản mẫu, còn đối với chữ ký số thì chỉ có thể kiểm tra thông qua thuật toán của chúng.

2.2.2. Định nghĩa.

Sơ đồ chữ ký số là một số (P, A, K, S, V) trong đó :

P là tập hữu hạn các văn bản có thể

A là một tập hữu hạn các chữ ký có thể

K là một tập hữu hạn các khóa có thể

S là tập các thuật toán ký

V là tập các thuật toán kiểm thử

Với mỗi k∈ K, có một thuật toán ký $sig_k \in S$, $sig_k : P \rightarrow A$ và một thuật toán kiểm thử $ver_k \in V$, $ver_k : P \times A \rightarrow$ {đúng, sai} thỏa mãn điều kiện sau đây với mọi $x \in P$, $y \in A$ ta có :

$Ver_k(x,y)$ = đúng nếu y= $ver_k(x)$

$Ver_k(x,y)$ = sai nếu $y \neq ver_k(x)$

Mật mã khóa công khai có thể tạo ra được chữ ký số, chữ ký số có thể sử dụng để chứng minh tính chính xác của thông báo. Để ký lên một thông báo, người ta dùng một hàm toán học để tạo ra một bản tóm tắt duy nhất của thông báo. Bản tóm tắt này được mã hóa bằng khóa bí mật của người gửi và được gọi là chữ ký số. Sau đó, chữ ký số nàu được nối vào cuối thông báo. Người nhận có thể kiểm định cả tính xác thực và toàn vẹn của thông báo mà mình nhận được bằng cách :

- Dùng khóa công khai của người gửi để giải mã phần chữ ký số của người gửi (thu được bản tóm tắt thông báo của người gửi).

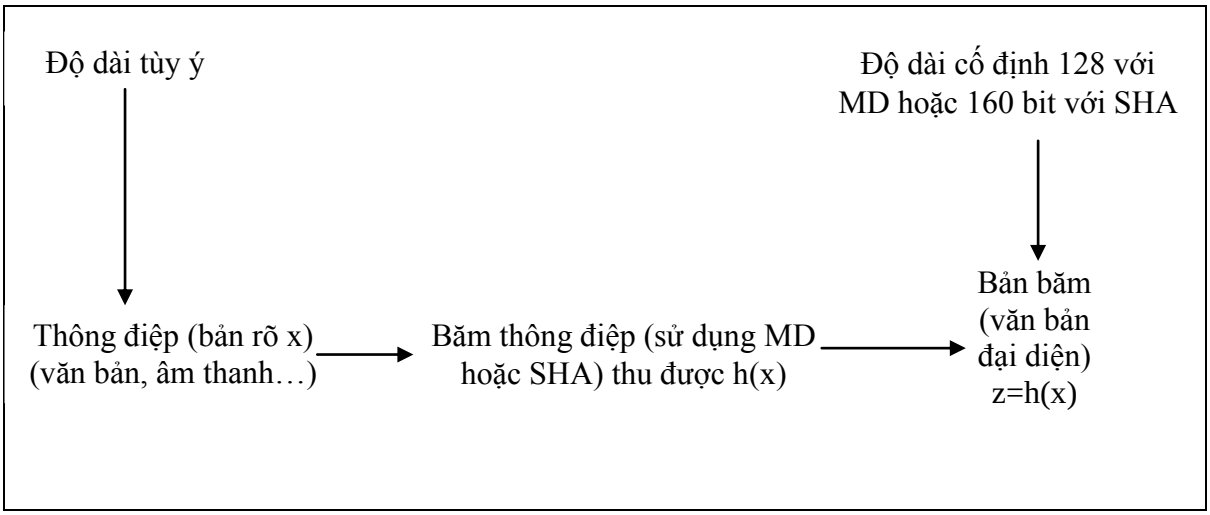
- Dùng cùng hàm toán học mà người gửi sử dụng để tạo ra bản tóm tắt của thông báo nhận được rồi so sánh hai bản tóm tắt này với nhau.

Cơ sở hạ tầng của khóa công khai làm nhiệm vụ quản lý việc sinh và phân phối các cặp khóa công khai và khóa bí mật cũng như việc xác thực quyền sử dụng để đảm bảo sự tin tưởng và cơ sở pháp lý của khóa. Mặc dù, về nguyên tắc các khóa công khai là mọi người đều biết nhưng quan trọng là tính xác thực và quyền sở hữu của chúng lại có thể thay đổi bởi PKI.

Quy trình ký và kiểm tra chữ ký được mô tả như hình bên dưới :

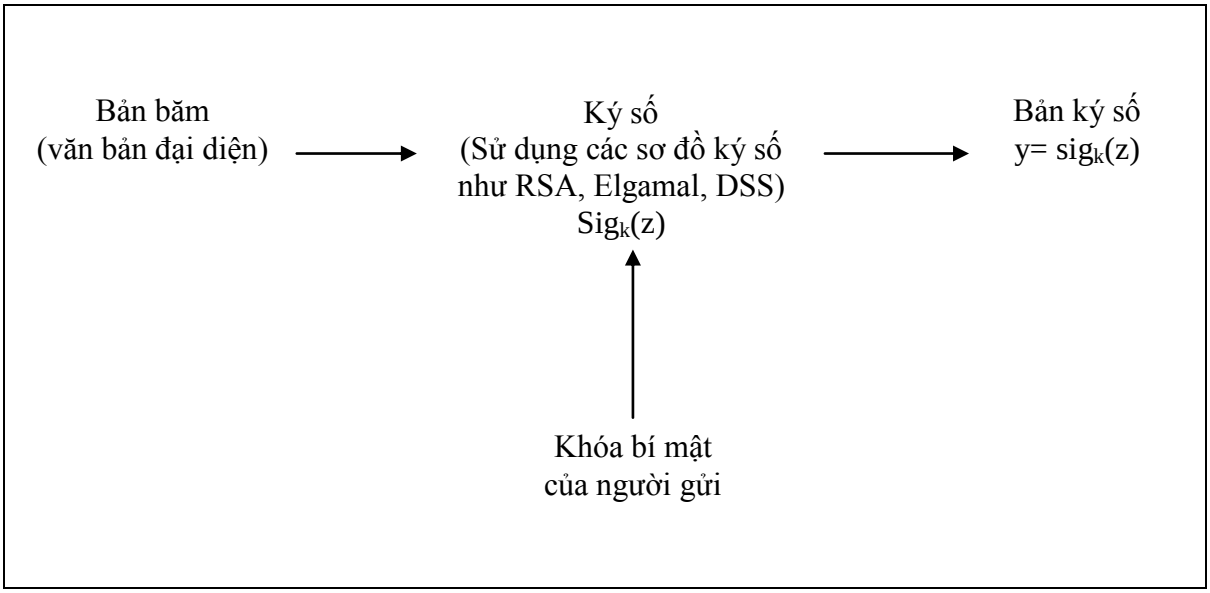
Giả sử A muốn gửi cho B thông điệp x thì A thực hiện như sau :

Bước 1 : A băm thông điệp x thu được bản đại diện z=h(x) có kích thước cố định 128 hoặc 160 bít.



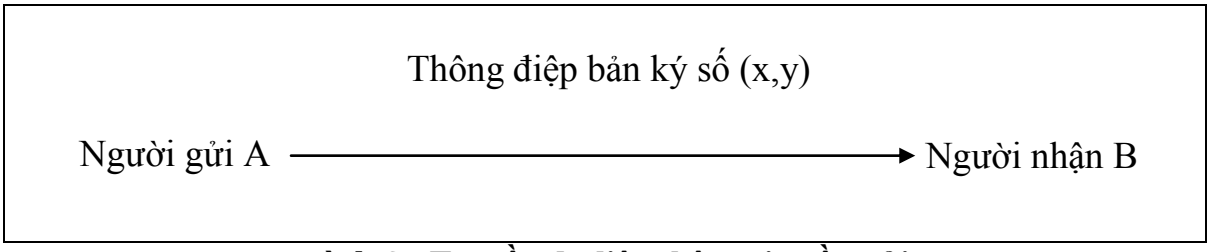
Hình 4 : Băm thông điệp

Bước 2 : A ký số trên bản đại diện z bằng khóa bí mật của mình, thu được bản ký số $y=sig_K(z)$



Hình 5 : Ký trên bản băm

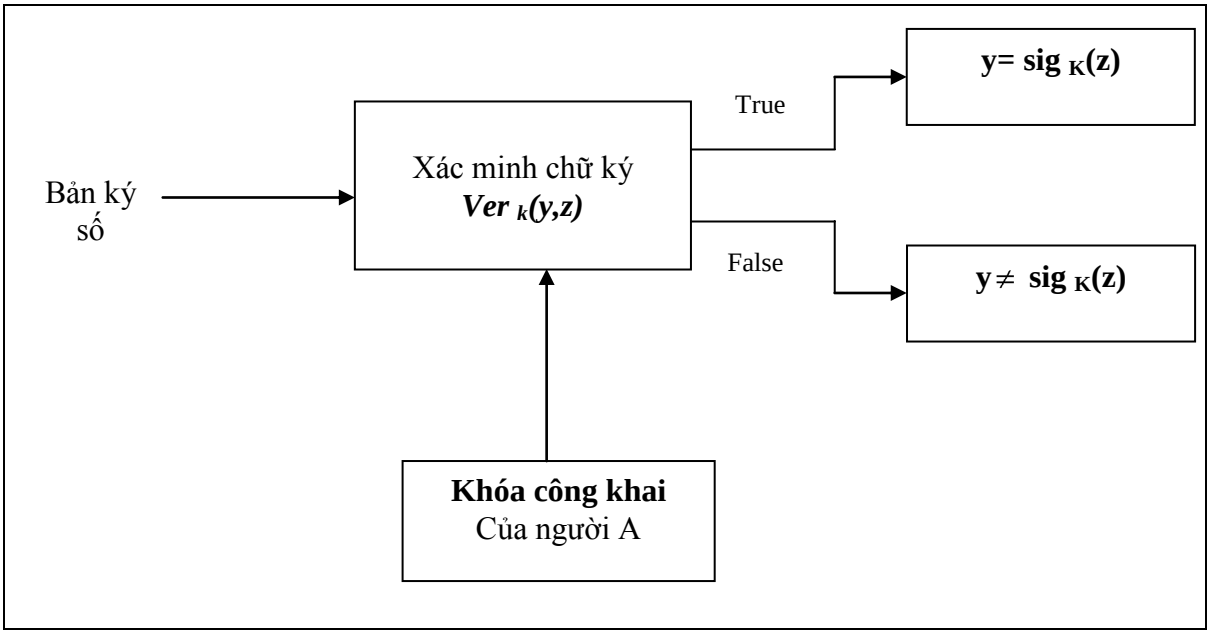
Bước 3 : A gửi (x,y) cho B



Hình 6 : Truyền dữ liệu thông tin cần gửi

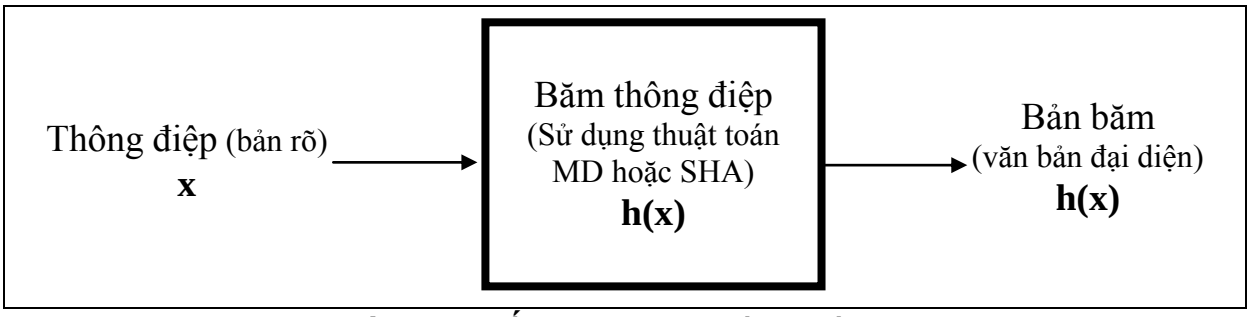
Khi B nhận được (x,y) thì B thực hiện các bước như sau :

Bước 1 : B kiểm tra chữ ký số để xác định xem thông điệp mà mình nhận được có phải được gửi từ A hay không bằng cách giải mã chứ ký số y, bằng khóa công khai A được z.



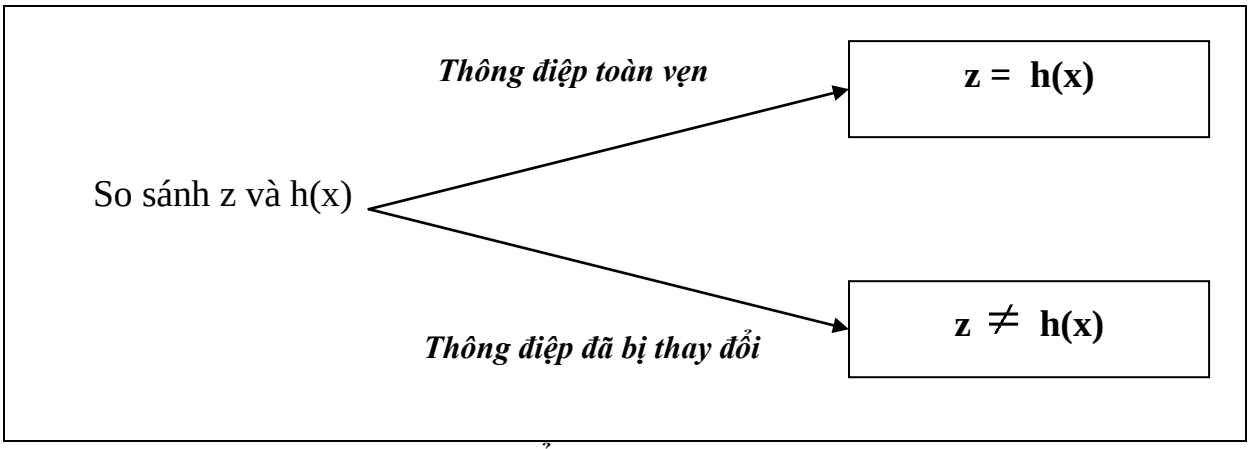
Hình 7 : Xác minh chữ ký

Bước 2 : B dùng thuật toán băm (tương đương vơus thuật toán băm mà A đã dùng) để băm thông điệp x đi kèm, nhậm được h(x)



Hình 8 : Tiến hành băm thông điệp

Bước 3 : B so sánh giá trị băm z và h(x) nếu giống nhau thì chắc chắn rằng thông điệp x là do A gửi cho B, còn nguyên vẹn, bên cạnh đó cũng xác thực được người gửi là ai.



Hình 9 : Kiểm tra tính toàn vẹn

2.2.3. Chữ ký dựa trên hệ mật RSA.

Sơ đồ chữ ký RSA

Cho n=p*q với p, q là số nguyên tố lớn. Đặt P=A=Z_n

K={(n, p, q, a, b) : n=p*q, ab ≡ 1 mod Φ(n)}

Trong đó (n,b) là công khai và (a, p, q) là bí mật

Với mỗi K=(n, p, q, a, b), mỗi x ∈ P, ta định nghĩa

$y= sig_K(x)=x^a \bmod n$, y ∈ A

$ver_K(x,y)$= đúng tương đương $x=y^b \bmod n$

Khi gửi người ta gửi cả cặp x và y (nếu không cần thiết x phải bảo mật mà chỉ cần an toàn thôi)

2.2.4. Chữ ký số dựa trên hệ mật Elgamal.

Sở đồ chữ ký số Elgamal được giới thiệu lần đầu tiên trên báo vào năm 1985 nhưng chưa hoàn chỉnh, sau đó Viện Tiêu Chuẩn và công nghệ quốc gia Mỹ (NIST) đã cải tiến và chuẩn hóa nó làm chữ ký số. Sơ đồ chữ ký Elgamal được thiết kế dành riêng cho chữ ký số, khác với sơ đồ RSA dùng cho cả hệ thống mã hóa công khai và chữ ký số.

