VÕ ĐĂNG PHI LONG

HỆ THỐNG THÔNG TIN

2020 – 2022

HÀ NỘI – NĂM 2022

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

VÕ ĐĂNG PHI LONG

NGHIÊN CỨU VÀ TRIỂN KHAI HỆ THỐNG HẠ TẦNG KHÓA CÔNG KHAI SỬ DỤNG BỘ PHẦN MỀM MÃ NGUỒN MỞ EJBCA

LUẬN VĂN THẠC SĨ KỸ THUẬT

(*Theo định hướng ứng dụng*)

HÀ NỘI - NĂM 2022

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

VÕ ĐĂNG PHI LONG

NGHIÊN CỨU VÀ TRIỂN KHAI HỆ THỐNG HẠ TẦNG KHÓA CÔNG KHAI SỬ DỤNG BỘ PHẦN MỀM MÃ NGUỒN MỞ EJBCA

Chuyên ngành: HỆ THỐNG THÔNG TIN
Mã số: 8.48.01.04

LUẬN VĂN THẠC SĨ KỸ THUẬT
(*Theo định hướng ứng dụng*)

NGƯỜI HƯỚNG DẪN KHOA HỌC : PGS. TSKH. HOÀNG ĐĂNG HẢI

HÀ NỘI - NĂM 2022

LỜI CAM ĐOAN

Tôi tên là Võ Đăng Phi Long, cam đoan: Luận văn Thạc sĩ Kỹ thuật "Nghiên cứu và triển khai hệ thống hạ tầng khóa công khai sử dụng bộ phần mềm mã nguồn mở EJBCA" đây là công trình nghiên cứu của tác giả dưới sự hướng dẫn của PGS. TSKH. Hoàng Đăng Hải. Các kết quả nghiên cứu trong luận văn là trung thực, không sao chép bất kỳ từ một nguồn nào và dưới bất kỳ hình thức nào. Các nguồn tài liệu tham khảo đã được trích dẫn và ghi nguồn đúng quy định.

Tác giả của luận văn

Võ Đăng Phi Long

LỜI CẢM ƠN

Với lòng biết ơn sâu sắc, tôi xin gửi lời cảm ơn chân thành tới những người đã giúp đỡ tôi trong quá trình học tập, nghiên cứu khoa học.

Tôi xin chân thành cảm ơn:

Đầu tiên tôi xin cảm ơn thầy PGS. TSKH. Hoàng Đăng Hải đã tận tình hướng dẫn truyền đạt những kinh nghiệm quý báu và giúp đỡ từ những ngày bắt đầu hướng dẫn đến ngày bảo vệ.

Tiếp theo, tôi xin cảm ơn các thầy cô trong Học viện Công nghệ Bưu chính Viễn thông đã truyền đạt những kiến thức quý báu và nhiệt tình dạy dỗ tôi trong quá trình học tập tại Học viện.

Tôi xin trân trọng cảm ơn đơn vị nơi tôi công tác và làm việc đã tạo mọi điều kiện thuận lợi cho tôi trong suốt quá trình học cao học.

Cuối cùng, tôi xin cảm ơn gia đình, đồng nghiệp, bạn bè đã luôn đồng hành, cổ vũ và giúp đỡ bản thân tôi hoàn thành luận văn này.

MỤC LỤC

MỤC LỤC 1

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT 4

DANH MỤC HÌNH ẢNH 5

MỞ ĐẦU 1

1. Lý do chọn đề tài 1

2. Mục đích nghiên cứu 2

3. Đối tượng và phạm vi nghiên cứu 2

4. Phương pháp nghiên cứu 2

5. Kết quả đã đạt được của luận văn 3

6. Cấu trúc của luận văn 3

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN TRONG HỆ THỐNG THÔNG TIN 4

1.1. Khái quát các vấn đề an toàn chung của hệ thống thông tin 4

1.2. Các mối hiểm họa về an toàn thông tin 7

1.3. Tạo lập môi trường an ninh 13

1.3.1. Nhận thực 13

1.3.2. Toàn vẹn số liệu 14

1.3.3. Bảo mật 14

1.3.4. Trao quyền 14

1.3.5. Cấm từ chối 15

1.4. Các kỹ thuật đảm bảo tính bảo mật, toàn vẹn, xác thực: 15

1.4.1. Mã hóa công khai 15

1.4.2. Chứng chỉ số 15

1.4.3. Mã hóa 16

1.4.4. Chữ ký số 16

1.4.5. Giao thức HTTPS 16

1.4.6. Phương pháp quản lý khóa công khai và khóa bí mật 16

1.5. Các công nghệ an ninh 16
1.5.1. Công nghệ mật mã 16
1.5.2. Các giải thuật đối xứng 17
1.5.3. Các giải thuật bất đối xứng 19
1.5.4. Nhận thực 20
1.5.5. Các chữ ký điện tử và tóm tắt bản tin 21
1.5.6. Các chứng chỉ số 23

1.6. Kết chương 24

CHƯƠNG 2: CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI PKI 25

2.1. Tổng quan về hạ tầng khóa công khai PKI 25

2.2. Kiến trúc và chức năng của PKI 28
2.2.1. Mô hình phân cấp 30
2.2.2. Mô hình mạng lưới 31
2.2.3. Mô hình danh sách tin cậy 32

2.3. Ưu điểm và nhược điểm của PKI 32

2.4. Một số phần mềm cung cấp hạ tầng khóa công khai 35
2.4.1. OpenSSL 35
2.4.2. EJBCA 35
2.4.3. Dogtag Certificate System 36
2.4.5. OpenXPKI 37
2.4.6. Step-ca 37
2.4.7. OpenCA 37

2.5. So sánh đặc điểm giữa OpenCA và EJBCA 38

2.6. Kết chương 39

CHƯƠNG 3: HỆ THỐNG CHỨNG THỰC SỐ PKI SỬ DỤNG BỘ PHẦN MỀM MÃ NGUỒN MỞ EJBCA 40

3.1. Giới thiệu về bộ phần mềm mã nguồn mở EJBCA 40

3.2. Kiến trúc của hệ thống PKI sử dụng EJBCA 41
3.2.1. Standalone CA/RA/VA 42
3.2.2. CA với các RA và/hoặc VA phân tán 43
3.2.3. Standalone VA 44
3.2.4. PKI lai với Public Cloud 45

3.3. Các khía cạnh khác cần lưu ý khi thiết kế hệ thống PKI 45
3.3.1. Quản lý khóa 45
3.3.2. Phân phối chứng chỉ 46

3.3.3. Tính phân cụm và sẵn sàng cao 46

3.4. Mô hình triển khai 48

3.5. Cấu hình và sử dụng 48

3.6. Kịch bản ứng dụng vào thực tiễn 51

3.7. Kết chương 54

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN TIẾP 56

TÀI LIỆU THAM KHẢO 58

PHỤ LỤC 61

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
PKI	Public Key Infrastructure	Hạ tầng khóa công khai
CA	Certificate Authority	Chứng thư số
RA	Registration Authority	Cơ quan đăng ký số
VA	Validation Authority	Cơ quan xác thực số
IETF	Internet Engineering Task Force	Lực lượng kỹ thuật internet đặc biệt
HSM	Hardware Security Module	Mô đun bảo mật phần cứng
REST	REpresentational State Transfer	Trạng thái chuyển đổi đại diện
MD	Message Digest	Hàm băm mã hóa

DANH MỤC HÌNH ẢNH

Hình 1.1 Mô hình Gordon-Loeb 10
Hình 1.2 Luồng số liệu của mật mã hóa đối xứng 18
Hình 1.3 Quá trình digest 22
Hình 2.1 Kiến trúc PKI 29
Hình 2.2 Mô hình phân cấp 30
Hình 2.3 Mô hình mạng lưới 31
Hình 2.4 Mô hình danh sách tin cậy 32
Hình 3.1 Cấu trúc hệ thống EJBCA 40
Hình 3.2 Standalone CA/RA/VA 42
Hình 3.3 CA được đặt phía sau tường lửa 43
Hình 3.4 CA với các RA và/hoặc VA phân tán 44
Hình 3.5 Standalone VA 44
Hình 3.6 PKI lai với Public Cloud 45
Hình 3.7 Khóa được lưu trong module bảo mật 45
Hình 3.8 Phân phối chứng chỉ 46
Hình 3.9 Các CA phân cụm 47
Hình 3.10 Cài đặt thành công EJBCA 48
Hình 3.11 Import chứng thư vào trình duyệt 49
Hình 3.12 Giao diện của EJBCA 49
Hình 3.13 Giao diện quản trị của EJBCA 50
Hình 3.14 Giao diện đăng ký chứng thư 51
Hình 3.15 Xác nhận và tải chứng thư về 51
Hình 3.16 Email sau khi được thêm chứng thư có nhãn dán đặc biệt 52
Hình 3.17 Thông tin về chứng thư đã ký vào email 53
Hình 3.18 Thông tin chi tiết hơn về chứng thư 53

MỞ ĐẦU

1. Lý do chọn đề tài

Trong thời đại công nghệ đang ngày càng phát triển, việc bảo vệ thông tin là vô cùng quan trọng, quyết định tương lai của bất kỳ một cá nhân hay tổ chức nào. Khi thông tin truyền đi trên mạng, nó sẽ bị đe dọa bởi các kẻ tấn công, họ có thể xem trộm, chỉnh sửa thông tin hay thậm chí giả mạo người nhận. Từ đó, thông tin truyền trên mạng luôn phải đáp ứng được ba yếu tố: xác thực, bí mật, toàn vẹn.

Các tác vụ trong thương mại điện tử như giao dịch điện tử, trao đổi thông tin, dịch vụ web... đã trở thành một phần tất yếu trong thời đại 4.0, nơi mà nền tảng kỹ thuật số đóng một vai trò cực kỳ quan trọng và có sức ảnh hưởng mạnh mẽ tới tất cả các khía cạnh trong cuộc sống. Việc giao dịch qua mạng internet này đặt ra vấn đề cũng chính là thách thức đối với các công ty cũng như tổ chức là phải đảm bảo được ba yếu tố xác thực, bí mật, toàn vẹn cho các giao dịch đó. Hiện nay, trên thế giới đã và đang có rất nhiều phương pháp để đảm bảo tính xác thực danh tính, đảm bảo tính bí mật thông tin, đảm bảo thông tin không bị thay đổi cũng như cung cấp bằng chứng chống việc chối bỏ một hành động đã thực hiện hay đã diễn ra trong giao dịch điện tử. Điển hình trong đó là sử dụng tài khoản cá nhân, chứng chỉ số sử dụng PKI, các thiết bị bảo mật vật lý như smart card, etoken...

Đứng trước các thách thức đã và đang xảy ra trong thực tiễn, các công ty bảo mật đã phối hợp cùng các công ty, tổ chức để nghiên cứu và phát triển ra các phương pháp cũng như sản phẩm nhằm bảo vệ yếu tố xác thực có liên quan tới các hoạt động trong giao dịch trực tuyến. Điển hình trong đó là phần mềm CA của Microsoft, OpenVPN, OpenCA hay IdentityGuard của Entrust và một trong số đó là phần mềm EJBCA của PrimeKey.

Chính vì những lý do trên, tôi đã chọn giải pháp sử dụng bộ phần mềm mã nguồn mở EJBCA trên nền tảng hệ điều hành CentOS 8. Việc nghiên cứu đề tài về "**Nghiên cứu và triển khai hệ thống hạ tầng khóa công khai sử dụng bộ phần mềm mã nguồn mở EJBCA**" là cực kỳ cấp thiết, đáp ứng được nhu cầu thực tiễn

trong công cuộc chuyển đổi số đang được áp dụng trên toàn quốc, đóng góp một phần vào sự phát triển của hệ thống công nghệ thông tin.

2. Mục đích nghiên cứu

Mục đích nghiên cứu: Mục tiêu của luận văn là xây dựng, thử nghiệm và đánh giá hệ thống cấp chứng thư số trên máy chủ cài đặt phần mềm mã nguồn mở EJBCA.

3. Đối tượng và phạm vi nghiên cứu

*** Đối tượng:** Luận văn nghiên cứu về hệ thống cung cấp hạ tầng khóa công khai PKI sử dụng phần mềm mã nguồn mở EJBCA nhằm đảm bảo được tính xác thực, toàn vẹn và bảo mật của hệ thống.

*** Phạm vi nghiên cứu:**

- Hệ thống cơ sở hạ tầng khóa công khai PKI.

- Hệ thống phần mềm EJBCA.

- Xây dựng và thử nghiệm mô hình truyền nhận được chứng thực bằng chứng thư số sinh ra bằng hệ thống EJBCA.

4. Phương pháp nghiên cứu

* Phương pháp nghiên cứu lý thuyết: Nghiên cứu tổng quan về hệ thống an toàn thông tin và các thuật toán cơ bản, nghiên cứu tổng quan về hạ tầng khóa công khai PKI, qua đó tìm hiểu một số vấn đề chính, như:

- Lý thuyết liên quan vấn đề nghiên cứu.
- Tìm hiểu về một số thuật toán mã hóa cơ bản.
- Cơ sở hạ tầng khóa công khai PKI.

* Phương pháp nghiên cứu thực nghiệm:

- Xây dựng môi trường thử nghiệm hệ thống.
- Cài đặt, cấu hình các thành phần.
- Thực nghiệm và đánh giá kết quả.

5. Kết quả đã đạt được của luận văn

- Phân tích yêu cầu chứng thực số đang ngày càng trở nên cấp thiết trong thực tiễn.
- Giải pháp áp dụng chứng thực số vào truyền nhận mail sử dụng bộ phần mềm EJBCA.
- Kết quả thực nghiệm.

6. Cấu trúc của luận văn

Ngoài phần mở đầu, kết luận, danh mục tài liệu tham khảo và phụ lục, luận văn gồm 03 chương như sau:

- Chương 1 trình bày tổng quan về an toàn trong hệ thống thông tin.
- Chương 2 trình bày về cơ sở hạ tầng khóa công khai PKI.
- Chương 3 trình bày kết quả thực nghiệm và đánh giá.

Chương 1: TỔNG QUAN VỀ AN TOÀN TRONG HỆ THỐNG THÔNG TIN

1.1. Khái quát các vấn đề an toàn chung của hệ thống thông tin

An toàn thông tin là hoạt động bảo vệ thông tin bằng cách giảm thiểu rủi ro thông tin. Đó là một phần của việc quản lý rủi ro thông tin. Điều này đồng nghĩa với việc ngăn chặn hoặc giảm khả năng truy cập trái phép dữ liệu hoặc truy cập dữ liệu không phù hợp hay việc sử dụng, tiết lộ, làm gián đoạn, xóa, làm thâm hụt, sửa đổi, kiểm tra, lưu lại hoặc làm giảm giá trị thông tin một cách bất hợp pháp. Nó cũng bao gồm các hành động nhằm làm giảm tác động bất lợi từ những sự cố như vậy. Thông tin được bảo vệ có thể ở bất kỳ dạng nào, ví dụ như ở dạng điện tử (trên lưu trữ đám mây), vật lý (trên thiết bị lưu trữ như usb, ổ cứng, trên giấy...) hoặc những thông tin vô hình như kiến thức. Trọng tâm chính của an toàn thông tin là bảo vệ cân bằng ba tính chất: tính bảo mật (confidentiality), tính toàn vẹn (intergrity) và tính sẵn sàng (availability) của dữ liệu trong khi vẫn duy trì được sự tập trung vào việc triển khai chính sách hiệu quả mà không cản trở năng suất của tổ chức. Điều này phần lớn đạt được thông qua quy trình quản lý rủi ro có cấu trúc bao gồm:

- Xác định thông tin và các tài sản liên quan cộng với các mối đe dọa, lỗ hổng và tác động tiềm ẩn.
- Đánh giá rủi ro.
- Quyết định cách xử lý và giải quyết rủi ro: điều này có nghĩa là tránh, giảm thiểu, chia sẻ hoặc chấp nhận các rủi ro này.
- Lựa chọn hoặc thiết kế các biện pháp kiểm soát an ninh, an toàn phù hợp và triển khai chúng ở những nơi cần giảm thiểu rủi ro.
- Giám sát các hoạt động, thực hiện các điều chỉnh cần thiết để giải quyết mọi vấn đề, mọi thay đổi và áp dụng các nâng cấp phù hợp.

Để chuẩn hóa nguyên tắc này, các học giả và chuyên gia đã hợp tác để đưa ra hướng dẫn, chính sách và tiêu chuẩn ngành về mật khẩu, phần mềm chống virus, tường lửa, phần mềm mã hóa, trách nhiệm pháp lý, nhận thức và đào tạo về bảo mật... Quá trình tiêu chuẩn hóa này có thể được thúc đẩy hơn nữa bởi nhiều luật và quy định

ảnh hưởng đến cách dữ liệu được truy cập, xử lý, lưu trữ, truyền và hủy. Tuy nhiên, việc thực hiện bất kỳ tiêu chuẩn và hướng dẫn nào trong một tổ chức có thể có tác dụng hạn chế nếu văn hóa cải tiến liên tục không được áp dụng trong tổ chức đó.

Các định nghĩa khác nhau về bảo mật thông tin được nhắc tới sau đây đã được tóm tắt từ nhiều nguồn khác nhau:

- "Duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin. Lưu ý: Ngoài ra, các thuộc tính khác, chẳng hạn như tính xác thực, trách nhiệm giải trình, tính không thoái thác và độ tin cậy cũng có thể liên quan." (ISO/IEC 27000:2009)[1]
- "Việc bảo vệ thông tin và hệ thống thông tin khỏi sự truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hủy trái phép nhằm cung cấp tính bảo mật, tính toàn vẹn và tính sẵn sàng." (CNSS, 2010)[2]
- "Đảm bảo rằng chỉ những người dùng được ủy quyền (bảo mật) mới có quyền truy cập vào thông tin chính xác và đầy đủ (tính toàn vẹn) khi được yêu cầu (tính khả dụng)." (ISACA, 2008)[3]
- "An ninh thông tin là quá trình bảo vệ tài sản trí tuệ của một tổ chức." (Pipkin, 2000)[16]
- "...bảo mật thông tin là một nguyên tắc quản lý rủi ro, có nhiệm vụ quản lý chi phí rủi ro thông tin cho doanh nghiệp." (McDermott và Geer, 2001)[4]
- "Một cảm giác đảm bảo đầy đủ thông tin rằng các rủi ro thông tin và các biện pháp kiểm soát được cân bằng." (Anderson, J., 2003)[5]
- “An toàn thông tin là bảo vệ thông tin và giảm thiểu nguy cơ lộ thông tin cho các bên trái phép.” (Venter và Eloff, 2003)[6]
- "An ninh thông tin là một lĩnh vực nghiên cứu đa ngành và hoạt động chuyên môn liên quan đến việc phát triển và triển khai các cơ chế bảo mật thuộc mọi loại hiện có (kỹ thuật, tổ chức, định hướng con người và pháp lý) để giữ thông tin ở tất cả các vị trí của nó (trong và ngoài bên ngoài phạm vi của tổ chức) và do đó, hệ thống thông tin, nơi thông tin được tạo, xử lý, lưu trữ, truyền và hủy, không có các mối đe dọa.[7] Các mối đe dọa đối với thông tin và hệ thống thông tin có thể được phân loại và mục tiêu bảo mật tương ứng có thể được xác định cho từng loại mối đe dọa.[8] Một tập hợp các mục tiêu bảo mật, được xác định là kết quả của quá trình phân tích

mối đe dọa, nên được sửa đổi định kỳ để đảm bảo tính đầy đủ và phù hợp với môi trường đang phát triển.[9] Tập hợp các mục tiêu bảo mật liên quan hiện tại có thể bao gồm : tính bảo mật, tính toàn vẹn, tính sẵn sàng, quyền riêng tư, tính xác thực và độ tin cậy, tính chống thoái thác, trách nhiệm giải trình và khả năng kiểm toán." (Chardantseva và Hilton, 2013)[10]

- Bảo mật thông tin và tài nguyên thông tin sử dụng hệ thống hoặc thiết bị viễn thông có nghĩa là bảo vệ thông tin, hệ thống thông tin hoặc sách khỏi bị truy cập trái phép, hư hỏng, trộm cắp hoặc phá hủy (Kurose và Ross, 2010).[11]

Cốt lõi của bảo mật thông tin là đảm bảo sự an toàn của thông tin, hành động duy trì tính bảo mật, tính toàn vẹn và tính sẵn sàng (CIA) của thông tin, đảm bảo rằng thông tin không bị xâm phạm theo bất kỳ cách nào khi phát sinh các vấn đề quan trọng. Nó bao gồm những vấn đề không lường trước được như thiên tai, trục trặc máy tính/máy chủ và trộm cắp tài sản vật chất. Mặc dù các hoạt động kinh doanh dựa trên giấy tờ vẫn còn phổ biến, đòi hỏi phải có bộ thực hành bảo mật thông tin riêng, nhưng các sáng kiến kỹ thuật số của doanh nghiệp đang ngày càng được chú trọng, cùng với việc đảm bảo an toàn thông tin hiện nay thường được xử lý bởi các chuyên gia bảo mật công nghệ thông tin (CNTT). Các chuyên gia này áp dụng bảo mật thông tin cho công nghệ (thường là một số dạng hệ thống máy tính). Cần lưu ý rằng máy tính không nhất thiết phải là máy tính để bàn tại nhà. Máy tính là bất kỳ thiết bị nào có bộ vi xử lý và có bộ nhớ. Các thiết bị như vậy có thể bao gồm từ các thiết bị độc lập không nối mạng đơn giản như máy tính bỏ túi, các thiết bị quan trắc môi trường, camera... cho tới các thiết bị điện toán di động nối mạng như smart phone, đồng hồ thông minh hay máy tính bảng. Các chuyên gia bảo mật CNTT hầu như luôn được tìm thấy trong bất kỳ doanh nghiệp/cơ sở lớn nào do tính chất và giá trị khổng lồ của dữ liệu trong các doanh nghiệp lớn đó. Họ chịu trách nhiệm giữ an toàn cho tất cả công nghệ trong công ty khỏi các cuộc tấn công mạng độc hại thường cố gắng lấy thông tin mật quan trọng hoặc giành quyền kiểm soát các hệ thống nội bộ.