Sơ đồ chữ ký Elgamal là không tất định, tức là có nhiều chữ ký hợp lệ trên một bức điện cho trước. Do đó thuật toán phải có khả năng chấp nhận bất kỳ chữ ký hợp lệ nào khi xác thực. Nếu chữ ký được thiết lập đúng thì khi xác minh sẽ thành công vì :

$$\beta^{\gamma}.\gamma^{\delta} \equiv \alpha^{a\gamma}\alpha^{k\gamma} \bmod p$$
$$\equiv \alpha^{x} \bmod p$$

Giả sử p là số nguyên tố và α là số nguyên thủy trên Z^*_p (căn nguyên thủy) của p, cho trước y. Việc tính x thỏa mãn $y=\alpha^x \bmod p$ được coi là khó nếu p được chọn cẩn thận, nghĩa là không có thuật toán nào để tính x trong thời gian thực tế cả. Trong khi đó nếu biết x thì việc tính y dễ dàng theo thuật toán tính nhanh. Đó là cơ sở toán học của hệ mạt Elgamal.

1/. Định nghĩa :

Cho p là số nguyên tố sao cho việc tính logarit rời rạc trong Z_p là khó và cho α ï Z^*_p là phần tử nguyên thủy. Cho $P=Z^*_p$, $A=Z^*_p * Z_{p-1}$ và xác định

$$K=\{(p, q, \alpha, \beta): \beta= \alpha^a \bmod p\}$$

Các giá trị p, α, β là công khai, còn a là bí mật.

Với K=(p, q, α, β) và với số ngẫu nhiên $K \in Z^*_{p-1}$, định nghĩa:

$$Sig_k(x,y)=(\gamma,\delta)$$

Trong đó $\gamma= \alpha^r \bmod p$

Và $\delta=(x-a\gamma)r^{-1} \bmod (p-1)$

Với $x, y \in Z^*_p$ và $\delta \in Z_{p-1}$, việc xác định (γ,δ) là chữ ký đúng tương đương với sự thỏa mãn đồng dư thức $\beta^\gamma.\gamma^\delta \equiv \alpha^x \bmod p$

Chữ ký trên x theo lược đồ Elgamal phụ thuộc vào đại lượng ngẫu nhiên r. Nghĩa là một thông báo x, nếu Bob kí ở 2 thời điểm khác nhau thì được 2 chữ ký khác nhau.

Bob muốn ký x cần :

- Chọn ngẫu nhiên $r \in Z^*_{p-1}$
- Tính $\gamma= \alpha^r \bmod p$ và $\delta=(x-a\gamma)r^{-1} \bmod (p-1)$

Alice kiểm tra chữ ký như sau :

- Tính $\beta^\gamma.\gamma^\delta$, $\alpha^x \bmod p$
- Nếu $\beta^\gamma.\gamma^\delta=\alpha^x \bmod p$ thì chấp nhận chữ ký đó là tin cậy và ngược lại thì bác bỏ chữ ký đó.

2/. Ví dụ : Giả sử p=467, α=2, a=127, khi đó :

$$\beta = \alpha^a \bmod p = 2^{127} \bmod 467 = 132$$

Nếu Bob muốn ký lên bức điện x=100 và chọn số ngẫu nhiên r=213 (UCLN(213, 467)=1) và $213^{-1} \bmod 466=431$. Khi đó :

$\gamma = 2^{213} \bmod 467 = 29$

và $\delta = (100 - 127*29)431 \bmod 466 = 51$

Bất kỳ ai cũng có thể xác minh chữ ký bằng cách kiểm tra :

$132^{29} 29^{51} \equiv 189 \bmod 467$

Và $2^{100} \equiv 189 \bmod 467$

Vì thế chữ ký hợp lệ.

2.3. CHUẨN CHỮ KÝ SỐ DSS

Đó là biến dạng của lược đồ Elgamal, nó được công bố trong Công báo Liên Bang vào ngày 19/5/1994 và được coi như là chuẩn vào ngày 1/12/1994.

Vì thế hệ Elgamal không an toàn hơn bài toán Logarit rời rạc nên cần dùng modun p lớn. Chắc chắn p cần ít nhất 512 bít và nhiều người còn đề xuất nên lấy p=1024 bít đẻ đảm bảo an toàn, nhưng p dài 512 bít thì chữ ký có 1024 bít, trong nhiều ứng dụng người ta cần chữ ký ngắn hơn.

DSS cải tiến lược đồ Elgamal theo hướng : sao cho một bức điện có độ dài được ký bằng chữ ký 320 bít, tuy thế việc tính toán lại được làm trên modun có p=512 bít. Khi đó hệ thống làm việc trong nhóm con của nhóm Z^*_p kích thước 2^{160}. Độ mật của hệ thống dựa trên sự an toàn của việc tìm Logarit rời rạc trong nhóm con của Z^*_p

Như vậy để ký x :

- Chọn ngẫu nhiên số r, r∈ [1, q-1]
- Tính $\gamma = (\alpha^r \bmod p) \bmod q$

$\delta = (x + a\gamma) r^{-1} \bmod q$

(γ, δ) là chữ ký của Alice trên x.

Bob kiểm tra chữ ký:

- Tính $e_1 = x\,\delta^{-1} \bmod p$

$e_2 = \gamma\,\delta^{-1} \bmod q$

- Kiểm tra đẳng thức : $(\alpha^{e1}\,\beta^{e2} \bmod p) \bmod q$

Nếu có đẳng thức: chữ ký tin cậy

Nếu không: Chữ ký số không tin cậy

1/. Định nghĩa:

Cho p là số nguyên tố 512 bít mà bài toán rời rạc trên Z_p là khó, q là số nguyên tố 160 bít là ước của p-1.

Giả sử $\alpha \in Z_p$ là căn bậc q của modun p. Cho $P=Z_{p*}A=Z_p.Z_p$ và định nghĩa:

$A=\{(p,q, \alpha,a, \beta): \beta \equiv \alpha^a \bmod p\}$

Các số p,q, α, β là công khai và a là bí mật

Với K= (p,q, α,a, β) và với một số ngẫu nhiên $r \in Z^*_p$ ta định nghĩa:

$Sig_r(x,r)=(\gamma,\delta)$

Trong đó:

$\gamma=(\alpha^r \bmod p) \bmod q$

$\delta=(x+a\gamma)r^{-1} \bmod q$

với $x \in Z_p$ và $\gamma,\delta \in Z_p$ quá trình xác minh sẽ hoàn toàn sau các tính toán:

$e_1=x\ \delta^{-1} \bmod p$

$e_2= \gamma\ \delta^{-1} \bmod q$

2/. Ví dụ :

Giả sử q=101, p=78.q+1=7879, 3 là phần tử nguyên thủy trong Z_{7879} nên có thể lấy : $\alpha=3^{78} \bmod 7879= 170$

Giả sử a=75, khi đó :

$\beta= \alpha^a \bmod p=170^{75} \bmod 7879 = 4576$

Bây giờ giả sử Bob muốn ký thông điệp x=1234 và anh ta chọn một số ngẫu nhiên r=50, vì thế: $r^{-1} \bmod 101=99$

khi đó : $\gamma=(\alpha^r \bmod p) \bmod q =(170^{50} \bmod 7879) \bmod 101=94$

và : $\delta=(x+a\gamma)r^{-1} \bmod q=(1234+75*94)*99 \bmod 101=96$

(γ,δ) là chữ ký của Alice trên x, còn Bob sé kiểm tra chữ ký như sau :

$e_1=x\ \delta^{-1} \bmod p = 1234*96^{-1} \bmod 7879 = 45$

$e_2= \gamma\ \delta^{-1} \bmod q= 94*96^{-1} \bmod 101=27$

Kiểm tra đẳng thức

$(\alpha^{e1}\beta^{e2} \bmod p) \bmod q =(170^{45}*4576^{27} \bmod 7879) \bmod 101=94$

Vì thế chữ ký hợp lệ.

2.4. HÀM BĂM

2.4.1 Định nghĩa và tính chất.

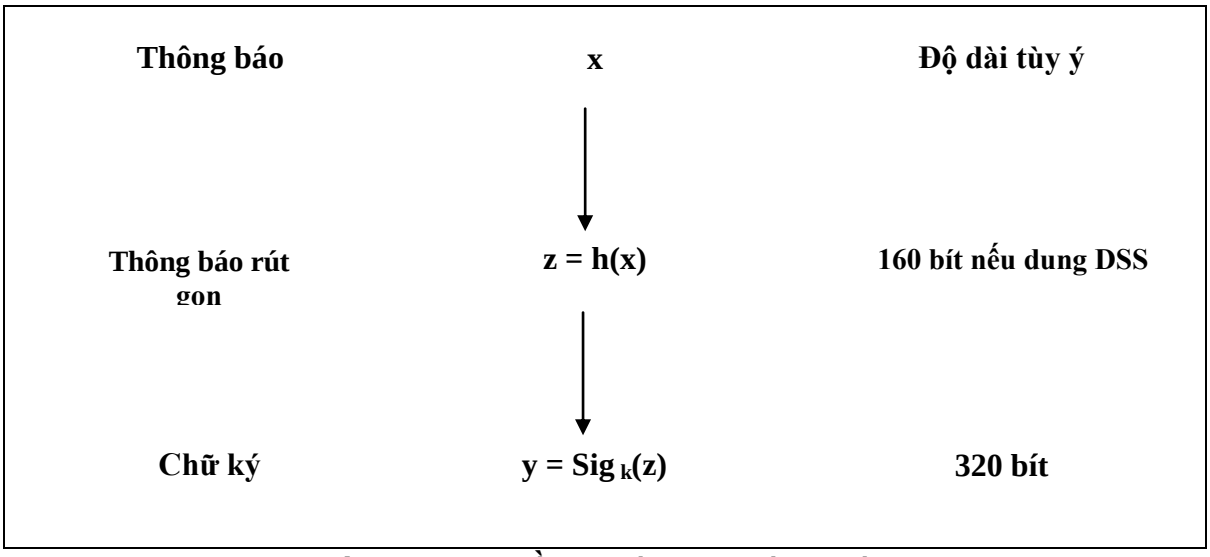
1). Đặt vấn đề : Các thuật toán liên quan đến xác thực, chữ ký số thì đầu vào là những đoạn ngắn thường 64, 128, 160 bít. Nhưng trong thực tế các bức điện cần ký có độ dài khác nhau, nhiều khi có độ dài rất lớn. Vậy ta phải làm thế nào ? Một cách đơn giản là chặt bức điện thành các đoạn nhỏ rồi ký độc lập trên các đoạn đó. Tuy nhiên biện pháp này xuất hiện một số vấn đề khi ta áp dụng cho chữ ký số :

- Nếu bức điện có kích thước là a thì sau khi ký bức điện có kích thước là 2a (nếu dùng DSS).
- Các sơ đồ chữ ký ‘’an toàn ’’ thì tốc độ chậm vì chúng dùng nhiều phép tính số học phức tạp như số mũ modulo.
- Vấn đề quan trọng nhất đó là nội dung sau khi ký, liệu chúng có bị mất mát, xáo trộn. Do đó cần phải đảm bảo tính toàn vẹn của thông điệp.

Giải pháp cho các vấn đề liên quan đến chữ ký số là dùng hàm băm để trợ giúp cho việc ký số.

2). Định nghĩa : Một hàm băm là một ánh xạ h từ không gian bản rõ có độ dài tùy ý vào không gian có giá trị có độ dài cố định. Không gian các bản rõ cũng như không gian các giá trị đều được giả thiết là những dãy bít nhị phân.

Hàm băm được đề cập ở đây là hàm một chiều có tác dụng trợ giúp cho các sơ đồ ký số nhằm làm giản dung lượng dữ liệu để truyền qua mạng, nó có nhiệm vụ băm thông điệp dựa theo thuật toán h một chiều nào đó rồi đưa ra một văn bản có kích thước cố định.



Hình 10 : Sơ đồ ký một bản thông điệp

Một số tính chất của hàm băm :

1. Tính một chiều : Nghĩa là khi cho trước dãy thông báo x thì việc tính giá trị băm y=h(x) là dễ dàng, cùng lắm là thời gian tính có độ phức tạp đa thức. Nhưng kho cho trước y việc tính x để y=h(x) là bài toán khó.

2. Tính không va chạm.

2.1Tính không va chạm yêu : Cho trước x, thì khó có thể tìm được một x' sao cho h(x')=h(x).

2.2 Tính không va chạm mạnh : khó tìm được 2 thông báo x, x' sao cho h(x)=h(x').

2.4.2 Một số hàm băm điển hình.

2.4.2.1 Hàm băm đơn giản.

Các hàm băm đều được thực hiện theo nguyên tắc chung như sau : đầu vào được biểu diễn dưới dạng các khối có độ dài n bít, các khối này đều được sử lý theo cùng một kiểu và lặp đi lặp lại để cuối cùng cho đầu ra có số bít cố định.

Hàm băm đơn giản nhất được thực hiện như sau :

$$C_i = b_{1i} \oplus b_{2i} \oplus \ldots \oplus b_{mi}$$

Trong đó : C_i : bít thứ i của hàm băm ($1 \le i \le n$)

m : số các khối đầu vào

b_{ij} : bít thứ i trong khối j

$\oplus$: phép cộng modulo 2

2.4.2.2 Kỹ thuật khối xích.

Người đề xuất kỹ thuật này là Rabin, sử dụng ký thuật mật mã xích chỗi nhưng không có khóa bí mật.

Chia thông báo M thành các khối có kích thước cố định là : M_1, M_2,…M_n sau đó dùng hệ mã thuận tiện để tính mã hash như sao :

H_0 = IV (IV là giá trị đầu)

$H_i = E_{Mi}(H_{i-1})$, i=1,1,…,n

$G = H_n$

2.2.4.3 Hàm băm Logarit rời rạc

Hàm này do Chaum, Van Heist, Pfitzmann phát minh, nếu hàm logarit đặc trưng của nó không thể tính toán được thì hàm băm này sẽ an toàn, tuy nó không đủ nhanh nhưng nó rõ ràng không có khả năng tìm ra giá trị này.

Định nghĩa :

Giả sử p là số nguyên tố lớn và q= (p-1)/2 cũng là một số nguyên tố lớn. Ta sử dụng 2 phần tử nguyên thủy của Z_p là α, β. Giá trị $\log_\alpha\beta$ không được công bố, ta giả định rằng không có khả năng tìm được giá trị này.

Hàm băm có dạng :

$$h:\{0,1,\ldots,q-1\}*\{0,1,\ldots,q-1\}\rightarrow Z^*_p$$

và được xác định như sau :

$$h(x_1,x_2) = \alpha^{x1}\,\beta^{x2} \bmod p$$

2.4.3 Ứng dụng hàm băm.

Ứng dụng chủ yếu của hàm băm là trong chữ ký số và trong việc tạo ra khóa liên lạc có bảo mật. Một ứng dụng khác của hàm băm đó là để kiểm tra tính toàn vẹn của thông điệp.

PHẦN B : CƠ SỞ HẠ TẦNG MẬT MÃ KHÓA CÔNG KHAI VÀ ỨNG DỤNG.

Chương 3 : CƠ SỞ HẠ TẦNG MẬT MÃ KHÓA CÔNG KHAI.

3.1. LỊCH SỬ HÌNH THÀNH PKI

Với sự phát triển của khoa học công nghệ, hầu hết các công việc hành chính đang dần dần số hóa, đặc biệt trong lĩnh vực quản lý, xin cấp phép…tin học ngày càng khẳng đinh được vai trò quan trọng của mình. Tuy nhiên nó cũng đặt ra vấn đề cấp thiết ta cần giải quyết đó là đảm bảo an ninh an toàn thông tin khi thực hiện tin học hóa đặc biệt là trong lĩnh vực thương mại điện tử.

Một ví dụ điển hình đó là Canada, khi xây dựng thương mại điện tử Canada rất chú trọng nghiên cứu, thực hiện xây dựng cơ sở hạ tầng khóa công khai, đây là điểm mấu chốt để đảm bảo an toàn thông tin khi tham gia thương mại điện tử, cũng như đảm bảo cho chó phát triển lâu dài. Ngoài ra để thực hiện thành công các giao dịch trong thương mại điện tử thì cần chú trọng xây dựng một cơ sở pháp lý hoàn chỉnh cùng những ràng buộc về mặt kĩ thuật.

Việc Diffie, Hellman, Shamir và Adleman công bố công trình nghiên cứu về trao đổi khóa an toàn và thuật toán PKI vào năm 1976 đã làm thay đổi hoàn toàn cách thức trao đổi thông tin mật. Cùng với sự phát triển của các hệ thống truyền tin tốc độ cao (Internet và các hệ thống trước nó), nhu cầu về trao đổi thông tin bí mật trở nên cấp thiết. Thêm vào đó một yêu cầu nứa phát sinh là việc xác định một danh tính, thông tin liên quan đến người tham gia vào quá trình trao đổi thông tin. Vì vậy ý tưởng về việc gắn định danh người dùng với chứng thực được bảo vệ bằng các kỹ thuật mật mã được hình thành và phát triển mạnh mẽ.

Nhiều giao thức sử dụng các kỹ thuật mật mã mới đã được ra đời và phát triển. Cùng với sự ra đời và phổ biến của WWW những nhu cầu về an toàn thông tin và xác thực người dùng càng trở nên cấp thiết. Chỉ tính riêng các nhu cầu ứng dụng cho thương mại (như giao dịch điện tử hay truy cập cơ sở dữ liệu bằng trình duyệt web) cũng đã đủ hấp dẫn các nhà nghiên cứu trong lĩnh vực này. Taher Elgamal và cộng sự tại Netscape đã phát triển giao thức SLL trong đó bao gồm thiết

lập khóa, nhận xác thực tử máy chủ… ElGamal là một trong những người đi tiên phong trong lĩnh vực này, là người đặt nền tảng quan trọng cho sự phát triển của PKI.

Ngày nay, việc đảm bảo an ninh, an toàn thông tin khi thực hiện tin học hóa, đặc biệt là tham gia thương mại điện tử càng được chú trọng. Các quốc gia, tổ chức tìm mọi cách đảm bảo, tạo lòng tin, tính tin cậy cho các cá nhân,tổ chức khi tham gia tức là bằng mọi cách để cho người sử dụng (người tham gia) tin tưởng vào dịch vụ mà mình đang sử dụng là hoàn toàn đúng, hoàn toàn có thật và thật sự an toàn. PKI chính là câu trả lời cho các vấn đề trên.

Các nhà doanh nghiệp rất hi vọng vào một thị trường hứa hẹn mới đã được hình thành, những công ty hoặc dự án về PKI bắt đầu được thành lập, đồng thời họ vận động các chính phủ hình thành nên khung phaps lý về lĩnh vực này. American Bar Association đi tiên phong nghiên cứu, xây dựng khung pháp lý cho PKI. Không lâu sau đó một vài tiểu bang của Hoa Kỳ mà đi đầu là Utah (năm 1995) đã thông qua những dự luật và quy định đầu tiên liên quan đến vấn đề này.

Tuy nhiên các luật và quy định đã được thông qua lại không thống nhất trên thế giới. Thêm vào đí là những khó khăn về kỹ thuật và vận hành khiến cho việc thực hiện các dự định về PKI trở nên khó khăn và đi vào bế tắc.

Tại thời điểm đầu thế kỷ 21, người ta nhận thấy rằng các kỹ thuật mật mã cũng như các quy trình, giao thức rất khó thực hiện chính xác và các tiêu chuẩn hiện tại chưa đáp ứng các yêu cầu thực tế đề ra.

Thị trưởng PKI thực sự đã tồn tại và phát triển nhưng quy mô không lớn kể từ những năm giữa của thập kỷ 1990. PKI chưa giải quyết được một số vấn đề mà người ta hy vọng. Tuy nhiên do tính cấp thiết của nó, cho đến nay PKI đã có chuẩn chung, đã được ứng dụng nhiều và không ngừng phát triển. Những PKI thành công nhất tới nay là các phiên bản do chính phủ một số nước thực hiện.

3.2. CƠ SỞ HẠ TẦNG MẬT MÃ KHÓA CÔNG KHAI

Cơ sở hạ tầng của khóa công khai viết tắt là PKI (Public Key Infrastructure), PKI là một hệ thống (phần cứng, phần mềm) có nhiệm vụ đảm bảo cho giao dịch điện tử, cho việc trao đổi các thông tin mật, thông qua việc sử dụng các khóa mã và

xác thực. PKI cho phép : đảm bảo sự tin cậy, quản lý truy nhập, đảm bảo tính toàn vẹn của thông tin, xác thực người dùng, chống trối bỏ các giao dịch thương mại điện tử và hỗ trợ các ứng dụng công nghệ thông tin. PKI dùng để quản lý việc sinh và phân phối các cặp khóa công khai và bí mật, công bố các khóa công khai (cùng với việc nhận dạng của người dùng) như giâyys chứng nhận người dùng trên các tạp chí nổi tiếng.

Khái niệm PKI thường được dùng để chỉ toàn bộ hệ thống bao gồm nhà cung cấp chứng thực số (CA) cùng các cở chế liên quan, đồng thời với toàn bộ việc sử dụng toàn bộ các thuật toán mật mã khóa công khai trong trai đổi thông tin. Tuy nhiên PKI không nhất thiết sử dụng các thuật toán mã hóa công khai.

3.3. NHỮNG YÊU CẦU CỦA PKI

Để đảm bảo thông suốt và tin cậy cho các giao dịch điện tử, tập các dịch vụ an ninh chung của cơ sở hạ tầng cần phải tạo thành một chuẩn. Chuẩn này phải có khả năng hỗ trợ về nhiều mặt, đáp ứng được đầy đủ các khả năng của các công nghệ được sử dụng trong các ứng dụng kinh doanh. Chẳng hạn, các giao dịch tài chính, tiền tệ sẽ được trao đổi một cách an toàn trên các hệ thống mạng mở nếu cơ sở hạ tầng về an ninh được thiết lập. Dịch vị đảm bảo an ninh cho thư điện tử có thể chống lại việc xem trộm của đối tượng giả mạo, nó cho phép người gửi và người nhận kiểm tra nhận dạng của nhau. Dịch vụ trao đổi dữ liệu điện tử (EDI) đảm bảo an toàn cho việc trao đổi các báo cáo điện tử. Các giao dịch tài chính cần phải được ký bằng chữ ký số và có thể xác thực để đảm bảo độ tin cậy ở nơi nhận. Thương mại điện tử có thể áp dụng trên phạm vi toàn cầu khi các tiêu chuẩn đảm bảo an ninh chung được thỏa thuận giữa các bên tham gia.

3.4. ỨNG DỤNG CỦA PKI

Mục tiêu chính của PKI là cung cấp khóa công khai và xác định mối liên hệ giữa khóa và định dạng người dùng. Nhờ vậy người dùng có thể sử dụng trong một số ứng dụng như :

- Mã hóa Email hoặc hoặc xác thực người gửi Email (OpenPGP hay S/MIME).

- Mã hóa hoặc xác thực văn bản (Các tiêu chuẩn chữ ký XML* hoặc mã hóa XML khi văn bản được thể hiện dưới dạng XML)

- Xác thực người dùng (Đăng nhập bằng thẻ thông minh - SmartCard).

Cơ chế này cũng cho phép gán cho mỗi người sử dụng trong hệ thống một cặp Public/Private. Các qua trình này thường được thực hiện bởi một phần mềm đặt tại trung tâm và các phần mềm khác đặt tại các địa điểm của người sử dụng. Khóa công khai thường được phân phối trong chứng thực khóa công khai.

Vai trò của PKI trong Thương mại điện tử

PKI là thành phần không thể thiếu để phát triển thương mại điện tử của mỗi quốc gia ; nó đảm bảo cho các giao dịch điện tử, các trao đổi thông tin giữa các bên thông suốt và an toàn.

Lợi ích kinh tế, xã hội của các đường truyền tốc độ cao sẽ mất đi ý nghĩa. Đảm bảo an ninh, an toàn thông tin là không thể thiếu trong các ứng dụng trên mạng, chẳng hạn như : chuyển nhận các thông tin về thư tín, hóa đơn mua hàng, thẻ tín dụng, các hợp đồng có ràng buộc về mặt pháp lý. Hệ thống thương mại điện tử phải bảo vệ được thông tin của các cá nhân, tổ chức, đảm bảo các giao dịch điện tử là có giá trị và hợp pháp.

3.5. CÁC THÀNH PHẦN CỦA PKI

Một hệ thống PKI gồm 4 thành phần như sau :

- **Certification Authorities (CA) :**

+ Cấp phát và thu hồi các chứng chỉ

- **Registration Authorities (RA) :**

+ Gắn kết giữa khóa công khai và định danh của người giữ chứng chỉ.

- **Clients :**

+ Người sử dụng chứng chỉ PKI (hay theo cách khác được xác định như những thực thể cuối).

+ Người sử dụng cuối hoặc hệ thống là chủ thể của chứng chỉ PKI.

- **Repository :**

+ Hệ thống lưu trữ chứng chỉ và danh sách các chứng chỉ bị thu hồi.

+ Cung cấp cơ chế phân phối chứng chỉ và CRLs đến các thực thể cuối.

3.5.1. Tổ chức chứng thực CA

Trong hạ tầng cơ sở khóa công khai, chứng chỉ có vai trò gắn kết giữa định danh với khóa công khai. Một CA là một thực thể PKI có trách nhiệm cấp chứng chỉ cho các thực thể khác trong hệ thống.

Tổ chức chứng thực CA cũng được gọi là bên thứ ba, chữ ký số do CA cung cấp được người sử dụng tin tưởng sử dụng trong quá trình trao đổi, giao dịch.

Thông thường CA thực hiện chức năng xác thực bằng cách cấp chứng chỉ cho các CA khác và thực thể cuối (người giữ chứng chỉ) trong hệ thống. Nếu CA nằm ở đỉnh của mô hình phân cấp PKI và chỉ cấp chứng chỉ cho những CA ở mức thấp hơn thì chứng chỉ này được gọi là chứng chỉ gốc ‘‘root certificate’’.

3.5.2. Trung tâm đăng ký (RA)

Mặc dù CA có thể thực hiện các chức năng đăng ký cần thiết nhưng đôi khi cần có thực thể độc lập thực hiện chức năng này. Thực thể này được gọi là ‘‘registration authority- RA’’ trung tâm đăng ký. Ví dụ khi số lượng thực thể cuối trong miền PKI tăng lên và số thực thể cuối này được phân tán khắp nơi về mặt địa lý thì việc đăng ký tại một CA trung tâm trở thành vấn đề khó giải quyết. Để giải quyết vấn đề này thì cần phải có một hoặc nhiều Ras (Trung tâm đăng ký địa phương), mục đích chính của Ras là giảm tải công việc của CA. Chức năng của CA cụ thể sẽ khác nhau tùy theo nhu cầu triển khai PKI nhưng chủ yếu bao gồm các chức năng sau :

- Xác thực cá nhân, chủ thể đăng ký chứng chỉ.
- Kiểm tra tính hợp lệ của thông báo do chủ thể cung cấp.
- Xác định quyền của chủ thể đối với những thuộc tính chứng chỉ được yêu cầu.
- Kiểm tra xem chủ thể có thực sự sở hữu khóa riêng đang được đăng ký hay không.
- Tạo cặp khóa bí mật/ công khai.
- Phân phối bí mật được chia sẻ đến thực thể cuối.
- Thay mặt chủ thể (thực thể cuối) khởi tạo quá trình đăng ký với CA.
- Lưu trữ khóa riêng.
- Khởi sinh quá trình khôi phục khóa.
- Phân phối thẻ bài vật lý chứa khóa riêng (Smart Card).

Nhìn chung RA xử lý việc trao đổi giữa chủ thể thực thể cuối và quá trình đăng ký, phân phối chứng chỉ và quản lý vòng đòi chứng chỉ/ khóa. Tuy nhiên trong bất kỳ trường hợp nào thì RA cũng chỉ đưa ra những khai báo tin cậy ban đầu về chủ thể. Chỉ CA mới có thể cung cấp chứng chỉ hay đưa ra thông tin trạng thái thu hồi chứng chỉ CRL.

3.5.3. Thực thể cuối (Người giữ chứng chỉ và Clients)

Thực thể cuối trong PKI có thể là con người, thiết bị và thậm chí có thể là chương trình phần mềm nhưng thường là người sử dụng hệ thống. Thực thể cuối sẽ thể hiện những chức năng mật mã (mã hóa, giải mã, ký số).

3.5.4. Hệ thống lưu trữ (Repositories)

Chứng chỉ (khóa công) và thông tin thu hồi chứng chỉ phải được phân phối sao cho những người cần đến chứng chỉ đều có thể truy cập và lấy được.

Có 2 phương pháp phân phối chứng chỉ :

3.5.4.1. Phân phối cá nhân

Phân phối cá nhân là cách phân phối cơ bản nhất. Trong phương pháp này thì mỗi cá nhân sẽ trực tiếp đưa ra chứng chỉ của họ cho người dùng khác. Việc này có thể thực hiện theo một số cơ chế khác nhau, như chuyển giao bằng tay chứng chỉ được lưu trữ trong đĩa mềm hay một số môi trường lưu trữ khác. Cũng có thể phân phối bằng cách gắn chứng chỉ trong Email để gửi cho người khác ; cách này thực hiện tốt trong một nhóm ít người dùng nhưng khi số lượng người dùng tăng lên thì có thể xảy ra vấn đề về quản lý.

3.5.4.2. Phân phối khóa

Một phương pháp cũng khá phổ biến là phân phối khóa, phân phối chứng chỉ và thông tin thu hồi chứng chỉ là công bố các chứng chỉ rộng rãi, các chứng chỉ này có thể sửa dụng một cách công khai và được đặt ở vị trí có thể truy cập dễ dàng. Những vị trí này được gọi là cơ sở dữ liệu. Dưới đây là ví dụ về một số hệ thống lưu trữ :

- X.500 Directory System Agents(DSAs)
- Lightweight Directory Access Protocol (LDAP) Server
- Online Certificate Status Protocol (OCSP) Responders
- Domain Nam System (DNS) và web Server
- File Transfer Protocol (FTP) Servers và Corporate Database

3.6. CHỨC NĂNG CỦA PKI

Những hệ thống PKI khác nhau thì có chức năng khác nhau nhưng nhìn chung có hai chức năng chính là : chứng thực và kiểm tra.

3.6.1 Chứng thực (Certification)

Chứng thực là chức năng quan trọng nhất của PKI. Đây là quá trình ràng buộc khóa công khai với định danh của thực thể. CA là thực thể PKI thực hiện chức năng chứng thực. Có hai phương pháp chứng thực :

- Tổ chức chứng thực (CA) tạo ra cặp khóa công khai/ khóa bí mật và tạo ra chứng chỉ cho phần khóa công khai của cặp khóa.
- Người sủ dụng tự tạo ra cặp khóa và đưa khóa công khai cho CA để CA tạo chứng chỉ cho khóa công khai đó. Chứng chỉ đảm bảo tính toàn vẹn của khóa công khai và các thông tin gắn cùng.