Lĩnh vực bảo mật thông tin đã lột xác và phát triển đáng kể trong những năm gần đây. Nó cung cấp nhiều lĩnh vực chuyên môn hóa, bao gồm bảo mật mạng và cơ sở hạ tầng đồng minh, bảo mật ứng dụng và cơ sở dữ liệu, kiểm tra bảo mật, kiểm

toán hệ thống thông tin, lập kế hoạch kinh doanh liên tục, khám phá hồ sơ điện tử và pháp y kỹ thuật số. Các chuyên gia bảo mật thông tin tỏ ra rất ổn định trong công việc của họ. Tính đến năm 2013, hơn tám mươi phần trăm chuyên gia không thay đổi chủ lao động hoặc việc làm trong khoảng thời gian một năm và số lượng chuyên gia đã liên tục tăng lên hơn mười phần trăm mỗi năm.

1.2. Các mối hiểm họa về an toàn thông tin

Các mối đe dọa an toàn thông tin có nhiều dạng khác nhau. Một số mối đe dọa phổ biến nhất hiện nay là tấn công phần mềm, trộm cắp tài sản trí tuệ, trộm danh tính, trộm thiết bị hoặc thông tin, phá hoại và tống tiền dựa trên thông tin thu thập được. Virus, worms, tấn công lừa đảo (phising attacks) và Trojan là một số ví dụ phổ biến về tấn công phần mềm. Trộm cắp tài sản trí tuệ cũng là một vấn đề nhức nhối đối với nhiều doanh nghiệp trong lĩnh vực công nghệ thông tin (CNTT). Trộm cắp danh tính là nỗ lực đóng vai người khác thường để lấy thông tin cá nhân của người đó hoặc lợi dụng quyền truy cập của họ vào thông tin quan trọng thông qua kỹ thuật xã hội. Ngày nay, hành vi trộm cắp thiết bị hoặc thông tin đang trở nên phổ biến hơn do hầu hết các thiết bị ngày nay đều là thiết bị di động, dễ bị đánh cắp và cũng trở nên đáng mong đợi hơn nhiều khi dung lượng dữ liệu tăng lên. Phá hoại thường bao gồm việc phá hủy trang web của một tổ chức nhằm cố gắng gây mất lòng tin đối với khách hàng của tổ chức đó. Tống tiền thông tin bao gồm hành vi trộm cắp tài sản hoặc thông tin của công ty nhằm cố gắng nhận khoản thanh toán để đổi lấy việc trả lại thông tin hoặc tài sản cho chủ sở hữu của nó, như với ransomware. Có nhiều cách giúp bảo vệ bạn khỏi một số cuộc tấn công này nhưng một trong những biện pháp phòng ngừa thiết thực nhất là tiến hành nâng cao nhận thức người dùng định kỳ. Mối đe dọa số một đối với bất kỳ tổ chức nào là người dùng hoặc nhân viên trong nội bộ tổ chức, chúng còn được gọi là mối đe dọa nội bộ.

Các mối đe dọa an ninh, an toàn thông tin có thể được phân theo loại và nguồn gốc của chúng:

- Các loại mối đe dọa:
  - Các tác nhân vật lý: lửa, nước, ô nhiễm.

  - Các sự kiện tự nhiên: khí hậu, địa chấn, núi lửa.
  - Mất các dịch vụ thiết yếu: điện, điều hòa không khí, viễn thông.
  - Xâm phạm thông tin: nghe lén, đánh cắp phương tiện, thu thập vật liệu đã loại bỏ.
  - Lỗi kỹ thuật: thiết bị, phần mềm, bão hòa công suất.
  - Lỗi chức năng: lỗi trong quá trình sử dụng, lạm dụng quyền, từ chối hành động.

  Cần lưu ý rằng một loại mối đe dọa có thể có nhiều nguồn gốc.

- Cố ý: nhằm vào tài sản thông tin
  - Do thám.
  - Xử lý dữ liệu bất hợp pháp.
- Tai nạn:
  - Lỗi thiết bị.
  - Lỗi phần mềm.
- Thuộc về môi trường:
  - Sự kiện tự nhiên.
  - Mất nguồn điện.
- Sơ suất: Các yếu tố đã biết nhưng bị bỏ qua, ảnh hưởng đến sự an toàn và bền vững của hệ thống.

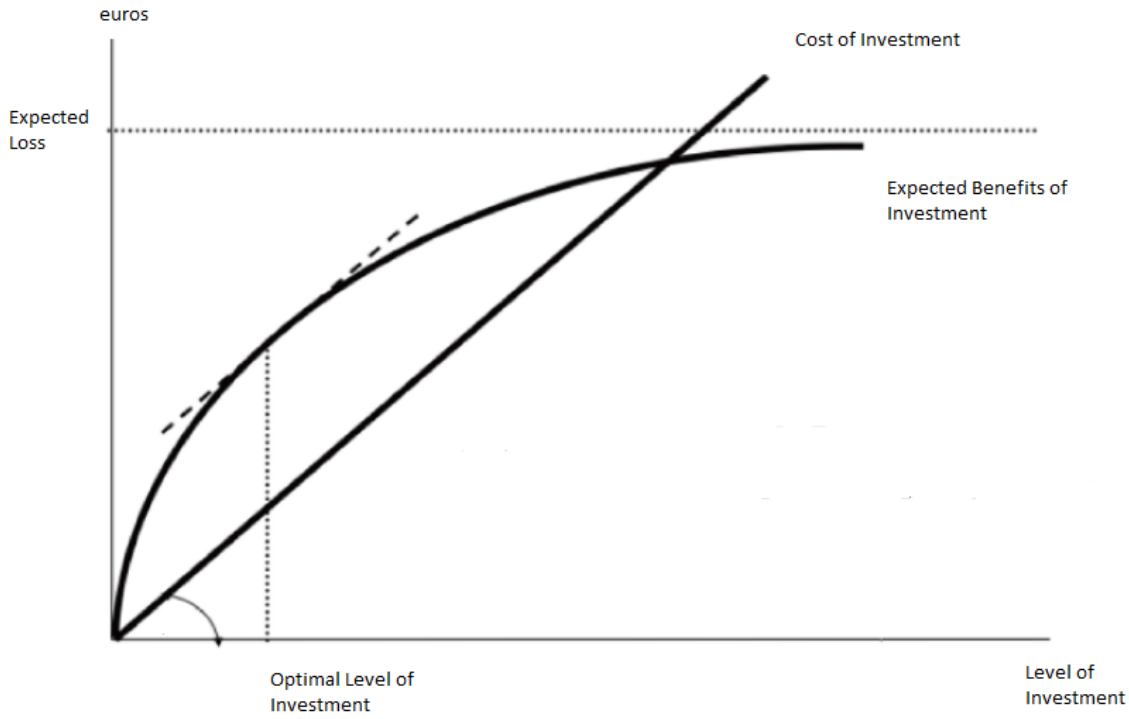
Ngoài cách phân loại trên thì Microsoft cũng đã công bố phương pháp phân loại của riêng mình theo sáu thể loại như sau:

- Spoofing identity: là một loại lừa đảo mà kẻ tấn công lấy cắp thông tin như tài khoản và mật khẩu của một doanh nghiệp hợp pháp, cá nhân, hay tổ chức nào đó và truy cập trái phép vào nó.
- Tampering with data: Giả mạo dữ liệu liên quan đến việc sửa đổi dữ liệu trái phép. Ví dụ bao gồm các thay đổi trái phép được thực hiện đối với dữ liệu liên tục, chẳng hạn như dữ liệu được giữ trong cơ sở dữ liệu và thay đổi dữ liệu khi dữ liệu truyền giữa hai máy tính qua mạng mở, chẳng hạn như Internet.

- Repudiation: Các mối đe dọa từ chối có liên quan đến những người dùng từ chối thực hiện một hành động mà các bên khác không có bất kỳ cách nào để chứng minh ngược lại, ví dụ: một người dùng thực hiện một hoạt động bất hợp pháp trong một hệ thống thiếu khả năng theo dõi các hoạt động bị cấm. Chống chối bỏ đề cập đến khả năng của một hệ thống chống lại các mối đe dọa từ chối. Ví dụ: người dùng mua một mặt hàng có thể phải ký nhận mặt hàng đó khi nhận. Sau đó, nhà cung cấp có thể sử dụng biên nhận đã ký làm bằng chứng cho thấy người dùng đã nhận được gói hàng.
- Information disclosure: các mối đe dọa tiết lộ thông tin liên quan đến việc tiết lộ thông tin cho những cá nhân không được phép truy cập thông tin đó, ví dụ: khả năng người dùng đọc một tệp mà họ không được cấp quyền truy cập hoặc khả năng kẻ xâm nhập đọc dữ liệu trong khi truyền giữa hai máy tính.
- Denial of service (DoS): Tấn công từ chối dịch vụ từ chối truy cập đối với người dùng hợp lệ, ví dụ: bằng cách làm cho máy chủ Web tạm thời không khả dụng hoặc không sử dụng được. Bạn phải bảo vệ chống lại một số loại mối đe dọa DoS chỉ để cải thiện tính khả dụng và độ tin cậy của hệ thống.
- Elevation of privilege: Với mối đe dọa này, người dùng không có đặc quyền chiếm được quyền truy cập đặc quyền và do đó có đủ quyền truy cập để gây hại hoặc phá hủy toàn bộ hệ thống. Sự gia tăng các mối đe dọa chiếm quyền bao gồm những tình huống trong đó kẻ tấn công đã xâm nhập hiệu quả qua tất cả các biện pháp phòng thủ của hệ thống và trở thành một phần của chính hệ thống được tin cậy, một tình huống thực sự nguy hiểm.

Các chính phủ, quân đội, tập đoàn, tổ chức tài chính, bệnh viện, tổ chức phi lợi nhuận và doanh nghiệp tư nhân tích lũy rất nhiều thông tin bí mật về nhân viên, khách hàng, sản phẩm, nghiên cứu và tình trạng tài chính của họ. Nếu thông tin bí mật về khách hàng hoặc tài chính hoặc dòng sản phẩm mới của doanh nghiệp rơi vào tay đối thủ cạnh tranh hoặc tin tặc mũ đen, doanh nghiệp và khách hàng của họ có thể bị tổn thất tài chính trên diện rộng, không thể khắc phục được, cũng như tổn hại đến danh tiếng của công ty. Từ góc độ kinh doanh, bảo mật thông tin phải được cân bằng

với chi phí. Mô hình Gordon-Loeb cung cấp một cách tiếp cận kinh tế toán học để giải quyết vấn đề này.



Hình 1.1 Mô hình Gordon-Loeb

Mô hình Gordon–Loeb là một mô hình kinh tế toán học phân tích mức đầu tư tối ưu cho bảo mật thông tin.

Đầu tư để bảo vệ dữ liệu của công ty liên quan đến chi phí, không giống như các khoản đầu tư khác, khoản đầu tư này không tạo ra lợi nhuận. Tuy nhiên, nó phục vụ mục đích ngăn chặn các chi phí phát sinh do rủi ro. Do đó, điều quan trọng là phải so sánh mức độ tốn kém của việc bảo vệ một tập hợp dữ liệu cụ thể với khả năng mất mát trong trường hợp dữ liệu nói trên bị đánh cắp, thất lạc, lỗi một phần hoặc hư hỏng toàn bộ. Để soạn thảo mô hình này, công ty phải có kiến thức về ba tham số sau đây:

- Dữ liệu đáng giá bao nhiêu.
- Mức độ rủi ro của dữ liệu.
- Xác suất một cuộc tấn công vào lỗ hổng hoặc dữ liệu sẽ thành công.

Ba tham số này được nhân với nhau để đưa ra mức thiệt hại trung bình khi một cuộc tấn công vào công ty/tổ chức xảy ra mà không được đầu tư vào việc bảo vệ an toàn thông tin.

Ví dụ: Một công ty có tệp dữ liệu trị giá 1 tỷ đồng, mức độ rủi ro bị tấn công là 20%, xác suất tấn công thành công là 70% thì thiệt hại tiềm tàng của công ty là:

1.000.000.000 x 0,2 x 0,7 = 140.000.000 (đồng)

Vì vậy, theo mô hình Gordon và Loeb thì chi phí đầu tư vào bảo mật thông tin không nên vượt quá: 140.000.000 x 0,37 = 51.800.000 (đồng)

Từ mô hình, chúng ta có thể thu thập được rằng số tiền mà một công ty chi để bảo vệ thông tin, trong hầu hết các trường hợp, chỉ là một phần nhỏ so với tổn thất dự đoán (ví dụ: giá trị tổn thất dự kiến sau khi an ninh thông tin bị vi phạm). Cụ thể, mô hình cho thấy việc đầu tư vào bảo mật thông tin (bao gồm các hoạt động liên quan đến an ninh mạng hoặc bảo mật máy tính) với số tiền cao hơn 37% tổn thất dự đoán là không phù hợp. Mô hình Gordon–Loeb cũng chỉ ra rằng, đối với một mức độ tổn thất tiềm năng cụ thể, lượng tài nguyên cần đầu tư để bảo vệ một tập hợp thông tin không phải lúc nào cũng tăng cùng với sự gia tăng tính dễ bị tổn thương của tập hợp đó. Do đó, các công ty có thể thu được lợi nhuận kinh tế lớn hơn bằng cách đầu tư vào các hoạt động an ninh mạng/an toàn thông tin nhằm tăng tính bảo mật của các tập dữ liệu có mức độ dễ bị tổn thương trung bình. Nói cách khác, khoản đầu tư vào việc bảo vệ dữ liệu của công ty làm giảm khả năng bị tổn thương với lợi nhuận gia tăng giảm dần.

Đối với cá nhân, bảo mật thông tin có ảnh hưởng đáng kể đến quyền riêng tư, điều này được nhìn nhận rất khác nhau ở các nền văn hóa khác nhau.

Muốn đưa ra các giải pháp an ninh, trước hết ta cần nhận biết các đe dọa tiềm ẩn có nguy hại đến an ninh của hệ thống thông tin. Sau đây là các đe dọa an ninh:

– Đóng giả: Là ý định của kẻ truy cập trái phép vào một ứng dụng hoặc một hệ thống bằng cách đóng giả người khác. Nếu kẻ đóng giả truy nhập thành công, họ có thể tạo ra các câu trả lời giả đối với các bản tin để đạt được hiểu biết sâu hơn và truy

cập vào các bộ phận khác của hệ thống. Đóng giả là vấn đề chính đối với an ninh Internet và vô tuyến Internet, kẻ đóng giả có thể làm cho người sử dụng tin rằng mình đang liên lạc với một nguồn tin cậy. Điều này vô cùng nguy hiểm, vì thế người sử dụng này có thể cung cấp thông tin bổ sung có lợi cho kẻ tấn công để chúng có thể truy nhập thành công các bộ phận khác của hệ thống.

– Giám sát: Mục đích của giám sát là theo dõi, giám sát dòng số liệu trên mạng. Trong khi giám sát có thể được sử dụng cho các mục đích đúng đắn, thì nó lại thường được sử dụng để sao chép trái phép dữ liệu mạng. Thực chất giám sát là nghe trộm điện tử, bằng cách này kẻ không được phép truy nhập có thể lấy được các thông tin nhạy cảm gây hại cho người sử dụng, các ứng dụng và các hệ thống. Giám sát thường được sử dụng kết hợp với đóng giả. Giám sát rất nguy hiểm vì nó dễ thực hiện nhưng khó phát hiện. Để chống lại các công cụ giám sát tinh vi, mật mã hóa số liệu là phương pháp hữu hiệu nhất. Dù kẻ sử dụng trái phép có truy nhập thành công vào số liệu đã được mã hóa nhưng cũng không thể giải mã được số liệu này. Vì vậy, ta cần đảm bảo rằng giao thức mật mã được sử dụng hầu như không thể bị phá vỡ.

– Làm giả: Làm giả số liệu hay còn gọi là đe dọa tính toàn vẹn của dữ liệu liên quan đến việc thay đổi số liệu so với dạng ban đầu với ý đồ xấu. Quá trình này liên quan đến cả chặn truyền số liệu lẫn các số liệu được lưu trên các Server hay Client. Số liệu bị làm giả (thay đổi) sau đó được truyền đi như bản gốc. Áp dụng mật mã hóa, nhận thực và trao quyền là các cách hữu hiệu để chống lại sự làm giả số liệu.

– Đánh cắp dữ liệu: Đánh cắp thiết bị là vấn đề thường xảy ra đối với thông tin di động. Ta không chỉ mất thiết bị mà còn mất cả thông tin bí mật lưu trong đó. Điều này đặc biệt nghiêm trọng đối với các thiết bị thông minh, vì chúng thường chứa số liệu không đổi và bí mật. Bộ nhớ của các thiết bị có chứa ít nhất một số dữ liệu kinh doanh, chẳng hạn như danh sách liên lạc, mật khẩu tài khoản, mật e-mail và file đính kèm. Một nghiên cứu của Nokia trước đây cho thấy 31% nhân viên Mỹ sử dụng thiết bị kỹ thuật số hỗ trợ cá nhân PDA (Personal Digital Assistant) như điện thoại di động, máy tính bảng, laptop... và 63% sử dụng điện thoại di động cho hoạt động kinh doanh. Trong khi những thiết bị này đang ngày càng được kết nối tốt, thì phần lớn chúng lại không có sự bảo vệ cần thiết và có thể gây ra rủi ro đáng kể cho mạng lưới kinh doanh

và dữ liệu. Để có thể giảm được rủi ro đó thì công ty hay tổ chức phải bắt đầu với việc thành lập một chính sách an ninh thông tin bằng thỏa thuận rằng tất cả nhân viên đều sử dụng các thiết bị di động do công ty sở hữu. Vì thế, ta cần tuân thủ theo các quy tắc sau để đảm bảo an ninh đối với các thiết bị di động:

- Khóa thiết bị bằng Username và Password để chống lại truy cập dễ dàng.
- Yêu cầu nhận thực khi truy nhập đến các ứng dụng lưu trong thiết bị.
- Tuyệt đối không lưu mật khẩu trên thiết bị.
- Mật mã hóa tất cả các phương tiện lưu số liệu cố định.
- Áp dụng các chính sách an ninh đối với những người sử dụng thiết bị di động. Nhận thực, mật mã và các chính sách an ninh là các biện pháp để ngăn chặn việc truy nhập trái phép số liệu từ các thiết bị bị mất hoặc bị lấy cắp.

1.3. Tạo lập môi trường an ninh

Sự bảo đảm an ninh đầu cuối là sự bảo đảm cho quá trình truyền dẫn số liệu được an toàn, nguyên vẹn, không bị thay đổi trên toàn bộ đường truyền từ đầu phát đến đầu thu. Để đảm bảo được điều này, cần phải xét đến toàn bộ môi trường truyền thông, bao gồm việc truy nhập mạng, các phần tử trung gian và các ứng dụng máy khách. Có năm mục tiêu quan trọng và liên quan đến việc tạo lập môi trường an ninh sẽ được đề cấp phía dưới.

1.3.1. Nhận thực

Nhận thực là quá trình kiểm tra tính hợp lệ của các đối tượng tham gia thông tin trong bất cứ mạng nào. Quá trình này được thực hiện tại hai lớp: lớp mạng và lớp ứng dụng. Lớp mạng đòi hỏi người sử dụng phải được nhận thực, trước khi được phép truy cập. Lớp ứng dụng nhận thực quan trọng tại hai mức máy khách (Client) và máy chủ (Server). Client phải chứng tỏ với Server rằng thông tin của nó là hợp lệ để có thể được cấp phép truy cập mạng. Đồng thời, trước khi Server được client cho phép kết nối tới, máy chủ đó phải tự nhận thực với ứng dụng nằm bên phía Client để xác minh danh tính của mình. Sử dụng Username và Password là phương pháp nhận thực

đơn giản nhất và cũng là phương pháp kém an toàn nhất. Một trong số những phương pháp tiên tiến nhất hiện nay là sử dụng chứng thư số (chữ ký điện tử).

1.3.2. Toàn vẹn số liệu

Toàn vẹn số liệu là sự đảm bảo số liệu truyền thông không bị thay đổi hay phá hoại trong quá trình truyền từ nơi phát đến nơi thu. Bằng cách áp dụng một giải thuật cho bản tin, một mã nhận thực bản tin MAC (MAC: Message Authentication Codes) được gõ bởi người sử dụng của một máy tính cho các tài khoản truy cập hoặc cổng thông tin. Mã này được đính kèm vào tin nhắn hoặc yêu cầu gửi của người dùng. Nếu chúng giống nhau thì chứng tỏ bản tin gốc không bị thay đổi, nếu nó khác nhau thì phía thu sẽ loại bỏ bản tin này. MAC thường được sử dụng trong các quỹ giao dịch chuyển tiền điện tử (Electronic Funds Transfer System - EFTS) để duy trì tính toàn vẹn thông tin.

1.3.3. Bảo mật

Bảo mật chính là khía cạnh quan trọng nhất của an toàn, an ninh thông tin cho nên đây cũng là vấn đề được nhắc tới nhiều nhất. Mục đích của bảo mật nhằm bảo đảm tính riêng tư của dữ liệu số và khiến cho dữ liệu không thể đọc được bởi bất cứ ai, ngoại trừ những người có quyền truy cập. Cách phổ biến nhất được sử dụng là mật mã hóa dữ liệu. Quá trình này bao gồm mã hóa bản rõ vào dạng không đọc được đối với bất kỳ thiết bị hay phần mềm nào, ngoại trừ thiết bị hay phần mềm được cấp quyền truy cập.