3.6.2. Thẩm tra (Verification)

Quá trình xác liệu chứng chỉ đã đưa ra có thể được sử dụng đúng mục đích thích hợp hay không được xem là quá trình kiểm tra tính hiệu lực của chứng chỉ. Quá trình này bao gồm một số bước :

- Kiểm tra liệu có đúng là CA được tin tưởng đã ký số lên chứng chỉ hay không (xử lý theo đường dẫn chứng chỉ).
- Kiểm tra chữ ký số của CA trên chứng chỉ để kiểm tra tính toàn vẹn.
- Xác định xem chứng chỉ còn trong thời gian hiệu lực hay không.
- Xác định xem chứng chỉ bị thu hồi hay chưa.
- Xác định xem chứng chỉ đang được sử dụng có đúng mục đích, chính sách, giới hạn hay không (bằng cách kiểm tra các trường mở rộng cụ thể như mở rộng chính sách chứng chỉ hay việc mở rộng việc sử dụng khóa).

3.6.3. Một số chức năng khác

Ngoài các chức năng chính như ở trên thì hệ thống PKI còn một số chức năng sau :

3.6.3.1. Đăng ký

Đăng ký là quá trình đến hoặc liên lạc với các tổ chức, trung tâm tin cậy để đăng ký các thông tin và xin cấp chứng chỉ. RA và CA là những thực thể trong quá

trình đăng ký. Quá trình đăng ký phụ thuộc vào chính sách của tổ chức. Nếu chứng chỉ được cung cấp với mục đích dùng cho những hoạt động bí mật thì sử dụng phương pháp gặp mặt trực tiếp. Nếu chứng chỉ chỉ được sử dụng cho những mục đích, hoạt động thường thì có thể đăng ký qua những ứng dụng viết sẵn hoặc ứng dụng điện tử.

3.6.3.2. Khởi tạo ban đầu

Khi hệ thống trạm của chủ thể nhận được các thông tin cần thiết để liên lạc với CA thì quá trình khởi tạo bắt đầu. Những thông tin này có thể là khóa công khai của CA , chứng chỉ của CA, cặp khóa công/ bí mật của chủ thể.

Một số hệ thống khác sử dụng cơ chế dựa trên password trong giai đoạn khởi tạo. Người dùng cuối liên lạc với CA khi nhận được password và sau đó thiết lập một kênh bảo mật để truyền những thông tin cần thiết. Giai đoạn khởi tạo thường tiếp tục với quá trình chứng thực.

3.6.3.3. Khôi phục cặp khóa

Hầu hết hệ thống PKI tạo ra hai cặp cho người sử dụng cuối, một để ký số và một để mã hóa. Lý do tạo 2 cặp khóa khác nhau xuất phát từ yêu cầu khôi phục và sao lưu dự phòng khóa.

Tùy theo chính sách của tổ chức, bộ khóa mã (mã và giải mã) và những thông tin liên quan đến khóa của người sử dụng phải được sao lưu để có thể lấy lại được dữ liệu khi người sử dụng mất khóa riêng hay rời khỏi đơn vị.

Còn khóa để ký số được sử dụng tùy theo mục đích cá nhân nên không được sao lưu. Riêng khóa bí mật của CA thì được lưu giữ dự phòng trong một thời gian dài để giải quyết những vấn đề nhầm lẫn có thể xảy ra trong tương lai. Hệ thống PKI có những công cụ để thực hiện chức năng sao lưu và khôi phục khóa.

3.6.3.4. Tạo khóa

Cặp khóa công khai/ bí mật có thể được tạo ở nhiều nơi. Chúng có thể được tạo ra bằng phần mềm từ phía client và được gửi tới CA để chứng thực.

CA cũng có thể tạo ra cặp khóa trước khi chứng thực. Trong trường hợp này, CA tự tạo ra cặp khóa và gửi cặp khóa bí mật này cho người sử dụng theo một cách an toàn. Nếu khóa do bên thứ ba tạo ra thì những khóa này phải được CA tin cậy trong miền xác định trước khi sử dụng.

3.6.3.5. Hạn chế sử dụng và cập nhật khóa

Một trong những thuộc tính của chứng chỉ là thời gian hiệu lực. Thời gian hiệu lực của mỗi cặp khóa được xác định theo chính sách dử dụng. Các cặp khóa của người sử dụng nên được cập nhật khi có thông báo về ngày hết hạn. Hệ thống sẽ thông báo về tình huống này trong một thời gian nhất định. Chứng chỉ mới sẽ được người cấp công bố tự động sau thời gian hết hạn.

3.6.3.6. Xâm hại khóa

Đầy là trường hợp không bình thường nhưng nếu xảy ra thì khóa mới sẽ được công bố và tất cả người sử dụng trong hệ thống sẽ nhận thấy điều này. Xâm hại đến khóa của CA là một trường hợp đặc biệt. Và trong trường hợp này thì CA sẽ công bố lại tất cả các chứng chỉ với CA- Certificate mới của mình.

3.6.3.7. Thu hồi

Chứng chỉ được công bố sẽ được sử dụng trong trong khoảng thời gian có hiệu lực. Nhưng trong trường hợp khóa bị xâm hại hay có sự thay đổi trong thông tin của chứng chỉ thì chứng chỉ sẽ được công bố, chứng chỉ cũ sẽ bị thu hồi.

3.6.3.8. Công bố và gửi thông báo thu hồi chứng chỉ

Một chứng chỉ được cấp cho người sử dụng cuối sẽ được gửi đến cho người nắm giữ và hệ thống lưu trữ để có thể truy cập công khai. Khi một chứng chỉ bị thu hồi vì một lý do nào đó, tất cả người sử dụng trong hệ thống sẽ được thông báo về việc này.

3.6.3.9. Xác thực chéo

Xác thực chéo là một trong những đặc tính quan trọng nhất của hệ thống PKI. Chức năng này được sử dụng để nối hai miền PKI khác nhau. Xác thực chéo là cách để thiết lập môi trường tin cậy giữa hai CA dưới những điều kiện nhất định. Những điều kiện này được xác định theo yêu cầu của người sử dụng**.** Những người sử dụng ở các miền khác nhau chỉ có thể giao tiếp an toàn với người khác sau khi việc xác thực chéo giữa các CA thành công.

Xác thực chéo được thiết lập bằng cách tạo ra chứng chỉ CA xác thực lẫn nhau. Nếu CA-1 và CA-2 muốn thiết lập xác thực chéo thì cần thực hiện một số bước sau :

+ CA-1 công bố CA- certificate cho CA-2

+ CA-2 công bố CA- certificate cho CA-1.

+ CA-1 và CA-2 sẽ sử dụng những trường mở rộng xác định trong chứng chỉ để đặt những giới hạn cần thiết trong CA- certificate. Việc xác thực chéo đòi hỏi phải có sự kiểm tra cẩn thận các chính sách PKI.

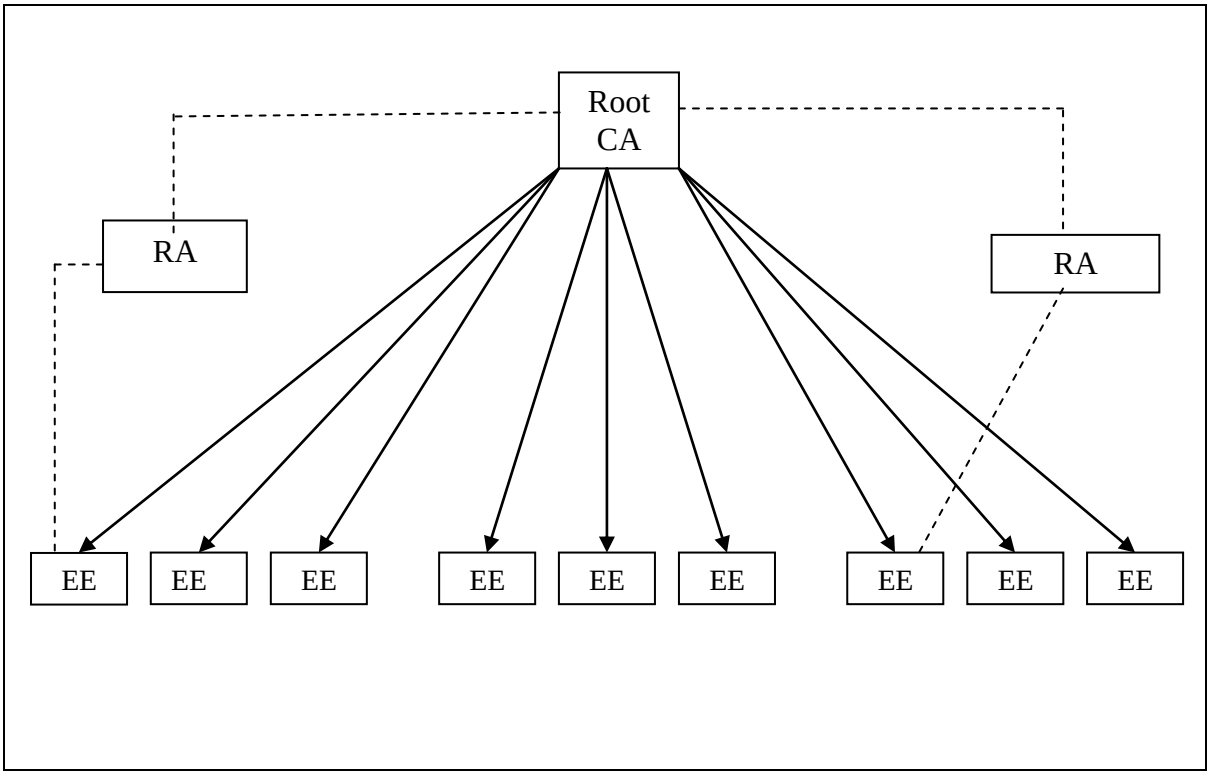
Nếu cả hai đều có cùng hoặc tương tự chính sách của nhau thì việc xác thực chéo sẽ có ý nghĩa. Ngược lại, sẽ có những tình huống không mong muốn xuất hiện trong trường hợp chính sách PKI của một miền trở thành một phần của miền khác.

3.7. MÔ HÌNH PKI

3.7.1. Mô hình đơn

Đây là mô hình tổ chức CA cơ bản và đơn giản nhất. Trong mô hình CA đơn chỉ có một CA xác nhận tất cả các thực thể cuối trong miền PKI. Mỗi người sử dụng trong miền nhận khóa công khai của CA gốc (root CA) theo một số cơ chế nào đó. Trong mô hình này không có yêu cầu xác thực chéo. Chỉ có một điểm để tất cả người sử dụng có thể kiểm tra trạng thái thu hồi của chứng chỉ đã được cấp. Mô hình này có thể được mở rộng bằng cách có thểm các RA ở xa CA nhưng ở gần các nhóm người dừng cụ thể.

Mô hình này được minh họa trong hình sau :



Hình 11 : Mô hình CA đơn

Ưu điểm :

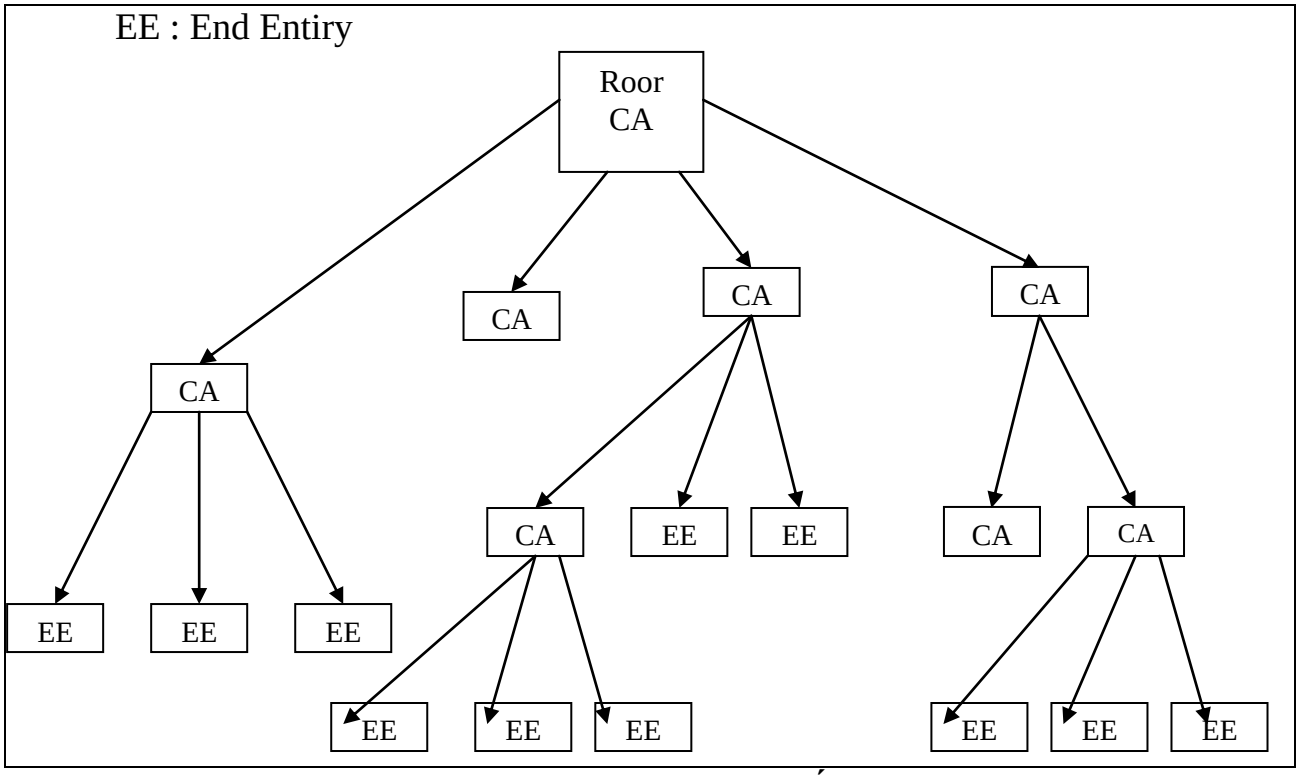
Mô hình này dễ để triển khai và giảm tối thiểu được những vấn đề về khả năng tương tác.

Nhược điểm :

- Không thích hợp cho miền PKI lớn vì một số người sử dụng ở những miền con có những yêu cầu khác nhau đối với những người ở miền khác.
- Có thể không có tổ chức nào tình nguyện vẫn hành CA đơn hoặc một số tổ chức lại có thể không tin tưởng vào những người vận hành CA này vì một vài lý do nào đó.
- Việc quản trị và khối lượng công việc ký thuật của việc vận hành CA đơn sẽ rất cao trong cộng đồng PKI lớn.
- Chỉ có một CA sẽ gây ra thiếu khả năng hoạt động và CA này có thể trở thành mục tiêu tấn công.

3.7.2. Mô hình phân cấp

Mô hình này tương ứng với cấu trúc phân cấp với CA gốc và các CA cấp dưới. CA gốc xác nhận với CA cấp dưới, các CA này lại xác nhận các CA cấp thấp hơn. Các CA cấp dưới không cần xác nhận các CA cấp trên.



Hình 12 : Mô hình phân cấp

Trong mô hình này, mỗi thực thể sẽ giữ bản sao khóa công khai của root CA và kiểm tra đường dẫn của chứng chỉ bắt đầu từ chữ ký của CA gốc. Đây là mô hình PKI tin cậy sớm nhất.

** Ưu điểm :*

- Mô hình này có thể dùng được trực tiếp cho những doanh nghiệp phân cấp và độc lập, cũng như những tổ chức chính phủ quân đội.
- Cho phép thực thi chính sách và chuẩn thông qua hạ tầng cơ sở.
- Dễ vận hành giữa các tổ chức khác nhau.

** Nhược điểm :*

- 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 các tổ chức khác.
- Có thể không thích hợp cho những mỗi quan hệ ngang hàng giữa chính phủ và doanh nghiệp.
- Những tổ chức thiết lập CA trước có thể không muốn trở thành một phần của mô hình.
- Có thể gây ra sự trội hơn của sản phẩm đối với vấn đề khả năng tương tác.
- Chỉ có một CA gốc nên có thể gây ra một số vấn đề như thiếu khả năng hoạt động. Thêm vào đó, 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 người sử dụng cuối trong hệ thống theo một số cơ chế khác nhau.

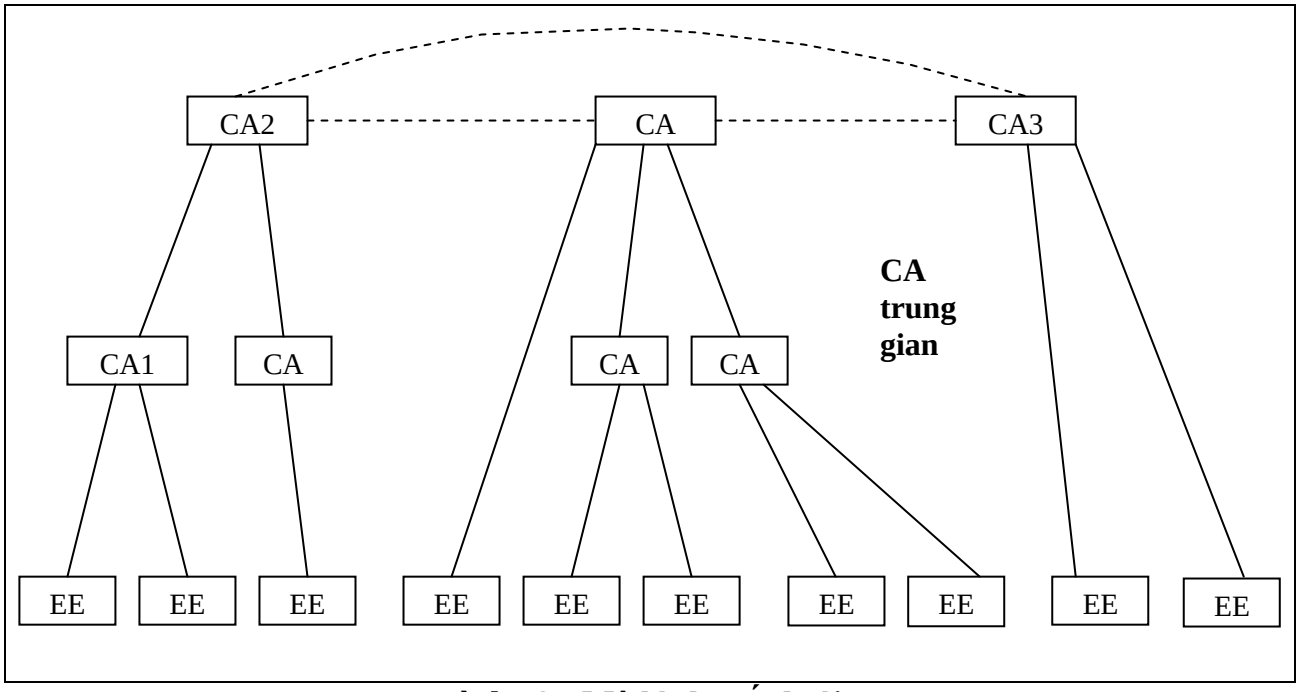
Mặc dù có những nhược điểm, song mô hình này vẫn thích hợp với yêu cầu của các tổ chức chính phủ vì cấu trúc phân cấp tự nhiên sẵn có.

3.7.3. Mô hình mắt lưới

Mô hình mắt lưới là mô hình đưa ra sự tin tưởng giữa hai hoặc nhiều CA. Mỗi CA có thể ở trong mô hình phân cấp hoặc trong mô hình mắt lưới khác. Trong mô hình này không chỉ có một CA gốc mà có nhiều hơn một CA gốc phân phối sự tin cậy giữa các CA với nhau. Thông qua việc xác thực chéo giữa các CA gốc, các CA có thể tin tưởng lẫn nhau. Xác thực chéo liên kết các miền khác nhau bằng việc

sử dụng thuộc tính BasicConstraints, Name Constraints, PolicyMapping và PolicyConstraints của X.509 v3 mở rộng.

Trong cấu hình mắt lưới đầy đủ, tất cả các CA gốc xác nhận chéo lẫn nhau. Điều này yêu cầu n^2 lần xác thực trong hạ tầng cơ sở.



Hình 12 : Mô hình mắt lưới

** Ưu điểm :*

- Linh hoạt hơn và phù hợp hơn với nhu cầu giao dịch hiện nay.

- Cho phép những nhóm người sử dụng khác nhau co thể tự do phát triển và thực thi những chính sách và chuẩn khác nhau.

- Cho phép cạnh tranh.

- Không phải là mô hình phân cấp và khắc phục được những nhược điểm của mô hình phân cấp tin cậy ở trên.

** Nhược điểm :*

- Phức tạp và khó để quản lý vì việc xác thực chéo.

- Khó có khả năng thực hiện và có thể không hoạt động vì những lý do giao tác.

- Phần mềm người sử dụng có thể gặp phải một số vấn đề khi tìm chuỗi chứng chỉ.

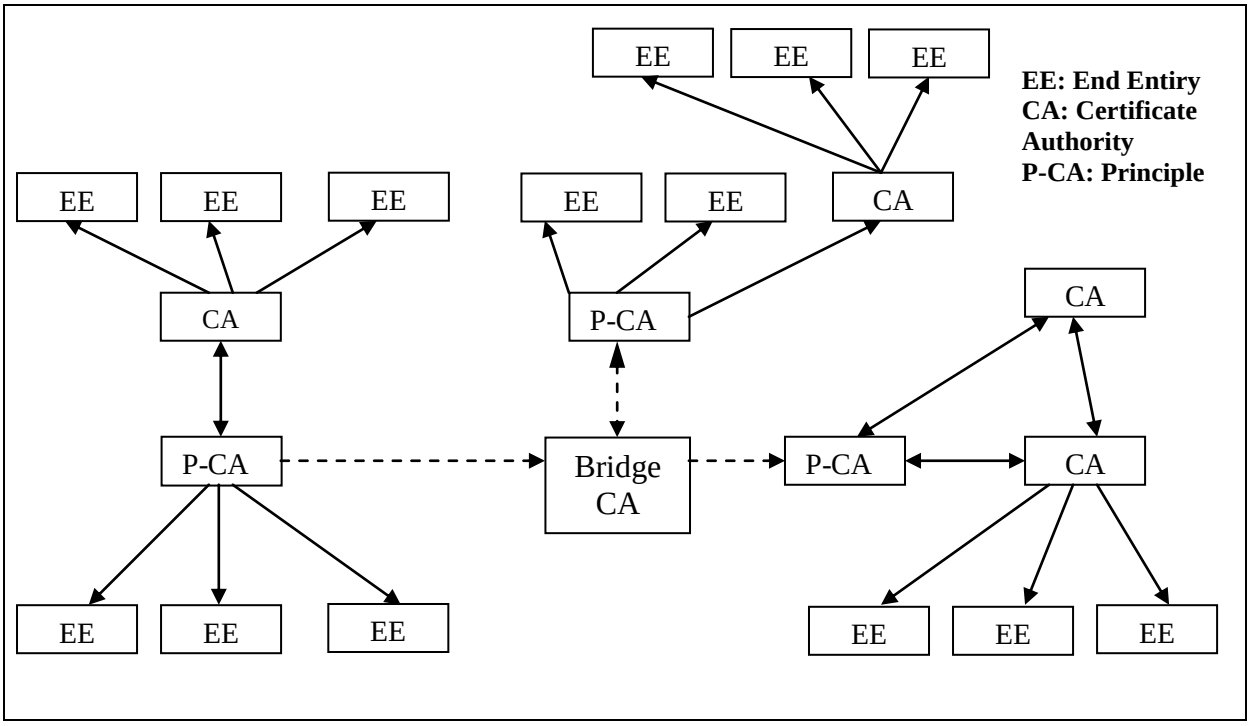
- Để tìm chuỗi chứng chỉ và CRLs với những mô hình khác thì việc sử dụng thư mục có thể trở nên khó hơn.

Hiện nay các tổ chức chính phủ và công ty đang thiết lập CA riêng theo yêu cầu PKI của mình. Khi có yêu cầu xử lý giao tiếp giữa các tổ chức khác nhau, những CA này sẽ tiến hành xác thực chéo độc lập với nhau dẫn đến sự phát triển của thế giới internet sẽ diễn ra trong mô hình tin cậy theo các hướng khác nhau.

3.7.4. Mô hình Hub và Spoke

Trong mô hình Hub và Spoke, thay bằng việc xác thực chéo giữa CA, mỗi CA gốc thiết lập xác thực chéo với CA trung tâm. CA trung tâm này làm cho việc giao tiếp được thuận lợi hơn. CA trung tâm được gọi là Hub (hoặc bridge) CA. Động cơ thúc đẩy mô hình này là giảm số xác thực chéo từ n^2 xuống n.

Một điểm quan trọng khác với cấu hình này là CA trung tâm không tạo ra sự phân cấp. Tất cả các thực thể trong cấu hình đều giữ khóa công khai của CA cục bộ, không có khóa của CA trung tâm. Như vậy, rõ ràng mô hình này giảm đi nhược điểm của mô hình mạng nhưng lại gặp phải khó khăn trong việc thiết lập bridge CA làm việc với các CA khác trong hạ tầng cơ sở để các CA này có thể hoạt động được với nhau.



Hình 13 : Mô hình Hub và Spoke

Mô hình này do US Federal PKI phát triển đầu tiên. Nó mở rộng PKIs qua một số tổ chức lớn chia sẻ những chính sách có khả năng tương thích một cách đặc biệt và có những CA được thiết lập trước đây.

3.7.5. Mô hình Web

Khái niệm về mô hình web được lấy ra từ tên của nó (www). Trong mô hình này, mỗi nhà cung cấp trình duyệt gắn vào trình duyệt một hoặc nhiều khóa công khai của một số root CA phổ biến hoặc nổi tiếng. Mô hình này thiết lập một mô hình tin tưởng tự động giữa các root CA mà khóa của các CA này được gắn trong trình duyệt và người sử dụng.

Danh sách tin cậy phần lớn được sử dụng để xác thực web server mà những web server này được CA xác nhận trong danh sách trình duyệt client. Quá trình này được thực hiện một cách tự động với giao thức SLL.

** Ưu điểm :*

- Dễ triển khai vì danh sách đã có sẵn trong trình duyệt.

- Không cần thay đổi khi làm việc với trình duyệt web (Internet Explorer, Netscape Navigator) và tiện ích Email (Outlook Express, Microsoft Outlook, Netscape Navigator).

** Nhược điểm :*

- Về mặt công nghệ thì có thể thêm háy sửa đổi một root CA mới nhưng hầu hết người dùng trình duyệt lại không quen thuộc với công nghệ PKI và phụ thuộc vào những CA ở trong trình duyệt này.

- Người sử dụng phải tin tưởng vào danh sách CA trong trình duyệt. Nhưng một câu hỏi đặt ra là làm thế nào để có thể đảm bảo chắc chắn về tính chất tin cậy của CA ? Các kết quả nghiên cứu cho thấy rằng hiện nay nay chưa có cách nào để phân biệt mức độ xác thực giữa các chứng chỉ khác.

- Không thể thông báo đến tất cả trình duyệt của người sử dụng nếu khóa công khai của một CA nào đó bị xâm hại. Mô hình này đơn giản trong việc thực thi và đối với người dùng. Do đó có khả năng để triển khai nhanh và sử dụng với các giải pháp COST (Commercial of the Shelf) sẵn có. Mô hình này đặc biệt thích hợp cho yêu cầu PKI của những ứng dụng dựa trên web.

3.7.6. Mô hình người sử dụng trung tâm

Trong mô hình này mỗi người sử dụng trực tiếp và hoàn toàn có trách nhiệm trong việc quyết định tin tưởng hay từ chối chứng chỉ. Mỗi người sử dụng giữ một khóa vòng và khóa này đóng vai trò như CA của họ. Khóa vòng chứa khóa 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 phần mềm bảo mật PGP.

Mô hình này có một số hạn chế như sau :

- Không có khả năng mở rộng và thích hợp với những miền lớn.
- Khó để đặt mức độ tin cậy đối với khóa công được lấy từ người khác. Không có sự nhất quán của quá trình xác thực vì nó phụ thuộc vào người sử dụng
- Người sử dụng phải quản lý PKI và cần phải hiểu sâu về nó.

Mặc dù có những nhược điểm song mô hình này vẫn thích hợp cho việc sử dụng cá nhân trên Internet.

Mỗi mô hình đều có ưu và nhược điểm riêng. Việc lựa chọn mô hình nào tùy thuộc vào những yêu cầu mục đích của cộng đồng người dùng, tổng chi phí, thời gian triển khai, nhân lực quản lý, công nghệ hỗ trợ và một số vấn đề liên quan khác.

Chương 4 : CHỨNG CHỈ SỐ CA

4.1. GIỚI THIỆU

Mật mã khóa công khai sử dụng cặp khóa là khóa công khai và khóa bí mật để đảm bảo yêu cầu ‘‘bí mật, xác thực, toàn vẹn và chống chối bỏ’’. Một đặc tính quan trọng khác của lược đồ khóa công khai là phần khóa công khai được phân phối một cách tự do. Ngoài ra trong hạ tâng mã khóa công khai thì khóa công khai ngoài việc phải luôn sẵn có để mọi người trong hệ thống có thể sử dụng còn phải đảm bảo về tính toàn vẹn, điều này là rất khó do vậy người ra nghĩ đến chứng chỉ số.

4.2. ĐỊNH NGHĨA

Chứng chỉ số là sự gắn kết giữa khóa công khai của thực thể với một hoặc nhiều thuộc tính liên quan đến thực thể. Thực thể có thể là người, thiết bị phần cứng như máy tính, router hay một phần mềm xử lý. Một chứng chỉ khóa công khai được trung tâm cấp chứng chỉ cấp, đảm bảo sự gắn kết giữa khóa công khai, thực thể sở hữu khóa này và tập các thuộc tính khác được viết trong chứng chỉ.

Chứng chỉ chứa những thông tin cần thiết như khóa công khai, chủ thể khóa công, người cấp và một số thông tin khác. Tính hợp lệ của các thông tin được đảm bảo bằng chữ ký số của người cấp chứng chỉ. Người nào muốn sử dụng chứng chỉ trước hết sẽ kiểm tra chữ ký số trong chứng chỉ. Nếu nó là chữ ký hợp lệ thì sau đó có thể sử dụng chứng chỉ theo mục đích mong muốn.

4.3. CHỨC NĂNG CỦA CHỨNG CHỈ

Chứng chỉ số là một tệp tin điện tử được sử dụng để nhận biết một cá nhân, hay một máy chủ, một công ty hoặc một vài đối tượng khác và gắn chỉ danh của đối tượng đó với một khóa công khai. Giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tở nhận diện cá nhân thông thường khác, chứng chỉ số cung cấp bằng chứng cho sự nhận diện của một đối tượng. Hệ mã hóa khóa công khai sử dụng chứng chỉ số để giải quyết vấn đề mạo danh.

Trong chứng chỉ số chứa một khóa công khai được gắn với một tên duy nhất của một đối tượng (như tên của một nhân viên hoặc server). Chứng chỉ số giúp ngăn chặn việc sử dụng khóa công khai cho việc giả mạo. Chỉ có khóa công khai được

chứng thực bởi chứng chỉ số mới làm việc với khóa riêng tương ứng được sở hữu bởi đối tượng mà chỉ có chỉ danh đã được chứng thực nằm trong chứng chỉ số.

Ngoài khóa công khai, một chứng chỉ số còn chứa thêm tên của đối tượng mà nó nhận diện, hạn dùng, tên của CA cấp chứng chỉ số đó, mã số thứ tự và những thông tin khác. Điều quan trọng nhất là một chứng chỉ số luôn luôn chứa chữ ký số của CA đã cấp chứng chỉ số đó, giúp người sử dụng biết và tin vào CA.