1.3.4. Trao quyền

Trao quyền là quá trình quy định quyền hạn truy cập của người sử dụng, người sử dụng được quyền thực hiện một số hành động mà người quản trị trao cho. Trao quyền liên quan mật thiết với nhận thực. Hệ thống có thể quyết định người sử dụng được làm gì sau khi người sử dụng đã được hệ thống nhận thực. Danh sách điều khiển truy cập ACL (Access List) thường được sử dụng cho quá trình này, đối với một hệ thống tập tin máy tính, là một danh sách các quyền gắn liền với một đối tượng. ACL quy định cụ thể mà người dùng hay các quy trình hệ thống được cấp quyền truy cập vào các đối tượng, cũng những gì được phép hoạt động trên các đối tượng nhất định. Mỗi mục trong một ACL điển hình quy định cụ thể một chủ đề và hoạt động một. Ví dụ, một người sử dụng

chỉ được cấp quyền để truy cập một số dữ liệu nhưng lại không thể xóa, di chuyển hoặc chỉnh sửa những dữ liệu đó. Trong khi đó người quản trị hệ thống hoặc một hay nhiều cá nhân tin cậy khác có thể truy cập để chỉnh sửa, di chuyển hay xóa các tập dữ liệu đó.

1.3.5. Cấm từ chối

Cấm từ chối hay chống chối bỏ là biện pháp buộc các phía phải chịu trách nhiệm về giao dịch mà họ đã tham gia, không được phép từ chối tham gia giao dịch. Điều này có nghĩa là cả bên truyền và bên nhận đều có thể chứng minh rằng cả bên đã truyền và bên nhận gói tin đã thu được bản tin tương tự. Để quá trình này có thể diễn ra, mỗi gói tin phải được ký bằng một chữ ký số được cung cấp bởi một bên thứ ba tin cậy kiểm tra và đánh dấu thời gian.

1.4. Các kỹ thuật đảm bảo tính bảo mật, toàn vẹn, xác thực:

Muốn đưa đảm bảo tính bảo mật, toàn vẹn, xác thực thì trước hết cần phải tìm hiểu về các kỹ thuật có khả năng đem đến những tính chất này cho hệ thống.

1.4.1. Mã hóa công khai

Hệ thống PKI sử dụng mã hóa khóa công khai để đảm bảo tính bảo mật của dữ liệu trong quá trình truyền tải. Trong quá trình này, mỗi người dùng sẽ có một cặp khóa, gồm khóa công khai và khóa bí mật. Khóa công khai sẽ được chia sẻ công khai để mọi người có thể mã hóa dữ liệu gửi đến người dùng đó. Còn khóa bí mật chỉ được người dùng đó biết để giải mã dữ liệu.

1.4.2. Chứng chỉ số

Chứng chỉ số là một tài liệu số được cấp phát bởi một tổ chức CA (Certificate Authority), xác nhận danh tính của một thực thể trong một hệ thống PKI. Sử dụng chứng chỉ số giúp đảm bảo tính xác thực và tính toàn vẹn của các dữ liệu được trao đổi qua mạng. Hệ thống PKI sử dụng chứng chỉ số để xác thực danh tính của người dùng. Chứng chỉ số là một tài liệu điện tử được cấp phát bởi một đơn vị xác thực, chứng nhận rằng khóa công khai được liên kết với chứng chỉ số đó thuộc về một người dùng cụ thể. Người dùng sử dụng chứng chỉ số để chứng thực danh tính của họ trong các giao dịch trực tuyến.

1.4.3. Mã hóa

Mã hóa là quá trình chuyển đổi thông tin sang dạng khó đọc được gọi là mã hóa, sử dụng các thuật toán mã hóa. Sử dụng mã hóa giúp bảo vệ tính bảo mật của các dữ liệu được trao đổi qua mạng. Hệ thống PKI sử dụng mã hóa để đảm bảo tính toàn vẹn của dữ liệu trong quá trình truyền tải. Kỹ thuật này được thực hiện bằng cách thêm một mã băm (hash) vào dữ liệu gửi đi. Mã băm là một chuỗi số nhỏ được tính từ dữ liệu gốc và được gửi cùng với dữ liệu. Nếu dữ liệu được sửa đổi trong quá trình truyền tải, mã băm sẽ thay đổi, cho phép người nhận phát hiện ra sự thay đổi này.

1.4.4. Chữ ký số

Chữ ký số là một dạng của chữ ký điện tử, được tạo ra bằng cách sử dụng khóa riêng (private key) của người ký để mã hóa thông tin kèm theo các thông tin khác như thời gian và địa chỉ IP. Chữ ký số giúp đảm bảo tính xác thực và tính toàn vẹn của các dữ liệu được trao đổi qua mạng.

1.4.5. Giao thức HTTPS

HTTPS là một giao thức mạng bảo mật, kết hợp giữa giao thức HTTP và SSL/TLS để đảm bảo tính bảo mật của các dữ liệu được trao đổi qua mạng.

1.4.6. Phương pháp quản lý khóa công khai và khóa bí mật

Hệ thống PKI nên sử dụng các phương pháp quản lý khóa công khai và khóa riêng như RSA, ECC, DSA... để đảm bảo tính bảo mật của hệ thống.

1.5. Các công nghệ an ninh

1.5.1. Công nghệ mật mã

Mục đích chính của mật mã là đảm bảo thông tin giữa hai đối tượng trên kênh thông tin không an toàn, để đối tượng thứ ba không thể hiểu được thông tin được truyền là gì. Thoạt nhìn có vẻ mật mã là khái niệm đơn giản, nhưng thực chất nó rất phức tạp.

- Các giải pháp và giao thức:

Công nghệ mật mã hoạt động trên nhiều mức, mức thấp nhất là các giải thuật mật mã. Các giải thuật mật mã trình bày các bước cần thiết để thực hiện một tính toán, thường là chuyển đổi số liệu từ một khuôn dạng này vào khuôn dạng khác. Giao thức lại được xây dựng trên giải thuật này, giao thức mô tả toàn bộ quá trình thực hiện các hoạt động của công nghệ mật mã. Một giải thuật mật mã tuyệt hảo không nhất thiết được coi là giao thức mạnh. Giao thức chịu trách nhiệm cho cả mật mã số liệu lẫn truyền số liệu và trao đổi khóa. Đỉnh của giao thức là ứng dụng, một giao thức mạnh chưa thể đảm bảo an ninh vững chắc bền vững. Vì bản thân ứng dụng có thể dẫn đến vấn đề khác, vì thế để tạo ra một giải pháp an ninh cần một giao thức mạnh cũng như thực hiện ứng dụng bền chắc.

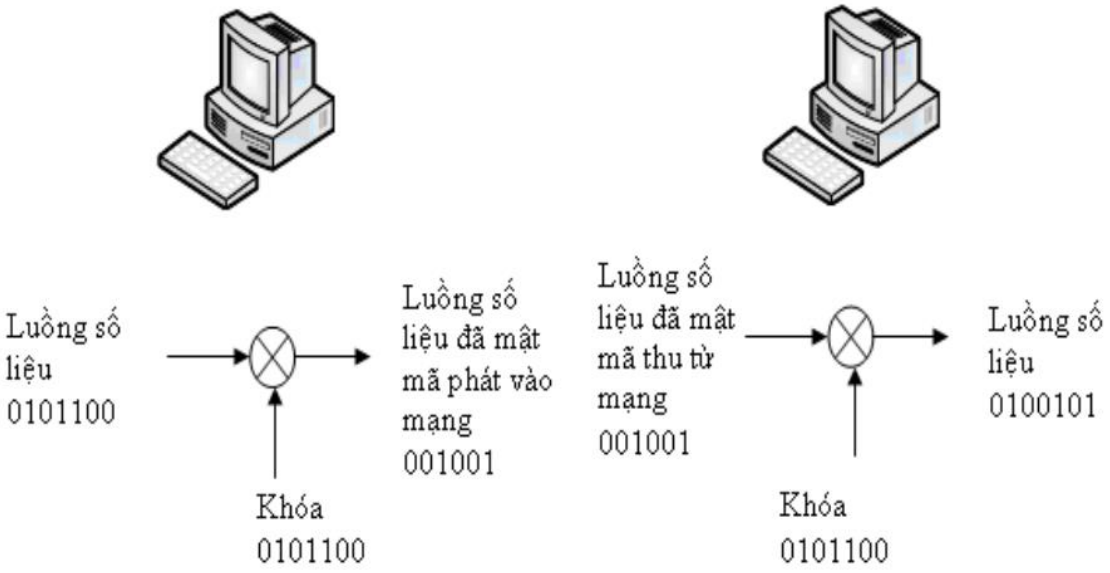
- Mật mã hóa số liệu:

Nền tảng của mọi hệ thống mật mã là mật mã hóa. Quá trình này được thực hiện như sau: tập số liệu thông thường (văn bản thô) được biến đổi về dạng không thể đọc được (văn bản đã mật mã). Mật mã cho phép ta đảm bảo tính riêng tư của số liệu nhạy cảm, ngay cả khi những kẻ không được phép truy nhập thành công vào mạng. Cách duy nhất có thể đọc được số liệu là giải mật mã. Các giải thuật hiện đại sử dụng các khóa để điều khiển mật mã và giải mật mã số liệu. Một khi bản tin đã được mật mã hóa, người sử dụng tại đầu nhận có thể dùng mã tương ứng để giải mật mã, các giải thuật sử dụng khóa mật mã gồm hai loại: Đối xứng và bất đối xứng.

1.5.2. Các giải thuật đối xứng

Các giải thuật đối xứng sử dụng khóa duy nhất cho cả mật mã hóa lẫn giải mật mã hóa tất cả các bản tin. Phía phát sử dụng khóa để mật mã hóa bản tin, sau đó gửi nó đến phía thu xác định. Sau khi nhận được bản tin phía thu sử dụng chính khóa này để giải mật mã. Giải thuật này chỉ làm việc tốt khi có cách an toàn để trao đổi khóa giữa bên phát và bên thu. Rất tiếc là phần lớn vấn đề lại xảy ra trong quá trình trao đổi khóa giữa hai bên. Trao đổi khóa là một vấn đề mà bản thân mật mã hóa đối xứng không thể tự giải quyết được nếu không có phương pháp trao đổi khóa an toàn. Mật mã hóa đối xứng còn được gọi là mật mã hóa bằng khóa bí mật, dạng phổ biến nhất của phương pháp này là tiêu chuẩn mật mã hóa số liệu (DES) được phát triển từ những

năm 1970. Từ đó đến nay, nhiều dạng mật mã hóa đối xứng an toàn đã được phát triển, đứng đầu trong số chúng là tiêu chuẩn mật mã hóa tiên tiến (AES) dựa trên giải thuật Rijindael, DES3, giải thuật mật mã hóa số liệu quốc tế (IDEA), Blowfish và họ các giải thuật của Rivert (RC2, RC4, RC5, RC6). Để giải thích mật mã hóa đối xứng ta xét quá trình mật mã cơ sở sau:



Hình 1.2 Luồng số liệu của mật mã hóa đối xứng

Luồng số liệu (văn bản thô) sử dụng khóa riêng duy nhất (một luồng số liệu khác) thực hiện phép tính cộng để tạo ra luồng số liệu thứ ba (văn bản đã được mật mã). Sau đó văn bản này được gửi qua kênh thông tin để đến bên thu. Sau khi thu được bản tin, phía thu sử dụng khóa chia sẻ (giống khóa bên phát) để giải mật mã (biến đổi ngược) để nhận được văn bản gốc. Phương pháp trên có một số nhược điểm: trước hết không thực tế khi khóa phải có độ dài bằng độ dài số liệu, mặc dù khóa càng dài càng cho tính an ninh cao và càng khó mở khóa. Thông thường các khóa ngắn được sử dụng (64 bit hoặc 128 bit) và chúng được lặp lại nhiều lần cho số liệu. Các phép toán phức tạp hơn có thể được sử dụng vì phép cộng không đủ để đảm bảo. Tiêu chuẩn mật mã hóa số liệu (DES) thường được sử dụng, mặc dù không phải là đảm bảo nhất. Nhược điểm thứ hai là phía phát và phía thu đều sử dụng một khóa chung

(khóa chia sẻ). Phần giải thuật bất đối xứng sẽ trả lời cho câu hỏi làm thế nào để gửi khóa này một cách an toàn từ phía phát đến phía nhận.

1.5.3. Các giải thuật bất đối xứng

Các giải thuật bất đối xứng giải quyết vấn đề chính xảy ra đối với các hệ thống khóa đối xứng. Năm 1975, Whitfield Diffie và Martin Hellman đã phát triển một giải pháp, trong đó hai khóa liên quan với nhau được sử dụng, một được sử dụng để mật mã hóa (khóa công khai) và một được sử dụng để giải mật mã hóa (khóa riêng). Khóa thứ nhất được phân phối rộng rãi trên các đường truyền không an toàn cho mục đích sử dụng công khai. Khóa thứ hai không bao giờ được truyền trên mạng và nó chỉ được sử dụng bởi phía đối tác cần giải mật mã số liệu. Hai khóa này liên hệ với nhau một cách phức tạp bằng cách sử dụng rất nhiều số nguyên tố và các hàm một chiều. Kỹ thuật này dẫn đến không thể tính toán được khóa riêng dựa trên khóa công khai. Khóa càng dài thì càng khó phá vỡ hệ thống. Các hệ thống khóa 64 bit như DES, có thể bị tấn công dễ ràng bằng cách tìm từng tổ hợp khóa đơn cho đến khi tìm được khóa đúng. Các hệ thống khóa 128 bit phổ biến hơn (ví dụ ECC đã được chứng nhận là không thể bị tấn công bằng cách thức như trên).

Khóa riêng và khóa công khai được tạo lập bởi cùng một giải thuật (giải thuật thông dụng là RSA - giải thuật mật mã của 3 đồng tác giả Ron Rivest, Adi Shamir và Leonard Adelman). Người sử dụng giữ khóa riêng của mình và đưa ra khóa công khai cho mọi người, khóa riêng không được chia sẻ cho một người nào khác hoặc truyền trên mạng. Có thể sử dụng khóa công khai để mật mã hóa số liệu, nhưng nếu không biết khóa riêng thì không thể giải mật mã số liệu được. Sở dĩ như vậy là các phép toán được sử dụng trong kiểu mật mã này không đối xứng. Nếu người dùng A muốn gửi số liệu được bảo vệ đến người dùng B, người dùng A sử dụng khóa công khai của người dùng B để mật mã hóa số liệu và yên tâm rằng chỉ có người dùng B mới có thể giải được mật mã và đọc được số liệu này.

Các kỹ thuật mật mã khóa riêng và mật mã khóa công khai là các công cụ chính để giải quyết các vấn đề an toàn, an ninh thông tin. Tuy nhiên, chúng không phải là các giải pháp đầy đủ, cần nhận thực để chứng minh danh tính của người sử

dụng là thật. Chúng ta sẽ xem xét các cách có thể sử dụng mật mã để giải quyết một số vấn đề an toàn cơ sở ở phần dưới.

Cũng có thể mật mã hóa bản tin bằng khóa riêng và giải mật mã bằng khóa công khai, nhưng để cho mục đích khác. Cách này có thể được sử dụng cho các số liệu không nhạy cảm để chứng minh rằng phía mật mã đã thật sự truy nhập vào khóa riêng.

Giải thuật khóa bất đối xứng nổi tiếng đầu tiên được đưa ra bởi Ron Rivest, Adishamir và Leonard Adelman vào năm 1977 với tên gọi là RSA. Các giải thuật phổ biến khác bao gồm ECC và DH. RSA bị thất thế trong môi trường di động do ECC rẻ tiền hơn xét về công suất xử lý và kích thước khóa.

Tuy nhiên, các giải pháp trên đây chưa phải là hoàn hảo, việc chọn một khóa riêng không phải là một việc đơn giản, nếu chọn không sai cách sẽ bị phá vỡ một cách dễ dàng. Ngoài ra, các bộ mật mã hóa bất đối xứng cung cấp các giải pháp cho vấn đề phân phối khóa bằng cách sử dụng khóa công khai và khóa riêng. Do tính phức tạp của mình mà các bộ mật mã bất đối xứng tính toán chậm hơn các bộ mật mã đối xứng. Đây là vấn đề không nhỏ khi xử lý các tập dữ liệu có dung lượng lớn. Việc kết hợp giữa các hệ thống đối xứng và bất đối xứng là một giải pháp lý tưởng để giải quyết vấn đề trên. Sự kết hợp này cho ta ưu điểm về hiệu năng cao hơn các giải thuật đối xứng bằng cách gửi đi khóa bí mật trên các kênh an toàn, dựa trên cơ sở sử dụng các hệ thống khóa công khai. Sau khi cả hai phía đã có khóa bí mật chung, quá trình tiếp theo sẽ sử dụng các giải thuật khóa đối xứng để mã hóa và giải mã. Đây là nguyên lý cơ sở của công nghệ mật mã khóa công khai được sử dụng phổ biến trên nhiều ứng dụng, thiết bị hiện nay.

1.5.4. Nhận thực

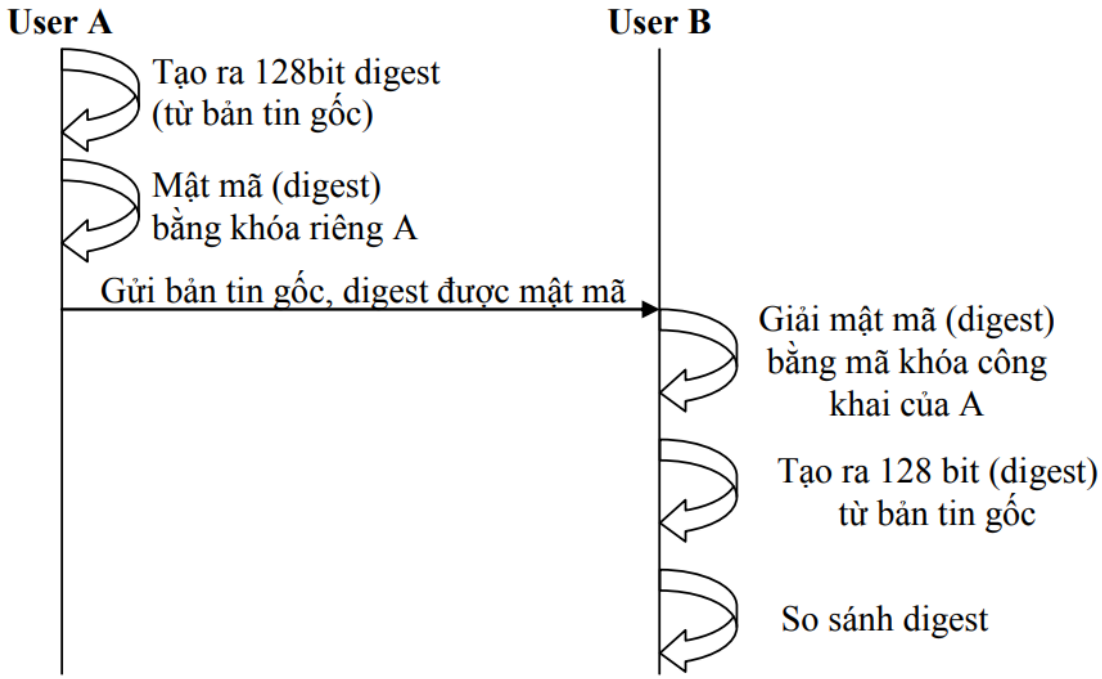
Nhận thực sử dụng mật mã hóa khóa công khai để có thể giải quyết vấn đề xác thực danh tính khiến cho một người sử dụng có thể tin chắc rằng họ đang trao đổi thông tin với đúng người cần trao đổi chứ không bị mắc lừa bởi người khác.

Một ví dụ đơn giản: Một người dùng A là người được cấp cho 2 khóa điện tử là khóa công khai X (public key) và khóa bí mật Y (private key). Người đó phải giữ gìn khóa 2 cẩn thận. Khi có một người dùng B dùng khóa X để mã hóa một bức thư rồi gửi cho người dùng A, thì người dùng A phải dùng khóa Y để giải mã thì mới đọc được bức thư này. Đồng nghiệp hay người thân của A dù có biết bức thư này cũng không có cách nào biết được nội dung vì không có cách nào giải mã được. Dùng khóa Y, cùng với một phần mềm phù hợp, người dùng có thể ký tên lên một văn bản hay tập tin dữ liệu nào đó. Chữ ký điện tử này tương tự như một dấu vân tay đánh dấu lên văn bản nên điều này khó có thể bị giả mạo. Ngoài ra, chữ ký còn đảm bảo phát giác được bất kỳ sự thay đổi nào trên dữ liệu đã được "ký". Để ký lên một văn bản, phần mềm ký tên sẽ nghiền dữ liệu nhỏ lại thành một vài dòng, được gọi là thông báo tóm tắt, bằng một tiến trình được gọi là kỹ thuật "băm" để tạo thành chữ ký điện tử. Cuối cùng, phần mềm ký tên sẽ gắn chữ ký điện tử này vào văn bản. Khi A gửi văn bản đã ký tên này đến cho một đồng nghiệp thì anh ta dùng khóa X giải mã chữ ký ngược trở lại thành một thông báo tóm tắt để biết có phải chính A đã ký tên vào văn bản này hay không. Đồng thời anh ta cũng dùng phần mềm của mình tạo một thông báo tóm tắt từ dữ liệu trên văn bản và so sánh với thông báo tóm tắt do A tạo ra. Nếu hai thông báo tóm tắt này giống nhau tức là dữ liệu trên văn bản là toàn vẹn, không bị thay đổi bởi người khác.