4.4. PHÂN LOẠI CHỨNG CHỈ SỐ

Hệ thống cung cấp chứng chỉ số (MyCA) được xây dựng trên nền hệ điều hành Red Hat Linux. Nó gồm 2 mô hình khác nhau :

- Mô hình cấp phát, quản lý và hủy bỏ chứng chỉ do người sử dụng tự sinh khóa.
- Mô hình cấp phát, quản lí và hủy bỏ chứng chỉ do trung tâm sinh khóa (được gọi là mô hình sinh khóa tập trung). Dĩ nhiên với mô hình nào thì việc quản lí khóa cũng đều do CA đảm nhiệm.

Một số loại chứng chỉ :

- Chứng chỉ khóa công X.509.
- Chứng chỉ khóa công đơn giản (Simple Public Key Certificates - SPKC).
- Chứng chỉ sử dụng Pretty Good Privacy (PGP).
- Chứng chỉ thuộc tính (Attribute Certificate - AC)

Tất cả các loại chứng chỉ này đều có cấu trúc định dạng riêng. Hiện nay chứng chỉ khóa công khai X.509 được sử dụng phổ biến trong hầu hết các hệ thống PKI., chính vì vậy trong phần tiếp theo tôi trình bày về chứng chỉ khóa công khai X.509.

4.5. CHỨNG CHỈ KHÓA CÔNG KHAI X.509

Chứng chỉ X.509 v3 là định dạng chứng chỉ được sử dụng phô biến và được hầu hết các nhà cung cấp sản phẩm PKI triển khai. Chứng chỉ khóa công khai X.509 được Hội viễn thống quốc tế (ITU) đưa ra lần đầu tiên vào năm 1988 như một bộ phận của dịch vụ thư mục X.509. Chứng chỉ gồm 2 phần : Phần đầu là những trường cơ bản cần thiết phải có trong chứng chỉ. Phần thứ hai chứa thêm một số trường phụ, những trường phụ này được gọi là trường mở rộng dùng để xác định và đáp ứng những yêu cầu bổ sung của hệ thống. Khuôn dạng của chứng chỉ X.509 được chỉ ở hình bên dưới :

Version Number
Serial Number
Signature
Issuer
Validity Period
Subject
Subject Public Key Infomation
Issuer Unique identifier
Subject Unique identifier
Extensions

Hình 15 : Khuôn dạng chứng chỉ X.509

4.5.1. Những trường cơ bản của chứng chỉ X.509

- **Version** : Xác định số phiên bản của chứng chỉ.

- **Certificate Serial Number** : do CA gán, là định danh duy nhất của chứng chỉ.

- **Signature Algorithm ID** : Chỉ ra thuật toán CA sử dụng để ký số chứng chỉ. Có thể là thuật toán RSA hoặc DSA…

- **Issuer** : chỉ ra CA cấp và ký chứng chỉ.

- **Validity Period** : khoảng thời gian chứng chỉ có hiệu lực. Trường này xác định thời gian chứng chỉ bắt đầu

- **Subject :** xác định thực thể mà khóa công khai của thực thể này xác nhận. Tên của subject phải duy nhất đối với mỗi thực thể CA xác nhận.

- **Subject public key infomation :** chứa khóa công khai và những tham số liên quan ; xác định thuật toán (ví dụ RSA hoặc DSA) được sử dụng cùng với khóa.

- **Issuer Unique ID :** là trường không bắt buộc, trường này cho phép sử dụng lại tên của subject khi quá hạn. Trường hợp này cũng ít được sử dụng.

- **Extensuons :** chỉ có trong chứng chỉ v3.

- **Certification Authority's Digital Signature :** chữ ký số của CA được tính từ những thông tin trên chứng chỉ với khóa riêng và thuật toán ký số được chỉ ra trong trường Signature Algorihm Identifier của chứng chỉ.

Tính toàn vẹn của chứng chỉ được đảm bảo bằng chữ ký số của CA trên chứng chỉ. Khóa công khai của CA được phân phối đến người sử dụng chứng chỉ theo một số cơ chế bảo mật trước khi thực hiện các thao tác PKI. Người sử dụng kiểm tra hiệu lực của chúng chỉ được cấp với chữ ký số của CA và khóa công khai của CA.

4.5.2. Những trường mở rộng của chứng chỉ X.509

Phần mở rộng là những thông tin thuộc tính cần thiết được đưa vào để gắn những thuộc tính này với người sử dụng hay khóa công. Những thông tin trong phần mở rộng thường được dùng để quản lý xác thực phân cấp, chính sách chứng chỉ, thông tin về chứng chỉ bị thu hồi… Nó cũng có thể được sử dụng để định nghĩa phần mở rộng riêng chứa những thông tin đặc trưng cho cộng đồng nhất định. Mỗi trường mở rộng trong chứng chỉ được thiết kế với cờ ''critical'' hoặc ''Uncritical''.

- **Authority Key Indentifier :** chứa ID khóa công khai của CA. ID này là duy nhất và được dùng để kiểm tra chữ ký số trên chứng chỉ. Nó cũng được sử dụng để phân biệt giữa các cặp khóa do một CA sử dụng (trong trường hợp nếu CA có nhiều hơn một khóa công khai). Trường này được sử dụng cho tất cả các chứng chỉ tự ký số (CA- certificates).

- **Subject Key Identifier :** chứa ID khóa công khai có trong chứng chỉ và được sử dụng để phân biệt giữa các khóa nếu như có nhiều khóa được gắn vào trong cùng chứng chỉ của người sử dụng (Nếu chủ thể có nhiều hơn một khóa công khai).

- **Key Usage :** chứa một chuỗi bít được dùng để xác định (hoặc hạn chế) chức năng hoặc dịch vụ được hỗ trợ qua việc sử dụng khóa công khai trong chứng chỉ.

- **Extended Key Usage :** chứa một hoặc nhiều OIDs (định danh đối tượng- Object Identifier) để xác định cụ thể việc sử dụng khóa công trong chứng chỉ. Các giá trị có thể là : (1) xác thực server TLS, (2) xác thực client TLS, (3) Ký Mã, (4) bảo mật email, (5) Tem thời gian.

- **CRL Distribution Point :** chỉ ra vị trí của CRL tức là nơi hiện có thông tin thu hồi chứng chỉ. Nó có thể là URI (Uniform Resource Indicator), địa chỉ của X.509 hoặc LDAP server.

- **Private Key Usage Period :** trường này cho biết thời gian sử dụng của khóa riêng gắn với khóa công khai trong chứng chỉ.

- **Certificate Policies :** trường này chỉ ra dãy các chính sách OIDs gắn với việc cấp và sử dụng chứng chỉ.

- **Policy Mappings :** trường này chỉ ra các chính sách xác thực tương đương giữa hai miền CA. Nó được sử dụng trong việc thiết lập xác thực chéo và kiểm tra đường dẫn chứng chỉ. Trường này chỉ có trong chứng chỉ CA.

- **Subject Alternative Name :** chỉ ra những dạng tên lựa chọn gắn với người sở hữu chứng chỉ. Những giá trị có thể là : địa chỉ e-mail, địa chỉ IP, địa chỉ URI…

- **Issuer Alternative Name :** chỉ ra những dạng tên lựa chọn gắn với người cấp chứng chỉ.

- **Subject Directory Attributes :** trường này chỉ ra dãy các thuộc tính gắn với người sở hữu chứng chỉ. Trường mở rộng này không được sử dụng rộng rãi. Nó được dùng để chứa những thông tin liên quan đến đặc quyền.

- **Basic Constrains Field :** trường này cho biết đây có phải là chứng chỉ CA hay không bằng cách thiết lập giá trị logic (true). Trường này chỉ có trong chứng chỉ CA. Chứng chỉ CA dùng để thực hiện một số chức năng. Chứng chỉ này có thể ở một trong hai dạng. Nếu CA tạo ra chứng chỉ để tự sử dụng, chứng chỉ này được gọi là chứng chỉ CA tự ký. Khi một CA mới được thiết lập, CA tạo ra một chứng chỉ CA tự ký để ký lên chứng chỉ của người sử dụng cuối trong hệ thống. Và dạng thứ hai là CA cấp chứng chỉ cho những CA khác trong hệ thống.

- **Path Length Contraint :** trường này chỉ ra số độ dài tối đa của đường dẫn chứng chỉ có thể được thiết lập. Giá trị ‘‘zero’’ chỉ ra rằng CA chỉ có thể cấp chứng chỉ cho thực thể cuối, không cấp chứng chỉ cho những CA khác. (Trường này chỉ có trong chứng chỉ của CA).

- **Name Constrainsts :** được dùng để bao gồm hoặc loại trừ các nhánh trong những miền khác nhau trong khi thiết lập môi trường tin tưởng giữa các miền PKI.

- **Policy Constraints :** được dùng để bao gồm hoặc loại trừ một số chính sách chứng chỉ trong khi thiết lập môi trường tin tưởng giữa các miền PKI.

4.5.3. Thu hồi chứng chỉ

Trong một số trường hợp như khóa bị xâm hại, hoặc người sở hữu chứng chỉ thay đổi vị trí, cơ quan… thì chứng chỉ đã được cấp không có hiệu lực. Do đó, cần

phải có một cơ chế cho phép người sử dụng chứng chỉ kiểm tra được trạng thái thu hồi chứng chỉ. X.509 cho phép kiểm tra chứng chỉ trong những trường hợp sau :

- Chứng chỉ không bị thu hồi.
- Chứng chỉ đã bị CA cấp thu hồi.
- Chứng chỉ do một tổ chức có thẩm quyền mà CA ủy thác có trách nhiệm thu hồi chứng chỉ thu hồi.

Cơ chế thu hồi X.509 xác định là sử dụng danh sách thu hồi chứng chỉ (CRLs). X.509 đưa ra sự phân biệt giữa ngày, thời gian chứng chỉ bị CA thu hồi và ngày, thời gian trạng thái thu hồi được công bố đầu tiên. Ngày thu hồi thực sự được ghi cùng với đầu vào chứng chỉ trong CRL. Ngày thông báo thu hồi được xác định trong header của CRL khi nó được công bố. Vị trí của thông tin thu hồi có thể khác nhau tùy theo CA khác nhau. Bản thân chứng chỉ có thể chứa con trỏ đến nơi thông tin thu hồi được xác định vị trí. Người sử dụng chứng chỉ có thể biết thư mục, kho lưu trữ hay cơ chế để lấy được thông tin thu hồi dựa trên những thông tin cấu hình được thiết lập trong quá trình khởi sinh.

Để duy trì tính nhất quán và khả năng kiểm tra, CA yêu cầu :

- Duy trì bản ghi kiểm tra chứng chỉ thu hồi.
- Cung cấp thông tin trạng thái thu hồi.
- Công bố CRLs khi CRL là danh sách trống.

4.5.4. Chính sách của chứng chỉ

Như được giới thiệu trong phần trên, một số mở rộng liên quan đến chính sách có trong chứng chỉ. Những mở rộng liên quan đến chính sách này được sử dụng trong khi thiết lập xác thực chéo giữa các miền PKI. Một chính sách chứng chỉ trong X.509 được định nghĩa là ‘‘ tên của tập các quy tắc chỉ ra khả năng có thể sử dụng của chứng chỉ cho một tập thể đặc thù và một lớp ứng dụng với yêu cầu bảo mật chung’’. Chính sách có định danh duy nhất (được biết đến như định danh đối tượng hay OID) và định danh này được đăng ký để người cấp và người sử dụng chứng chỉ có thể nhận ra và tham chiếu đến. Một chứng chỉ có thể được cấp theo nhiều chính sách. Một số có thể là thủ tục và mô tả mức đảm bảo gắn với việc tạo và quản lý chứng chỉ. Những chính sách khác có thể là kỹ thật và mô tả mức đảm bảo gắn với an toàn của hệ thống được dử dụng để tạo chứng chỉ hay nơi lưu trữ khóa.

Một chính sách chứng chỉ cũng có thể được hiểu là việc giải thích những yêu cầu và giới hạn liên quan đến việc sử dụng chứng chỉ được công bố theo chính sách này. Chính sách chứng chỉ- Certificate Polices (CP) được chứa trong trường mở rộng chuẩn của chứng chỉ X.509. Bằng việc kiểm tra trường này trong chứng chỉ, hệ thống sử dụng chứng chỉ có thể xác định được một chứng chỉ cụ thể có thích hợp cho mục đích sử dụng hay không.

Một thuật ngữ chuyên môn khác « Certificate Practice Statement (CPS) » được sử dụng để mô tả chi tiết những thủ tục hoạt động bên trong của CA và PKI cấp chứng chỉ với chính sách chứng chỉ đã quy định.

Chính sách chứng chỉ đặc biệt quan trọng khi đưa ra quyết định để xác nhận chéo hai PKI khác nhau.

4.5.5. Công bố và gửi thông báo thu hồi chứng chỉ

Thông thường chứng chỉ sẽ hợp lệ trong khoảng thời gian có hiệu lực. Nhưng trong một số trường hợp chứng chỉ lại không hợp lệ trước thời gian hết hạn, ví dụ như :

- Khóa riêng của chủ thể bị xâm phạm
- Thông tin chứa trong chứng chỉ bị thay đổi
- Khoá riêng của CA cấp chứng chỉ bị xâm phạm.

Trong trường hợp này cần có một cơ chế để thông báo đến người sử dụng khác. Một trong những phương pháp để thông báo đến người sử dụng về trangj thái của chứng chỉ là công bố CRLs định kỳ hoặc khi cần thiết. Ngoài ra, có một số cách lựa chọn khác để thông báo đến người sử dụng như dùng phương pháp trực tuyến Online Certificate Status Protocol.

4.5.5.1. Certìicate Revolucation List (CRLs)

CRLs là cấu trúc dữ liệu được ký như chứng chỉ người sử dụng. CRLs chứa danh sách các chứng chỉ của người sử dụng .CRLs thường do một CA cung cấp. Tuy nhiên, CRL cũng có thể được sử dụng để cung cấp thông tin cho nhiều CA nếu nó được định nghĩa như một CRL gián tiếp. Những thông tin này được chứa trong trường mở rộng CRL Scope.

Những chứng chỉ đã bị CA thu hồi được ghi vào danh sách theo thứ tự của revoked Certificate. Mỗi đầu vào nhận biết chứng chỉ thông qua số serial và ngày thu hồi trên đó có ghi rõ thời gian và ngày khi chứng chỉ bị CA thu hồi

Version number	
Signature	
Issuer	
This update	
Next update	
User certificate serial number	Date of revocation
Revocation reason	
User certificate serial number	Date of revocation
Revocation reason	
CRL extensions	

Hình 16 : Khuôn dạng danh sách bị thu hồi

Trong đó :

- **Version number** : chỉ ra phiên bản của CRL
- **Signature** : nhận biết loại hàm băm và thuật toán ký được sử dụng để ký danh sách thu hồi CRL
- **Issuer** : tên của thực thể cấp và ký CRL
- **This Update** : chỉ ra ngày và thời gian CRL được công bố
- **Next Update** : chỉ ra ngày và thời gian danh sách thu hồi kế tiếp được cấp
- **List of revoked certificates :** chứa danh sách cùng với serial của những chứng chỉ bị thu hồi

4.5.5.2. Authority Revocation List (ARLs)

ARL là một CRL đặc biệt chứa thông tin thu hồi về chứng chỉ CA. ARLs không chứa chứng chỉ của người sử dụng cuối. Những thay đổi thông thường trong ARL thường hiếm khi xảy ra bởi vì chứng chỉ của CA chỉ bị thu hồi khi khoá riêng của CA bị xâm hại và đó lại là trường hợp không thường xảy ra. Nếu chứng chỉ chéo bị thu hồ thì người cấp chứng chỉ chéo này sẽ công bố một ARL mới để thông báo với tất cả các thực thể khác về tình huống này. ARLs được sử dụng chủ yếu trong quá trình thẩm tra đường dẫn chứng chỉ nếu môi trường tin cậy bao gồm CA có chứng chỉ xác thực chéo.