1.5.5. Các chữ ký điện tử và tóm tắt bản tin

Chữ ký điện tử được sử dụng để kiểm tra xem bản tin nhận được có phải là từ phía phát hợp lệ hay không. Nó dựa trên nguyên tắc chỉ người tạo ra chữ ký mới có khóa riêng và có thể kiểm tra khóa này bằng khóa công khai. Chữ ký điện tử được tạo ra bằng cách tính toán tóm tắt bản tin gốc thành bản tin tóm tắt (MD). Sau đó, MD được kết hợp với thông tin của người ký, nhãn thời gian và thông tin cần thiết khác. MD là một hàm nhận số liệu đầu vào có kích cỡ bất kỳ và tạo ra ở đầu ra một kích cỡ cố định (vì thế được gọi là tóm tắt hay digest). Tập thông tin này, sau đó được mật mã hóa bằng khóa riêng của phía phát và sử dụng các giải thuật bất đối xứng. Khối thông tin nhận được sau mã hóa được gọi là khóa điện tử.

Do MD là một hàm nên nó cũng thể hiện phần nào trạng thái hiện thời của bản tin gốc. Nếu bản tin gốc thay đổi thì MD cũng thay đổi. Bằng cách kết hợp MD vào chữ ký điện tử, phía thu có thể dễ dàng phát hiện bản tin gốc có bị thay đổi kể từ khi chữ ký điện tử được tạo hay không. Quá trình sử dụng các digest (tóm tắt) bản tin để tạo ra các chữ ký điện tử như sau:



Hình 1.3 Quá trình digest

User A tạo ra một digest từ bản rõ, digest thực ra là một xâu có độ dài cố định được tạo ra từ một đoạn có độ dài bất kỳ của bản rõ. Rất khó để hai bản tin có cùng một digest, nhất là khi digest có độ dài ngắn nhất là 128bit. Các giải thuật thường được sử dụng để tạo ra một digest là MD5, thuật toán rối an ninh (SHA). Quá trình tạo ra một digest và mã hóa nó bằng khóa riêng X nhanh hơn rất nhiều so với mật mã toàn bộ bản tin. Sau đó, người dùng A gửi đi bản rõ và digest đã mã hóa đến người dùng B, sau khi nhận được bản tin người dùng B có thể sử dụng khóa công khai của người dùng A để giải mã digest, đồng thời người dùng B cũng tạo ra một digest từ văn bản gốc và so sánh hai xâu bit này với nhau. Nếu hai digest giống nhau thì người dùng B có thể tin tưởng rằng văn bản gốc không bị phá hoại trên đường truyền.

Vấn đề chính của quá trình xét ở trên là ta phải giả thiết rằng người dùng B có khóa công khai hợp lệ với người dùng A. Nhưng làm thế nào để người dùng B biết được đã nhận được khóa công khai hợp lệ, làm thế nào để người sử dụng biết rằng email cùng với khóa công khai thực sự là của nhà quản lý ngân hàng. Ý tưởng sử dụng các chứng chỉ số đã ra đời để giải quyết các vấn đề đã nêu trên. Cơ quan cấp chứng chỉ là một tổ chức phát hành các chứng thư ủy nhiệm điện tử và người dùng A, người dùng B tạo ra digest từ bản rõ, mã hóa digest bằng khóa riêng X, giải mã digest bằng mã khóa công khai của A tạo ra digest từ bản rõ. So sánh digest, gửi bản rõ, digest được mật mã cung cấp các chứng chỉ số. Một chứng chỉ số thường bao gồm: tên người sử dụng, thời hạn sử dụng và khóa công khai của người sử dụng. Chứng chỉ được cơ quan cấp chứng chỉ ký bằng chữ ký số, để người sử dụng có thể xác thực chứng chỉ là đúng và có thể tin cậy được.

1.5.6. Các chứng chỉ số

Chứng chỉ số đảm bảo khóa công khai thuộc về đối tượng mà nó đại diện. Cần đảm bảo rằng chứng thư số đại diện cho thực thể yêu cầu (cá nhân hoặc tổ chức), một đối tượng thứ ba là thẩm quyền chứng nhận CA (Certificate Authority). Các nhà cung cấp chứng nhận có thẩm quyền nổi tiếng là Verisign, Entrust, Comodo và GlobalSign. Người sử dụng có thể mua chứng chỉ số từ các nhà cung cấp CA và sử dụng chúng để nhận thực và phân phối khóa riêng của họ. Khi bên nhận đã nhận được khóa riêng của họ thì có thể yên tâm rằng bên gửi chính là nơi họ yêu cầu. Sau đó, bên gửi có thể gửi các bản tin được mật mã bằng khóa công khai đến phía nhận. Bên nhận có thể giải mã chúng bằng khóa riêng của mình. Thông thường chứng thư số bao gồm:

- Tên người sử dụng, thông tin nhận dạng duy nhất người này.
- Khóa công khai của người sở hữu.
- Thời gian chứng thư có hiệu lực.
- Chữ ký số từ CA có tác dụng phát hiện ra nếu truyền dẫn bị làm giả.

Người sử dụng sở hữu chứng chỉ số cũng có thể tự ký chứng nhận số để trở thành CA (self-signed CA). Khi đó CA này là đáng tin cậy nếu được ký nhận bởi một

khóa đáng tin cậy khác. X.509 là tiêu chuẩn nhận thực hàng đầu cho các chứng nhận số. Các chứng nhận này thường xuất hiện trong các ứng dụng Internet.

1.6. Kết chương

Hiện nay vấn đề an toàn thông tin trong thời đại chuyển đổi số là một trong những mục tiêu hàng đầu của bất cứ tổ chức hay cá nhân nào. Từ các công ty nhỏ cho tới các tập đoàn lớn hay tổ chức chính phủ đều đặt vấn đề bảo mật thông tin làm trọng tâm trong công cuộc chuyển đổi số của mình. Các phương pháp tấn công phát triển đòi hỏi các kỹ thuật phòng thủ cũng như xử lý sự cố cũng phải vượt lên trên để có thể ngăn chặn được kẻ xấu lợi dụng các kẽ hở để tấn công, phá hoại, trục lợi.

Chương 2: CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI PKI

2.1. Tổng quan về hạ tầng khóa công khai PKI

Hạ tầng khóa công khai PKI (Public Key Infrastructure) là một thuật ngữ dùng để mô tả một hệ thống hoàn thiện của một tập hợp các vai trò, chính sách, quy tắc, phần cứng, phần mềm và quy trình cần thiết để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi chứng chỉ kỹ thuật số cũng như quản lý mã hóa công khai. Nhóm đặc trách kỹ thuật Internet (IEFT) X.509 định nghĩa PKI như sau: “PKI là một tập bao gồm phần cứng, phần mềm, con người và các thủ tục cần thiết để tạo lập, quản lý, lưu trữ và hủy các chứng nhận số dựa trên mật mã khóa công khai”. Mục đích của PKI là tạo điều kiện thuận lợi cho việc chuyển thông tin điện tử an toàn cho một loạt các hoạt động mạng như thương mại điện tử, ngân hàng trực tuyến và email bí mật. PKI sinh ra để phục vụ các hoạt động mà trong đó các mật khẩu đơn giản được coi là phương pháp xác thực không đầy đủ, vì vậy cần có bằng chứng nghiêm ngặt hơn để xác nhận danh tính của các bên liên quan đến giao tiếp nhằm xác thực thông tin được truyền.

Trong mật mã học, PKI là một sự sắp xếp liên kết các khóa công khai với danh tính tương ứng của các thực thể (như người và tổ chức). Ràng buộc được thiết lập thông qua quy trình đăng ký tại cơ quan chuyên cung cấp chứng chỉ CA rồi được cấp chứng chỉ bởi chính cơ quan đó. Tùy thuộc vào mức độ đảm bảo của ràng buộc, điều này có thể được thực hiện bởi một quy trình tự động hoặc dưới sự giám sát của một nhóm chuyên gia. Khi được thực hiện qua mạng, điều này yêu cầu sử dụng giao thức đăng ký chứng chỉ hoặc quản lý chứng chỉ an toàn, chẳng hạn như giao thức quản lý chứng chỉ CMP (Certificate Management Protocol) được chuẩn hóa bởi IETF.

Trong hệ thống PKI, vai trò của cơ quan đăng ký RA (Registration Authority) là đảm bảo đăng ký hợp lệ và chính xác. Về cơ bản, RA chịu trách nhiệm chấp nhận các yêu cầu về chứng chỉ kỹ thuật số và xác thực thực thể đưa ra yêu cầu. RFC 3647 của Lực lượng đặc nhiệm kỹ thuật Internet IETF định nghĩa RA là "Một thực thể chịu trách nhiệm cho một hoặc nhiều chức năng sau: nhận dạng và xác thực bên yêu cầu cấp chứng chỉ, phê duyệt hoặc từ chối đề nghị cấp chứng chỉ, tiến hành thu hồi hoặc đình chỉ chứng chỉ trong một số trường hợp nhất định , xử lý các yêu cầu của bên đăng ký để thu hồi hoặc đình chỉ

chứng chỉ của họ và phê duyệt hoặc từ chối yêu cầu của bên đăng ký gia hạn hoặc nhập lại chứng chỉ của họ. Tuy nhiên, RA không ký hoặc cấp chứng chỉ (nghĩa là RA được ủy quyền một số nhiệm vụ thay mặt cho một CA)." Mặc dù Microsoft có thể đã gọi CA cấp dưới là RA, nhưng điều này không đúng theo tiêu chuẩn PKI X.509. RA không có quyền ký của CA và chỉ quản lý việc kiểm tra và cung cấp chứng chỉ. Vì vậy, trong trường hợp PKI của Microsoft, chức năng RA được cung cấp bởi trang web Dịch vụ chứng chỉ của Microsoft (Microsoft Certificate Services) hoặc thông qua dịch vụ chứng chỉ Active Directory. Dịch vụ này thực thi chính sách chứng chỉ và CA doanh nghiệp của Microsoft thông qua các mẫu chứng chỉ và quản lý việc đăng ký chứng chỉ (đăng ký thủ công hoặc tự động). Trong trường hợp các CA độc lập của Microsoft, chức năng của RA không tồn tại vì tất cả các quy trình kiểm soát CA đều dựa trên quy trình quản trị và truy cập được liên kết với hệ thống lưu trữ CA và chính CA đó chứ không phải Active Directory. Hầu hết các giải pháp PKI thương mại không phải của Microsoft đều cung cấp thành phần RA độc lập.

Một thực thể phải được nhận dạng duy nhất trong mỗi miền CA trên cơ sở thông tin về thực thể đó. Cơ quan xác thực bên thứ ba VA (third-party Validation Authority) có thể xác thực sau đó cung cấp thông tin về thực thể này thay mặt cho CA.

Tiêu chuẩn X.509 được xác định là định dạng được sử dụng phổ biến nhất cho chứng chỉ khóa công khai. PKI cung cấp "các dịch vụ tin cậy" (trust services), nói một cách dễ hiểu là tin tưởng vào các hành động hoặc kết quả đầu ra của các thực thể, có thể là con người hoặc máy tính. Có ba mục tiêu chính của các dịch vụ ủy tin cậy như sau: Tính bảo mật (Confidentiality), tính toàn vẹn (Integrity) và tính xác thực (Authenticity), gọi tắt là CIA.

- Tính bảo mật: Đảm bảo rằng không thực thể nào có thể xem một tập tin dưới dạng bản rõ dù cố ý hay vô tình. Dữ liệu được mã hóa để giữ bí mật, sao cho ngay cả khi được đọc, nó vẫn có vẻ vô nghĩa. Có lẽ việc sử dụng PKI phổ biến nhất cho các mục đích bảo mật là trong bối cảnh của TLS. TLS là một giao thức củng cố tính bảo mật của dữ liệu khi truyền, tức là trong quá trình truyền. Một ví dụ kinh điển về bảo mật TLS là khi sử dụng trình duyệt internet để đăng nhập vào một dịch vụ web trên internet bằng cách nhập mật khẩu.

- Tính toàn vẹn: Đảm bảo rằng nếu dữ liệu được truyền, dù có bị một thực thể thay đổi (giả mạo) theo cách nhỏ nhất, thì vẫn bị phát hiện ra. Khi điều này xảy ra có nghĩa là tính toàn vẹn của nó đã bị xâm phạm. Thông thường, việc ngăn chặn sự xâm phạm (bằng chứng giả mạo) tính toàn vẹn không phải là quan trọng nhất. Điều quan trọng nhất là phải có bằng chứng rõ ràng về việc tính toàn vẹn đã bị xâm phạm (bằng chứng giả mạo).
- Tính xác thực: Đảm bảo rằng mọi thực thể đều chắc chắn nó đang kết nối tới đâu hoặc có thể chứng minh tính hợp pháp của nó khi kết nối với một dịch vụ được bảo vệ. Vế trước được gọi là xác thực phía máy chủ (server), thường được sử dụng khi xác thực với máy chủ web bằng mật khẩu. Vế sau được gọi là xác thực phía máy khách (client), đôi khi được sử dụng khi xác thực bằng thẻ thông minh smart card (lưu trữ chứng chỉ kỹ thuật số và khóa riêng).

PKI cho dù thuộc loại này hay loại khác và từ bất kỳ nhà cung cấp nào, có nhiều cách sử dụng khác nhau, bao gồm cả cung cấp khóa công khai cùng với ràng buộc với danh tính người dùng đều được sử dụng cho những mục đích sau:

- Mã hóa và/hoặc xác thực người gửi của thông điệp email (ví dụ: sử dụng OpenPGP hoặc S/MIME).
- Mã hóa và/hoặc xác thực tài liệu (ví dụ: tiêu chuẩn Chữ ký XML hoặc Mã hóa XML nếu tài liệu được mã hóa dưới dạng XML).
- Xác thực người dùng với các ứng dụng (ví dụ: đăng nhập thẻ thông minh, xác thực ứng dụng khách bằng SSL/TLS). Có cách sử dụng thực nghiệm để xác thực HTTP được ký điện tử trong các dự án như Enigform và mod_openpgp.
- Khởi động các giao thức liên lạc an toàn, chẳng hạn như trao đổi khóa Internet (IKE) và SSL/TLS. Trong cả hai cách này, thiết lập ban đầu của một kênh an toàn sử dụng khóa bất đối xứng (phương pháp khóa công khai), trong khi đó giao tiếp thực tế sử dụng khóa đối xứng (phương pháp khóa bí mật).
- Chữ ký di động hay chữ ký số di động là chữ ký điện tử được tạo bằng thiết bị di động và dựa vào chữ ký hoặc dịch vụ chứng nhận trong môi trường viễn thông độc lập về địa điểm.

- Internet vạn vật IoT (Internet of Things) yêu cầu liên lạc an toàn giữa một tập hợp các thiết bị tin cậy lẫn nhau. Cơ sở hạ tầng khóa công khai cho phép các thiết bị nhận và gia hạn chứng chỉ X.509 được sử dụng để thiết lập sự tin cậy giữa các thiết bị và mã hóa thông tin liên lạc bằng giao thức TLS.

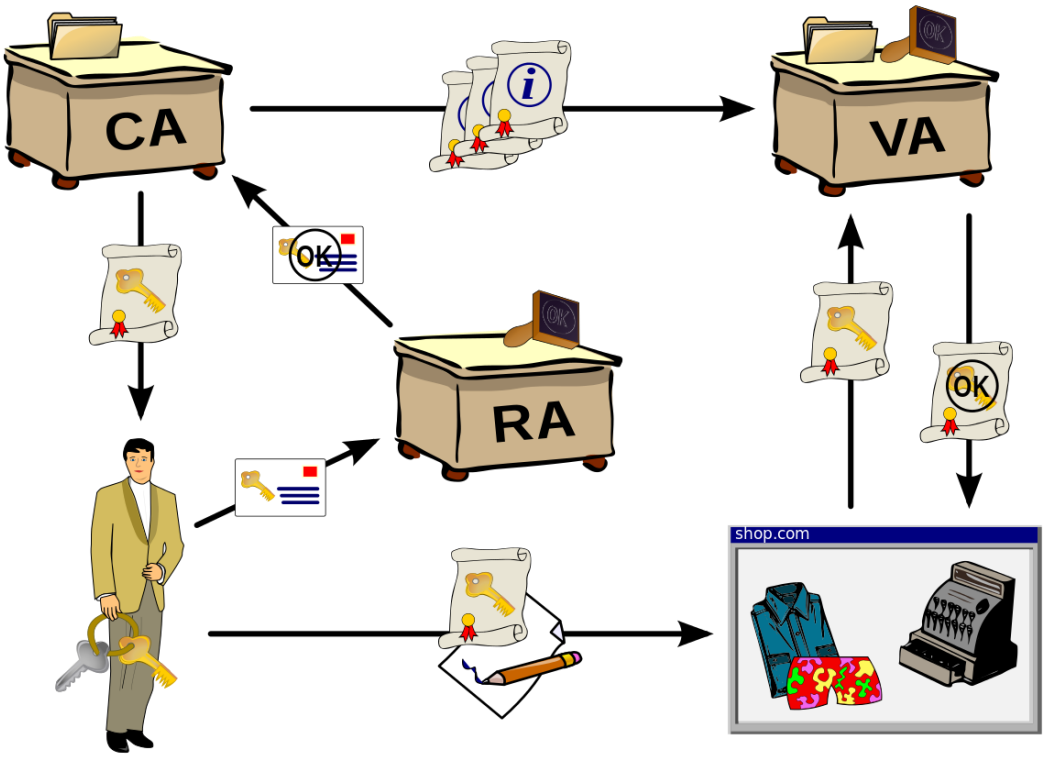
2.2. Kiến trúc và chức năng của PKI

Mật mã khóa công khai là một kỹ thuật mã hóa cho phép các thực thể giao tiếp an toàn trong môi trường không an toàn của mạng công cộng và xác minh danh tính của một thực thể một cách đáng tin cậy thông qua việc sử dụng chữ ký số.[6]

Cơ sở hạ tầng khóa công khai (PKI) là một hệ thống tạo, lưu trữ và phân phối chứng chỉ kỹ thuật số được sử dụng để xác minh rằng một khóa công khai cụ thể thuộc về một thực thể nhất định duy nhất. PKI tạo chứng chỉ kỹ thuật số ánh xạ khóa công khai tới các thực thể, lưu trữ an toàn các chứng chỉ này trong kho lưu trữ trung tâm và thu hồi chúng nếu cần thiết.

Một PKI bao gồm:

- Cơ quan cấp chứng chỉ (CA) có nhiệm vụ lưu trữ, phát hành và ký chứng chỉ kỹ thuật số.
- Cơ quan đăng ký (RA) có nhiệm vụ xác minh danh tính của các thực thể yêu cầu chứng chỉ kỹ thuật số của họ được lưu trữ tại CA.
- Một thư mục trung tâm là một vị trí an toàn trong đó các khóa được lưu trữ và lập chỉ mục.
- Một hệ thống quản lý chứng chỉ quản lý những thứ như quyền truy cập vào chứng chỉ được lưu trữ hoặc phân phối chứng chỉ sẽ được cấp.
- Chính sách về chứng chỉ nêu rõ các yêu cầu của PKI liên quan đến các thủ tục của nó. Mục đích của nó là cho phép những người ngoài phân tích độ tin cậy của PKI.
- Một cơ quan xác thực bên thứ ba (VA) có thể cung cấp xác thực thực thể cho CA.



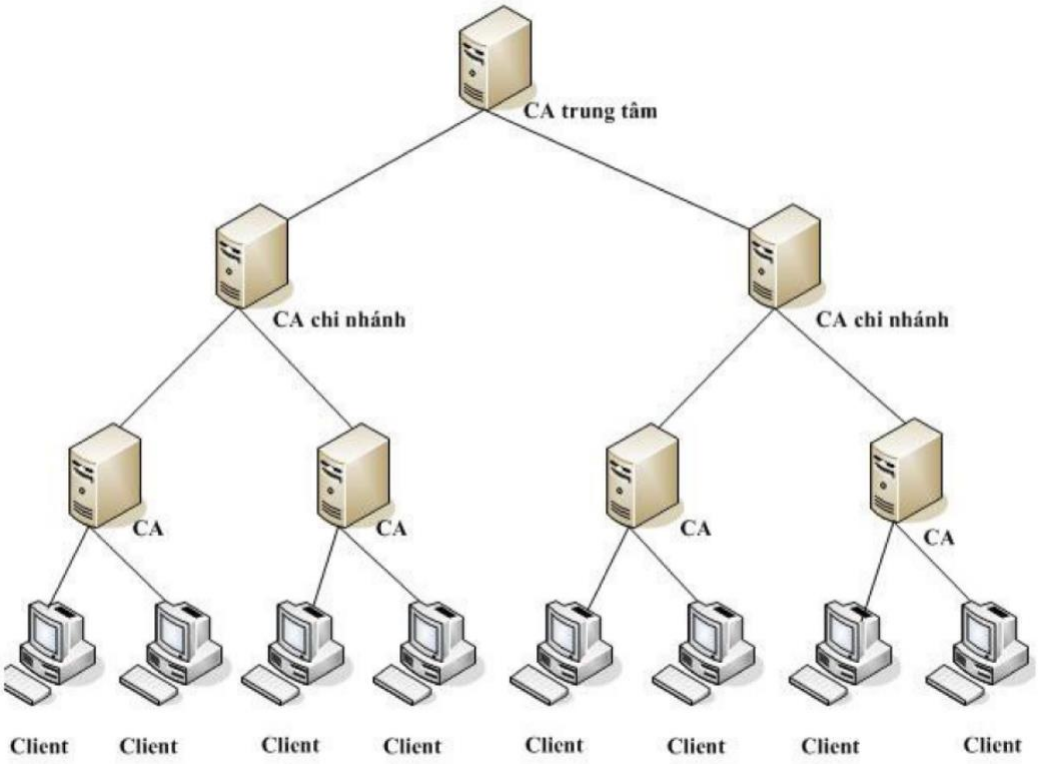
Hình 2.1 Kiến trúc PKI

Sơ đồ PKI cho phép các tổ chức và người dùng trao đổi dữ liệu an toàn và xác thực thông tin với nhau. Khi một người dùng muốn trao đổi dữ liệu với một người khác, họ sử dụng khóa công khai của người nhận để mã hóa dữ liệu. Người nhận sau đó sử dụng khóa bí mật của mình để giải mã dữ liệu. Khi người gửi muốn xác thực danh tính của người nhận, họ sử dụng chữ ký số của mình, được tạo ra bằng khóa bí mật, để xác nhận rằng họ là người gửi. Chữ ký số này sau đó được xác minh bằng cách sử dụng khóa công khai của người gửi. PKI đảm bảo rằng các khóa công khai được xác thực và quản lý đúng cách và bảo vệ tính toàn vẹn và bảo mật của dữ liệu được trao đổi qua mạng.

Tùy từng mục đích sử dụng mà PKI sử dụng tiêu chuẩn thiết kế phù hợp, có 3 mô hình kiến trúc PKI chính, đó là:

- Mô hình phân cấp.
- Mô hình mạng lưới.
- Mô hình danh sách tin cậy.

2.2.1. Mô hình phân cấp



Hình 2.2 Mô hình phân cấp

Đây là mô hình được sử dụng phổ biến rộng rãi nhất hiện nay với những ưu nhược điểm như sau.

Ưu điểm:

– Tương thích với cấu trúc phân cấp của hệ thống quản lý trong các tổ chức lớn, tổ chức chính phủ.

– Do có hình thức phân cấp tương tự như tổ chức thư mục nên dễ sử dụng.

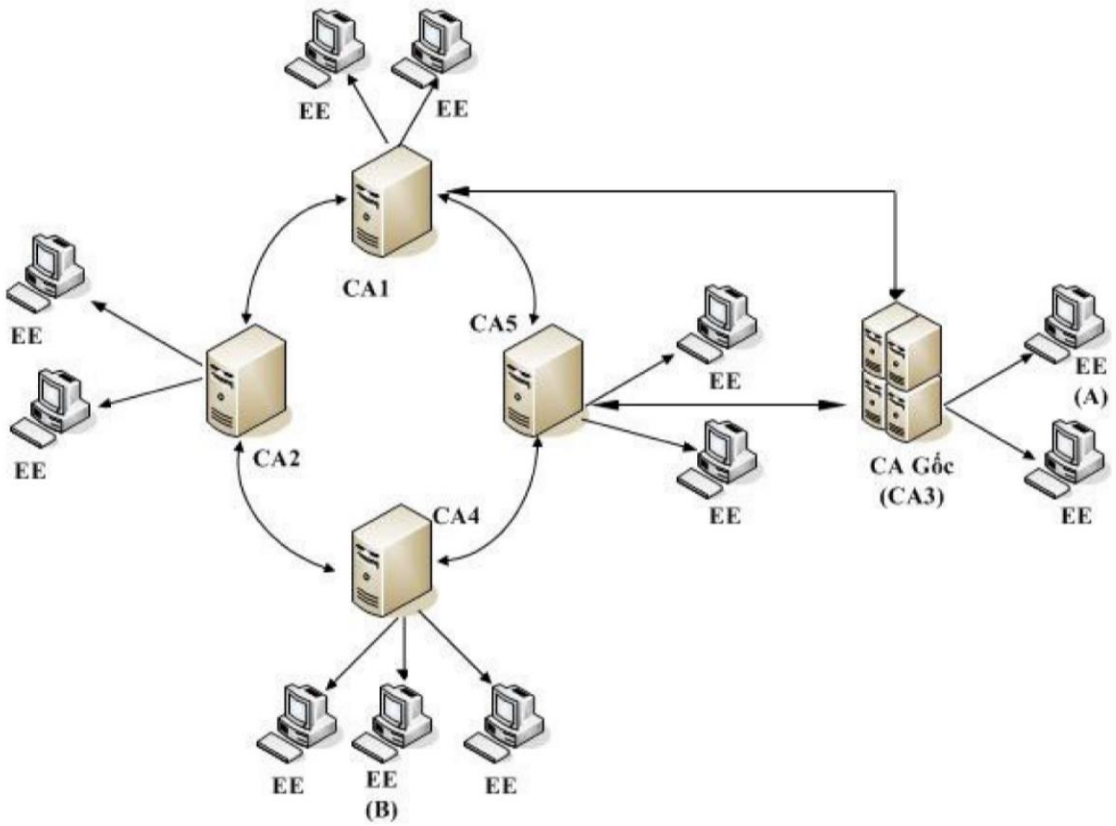
– Tìm nhánh xác thực đơn giản và ko bị vòng lặp.

Nhược điểm:

– Các quan hệ kinh doanh, thương mại đôi khi không thể phân cấp được.

– Nếu khóa RootCA bị lộ thì toàn bộ hệ thống sẽ sụp đổ.

2.2.2. Mô hình mạng lưới



Hình 2.3 Mô hình mạng lưới

Ưu điểm:

– Đây là mô hình thích hợp với các mối liên hệ kinh doanh thương mại ngang hàng vì tính linh động của nó trong thực tế.

– Do xác thực ngang hàng trực tiếp nên các đối tượng sử dụng CA có thể làm việc trực tiếp với nhau làm giảm tải lưu lượng đường truyền và thao tác xử lý.

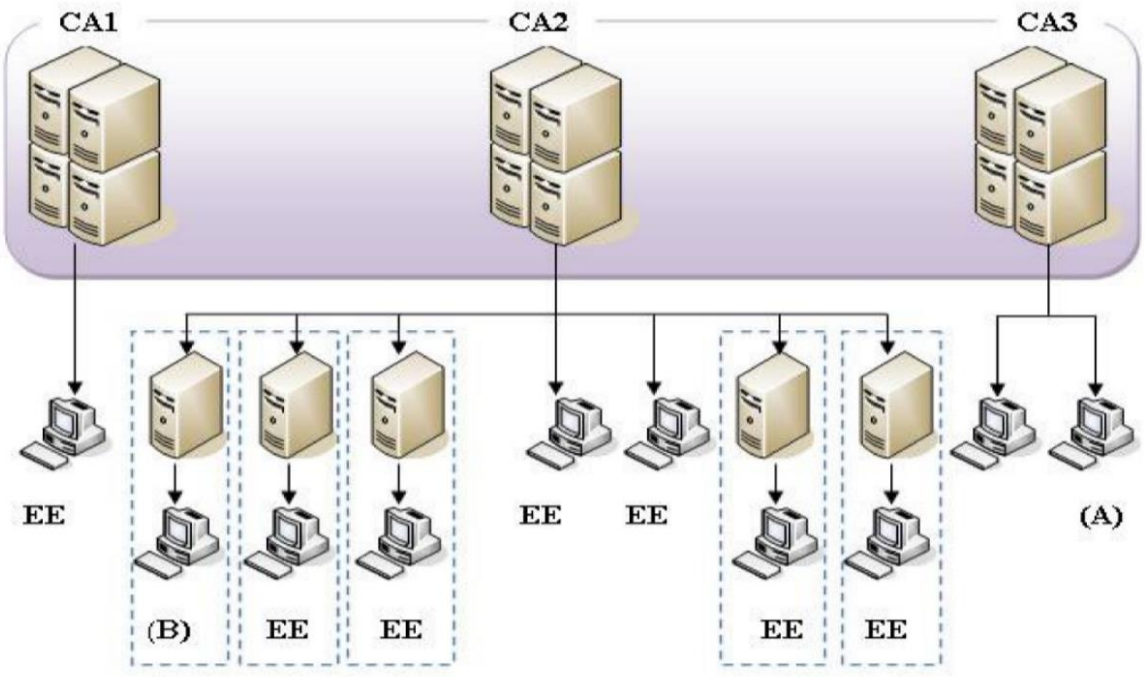
– Khi một CA bị lộ khóa chỉ cần cấp phát chứng chỉ CA mới tới các đối tượng có thiết lập quan hệ tin cậy với CA này.

Nhược điểm:

– Do cấu trúc phức tạp của mạng nên việc tìm kiếm các đối tượng trong một cơ sở dữ liệu lớn là khá khó khăn.

– Một thực thể không thể đưa ra một nhánh xác thực duy nhất có thể đảm bảo rằng tất cả các đối tượng trong hệ thống có thể tin cậy được.

2.2.3. Mô hình danh sách tin cậy



Hình 2.4 Mô hình danh sách tin cậy

Ưu điểm:

- Kiến trúc đơn giản, dễ dàng triển khai.
- Các thực thể có toàn quyền sử dụng với danh sách các CA tin cậy.
- Các thực thể làm việc trực tiếp với CA trong danh sách các CA được tin cậy.

Nhược điểm:

- Khó khăn trong việc quản lý danh sách các CA tin cậy.
- Không có hỗ trợ trực tiếp với các cặp chứng chỉ ngang hàng, do đó hạn chế CA trong việc quản lý sự tin cậy của mình với các CA khác.
- Nhiều ứng dụng không hỗ trợ tính năng tự động lấy thông tin trạng thái hoặc hủy bỏ của chứng chỉ.

2.3. Ưu điểm và nhược điểm của PKI

PKI cung cấp tiêu chuẩn bảo mật cao hơn cho các tổ chức so với xác thực bằng mật khẩu. PKI, hoặc cơ sở hạ tầng khóa công khai, sử dụng Secure Shell để xác thực đăng nhập và cấp đặc quyền cho người dùng tương ứng.

Tính năng bảo mật bổ sung này cho phép truyền thông tin và dữ liệu an toàn hơn qua các dịch vụ dựa trên đám mây và Internet vạn vật. PKI là một phương thức ủy quyền và khả năng truy cập đa yếu tố được sử dụng bởi các tổ chức đang tìm cách tăng cường bảo mật trong các giao dịch công khai và riêng tư của họ. PKI yêu cầu chứng chỉ gốc cùng với cơ quan phát hành được kết nối với chứng chỉ đó.

Chi phí quá lớn phải bỏ ra ban đầu để triển khai hạ tầng khóa công khai PKI ngăn cản nhiều tổ chức triển khai dịch vụ này. Tuy nhiên ngày nay có sẵn rất nhiều lựa chọn outsource sẵn có. Hạ tầng khóa công khai PKI có một số ưu điểm như sau:

- Tính không từ chối: PKI là một giải pháp bảo mật hấp dẫn vì nhiều lý do, một trong số đó là tính không từ chối (non-repudiation). Các thuật toán để khớp khóa cá nhân và cho phép truy cập chéo trên các nền tảng khác nhau. Điều này tạo ra trải nghiệm thân thiện cho người dùng dù là trên phần cứng hay phần mềm của mỗi tổ chức.
- Hiệu quả về chi phí: Mặc dù đối với một số cá nhân, tổ chức thì chi phí ban đầu phải bỏ ra là khó chấp nhận được nhưng về lâu về dài, thuật toán cố định của PKI khiến mọi thứ trở nên rẻ hơn.
- Mức độ bảo mật cao: Các bên có thể làm việc trực tiếp với nhau nếu CA của họ đều nằm trong danh sách các CA được tin cậy.
- Được các chính phủ chấp nhận: PKI được sử dụng bởi các tổ chức chính phủ. Các tổ chức này coi PKI là giải pháp mang tính chiến lược đối với các mục tiêu bảo mật của họ. Quốc phòng an ninh, tài chính ngân hàng và ngay cả lĩnh vực y tế cũng dựa vào PKI để xác thực và cấp phép.

Cùng với các ưu điểm của PKI thì hạ tầng này cũng có một số nhược điểm như sau:

- Chi phí triển khai cao: Như đã được nhắc tới ở trên, một trong những nhược điểm lớn nhất của PKI là lượng tài nguyên cần thiết để bắt đầu. Chi phí đầu tư đắt đỏ vào hạ tầng PKI bao gồm việc soạn thảo chính sách, chỉ định và đào tạo người quản trị có thể diễn ra liên tục, vừa tốn thời gian lẫn tiền bạc. Chính điều này đã tạo nên sự bùng nổ dịch vụ PKIaas (PKI-as-a-service) chuyên cung cấp chứng thư số bởi các công ty/tổ chức tạo

ra giải pháp hạ tầng khóa công khai. Điều này cho phép một tổ chức đang tìm cách triển khai PKI có thể mua từ bên thứ ba và áp dụng ngay mà không cần thiết phải tự xây dựng nên hệ thống của riêng mình.

- Chi phí phát sinh: Việc quản lý chứng chỉ PKI có thể gặp khó khăn do chi phí hoạt động phát sinh. Việc sử dụng giao tiếp HTTPs yêu cầu một số chi phí hoạt động cao hơn dự kiến và có thể coi là một điểm trừ đối với các tổ chức nhỏ.
- Cần đội ngũ quản trị viên được đào tạo bài bản: Bản chất phức tạp của hệ thống PKI có thể gây khó khăn cho các tổ chức nhỏ trong việc triển khai hiệu quả nếu không có các quản trị viên được đào tạo bài bản và hiểu về hệ thống này.

Một số sai lầm thường mắc phải khi sử dụng hạ tầng khóa công khai PKI:

- Sử dụng các thuật toán cũ: Việc sử dụng các thuật toán cũ khi đã có sự xuất hiện của các thuật toán mới hơn có thể gây ra sự cố và cho phép các cuộc tấn công trong đó các tác nhân xấu có thể làm giả và tạo ra các chứng chỉ gian lận. Thuật toán SHA2 được NSA thiết kế để vượt qua các lỗi tiềm ẩn trong SHA1. Vì vậy, SHA2 được coi là an toàn hơn SHA1. Khi so sánh thuật toán ECC với RSA, sự khác biệt lớn nhất là kích thước khóa so với độ mạnh của mật mã.
- Không lưu trữ chứng thư gốc RootCA ngoại tuyến: Chứng chỉ gốc phải được lưu giữ trong thiết bị ngoại tuyến. Cơ quan chứng nhận ngoại tuyến phụ thuộc vào hệ thống phân cấp bậc. Hệ thống phân cấp được chia thành các cấp, các cấp này có thể hoạt động theo 2 cấp, 3 cấp hoặc nhiều hơn. Hệ thống phân cấp được quyết định sử dụng sẽ cho biết cần phải làm việc với bao nhiêu CA ngoại tuyến. Hệ thống phân cấp 3 tầng cần phải có ít nhất 2 CA ngoại tuyến, hệ thống phân cấp 2 tầng cần phải có một CA ngoại tuyến.
- Không sử dụng khóa bảo vệ cứng cho Tổ chức phát hành chứng chỉ: Khóa bảo vệ cứng luôn được khuyến nghị sử dụng để bảo vệ khóa bí mật của CA. Phần đính kèm có thể được tạo qua mạng hoặc được gắn trực tiếp vào CA.
- Không sử dụng các dịch vụ của cơ quan xác thực như OCSP: Kỹ sư bảo mật và người triển khai PKI trong các cơ quan, tổ chức chính phủ phải luôn sử dụng các dịch vụ của cơ quan xác thực, chẳng hạn như bộ giao thức trạng thái chứng chỉ trực tuyến

OCSP (Online Certificate Status Protocol). Giao thức phản hồi này quản lý các yêu cầu xác thực bằng cách làm việc thông qua các CRL giới hạn để kiểm tra trạng thái của chứng chỉ bằng cách sử dụng số sê-ri do máy khách cung cấp.

- Sử dụng CRL quá dài: Chứng chỉ bị thu hồi khiến số lượng CRL tăng lên. Chứng chỉ hết hạn thường không được lưu trữ trong CRL. Có thể giữ CRL ở độ dài có thể quản lý được bằng cách cung cấp cho chứng chỉ thời gian tồn tại ngắn hơn theo mục đích sử dụng của tổ chức.
- Tạo khóa tập trung: Một khóa bị lộ đồng nghĩa với việc toàn bộ hệ thống sụp đổ. Các khóa cần phải được bảo vệ nghiêm ngặt. Các khóa phải được tạo ngẫu nhiên bằng trình sinh chứng thư phù hợp sau khi quá trình phát triển PKI đã kết thúc.

2.4. Một số phần mềm cung cấp hạ tầng khóa công khai

2.4.1. OpenSSL

OpenSSL là dạng CA đơn giản nhất và cũng là công cụ cho PKI được phát triển từ năm 1998. Nó là một bộ công cụ được bao gồm trong tất cả các bản phân phối chính của Linux và có thể được sử dụng để xây dựng CA đơn giản của cá nhân và cho các ứng dụng có hỗ trợ PKI. Là một thư viện phần mềm dành cho các ứng dụng, OpenSSL cung cấp thông tin liên lạc an toàn qua mạng máy tính chống nghe lén hoặc cần xác định đối tác ở đầu bên kia. Nó được sử dụng rộng rãi bởi các máy chủ Internet, bao gồm phần lớn các trang web HTTPS.

OpenSSL chứa mã nguồn mở của các giao thức SSL và TLS. Thư viện lõi được viết bằng ngôn ngữ lập trình C, thực hiện các chức năng mật mã cơ bản và cung cấp các chức năng tiện ích khác nhau. Có sẵn các chương trình cho phép sử dụng thư viện OpenSSL bằng nhiều ngôn ngữ máy tính phù hợp. OpenSSL khả dụng cho hầu hết các hệ điều hành giống Unix (bao gồm Linux, macOS và BSD), Microsoft Windows và OpenVMS.

2.4.2. EJBCA

EJBCA là một hệ thống CA mã nguồn mở được phát triển bằng Java. EJBCA có đầy đủ toàn bộ tính năng của hệ thống PKI, chuyên cung cấp cho doanh nghiệp, tổ chức sử dụng. Nó có thể được sử dụng để thiết lập một CA cho cả mục đích sử

dụng nội bộ hay mục đích sử dụng như một dịch vụ.

EJBCA là một giải pháp PKI dựa trên Java cung cấp cả phiên bản dành cho doanh nghiệp và cộng đồng. EJBCA Community Edition (CE) được tải xuống miễn phí và có tất cả các tính năng cốt lõi cần thiết để cấp và quản lý chứng chỉ. Nó bao gồm nhiều phương thức đăng ký chứng chỉ, cũng như API REST. EJBCA được phát triển bởi PrimeKey, hiện là một phần của Keyfactor và là giải pháp được chấp nhận và tin cậy rộng rãi nhất cho PKI CA nguồn mở hiện nay.

Các đặc điểm nổi bật của EJBCA bao gồm:

- Quản lý vòng đời và phát hành chứng chỉ X.509 và SSH.
- Cơ quan cấp chứng chỉ (CA), cơ quan đăng ký (RA) và chức năng OCSP.
- Khả năng mở rộng thông qua API CMP, SCEP và REST.
- Kiểm tra ghi nhật ký vào tệp hoặc cơ sở dữ liệu.
- Hỗ trợ HSM cơ bản sử dụng Java PKCS#11.

EJBCA Enterprise Edition (EE) bao gồm các tính năng dành cho môi trường doanh nghiệp, tổ chức. Nó bao gồm tính khả dụng cao, phân cụm, xác thực, giao thức nâng cao và hỗ trợ HSM, dịch vụ và hỗ trợ chuyên nghiệp cũng như tính linh hoạt trong triển khai. EJBCA Enterprise có thể được triển khai dưới dạng thiết bị phần cứng chìa khóa trao tay, thiết bị phần mềm, dựa trên đám mây hoặc PKI do SaaS phân phối.

2.4.3. Dogtag Certificate System

Hệ thống chứng chỉ Dogtag (còn được gọi là Dogtag PKI) là cơ quan cấp chứng chỉ nguồn mở (CA) hỗ trợ nhiều trường hợp sử dụng PKI phổ biến. Nó cung cấp một giao diện quản lý dựa trên web cho phép bạn kiểm soát các chứng chỉ của mình đồng thời hỗ trợ nhiều định dạng để chúng có thể dễ dàng phù hợp với các trường hợp sử dụng khác nhau.

Các đặc điểm chính của Dogtag bao gồm:

- Cấp chứng chỉ X.509 và quản lý chứng chỉ.

- Tạo và xuất bản CRL.
- Đăng ký theo địa phương (LRA) để xác thực và đưa ra chính sách phù hợp.
- Khả năng mở rộng thông qua API như ACME, SCEP và REST.
- Không hỗ trợ cơ sở dữ liệu quan hệ – yêu cầu LDAP.

2.4.5. OpenXPKI

OpenXPKI là bộ công cụ dựa trên OpenSSL và Perl có thể tạo, quản lý và triển khai các chứng chỉ kỹ thuật số. Nó bao gồm hỗ trợ cho nhiều định dạng chứng chỉ và giao diện trực tuyến để giúp bạn giám sát khối lượng công việc PKI của mình.

Các đặc điểm chính của OpenXPKI bao gồm:

- Cấp chứng chỉ X.509 và quản lý chứng chỉ.
- Giao diện người dùng GUI dựa trên web tương thích với tất cả các trình duyệt phổ biến.
- Khả năng mở rộng thông qua SCEP và EST.

2.4.6. Step-ca

Step-ca là một công cụ PKI mã nguồn mở dựa trên dòng lệnh command line CLI đơn giản nhưng linh hoạt có thể tạo và quản lý các chứng chỉ kỹ thuật số. Tương tự, nó bao gồm hỗ trợ cho nhiều định dạng chứng chỉ và có khả năng tích hợp với các công cụ như Kubernetes, Nebula và Envoy.

Các đặc điểm chính của Step-ca bao gồm:

- Quản lý và phát hành chứng chỉ X.509 và SSH.
- Giao diện dựa trên CLI cho chứng chỉ.
- Khả năng mở rộng thông qua giao thức ACME và SCEP.
- Yêu cầu chuyên môn kỹ thuật về các khái niệm PKI và JSON.

2.4.7. OpenCA

OpenCA là một dự án xây dựng một hệ thống PKI hoàn chỉnh, chuyên nghiệp cho các doanh nghiệp, cơ quan, tổ chức cỡ vừa và lớn. Bắt đầu được phát triển vào năm 1999 và liên tục nâng cấp cho tới nay, OpenCA đã trở thành một trong những

phần mềm mã nguồn mở được sử dụng nhiều nhất. OpenCA có các đặc điểm chính như sau:

- Giao diện web hỗ trợ hầu hết các trình duyệt hiện có.
- Hỗ trợ giao tiếp LDAP, module RA, OCSP.