4.5.5.3. Cơ chế truy vấn On – line (On – line Query Mechanisms)

CRLs và ARLs giúp người sử dụng cuối nhận biết được về tình trạng thu hồi chứng chỉ. Nhưng có một vấn đề nảy sinh là điều gì sẽ xảy ra nếu CA thu hồi chứng chỉ ngay sau khi vừa công bố CRL. Không có người sử dụng nào nhận biết được về việc thu hồi này đến khi một CRL mới được thông báo.

Một lược đồ khác để kiểm soát được trạng thái của chứng chỉ do IETF phát triển là OCSP (Online Certificate Status Responder). Lược đồ này dựa trên cơ chế truy vấn trực tiếp hơn việc công bố định kỳ CRLss và ARLs. OCSP là giao thức yêu cầu trả lời đưa ra cơ chế để nhận được thông tin thu hồi trực tuyến từ thực thể tin cậy là 'OCSP Reply' với trạng thái của mỗi chứng chỉ. Chứng chỉ có thể ở một trong ba trạng thái sau : 'good', 'revoked' và 'unknown'.

Sử dụng dịch vụ online có một số ưu điểm sau :

- Trả lời thường xuyên và luôn có tính chất mới
- Thời gian trả lời nhanh
- Giảm thiểu việc sử dụng băng thông mạng sẵn có.
- Tổng phí xử lý phía client thấp

Tuy nhiên dịch vụ online có hạn chế trong trường hợp cần kiểm tra trạng thái thu hồi nhưng không online. Vấn đề về bảo mật cũng được đặt ra khi sử dụng dịch vụ này. Hình 2.5 là dịch vụ kiểm tra online với OCSP Responder là dịch vụ khác nhau.

4.6. MỘT SỐ CÔNG NGHỆ SỬ DỤNG TRONG PKI

4.6.1. Công nghệ SSL (Secure Socket Layer)

SSL là một giao thức có thể được đặt ở tầng mạng và tầng ứng dụng. SSL cung cấp dịch vụ truyền thông có bảo mật giữa client và server bằng việc cho phép client và server xác thực lẫn nhau sử dụng chữ ký số và bảo mật thông tin trao đổi qua lại bằng cách mã hoá các thông tin đó.

Giao thức này được thiết kế để có thể trợ giúp một loạt các thuật toán sử dụng cho việc mã hoá, hàm băm, chữ ký số. Giao thức SSL có ba phiên bản :

- SSLv2 : đây là phiên bản đầu tiên của giao thức SSL do Netscape Corporation thiết kế, chưa có trợ giúp chain certificate

- SSLv3 : đây là phiên bản SSL version 3.0 do Netscape Corporation thiết kếm, được tung ra thị trường vào tháng 3 năm 1996, có trợ giúp quản lí chuỗi (chain certificate) và được suport cho tất cả các trình duyệt phổ thông

- TLSv1 : đây là giao thức Transport Layer Security version 1.0, dựa trên cơ sở của SSLv3 được thiết kế bởi IETF (Internet Engineering Task Porce) nhưng hiện nó chưa được suport cho các trình duyệt.

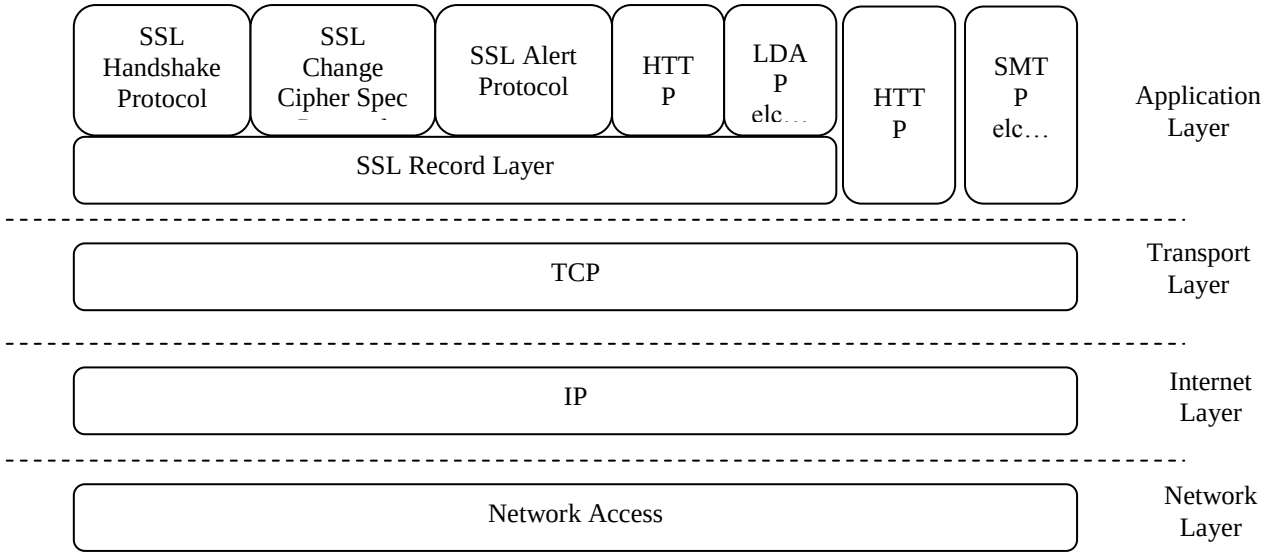
Một số điểm chú ý :

- Một đặc điểm quan trọng của SSLv3 và TLSv1 là có trợ giúp việc nạp chuỗi. Với đặc điểm được bổ sung này sẽ cho phép server và client có thể thực hiện việc xác thực lẫn nhau mà có thể đối tượng thực hiện xác thực không cần phải cài các intermediate issuers.

- TLSv1 dực trên nền tảng là SSLv3 trong đó có bổ sung phần block padding cho các thuật toán mã khối, chuẩn hoá thứ tự các message và bổ sung thêm các thông báo trong phiên liên lạc.

- Các phiên bản trên cũng như các thuật toán mã hoá, thuật toán trao đổi khoá, hàm băm hoàn toàn có thể được chỉ ra cụ thể khi thiết lập cấu hình sử dụng SSL cho Web server và một số trình duyệt.

Với nhu cầu thực tế hiện nay SSL2 ít được sử dụng. Bên cạnh đó do có sự tương ứng giữa SSLv3 và TLSv1, hơn nữa hiện tại trong thực tế TLSv1 chưa được tích hợp co một số trình duyệt phổ thông, nên tôi chỉ đề cập đến SSlv3. Giao thức SSLv3 gồm hai thành phần Handshake và Record porocol. SSLv3 Record protocol cung cấp cơ chế bảo mật với thuật toán mã hoá như DES, RC4 ... và giao thức kết nối có sử dụng hàm kiểm tra MAC trong quá trình trao đổi dữ liệu. Còn SSLv3 Handshake protocol thực hiện xác thực đối tác, trao đổi các giá trị secure (an toàn) sử dụng cho SSLv3 Record protocol. Toàn bộ giao thức SSLv3 và mối liên hệ của nó với tầng ứng dụng và tầng TCP có thể mô tả như sơ đồ dưới đây.



Hình 17 : Giao thức SSL

4.6.1.1. Record protocol

Giao thức SSLv3 Record là một tầng giao thức. Đối với mỗi giao thức nói chung, một gói dữ liệu sẽ bao gồm các trường độ dài, mô tả và nội dung dữ liệu. SSLv3 Record nhận dữ liệu cần gửi từ tầng trên phân nhỏ thành từng block, nén dữ liệu, bổ sung dữ liệu kiểm tra, mã hoá và gửi. Khi nhận dữ liệu về tiến trình được thực hiện ngược lại : giải mã, mã hoá và gửi. Khi nhận dữ liệu về tiến trình được thực hiện ngược lại : giải mã, kiểm tra, gỡ nén và sắp xếp lại rồi gửi lên tầng trên.

4.6.1.2. Handshake protocol

Các tham số mật mã liên quan đến phiên liên lạc được thực hiện thông qua SSLv3 Handshake protocol, nó nằm ngay bên trên SSL Record Layer. Khi SSL client và SSL server bắt đầu một phiên liên lạc chúng cần thống nhất về phiên bản của giao thức sẽ được dùng, lựa chọn thuật toán mã hoá cho phiên liên lạc, có thể có hoặc không việc xác thực lẫn nhau và sử dụng thuật toán mã hoá khoá công khai để sinh khoá chung cho phiên liên lạc đó.

Những đặc tính SSL giúp bảo mật dữ liệu :

1. Các bên giao tiếp (nghĩa là client và server) có thể xác thực nhau bằng cách sử dụng mật mã khoá chung

2. Tính bảo mật của dữ liệu được đảm bảo vì trong suốt quá trình truyền luôn luôn được bảo vệ

3. Tính xác thực và tính toán vẹn của dữ liệu cũng được đảm bảo vì trong quá trình truyền dữ liệu được xác thực, kiểm tra bằng cách sử dụng MAC.

Hạn chế của SSL : SSL không ngăn chặn được một số cuộc tấn công của đối phường nhằm vào phân tích lưu lượng. (Địa chỉ IP nguồn và đích không được mã hoá, số cổng TCP là những đối tượng thường bị tấn công trên cơ sở đó chúng có thể xác định được các bên tham gia, các thông tin liên quan)

4.6.2. Công nghệ LDAP

Hiện nay một điều tối quan trọng để viết được những phần mềm lớn là phải biết khai thác, tích hợp dữ liệu từ các hệ thống khác nhau. Một chương trình lớn có rất nhiều modul, mỗi modul lại được thiết kế trên một nền tảng dữ liệu khác nhau như : có người dùng Oracle với AS Portal, có người dùng DB2 với WebSphere, MýQL với PHPnuke...vậy phải làm thế nào ? Câu trả lời chính là sử dụng LDAP. Vậy LDAP là gì ?

LDAP(Lightweight Directory Access Protocol) tạ dịch là Giao thức truy cập nhanh các dịch vụ thư mục.

LDAP là một giao thức Client/Server để truy một Directory Server(Dịch vụ thư mục), có thể xem Directory như một cơ sở dữ liệu, tuy nhiên đối với các directory thường việc đọc được các dữ liệu hiệu quả hơn việc ghi dữ liệu. Có nhiều cách khác nhau để thiết lập một Directory và cũng có nhiều cách để tham chiếu, truy vấn, truy nhập đến cơ sở dữ liệu trong Directory và LDAP cũng dựa trên mô hình Client/Server. Một hoặc nhiều LDAP server lưu dữ liệu tạo lên các cây thư mục LDAp hoặc các backed database. LDAP client kết nối tới LDAP server, đưa yêu cầu để LDAP server thực hiện và trả lại kết quả cho client.

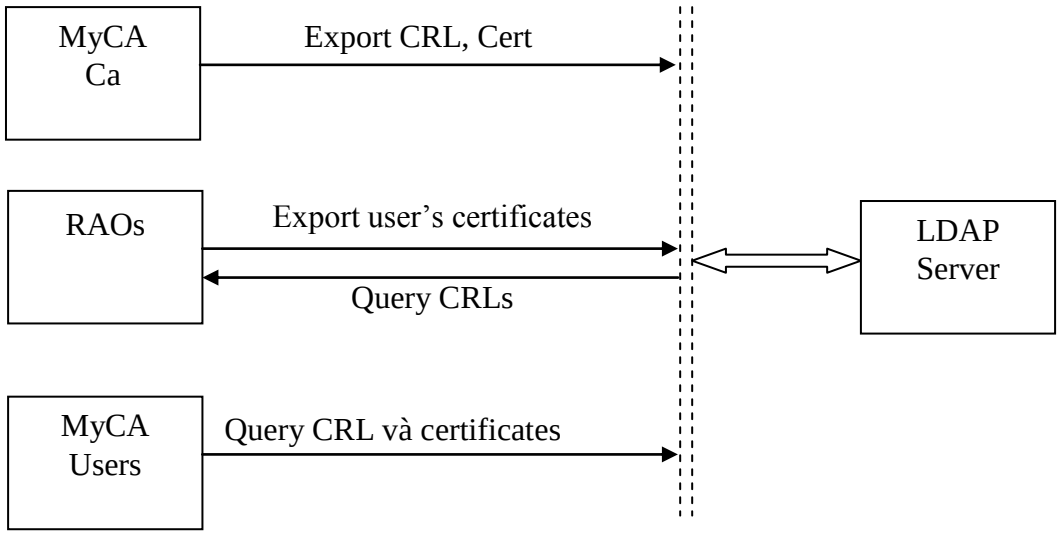
Pulic Database Server là một hoặc nhiều máy cài đặt LDAP server, trên đó lưu trữ các chứng chỉ đã được phát hành cho người sử dụng, các chứng chỉ của máy server thuộc hệ thống, các CRL do các CA server phát hành. Một số chức năng chính giành cho người sử dụng khi truy cập đến Web Pulic Database :

Tên mục, chức năng	Mô tả chức năng chính
Chức năng « Dowload CA certificase chain from LDAP » bao gồm 2 mục :	
« Get CA certificate for IE & IIS	Người sử dụng dùng chức năng để tìm kiếm và tải chứng chỉ của Root CA từ database server về cho người sử dùng Window. (Trong trường hợp CA nhiều cấp tìm kiếm theo tên vủa CA có các chứng chỉ trogn chuỗi các chứng chỉ cần tìm)
« Get CA certificate for Apache & Netscape	Người sử dụng dùng chức năng để tìm kiếm và tải chứng chỉ của Root CA từ database server về cho người sử dụng dùng Netscape và Apache trên môi trường Linux. (Trong trường hợp CA nhiều cấp tìm kiê theo tên của CA bậc thấp trong các CA có các chứng chỉ trong chuỗi các chững chỉ cần tìm
Chức năng « Dowload certificates from LDAP » bao gồm 2 mục :	
« Get Certificate for Netscape Brower, Apache server »	Người sử dụng dùng chức năng để tìm kiếm(theo mail được đăng ký trong chứng chỉ cần tìm) và tải chứng chỉ từ database server về cho người sử dụng dùng Linux
« Get Certifi for IE & IIS »	Người sử dụng dùng chức năng để tìm kiếm (theo mail được đăng ký trong chứng chỉ cần tìm) và tải chứng chỉ từ database server về cho người sử dụng dùng Windows
Chức năng « Update CRLs » bao gồm có 3 mục sau :	
« Update current CRLs for Netscape	Người sử dụng dùng chức năng tìm kiếm (theo tên của CA phát hành ra CRL cần tìm) và cập nhật CRL đó cho Netscape trên Linux
« Get current CRLs for Apache server	Người sử dụng dùng chức năng để tìm kiếm (theo tên của CA phát hành ra CRL cần tìm) và tải CRL đó về cho người sử dụng để cài đặt cho IE và IIS trên Windows
« Get current CRLs for IE & IIS »	Người sử dụng dùng chức năng để tìm kiếm (theo têncủa CA phát hành ra CRL cần tìm) và tải CRL đó về cho người sử dụng dùng để cài đặt cho IE và IIS trên WIndows

- Là một giáo thức tìm, truy cập các thông tin dạng thư mục trên server.
- Nó là giao thức dạng Client/Server dùng để truy cập dịch vụ thư mục
- LDAP chạy trên TCP/IP hoặc các dịch vụ hướng kết nối khác.
- Cho phép xác định cấu trúc và đặc điểm của thông tin trong thư mục.
- Một mô hình các thao tác cho phép xác định các tham chiếu và phân bố dữ liệu.
- Là một giao thức mở rộng.

Thư mục trong LDAP được hiểu rộng hơn khái niệm thư mục trong Windows, nó bao gồm các cấu trúc dữ liệu dạng liệt kê theo thư mục. Trong hệ thống MyCA các chứng chỉ và CRL của người sử dụng được trung tâm phát hành lưu trữ trên một cơ sở dữ liệu công khai, để người sử dụng có thể tải các chứng chỉ và cập nhật CRL từ cơ sở đó. Đồng thời đảm bảo yêu cầu việc cập nhật dữ liệu từ các máy chủ (CA server) phải nhanh chóng, chính xác, phù hợp với kiểu dữ liệu có cấu trúc như các chứng chỉ. Để làm được điều này có rất nhiều hệ quản trị cơ sở đữ liệu có thể đáp ứng, hiện nay có LDAP được sử dụng phổ biến và hiệu quả.