2.5. So sánh đặc điểm giữa OpenCA và EJBCA

Đặc điểm	OpenCA	EJBCA
Tính bí mật	Có (Sử dụng mã hóa)	Có (Sử dụng mã hóa)
Tính toàn vẹn	Có (Sử dụng mã hóa)	Có (Sử dụng mã hóa)
Tính xác thực	Có (Sử dụng chữ ký số)	Có (Sử dụng chữ ký số)
Tính chống chối bỏ	Không	Có
Chọn thuật toán để sử dụng OSCP	Không	Có
Khả năng chọn CSP	Bằng tay	Có
Cập nhật CRL	Không	Có
Hỗ trợ thẻ thông minh	Miễn phí	Tự động
Độ khó khi cấu hình	Cao	Rất cao
Các tính năng mở rộng	Có	Có
Môi trường nền	Perl CGI trên Unix	Miễn phí

Cơ sở dữ liệu	MySQL	Java J2EE, PostgreSQL, MySQL, MS SQL, Oracle
Hỗ trợ giao thức LDAP	Có	Có
Module	Perl	EJB
Trình duyệt hỗ trợ	Đa số	Đa số
Thành phần độc lập	Chỉ có thể quản trị PKI thông qua giao diện web	Có thể quản trị PKI thông qua giao diện web hoặc command line
Khả năng mở rộng	Khó mở rộng với độ phức tạp cao	Dễ dàng mở rộng

Bảng 1

Bảng 1. So sánh OpenCA và EJBCA

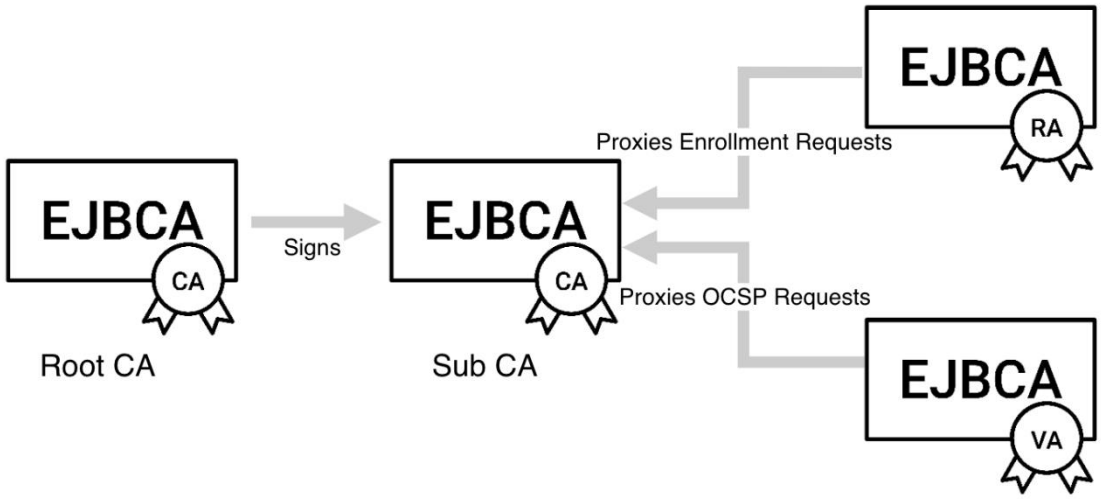
2.6. Kết chương

Qua nghiên cứu và thực nghiệm xây dựng chương trình, bản thân tôi thấy EJBCA là một trong những hệ thống PKI tiên tiến, hiệu quả trong giải quyết vấn đề chứng thực danh tính của hai hay nhiều thực thể trong quá trình liên lạc trên mạng Internet, điều này hứa hẹn sẽ đem lại hiệu quả cao hơn trong việc giải quyết vấn đề đặt ra.

Chương 3: HỆ THỐNG CHỨNG THỰC SỐ PKI SỬ DỤNG BỘ PHẦN MỀM MÃ NGUỒN MỞ EJBCA

3.1. Giới thiệu về bộ phần mềm mã nguồn mở EJBCA

EJBCA, viết tắt của cụm từ Enterprise Java Bean Certificate Authority, là một trong những nền tảng cơ sở hạ tầng khóa công khai (PKI) phổ biến nhất trên thế giới. EJBCA đáp ứng tất cả các nhu cầu của người dùng từ quản lý chứng chỉ, đăng ký và ghi danh đến xác thực chứng chỉ. Nó bao gồm tất cả các thành phần PKI cần thiết như Cơ quan cấp chứng chỉ (CA), Cơ quan đăng ký (RA) và Cơ quan xác thực (VA).



Hình 3.1 Cấu trúc hệ thống EJBCA

Dự án cộng đồng EJBCA là một dự án mã nguồn mở do Keyfactor tài trợ và có sẵn theo giấy phép LGPL v2.1. Điều này có nghĩa là nó có sẵn để tải xuống và sử dụng miễn phí dưới dạng bộ chứa Docker hoặc mã nguồn. Ngoài ra, EJBCA có sẵn dưới dạng phiên bản Doanh nghiệp và có bản dùng thử miễn phí 30 ngày trên AWS và Azure.

EJBCA độc lập với nền tảng và cung cấp tính linh hoạt cũng như khả năng mở rộng để hỗ trợ hầu hết mọi trường hợp sử dụng PKI bao gồm DevOps, Internet of Things (IoT), IoT trong công nghiệp, PKI doanh nghiệp, v.v... Cũng như tích hợp liền mạch vào các hệ thống của bên thứ ba để tự động hóa hoàn toàn và dễ vận hành. Nó là một hệ thống cho phép phục vụ nhiều khách hàng trong cùng một thời điểm và có

thể lưu trữ nhiều CA và PKI trong một lần cài đặt máy chủ. Các khách hàng có thể yên tâm vì hệ thống EJBCA có thể đảm bảo tính riêng tư, khách hàng này không thể truy cập vào dữ liệu của khách hàng khác.

Phần mềm này phổ biến đối với các kỹ sư vì tính mở, ổn định, linh hoạt và cung cấp hỗ trợ cho các dự án của họ từ việc tạo nguyên mẫu cho đến triển khai đầy đủ. Ví dụ như người sử dụng dễ dàng bắt đầu bằng cách sử dụng bộ chứa Docker. Và vì hầu hết các giao thức đăng ký PKI phổ biến, các định dạng chứng chỉ và nhiều mô hình triển khai đều có thể được sử dụng nên bạn có nền tảng cần thiết để cho phép dự án của mình phát triển theo thời gian.

Là một trong những dự án CA mã nguồn mở hoạt động lâu nhất, EJBCA PKI cung cấp độ tin cậy và độ bền đã được chứng minh qua thời gian. Phiên bản đầu tiên của EJBCA được phát hành vào năm 2001 bởi Tomas Gustavsson và các cộng sự với tham vọng tạo ra một PKI Doanh nghiệp, dựa trên công nghệ hiện đại, phổ biến rộng rãi. Năm 2002, PrimeKey được thành lập xung quanh EJBCA và bắt đầu với vai trò tư vấn về sản phẩm nguồn mở.

Kể từ đó, EJBCA đã phát triển để trở thành một trong những PKI được sử dụng rộng rãi nhất trên thế giới và hiện có sẵn dưới dạng phiên bản Doanh nghiệp được chứng nhận tiêu chí chung có thể được triển khai dưới dạng SaaS, đám mây hoặc phần mềm hoặc thiết bị phần cứng. Việc nâng cấp công nghệ liên tục đã được thực hiện đối với mã nguồn để giữ cho mã nguồn luôn hiện đại và phù hợp với thời đại đám mây hiệu suất cao. Đối với các tổ chức yêu cầu chức năng PKI nâng cao cũng như sự ổn định và hỗ trợ được đảm bảo, phiên bản EJBCA Enterprise là một lựa chọn tuyệt vời.

Kể từ tháng 6 năm 2021, PrimeKey trở thành một phần của Keyfactor và trong năm 2022, hai công ty đã hợp nhất dưới thương hiệu Keyfactor.

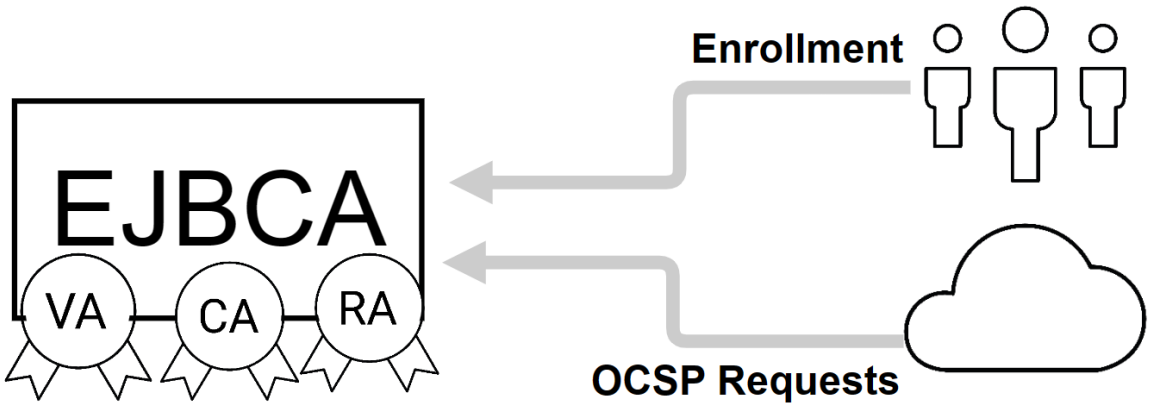
3.2. Kiến trúc của hệ thống PKI sử dụng EJBCA

Các phần sau đây phác thảo một danh sách các kiến trúc PKI phổ biến được triển khai và các khía cạnh khác của kiến trúc PKI tích hợp doanh nghiệp như quản

lý khóa, phân phối chứng chỉ, phân cụm và tính sẵn sàng cao. Có nhiều cách để có thể triển khai và kiến trúc một giải pháp PKI, từ đơn giản và chi phí thấp đến rất phức tạp và tốn kém. EJBCA cho phép triển khai hầu như bất kỳ loại kiến trúc PKI nào và các phần sau mô tả lựa chọn các kiến trúc PKI phổ biến được triển khai. Phần sau đây mô tả các cách khác nhau để thiết lập EJBCA như một phần của PKI.

3.2.1. Standalone CA/RA/VA

Một bản cài đặt EJBCA độc lập hoạt động như CA, RA và VA. EJBCA hỗ trợ nhiều bên thuê đầy đủ, do đó, nhiều phiên bản CA có thể nằm trong cùng một cài đặt. Bạn có thể triển khai một PKI hoàn chỉnh trong một môi trường duy nhất. Vì EJBCA có mọi thứ được tích hợp sẵn nên bạn có thể có một phiên bản duy nhất hoạt động như cả CA và RA. Đây là một giải pháp rất hiệu quả, dễ quản lý và tiết kiệm chi phí, phù hợp cho nhiều doanh nghiệp vừa và nhỏ triển khai.



Hình 3.2 Standalone CA/RA/VA

Nhiều CA tùy các trường hợp sử dụng khác nhau có thể cùng tồn tại trong một phiên bản duy nhất và các mức bảo mật có thể được điều chỉnh theo quy mô, ví dụ:

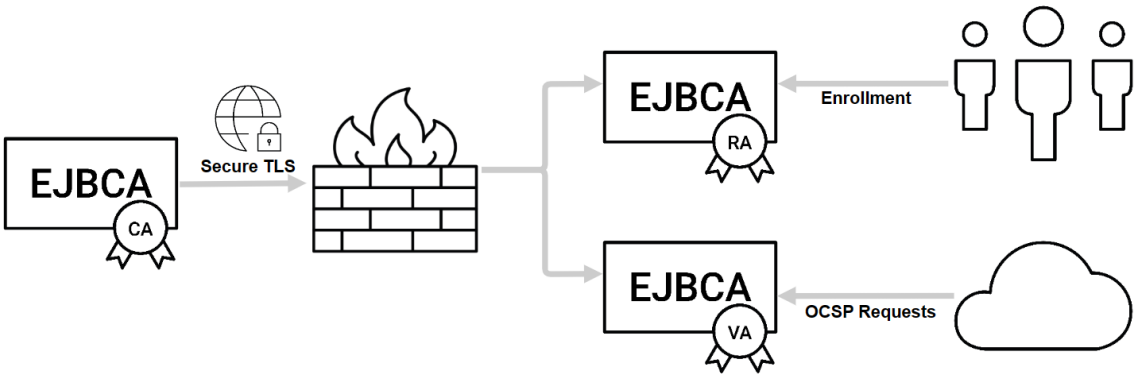
- Quản trị viên có thể sử dụng thẻ thông minh smart card hoặc token mềm để truy cập giao diện quản trị.
- CA có thể sử dụng HSM hoặc token mềm cho các khóa ký CA.
- Người dùng và máy có thể được cấp token mềm hoặc thẻ thông minh/USB token.

– Các tùy chọn lọc khác nhau có thể được triển khai trong tường lửa.

3.2.2. CA với các RA và/hoặc VA phân tán

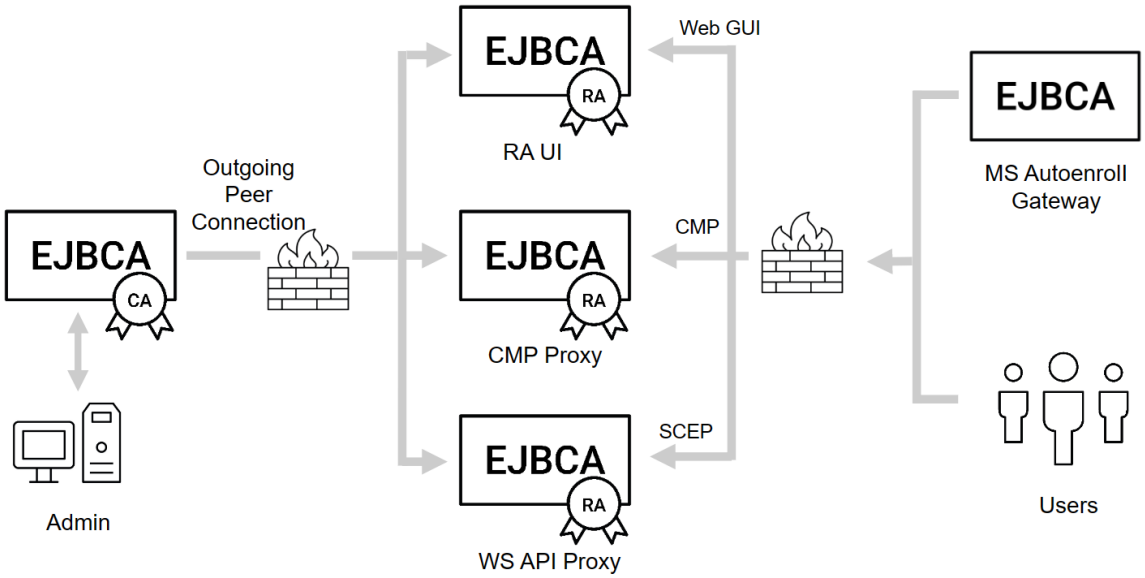
EJBCA có thể được thiết lập bằng cách sử dụng Giao thức ngang hàng của PrimeKey để giao tiếp với các phiên bản khác của EJBCA đóng vai trò là RA và/hoặc VA thay cho nó nhằm cải thiện hiệu suất và tăng cường bảo mật bằng cách có thể đặt CA phía sau tường lửa chỉ cho phép các kết nối gửi đi. Đây là tính năng chỉ có ở phiên bản Enterprise.

Để thiết lập một PKI có khả năng đăng ký một nhóm người dùng và thiết bị đa dạng, thông thường cần phải giới thiệu nhiều loại Cơ quan đăng ký (RA), cho các mục đích khác nhau.



Hình 3.3 CA được đặt phía sau tường lửa

Sử dụng EJBCA, bạn có thể kết nối vô số RA phân tán, giao tiếp với CA bằng các giao thức tiêu chuẩn như CMP, SCEP và dịch vụ Web. RA có thể ở dạng các thành phần EJBCA, RA được phát triển tùy chỉnh hoặc các sản phẩm tiêu chuẩn như MdM hoặc các sản phẩm quản lý mã thông báo. Các mức bảo mật có thể được tăng và giảm như trong ví dụ trước và RA có thể sử dụng các phương tiện xác thực khác nhau như bí mật được chia sẻ, xác thực chứng chỉ ứng dụng khách, v.v. CA sử dụng kiểm soát truy cập dựa trên vai trò để quyết định mỗi RA có quyền truy cập để thực hiện. Có thể dễ dàng cấu hình nhiều CA để phục vụ các mục đích khác nhau (VPN, MdM, TLS, v.v.).



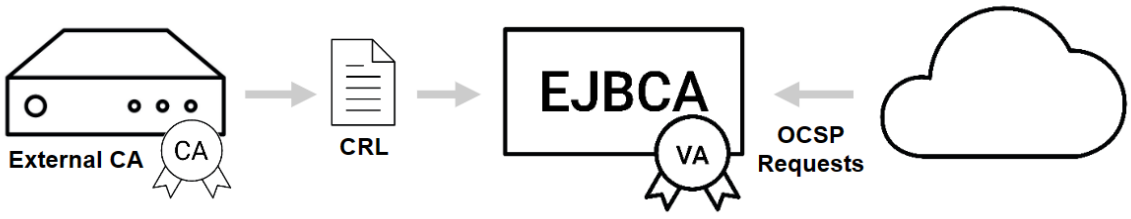
Hình 3.4 CA với các RA và/hoặc VA phân tán

Các giao thức khác nhau phù hợp cho hoạt động RA là:

- CMP
- EST
- Giao diện dịch vụ web
- API REST
- ACME
- SCEP

3.2.3. Standalone VA

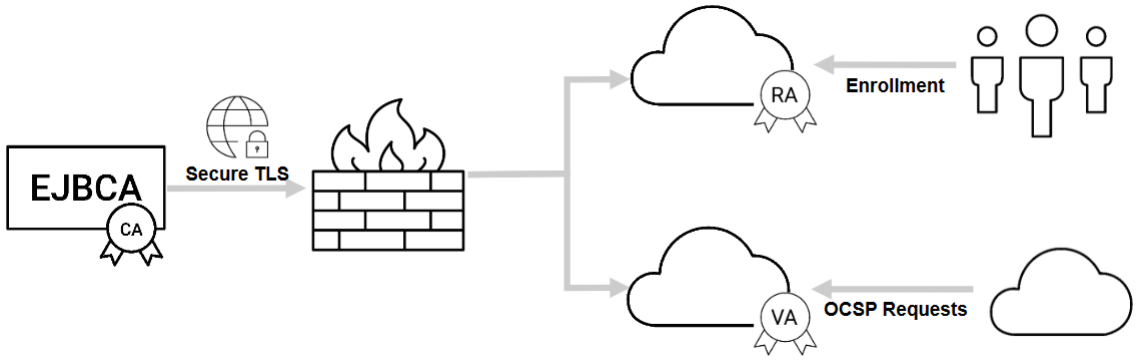
EJBCA có thể được triển khai như một VA độc lập phục vụ nhu cầu OCSP của các bản cài đặt không phải EJBCA bằng cách đọc CRL định kỳ.



Hình 3.5 Standalone VA

3.2.4. PKI lai với Public Cloud

EJBCA phù hợp để triển khai cài đặt trên dịch vụ đám mây hoặc trong môi trường đám mây kết hợp với cơ sở hạ tầng nội bộ. Một ví dụ điển hình là lưu trữ CA nhạy cảm trong nội bộ, đồng thời tận dụng các dịch vụ phân tán trên đám mây công cộng và tính linh hoạt cho cơ quan xác thực VA hoặc cơ quan đăng ký RA.



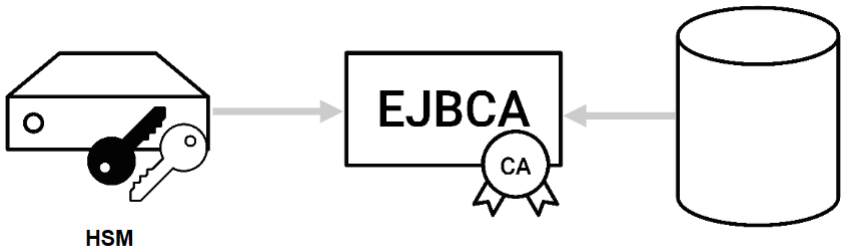
Hình 3.6 PKI lai với Public Cloud

Người dùng có thể tận dụng Phiên bản EJBCA Enterprise Cloud trong Amazon Web Services (AWS), để thiết lập các nút đám mây của mình.

3.3. Các khía cạnh khác cần lưu ý khi thiết kế hệ thống PKI

3.3.1. Quản lý khóa

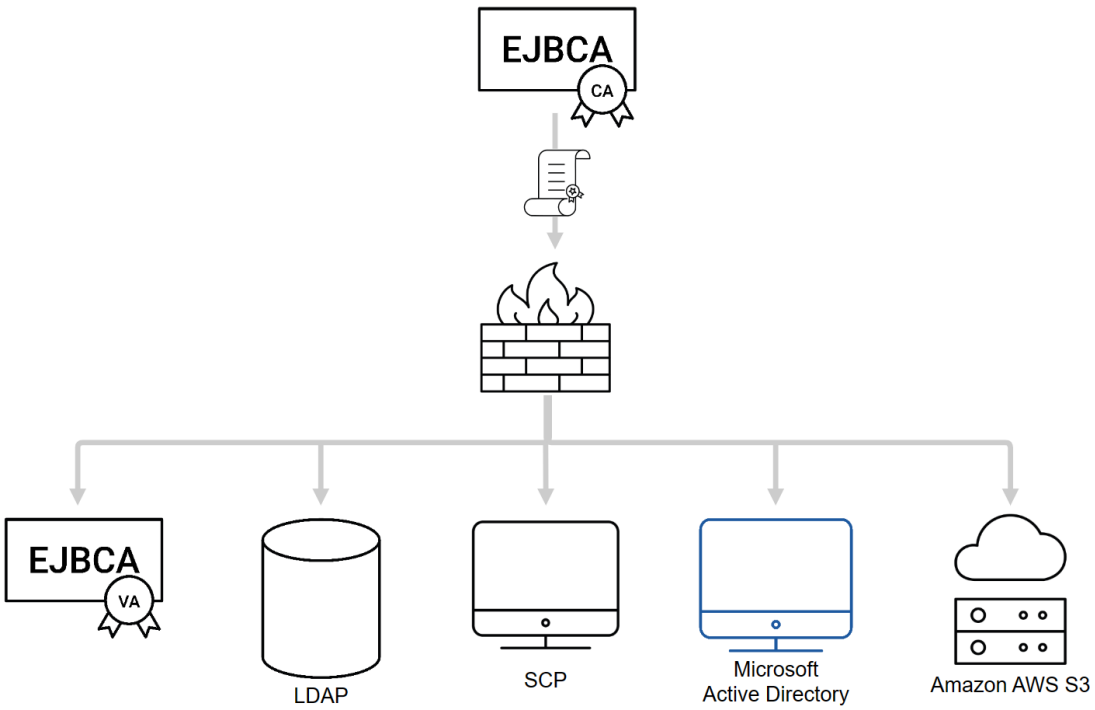
Đối với các cài đặt yêu cầu mức độ tin cậy và bảo mật nhất định, các khóa cần được lưu trữ trong Mô-đun bảo mật phần cứng (HSM).



Hình 3.7 Khóa được lưu trong module bảo mật

3.3.2. Phân phối chứng chỉ

Vì PKI thực sự là một cơ sở hạ tầng bảo mật nên nó cần được tích hợp phù hợp với nhu cầu bảo mật của tổ chức và tùy theo trường hợp sử dụng. Mỗi trường hợp sử dụng khác nhau và tổ chức khác nhau đều có nhu cầu đặc biệt của riêng họ, khiến cho việc tích hợp thực sự đa dạng. Một điểm tích hợp thường xuyên xảy ra là tích hợp với các thư mục hoặc cơ sở dữ liệu của công ty. EJBCA có thể xuất bản thông tin lên các thư mục, cơ sở dữ liệu hoặc các máy chủ khác, sử dụng vô số module xuất bản của nó.

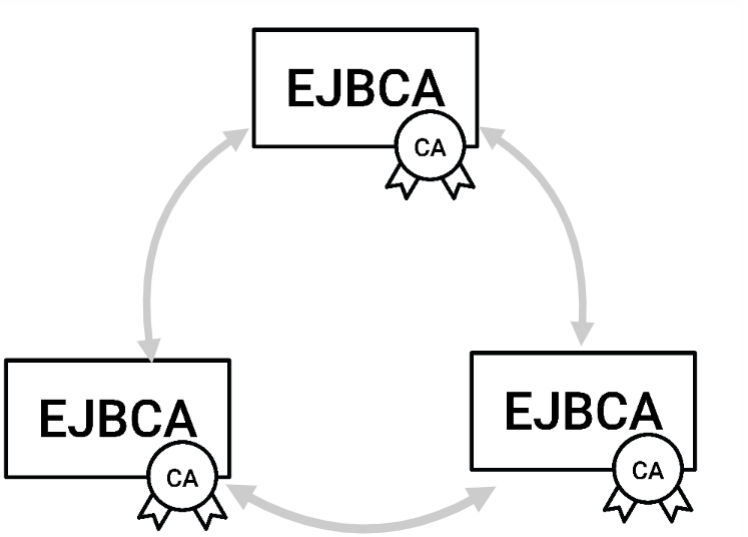


Hình 3.84 Phân phối chứng chỉ

3.3.3. Tính phân cụm và sẵn sàng cao

Cơ sở hạ tầng PKI càng trở nên quan trọng đối với nhiệm vụ thì càng đòi hỏi về tính sẵn sàng cao và tính phân cụm nhiều hơn. EJBCA bao gồm cả CA và VA có thể dễ dàng được nhóm lại để đảm bảo tính khả dụng và hiệu suất. Bản thân kiến trúc PKI không khác nhau dù có hoạt động theo nhóm hay không, tuy nhiên sẽ có nhiều máy chủ tham gia hơn. Có thể dễ dàng thiết lập phân cụm cho tính sẵn sàng cao và

khôi phục sau thảm họa bằng cách sử dụng công cụ PKI, như được mô tả trong bài đăng trên blog "Tính sẵn sàng cao cho PKI trong 8 bước đơn giản".



Hình 3.9 Các CA phân cụm

Để tăng cường kiến trúc trung tâm tin cậy được kiểm tra đầy đủ, bạn sẽ tách nhiều chức năng hơn thành các thành phần riêng biệt và giới thiệu nhiều quyền truy cập dựa trên vai trò hơn vào các phần khác nhau của hệ thống. Một số đặc điểm của một hệ thống như vậy là:

- Tách CA gốc và CA phát hành.
- Nhật ký kiểm tra đã ký, tổng hợp nhật ký được lưu trong các máy chủ nhật ký riêng biệt.
- Các phiên bản cơ sở dữ liệu riêng biệt, với nội dung cơ sở dữ liệu được bảo vệ toàn vẹn (tách biệt vai trò giữa các nhà khai thác DBA và CA).
- Cơ quan xác nhận VA riêng biệt.
- Các phân đoạn mạng riêng biệt cho tất cả các thành phần khác nhau.
- Giám sát và phát hiện xâm nhập.
- Tự động hóa và vận hành quy mô lớn.

Trong nhiều trường hợp sử dụng hiện đại (thường là IoT, Công nghiệp 4.0, v.v...), bạn thực sự muốn có các quy trình công nghiệp tự động, trong một số trường

hợp, tốc độ rất cao và khối lượng lớn. Tất cả các giao diện tích hợp có tên ở trên, CMP, dịch vụ Web và SCEP đều phù hợp với các hoạt động tự động. Trong EJBCA, bạn có thể định cấu hình vô số tùy chọn cho các cấp độ tự động hóa khác nhau, các chính sách và mô hình tin cậy khác nhau, v.v. Tìm các tùy chọn phù hợp, bạn có thể tích hợp với hầu hết mọi thứ, cấp chứng chỉ cho mọi thứ.

Vì EJBCA sử dụng cơ sở dữ liệu quan hệ tiêu chuẩn, phù hợp với quy mô lớn và hiệu suất cao nên bạn có thể dễ dàng mở rộng quy mô EJBCA thành hàng trăm triệu chứng chỉ được cấp và thậm chí hàng tỷ chứng chỉ đã được cấp. Tùy thuộc vào kiến trúc và giao diện đã chọn, bạn có thể đạt được độ trễ rất thấp (dưới 100 mili giây) và thông lượng rất cao (>100 certs/giây).

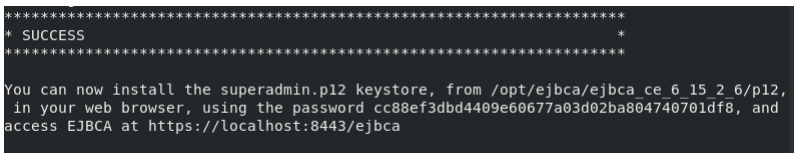
3.4. Mô hình triển khai

Hệ thống cần thiết:

- Máy ảo VMware chạy hệ điều hành CentOS 8.
- Máy chủ EJBCA server (phiên bản ejbca_ce_6_15_2_6) cài đặt theo mô hình Standalone CA/RA/VA.
- Các gói phần mềm cài đặt trên server: openjdk-8-jdk-devel, ant, psmisc, mariadb-server, java-1.8.0-openjdk-amd64.

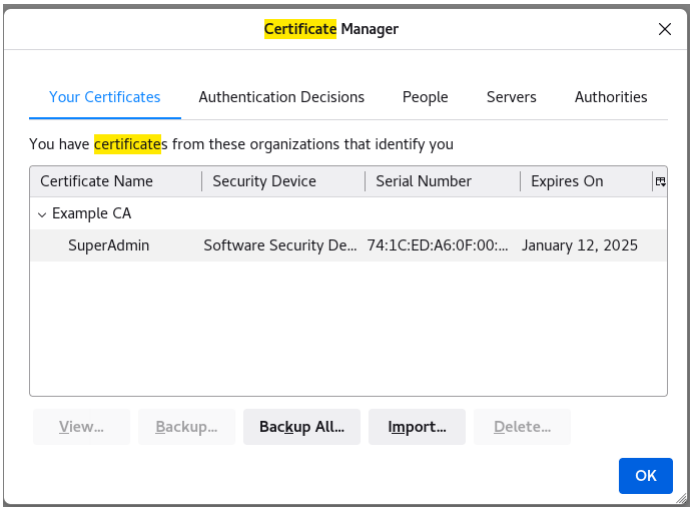
3.5. Cấu hình và sử dụng

Sau khi cài đặt xong phần mềm EJBCA trên CentOS sẽ có dòng thông báo như sau:



Hình 3.10 Cài đặt thành công EJBCA

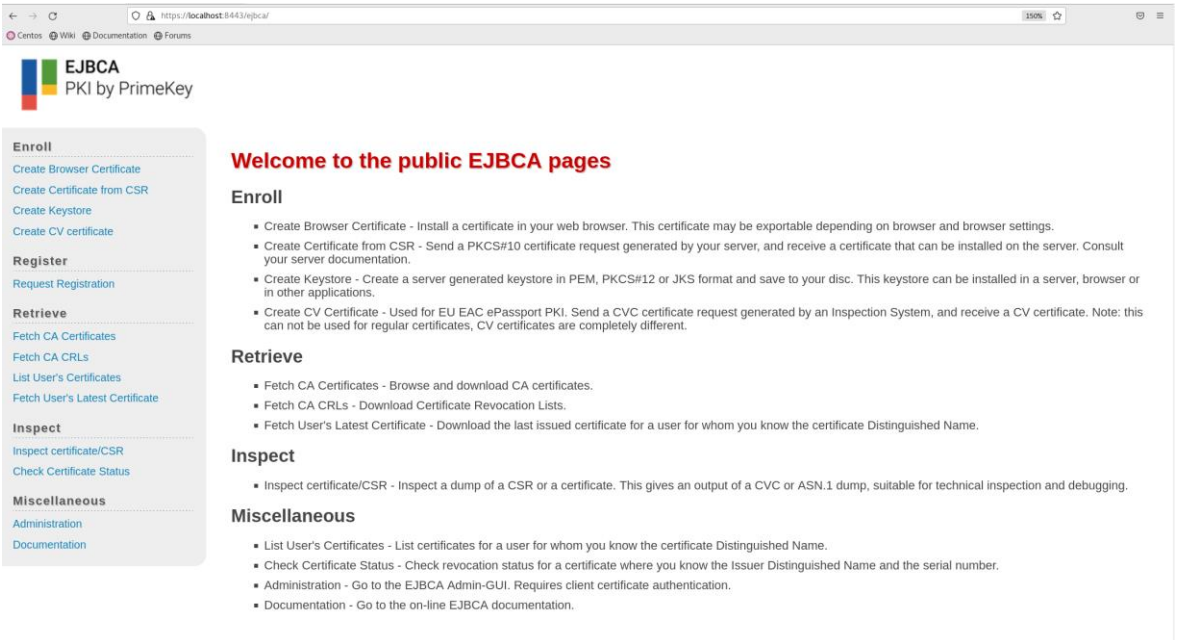
Mở trình duyệt firefox có sẵn trên CentOS 8, sau đó vào **Settings -> Certificates -> View Certificates**



Hình 3.11 Import chứng thư vào trình duyệt

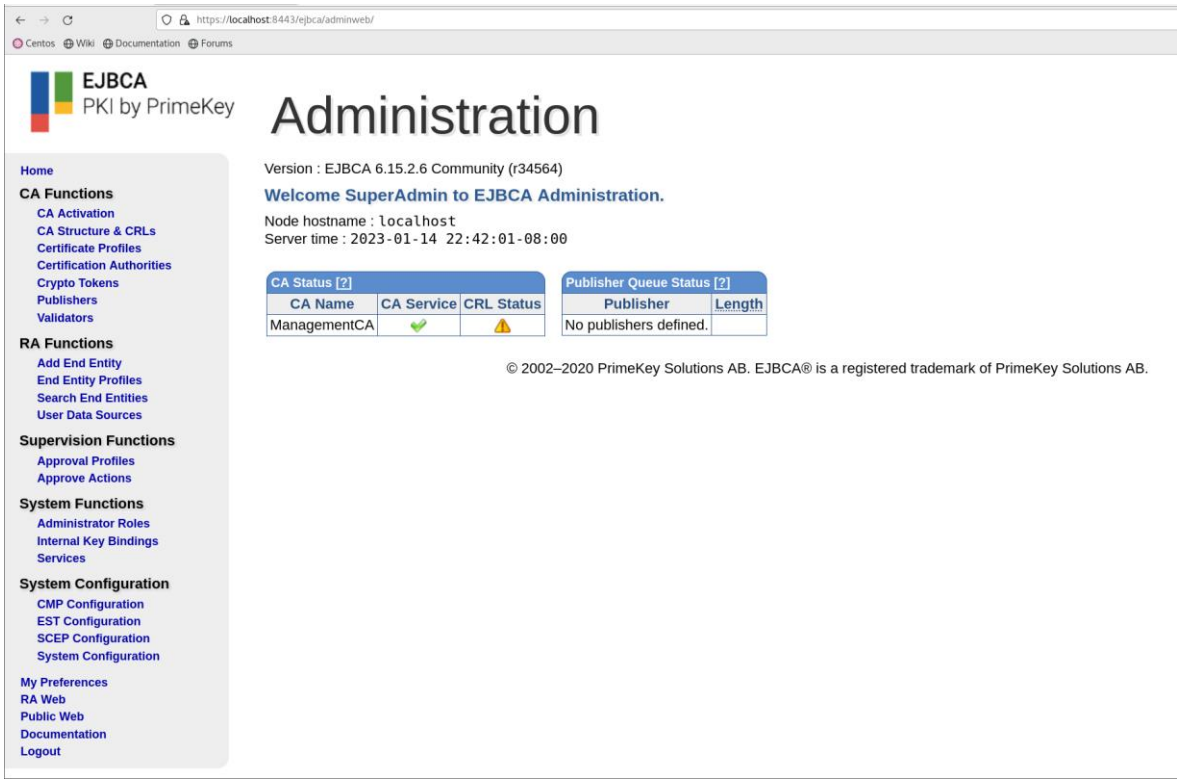
Tại đây, chọn **Import** rồi chọn file **superadmin.p12** tại thư mục ***/opt/ejbca/ejbca_ce_6_15_2_6/p12*** rồi chọn OK, sau đó truy cập vào giao diện quản trị web bằng đường dẫn: ***https://localhost:8443/ejbca***

*Lưu ý: nếu không thực hiện thao tác trên thì không thể truy cập vào giao diện web của EJBCA.



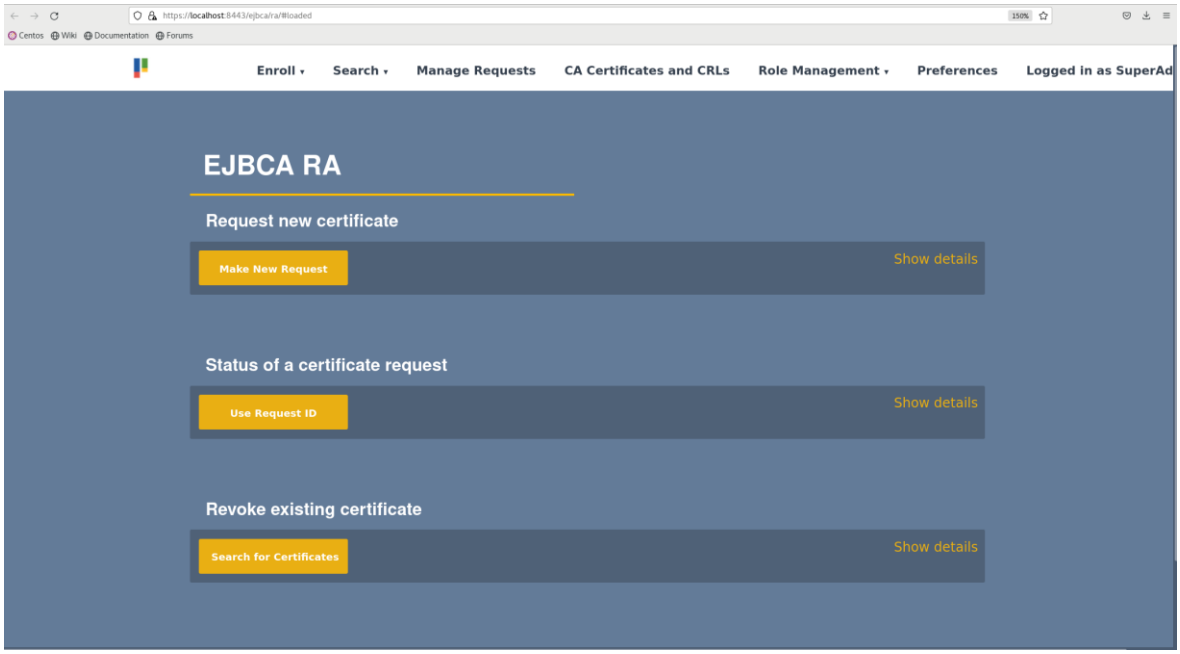
Hình 3.12 Giao diện của EJBCA

Để vào giao diện quản trị, chọn **Administration.**

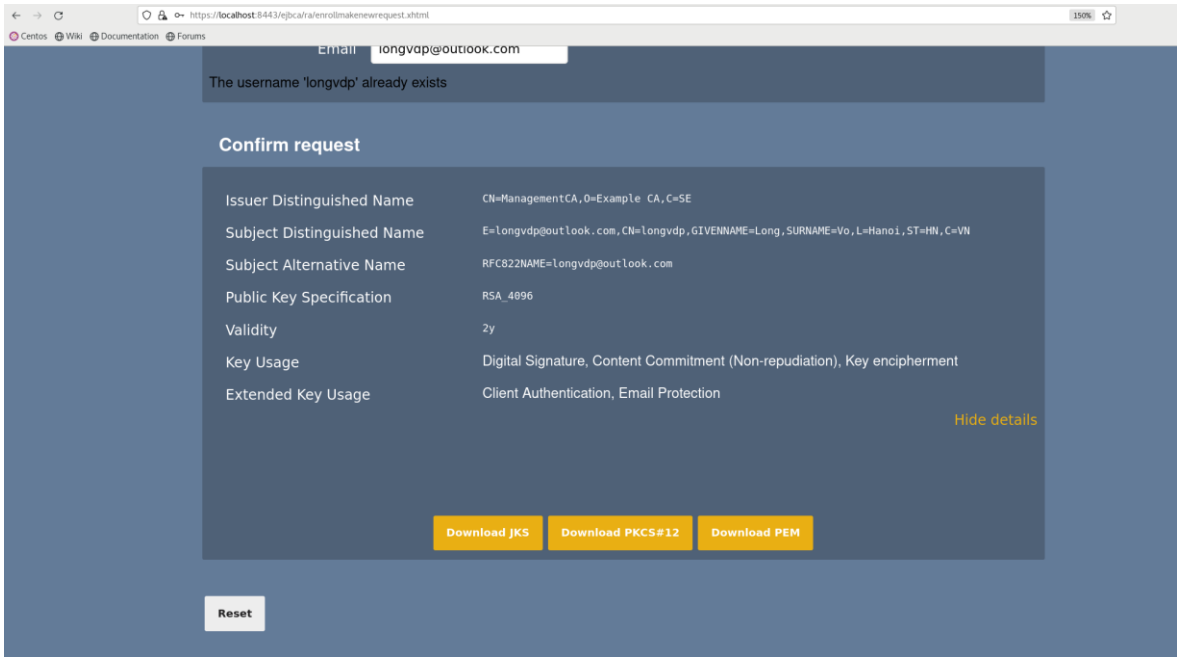


Hình 3.13 Giao diện quản trị của EJBCA

Để có thể tạo chứng chỉ p12, chọn **RA Web,** sau đó chọn **Make New Request.**



Hình 3.14 Giao diện đăng ký chứng thư



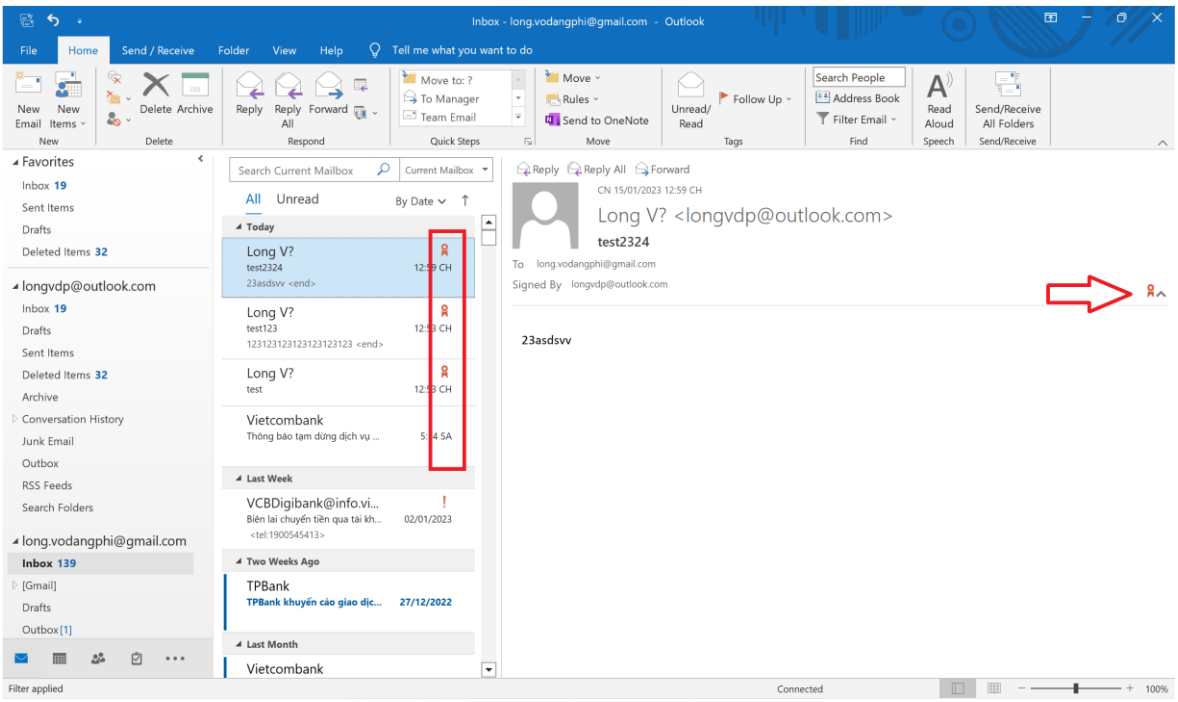
Hình 3.15 Xác nhận và tải chứng thư về

Tại đây, người quản trị có thể thiết lập các tham số cũng như thêm các thông tin về chứng thư chuẩn bị được cấp. Sau khi nhập đầy đủ thông tin, người quản trị có thể xuất file chứng thư dưới dạng JKS, PKCS#12 (p12) hoặc PEM.