Mối quan hệ và trao đổi dữ liệu giữa các thành phần với Pulic Database Server được minh hoạ bằng hình sau :



Hình 18 : Mô hình quan hệ và trao đổi dữ liệu giữa các thành phần trong hệ thống

Mối quan hệ giữa LDAP server với các máy chủ trong hệ thống có thể phân làm 2 loại :

- Máy CA trong hệ thống khi phát hành CRL sẽ cập nhật CRL này ra LDAP server. Khi người sử dụng đến trung tâm nhận chứng chỉ, đồng thời với việc cấp chứng chỉ cho người sử dụng, chứng chỉ đó cũng được export ra LDAP từ máy CA, ngược lại khi có chứng nhận cho việc chứng chỉ của người sử dụng đã được huỷ bỏ, từ máy CA người quản trị truy cập tới LDAP để truy vấn CRL.

- Người sử dụng có thể dùng một trang web riêng có thể truy cập đến LDAP Database server bất cứ lúc nào để tải chứng chỉ cũng như cập nhật các CRL.

Chương 5 : ỨNG DỤNG CỦA CA

5.1. ỨNG DỤNG CA TRONG DỊCH VỤ WEB

5.1.1. Đặt vấn đề

Hiện nay Internet đang được sử dụng phổ biến trong đời sống của chúng ta, chúng ta không thể phủ nhận vai trò to lớn của Internet. Việc kết nối quan mạng Internet hiên nay chủ yêu sử dụng giao thức TCP/IP cho phép thông tin gửi từ máy này tới máy khác thông qua một hoặc nhiếu trạm trung gian. Tuy nhiên, chính vì tính linh hoạt náy đã tạo điều kiện cho bên thứ 3 có thể : nghe trộm, giả mạo, mạo dạnh, lấy cắp...thông tin cần truyền. Đặc biệt trong lĩnh vực thương mại điện tử thì nộ dung trên web rất cần được bảo vệ. Cũng xuất phát từ thực tế đó nên yêu cầu cần bảo vệ thông tin trên web được đặt ra.

5.1.2. Giải quyết vấn đề

Hệ mật mã khoá công khai với chứng chỉ số có thể giải quyết được một số vấn đề liên quan đến đảm bảo thông tin trên web như :

- Mã hoá và giải mã : Cho phép hai bên trao đổi thông tin với nhau nhưng thông tin đó sẽ được che giấu mà chỉ họ mới biết. Người gửi sẽ mã hoá thông tin trước khi gửi chúng đi, người nhận sẽ giải mx nó để đọc được thông tin.

- Chống giả mạo : Cho phép người nhận kiểm tra thông tin có bị thay đổi hay không, bất cứ một sự thay đổi nào cũng bị phát hiện.

- Xác thực : Cho phép người nhận xác định được bí danh của người gửi.

- Không thể chối cãi nguồn gốc : ngăn chặn người gửi chối cãi nguồn gốc tài liệu mình đã gửi.

5.1.3. Cài đặt chứng chỉ chi trình duyệt Internet Explorer

a. Các chứng chỉ do hệ thống MyCA cấp cho người sử dụng đều dùng thuật toán RSA với modulo 1024 bít nhưng đối với trình duyệt IE 5.0 cho phép cài đặt các chứng chỉ có độ dài khoá công khai không quá 512bít. Để cài được thì ta cần phải cài dặt phần mềm hỗ trợ trước (tệp ie5dom.exe).

Để cài đặt người sử dụng chỉ cần kích vào tệp ie5dom.exe rồi làm tiếp theo hướng dẫn. Sau khi thực hiện xong bạn cần khởi động lại để tiện ích có hiệu lực.

Sau khi cài đặt, người sử dụng mở IE, chọn menu/Tools/Internet Options, chọn Tab ‘‘contents ’’ rồi chọn nút lệnh ‘‘Certificate ’’ sẽ thấy xuất hiện chứng chỉ vừa được cài trong thư mục.

Muốn xem lại thông tin về chứng chỉ của mình sử dụng chọn nút ‘‘ View’’, cưar sổ hiện ra các thông số. Cùng với việc vài đặt chứng chỉ của người sử dụng, các chứng chỉ của CA cũng đồng thời được cài đặt, nếu chọn tab ‘‘ Trust Root Ceriticate Authorities ’’ sẽ xuất hiện RootCA phát hành ra chứng chỉ của người sử dụng.

Nội dung chứng chỉ của RootCA sẽ được lưu vào Registry. Sau khi cài đặt xong các chứng chỉ, người sử dụng cần thiết lập cấu hình cho IE : Chọn menu Tools/Internet Options/ Advance. Trong mục Setting bạn chọn ‘‘ Use SSL 3.0 ’’ hoặc ‘‘ Use TLS 1.0 ’’ rồi nhấn OK.

a. Cài đặt chứng chỉ cho IE.

Quá trình cài đặt chứng chỉ cho Netscape tiến hành theo các bước sau :

- Trên menu của trình duyệt Netscape bạn chọn chức năng ‘‘ Security ’’

- Chọn ‘‘ Your ’’ trong thư mục ‘‘ Your Certificates ’’, rồi chọn ‘‘ Import a Certificate ’’

- Người sử dụng nhập mật khẩu để truy nhập tới cơ sở dữ liệu lưu chứng chỉ của Netscape, chọn OK.

- Người sử dụng chọp tệp chứng chỉ cần cài đặt rồi nhấp OK, sau đó nhập mật khẩu.

- Bước tiếp theo là nhập tên chứng chỉ rồi chọn OK/

Để chứng chỉ có hiệu lực, người sử dụng nhất cần thiết lập thuộc tính cho Netscape chấp nhận RootCA vừa cài là Certificate Authority.

5.2. ỨNG DỤNG CA TRONG DỊCH VỤ E-MAIL

5.2.1. Đặt vấn đề

Email (Electrolic Mail) hay còn gọi là thư điện tử ngày càng đóng vai trò quan trọng trong đời sống vì những ưu điểm như : thông điệp có thể gửi đi nhanh chóng (phổ biến nhất là qua mạng Internet) đến khách hàng, đồng nghiệp, đối tác...mà giá thành rẻ, dễ thao tác. Những thông tin đó có thể là thông tin cá nhân (thăm hỏi sức

khoẻ, thông báo tình hình gia đình...), hợp đồng thương mại, nói chung là có rất nhiều thông tin mang tính nhạy cảm, không nên để lộ hoặc để người khác biết được. Vì những thông tin này có thể bị người khác đọc được, lấy được, giả mạo...Đây chính là vấn đề đặt ra đối với công tác đảm bảo an toàn thông tin : làm thế nào để đảm bảo thông tin khi truyền qua dịch vụ mail vẫn còn nguyên vẹn ?

Một trong những ứng dụng quan trọng của chứng chỉ số là mã hoá và xác thực thư điện tử. Người sử dụng có thể cài đặt chứng chỉ số đã được phát hành từ một Trung tâm cấp chứng chỉ số nào đó để thực hiện trao đổi thư điện tử có bảo mật với người dùng khác mà cùng chung hệ thống CA. Trong chương này, tôi giới thiệu cách sử dụng chừng chỉ số được cấp bởi hệ thống MyCA trên Outlook Express.

5.2.2. Cài đặt chứng chỉ số

Để dễ hình dung, tôi xin chọn dịch vụ của Công ty phần mềm và truyền thông VASC để mô tả quá trình đăng ký chứng chỉ cho email của bạn. Hiện tại, Công ty có 2 sản phẩm cho bạn lựa chọn là VASC Individual-Demo và VASC Individual Class3. Với bản demo thì thời gian sử dụng là 30 ngày, miễn phí nhưng công ty sẽ không chịu trách nhiệm về nội dung chương trình còn ngược lại bản Class3 bạn phải trả phí do đó bạn sẽ được hưởng các dịch vụ tốt nhất. Sau đây tôi mô tả cách đăng ký dịch vụ VASC Individual

- Ban vào camaster@vasc.com.vn để đăng ký, bạn cần nhập đầy đủ các thông tin:

Thông tin cá nhân :

+ Họ và tên + Địa chỉ email

+ Tổ chức + Đơn vị

+ Tỉnh/ Thành phố + Quận/ Huyện

+ Quốc tịch

Mật khẩu : + Mật khẩu

+ Xác nhận

Thông tin thêm : Nếu có bát kỳ yêu cầu nào thì bạn nhập vào đây

Sau khi đăng ký xong thi vào email của bạn yêu cầu xác nhận thông tin, nếu thông tin được xác nhận thì hiện lên bảng :

KẾT LUẬN

Qua 2 phần đã trình bày ở trên, ta thấy rằng tất cả vấn đề đều liên quan đến an ninh thông tin - một vấn đề hết sức nhạy cảm, có liên quan mật thiết đến chính trị, an ninh, tình báo, kinh tế và đối ngoại...Hiện nay nước ta đang nghiên cứu, xây dựng và triển khai một hệ thống PKI gồm một số CA. Về CA có khoa tập trung dự kiến đặt Roof CA tại Ban Cơ yếu thuộc Bộ nội vụ, nó được sử dụng chủ yếu cho các cơ quan Nhà nước hoặc cơ quan ban ngành liên quan. Còn CA không mang khoá tập trung phục vụ cho tất cả lĩnh vực kinh tế - xã hội như thương mại điện tử, thì sẽ được đặt tại Bộ Bưu chính Viễn thông.

Một câu hỏi tự nhiên đặt ra là : vậy ai sẽ chịu trách nhiệm kiểm soát, giám sát về sự an toàn thông tin khi PKI đi vào hoạt động ? Em thấy rằng không ai khác ngoài Bộ Công an. Theo em được biết các cơ quan chức năng được Bộ giao giám sát/ kiểm soát an ninh thông tin là Tổng cục An ninh. Nhưng em tin rằng chưa có đơn vị nào nghiên cứu vấn đề PKI cả. Để kiểm soát, giám sát an toàn thông tin trên hệ thống PKI, trước hết chúng ta cần nghiên cứu ngay từ bây giờ, những lỗ hổng của hệ thống và cách thức giám sat/kiểm soát như thế nào để đảm bảo yêu cầu đặt ra. Theo em biết ở đây là điều đáng tiếc. Bởi vì ở các nước có hệ thống này đều nằm dưới sự chỉ đạo của Có quan An ninh Quốc gia.

Để chủ động trong việc giám sát/kiểm soát đối với PKI, em xin mạnh dạn đề xuất :

Ngành Công an nên thành lập một đơn vị gồm các chuyên viên khá sâu về công nghệ thông tin để tập trung nghiên cứu những lỗ hổng (chắc chắn có thể xảy ra) đối với hệ thống PKI và Cas (Certificate Authorities). Để làm việc tốt chúng ta cần có mạng kiểm soát, cho phép kết nối với các Roof CA, nghiên cứu các tiêu chuẩn cho PKI ở Việt Nam và các nước trên thế giới. Từ đó phát hiện ra các lỗ hổng trên lĩnh vực xác thực, chữ ký số và đề xuất các biện pháp gửi lên cơ quan có thẩm quyền cao nhất ra quyết định. Ngay từ bây giờ, khoa Toan-Tin của học viên An ninh nhân dân có vai trò đóng góp nguồn nhân lực trẻ được đào tạo tốt về công nghệ thông tin nói chung, về lĩnh vực an ninh, an toàn thông tin quốc gia nói riêng.

Em được biết hiện nay Bộ công an có một đơn vị đảm nhiệm chức năng đảm bảo an ninh, an toàn thông tin quốc gia đó là A22(tức Cục kỹ thuật nghiệp vụ I). Nhưng đơn vị này chưa có một phòng nghiệp vụ Thương mại điện tư, thậm chí cũng chưa ai nghiên cứu công nghệ đầy hứa hẹn mà các nước xung quanh như Nhật Bản, Hàn Quốc, Singapore, Trung Quốc, Thái Lan...đã và đang ứng dụng công nghệ này.

Đây là nhiệm vụ rất khó khăn ví nó liên quan đến các kỹ thuật cao cũng như kiến thức toán học sâu sắc. Do đó chúng ta nên chuẩn bị trước như nhân lực, công nghệ và tổ chức thực hiện.

Trên đây là một vài ý kiến và đề xuất của em. Có thể còn rất nhiều vấn đề em chưa đi thật sâu trong khuôn khổ của một khoa luận tốt nghiệp Đại học. Em kính mong được sự đóng góp ý kiến, chỉ bảo của các các thầy, cô cũgn như các bạn để em có thể hoàn thiện hơn nữa nội dung của khoá luận. Em xin chân thành crm ơn.

Mốt số vấn đề đang được tiếp tục nghiến cứu phát triển :

- Tìm hiểu về đường cong Elliptic. Cài đặt hệ chữ ký số trên đường cong Elliptic ECDSA.

- Tích hợp thiết bị lưu khoá cùng với chứng chỉ số ứng dụng trong VPN.

TÀI LIỆU THAM KHẢO

Tài liệu tiếng Việt :

1. Phan Huy Điển, Hà Duy Khoái (2003), Mã hoá thông tin cơ sở toán học và ứng dụng, Nhà xuất bản Đại học Quốc gia Hà Nội.

2. Phan Đình Diệu (2002), Lý thuyết mật mã và an toàn thông tin, Đại học Quốc gia Hà Nội.

3. Trịnh Nhật Tiến (2004), Một số vấn đề an toàn dữ liệu, Hà Nội.

Tài liệu tiếng Anh :

4. Adam, C. (1999), Understanding Public Key Infrastructures, New Riders Publishing, Indianapolis.

5. NIST PKI Project Team (2001), 'Certificate Issuing and Management Components Protection Profile'.

Một số trang wed :

http://en.wikipedia.org/wiki

http://www.cryptography.com/

http://www.cryptography.org/

http://www.ietf.org/ids.by.wg/pkix.html

http://www.openca.org

LỜI CẢM ƠN

Lời đầu tiên, em xin chân thành cảm ơn Tiến Sỹ Hồ Văn Canh, người thầy đã cho em những định hướng, những ý kiến quý báu về công nghệ PKI.

Em xin tỏ lòng biết ơn sâu sắc tới thầy cô, bạn bè cùng khoá đã dìu dắt, giúp đỡ em tiến bộ trong suốt 4 năm học, những người luôn khuyến khích và giúp đỡ em trong mọi hoàn cảnh khó khăn.

Được hoàn thành trong thời gian ngắn khoá luận này chắc chắn còn nhiều khiếm khuyết. Em xin cảm ơn thầy cô, bạn bè và người thân đã và sẽ có những góp ý chân tình cho nội dung của khoá luận này, để em có thể tiếp tục đi sâu tìm hiểu và đưa PKI vào ứng dụng trong thực tế.

Em xin chân thành cảm ơn!

Hải Phòng, tháng năm 2010

Sinh viên

Nguyễn Văn Cương

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

ARLs:	Authority Revocation Lists
CA:	Certificate Authority
COST:	Commercial of the Shelf
CRLs:	Certificate Revocation Lists
DES:	Data Encryption Standard
CSP :	Certification Service Provider
DSS :	Digital Signature Standard
DAP :	Directory Access Protocol
LDAP :	Lightweight Directory Access Protocol
PGP:	Pretty Good Privacy
PKCS:	Public Key Cryptography Standard
PKI:	Public Key Infrastructure: Cơ sở hạ tầng mật mã công khai.
PKC:	Public Key Certificate
RSA:	Rivest Shamir Adleman
RA:	Registration Authorities
SSL:	Secure Socket Layer
TLS:	Transport Layer Security
VPN:	Virtual Private Network
WWW:	World Wide Web

DANH MỤC HÌNH VẼ