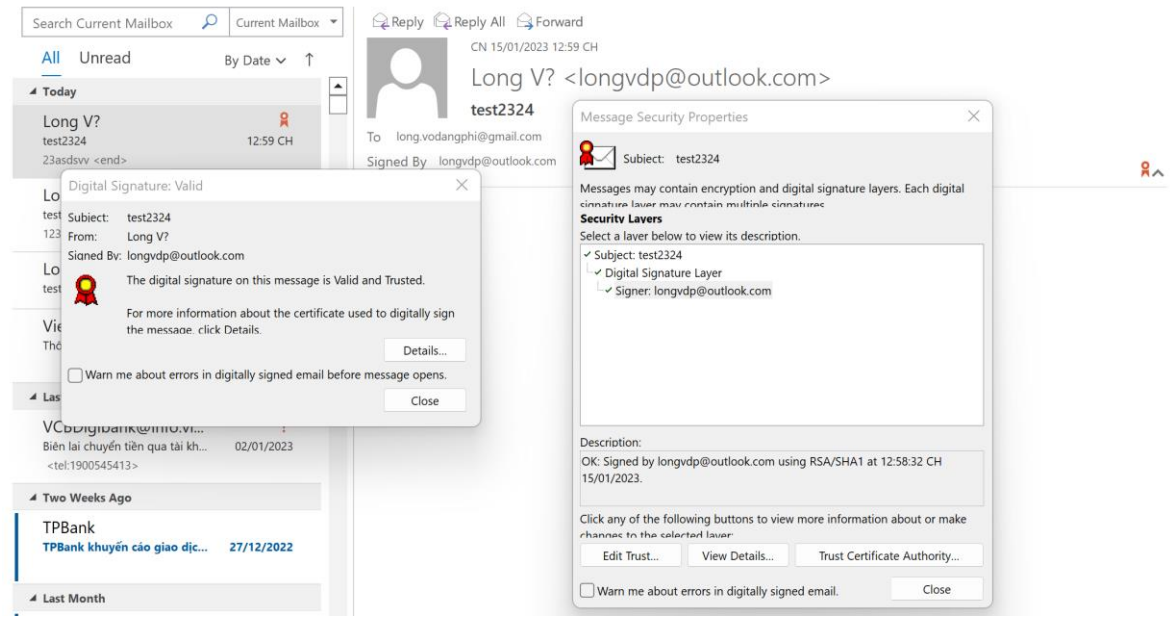
3.6. Kịch bản ứng dụng vào thực tiễn

Cấp chứng chỉ cho người dùng để người dùng có thể ký thư điện tử trong ứng dụng Microsoft Outlook. Tại giao diện của Microsoft Outlook, chọn **File -> Options -> Trust Center -> Email Security -> Import/Export.** Sau đó chọn file p12 mới sinh ra và nhập mật khẩu rồi import.

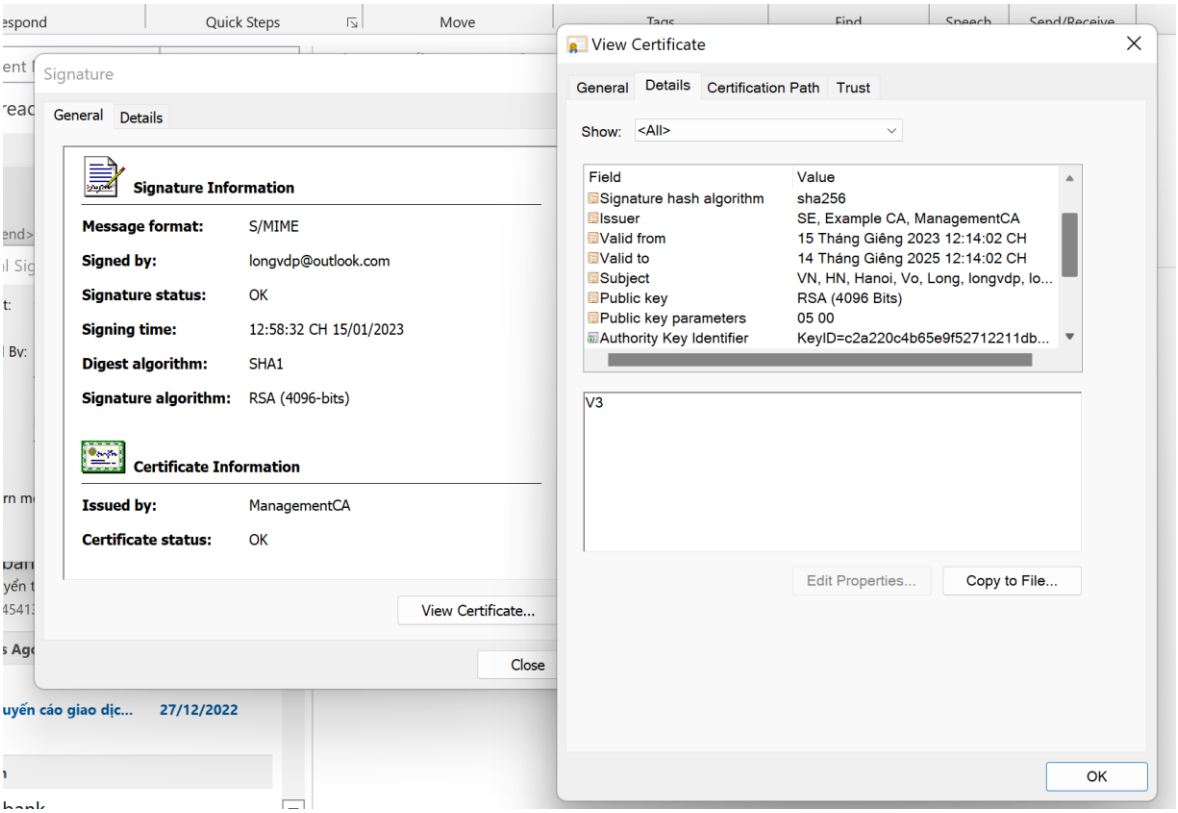
Lần tiếp theo, thư gửi từ địa chỉ email này sẽ được gán nhãn đã ký số điện tử như hình dưới. Người dùng có thể click vào nhãn dán ở góc bên phải của tiêu đề email để có thể xem được thông tin về chữ ký số gắn với email đã gửi.



Hình 3.16 Email sau khi được thêm chứng thư có nhãn dán đặc biệt



Hình 3.17 Thông tin về chứng thư đã ký vào email



Hình 3.18 Thông tin chi tiết hơn về chứng thư

Người dùng cũng có thể ký và mã file văn bản đính kèm theo thư.

Kết quả thử nghiệm: Email đã được mã hóa và ký số từ Microsoft Outlook sau khi gửi đi chỉ có người nhận có chứng chỉ số được cung cấp từ cùng hệ thống EJBCA mới có thể đọc được nội dung thư. Người nhận có thể kiểm tra được tính xác thực của người gửi cũng như tính toàn vẹn của email nhờ chữ ký số.

So sánh giữa email gốc với email đã mã hóa/ký số:

Nội dung	**Thư chưa mã hóa/ký số**	**Thư đã mã hóa/ký số**
Thời gian truyền tải	56 giây	62 giây
Dung lượng	19.901 KB	20.521 KB
Tính bảo mật	Không	Có (đã mã hóa nội dung bằng thuật toán RSA-4096, hàm băm SHA-256)
Tính toàn vẹn	Không	Có (đã được ký số đảm bảo sự toàn vẹn của nội dung)
Tính xác thực	Không	Có (đã được ký số xác thực danh tính người gửi)

3.7. Kết chương

Từ kết quả thực nghiệm trên ta có thể thấy, hệ thống chứng thực số PKI sử dụng bộ phần mềm mã nguồn mở EJBCA hoàn toàn có thể triển khai một hệ thống PKI đầy đủ, hoàn chỉnh chức năng. Cụ thể:

Ưu điểm và hạn chế:

Hệ thống này đáp ứng đầy đủ các tiêu chí cần thiết của một hệ thống PKI như tính bảo mật, tính toàn vẹn, tính xác thực và tính chống chối bỏ để đem lại một môi trường truyền tin an toàn, tin cậy thông qua internet.

Tuy nhiên, bên cạnh những kết quả đã đạt được thì nội dung kết quả thực nghiệm chưa thể hiện hết được toàn bộ các chức năng của hệ thống cũng như các mô hình triển khai theo kiến trúc khác.

Đối tượng áp dụng phù hợp:

EJBCA là một hệ thống phức tạp, tuy nhiên trong thực nghiệm đã sử dụng bản cài đặt EJBCA độc lập hoạt động đã tích hợp sẵn cả CA, RA và VA. Bản EJBCA Standalone này hỗ trợ nhiều bên thuê đầy đủ do đó có thể triển khai một PKI hoàn chỉnh trong một môi trường duy nhất. Đây là một giải pháp rất hiệu quả, dễ quản lý và tiết kiệm chi phí, phù hợp cho nhiều doanh nghiệp vừa và nhỏ triển khai.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN TIẾP

Mặc dù hiện nay nhiều giải pháp cung cấp hệ thống PKI đã ra đời, đạt được hiệu quả, hiệu suất cao, nhưng EJBCA vẫn là một hệ thống nổi bật được tin cậy trên toàn thế giới. PKI là một hệ thống tương đối phức tạp, việc nắm vững và sử dụng thành thạo PKI đòi hỏi một tập thể lớn với nhiều thời gian và công sức. Qua những gì đã trình bày ở trên, đề tài đã đưa ra một cái nhìn tổng quát về vấn đề an toàn trong hệ thống thông tin, cơ sở hạ tầng khóa công khai PKI cũng như các mục tiêu và chức năng của nó. Đồng thời, đề tài cũng đã trình bày được các vấn đề cơ bản về hệ thống chứng thực số PKI sử dụng bộ phần mềm mã nguồn mở EJBCA như cách cài đặt, cấu hình, sinh và áp dụng chứng thư số vào thực tế. Từ đó có thể thấy rằng, việc ứng dụng những đặc tính ưu việt của hệ thống này là điều khả thi, góp phần phục vụ hiệu quả nhu cầu thực tế của của các cá nhân cũng như tổ chức.

Trong phạm vi nghiên cứu, luận văn đã trình bày về hệ thống EJBCA được xây dựng dựa trên cơ sở hạ tầng khóa công khai PKI. Từ đó xây dựng hệ thống EJBCA cung cấp chứng thư số, có khả năng đảm bảo tính xác thực, toàn vẹn, bảo mật của email được truyền đi qua mạng internet.

Bám sát mục tiêu, nhiệm vụ, sử dụng đúng đắn các phương pháp nghiên cứu khoa học, luận văn đã thu được một số thành công và về cơ bản đã đạt được mục tiêu, nhiệm vụ đặt ra. Trong tương lai, để cải thiện hiệu suất của hệ thống, luận văn định hướng mở rộng nghiên cứu về các mô hình triển khai khác của hệ thống; đồng thời, cần xem xét, nghiên cứu những ứng dụng khác của hệ thống như khả năng ký số các loại văn bản, tài liệu dưới dạng file doc, pdf hay các file thực thi để chứng thực các file đó. Mã hóa thông tin để đảm bảo bí mật với các thực thể khác, thực hiện các kênh liên lạc trao đổi thông tin mật giữa các thực thể khác nhau trên mạng.

Hướng phát triển tiếp: có thể áp dụng mô hình vào thực tế nhiều hơn chứ không phải chỉ dừng lại ở mức lý thuyết. Chúng ta có thể triển khai thử nghiệm một hệ thống chứng thực tập trung theo kiến trúc PKI phân cấp đơn giản có thể sử dụng ngay trong thực tế. Hệ thống được triển khai này mang lại đầy đủ các tính chất cần thiết nhằm thiết lập môi trường an toàn, tin cậy để giao tiếp với các đặc tính như tính bảo mật,

tính toàn vẹn, tính xác thực và tính không thể chối bỏ. Hơn nữa, hệ thống còn có khả năng mở rộng, tích hợp với nhiều hệ thống khác một cách dễ dàng.

Luận văn là công trình nghiên cứu công phu, nghiêm túc, song do PKI nói chung và EJBCA nói riêng là một hệ thống lớn và phức tạp, phạm vi nghiên cứu rộng, cộng thêm những khó khăn khách quan, cũng như kiến thức còn hạn chế nên chắc chắn còn nhiều khiếm khuyết. Rất mong nhận được sự quan tâm, góp ý của các nhà khoa học, nhà hoạt động thực tiễn và đồng nghiệp. Cuối cùng, xin chân thành cảm ơn các đơn vị liên quan, các đồng chí, đồng nghiệp, các thầy cô trong học viện, đặc biệt là thầy hướng dẫn khoa học đã tận tình giúp đỡ để hoàn thành luận văn này./.

TÀI LIỆU THAM KHẢO

[1] A. Woodbury, “Increasing Medication Safety with Deep Learning Image Recognition,” RxVision, 2020.

[2] Arpan Kumar, Anamika Tiwari , “A Comparative Study of Otsu Thresholding and K-means Algorithm of Image Segmentation,” International Journal of Engineering and Technical Research (IJETR), tập 9, số 5, p. 1, 2019.

[3] Chen, J. Yu and Z., “Accurate system for automatic pill recognition using imprint information,” IET Image Process., tập 9, 2015.

[4] Gershenson, Carlos, “Artificial Neural Networks for Beginners,” 2003.

[5] Girshick, Ross, “Fast r-cnn.,” tập 10.1109/ICCV.2015.169. , 2015.

[6] H. Bandyopadhyay, “An Introduction to Image Segmentation: Deep Learning vs...

[7] J.S. Wang, A. Ambikapathi, Y. Han, S.L. Chung, H.W. Ting and C.F. Chen, “Highlighted deep learning based identification of pharmaceutical blister packages,” IEEE 23rd Int. Conf. on Emerging Technologies and Factory Automation (ETFA), Turin, 2018.

[8] K V, Lalitha & .R, Amrutha & Michahial, Stafford , “Implementation of Watershed Segmentation,” IJARCCE, tập 5, số 10.17148/IJARCCE.2016.51243. , pp. 196-199, 2016.

[9] Kapil G Zirpe, Bhavika Seta, Sharvari Gholap, “Incidence of Medication Error in Critical Care Unit of a Tertiary Care Hospital: Where Do We Stand?,” PMC, 2020.

[10] Maier, Andreas & Syben, Christopher & Lasser, Tobias & Riess, Christian, “A Gentle Introduction to Image Segmentation for Machine Learning,” A gentle introduction to deep learning in medical image processing. Zeitschrift für Medizinische Physik., tập 29, số 10.1016/j.zemedi.2018.12.003. , 2021.

[11] M.A.V. Neto, J.W.M. de Souza, P.P. Reboucas Filho and W.D.O. Antonio, “CoforDes: An invariant feature extractor for the drug pill identification,” IEEE 31st Int. Symp. on Computer-Based Medical Systems (CBMS), Karlstad, 2018.

[12] M.A.V. Neto, J.W.M. de Souza, P.P. Reboucas Filho and W.D.O. Antonio, “CoforDes: An invariant feature extractor for the drug pill identification,” IEEE 31st Int. Symp. on Computer-Based Medical Systems (CBMS), Karlstad, 2018.

[13] Michielan, Lisa & Terfloth, Lothar & Gasteiger, Johann & Moro, Stefano, “Comparison of Multilabel and Single-Label Classification Applied to the Prediction of the Isoform Specificity of Cytochrome P450 Substrates.,” Journal of chemical information and modeling, tập 49. 10.1021/ci900299a., pp. 2588-605, 2009.

[14] N. Barla, “The Complete Guide to Panoptic Segmentation,” PerceptronAI, https://www.v7labs.com/blog/panoptic-segmentation-guide, 2022.

[15] N. Usuyama, L. Naoto, “ePillID Dataset: A Low-Shot Fine-Grained Benchmark for Pill Identification,” arXiv, 2020

[16] Hyuk-Ju Kwon, Hwi-Gang Kim, Sung-Hak Lee, “Pill Detection Model for Medicine Inspection Based on Deep Learning,” *chemosensors - MDPI*, 2021.

[17] K V, Lalitha & .R, Amrutha & Michahial, Stafford , “Implementation of Watershed Segmentation,” *IJARCCE,* tập 5, số 10.17148/IJARCCE.2016.51243. , pp. 196-199, 2016.

[20] N. Usuyama, L. Naoto, “ePillID Dataset: A Low-Shot Fine-Grained Benchmark for Pill Identification,” *arXiv,* 2020.

[21] Olaf Ronneberger, Philipp Fischer, Thomas Brox, “U-Net: Convolutional Networks for Biomedical Image Segmentation,” MICCAI, 2015.

[22] Radhamadhab Dalai, Kishore Kumar Senapati, “Comparison of Various RCNN techniques for Classification of Object from Image,” International

Research Journal of Engineering and Technology (IRJET), tập 04, số 07, 2017.

[23] Shaoqing Ren, Kaiming He, Ross Girshick, and Jian Sun, “Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks,” arXiv, 2016.

[24] Suiyi Ling et al, “Few-Shot Pill Recognition,” IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) , tập doi: 10.1109/CVPR42600.2020.00981, pp. 9786-9795, 2020.

[25] S. Prasad, “analytixlabs,” 2022. [Trực tuyến]. Available: https://www.analytixlabs.co.in/blog/what-is-image-segmentation/. [Đã truy cập 2022].

[26] S. Tangwattananuwat, “The Identification of Pill Images Using Convolutional,” 2020.

[27] Tariq, Rayhan A.; Vashisht, Rishik; Sinha, Ankur; Scherbak, Yevgeniya, “Medication Dispensing Errors And Prevention,” NCBI, 01/2021.

[28] Wong, Y. F. et al., “Development of fine-grained pill identification algorithm using deep convolutional network,” J. Biomed. Inform. 74, 2017.

[29] World Health Organization, Medication Errors, ISBN 978-92-4-151164-3, 2016.

PHỤ LỤC
CÀI ĐẶT EJBCA TRÊN HỆ ĐIỀU HÀNH CENTOS 8

Cài đặt các gói phần mềm bổ trợ:

$ sudo yum install -y nano tar unzip java-1.8.0-openjdk-devel ant psmisc mariadb bc patch

Cài đặt MariaDB:

$ sudo yum install -y mariadb-server

$ sudo systemctl enable --now mariadb

Tạo password cho root user MariaDB:

$ sudo mysql_secure_installation

Tạo database, user database mới:

$ sudo mysql -u root -p

mysql> CREATE DATABASE ejbcatest CHARACTER SET utf8 COLLATE utf8_general_ci;

mysql> GRANT ALL PRIVILEGES ON ejbcatest. TO 'ejbca'@'localhost' IDENTIFIED BY 'ejbca';*

mysql> exit

Tiến hành cài đặt hệ thống EJBCA:

$ sudo useradd -m -U -r -d /opt/ejbca ejbca

$ passwd ejbca

$ sudo usermod -aG wheel ejbca

$ sudo su - ejbca

$ cd

Tải bản nén của EJBCA về rồi giải nén:

$ wget https://netcologne.dl.sourceforge.net/project/ejbca/ejbca6/ejbca_6_15_2_6/ejbca_ce_6_15_2_6.zip

$ unzip ejbca_ce_6_15_2_6.zip

Khởi chạy cài đặt EJBCA bằng shell script:

$ ./ejbca_ce_6_15_2_6/bin/extra/ejbca-setup.sh

Tinh chỉnh các cổng trên tường lửa:

$ sudo firewall-cmd --add-port=8443/tcp --permanent

$ sudo firewall-cmd --add-port=8442/tcp --permanent

$ sudo firewall-cmd --add-port=8080/tcp --permanent

$ sudo firewall-cmd –reload

Tạo file dịch vụ ejbca.service với nội dung bên dưới:

$ sudo nano /etc/systemd/system/ejbca.service

[Unit]

Description=EJBCA Server Daemon

After=network-online.target

[Service]

Type=simple

User=ejbca

Group=ejbca

UMask=007

WorkingDirectory=/opt/ejbca

ExecStart=/opt/ejbca/wildfly/bin/standalone.sh -b 0.0.0.0

ExecReload=/opt/ejbca/wildfly/bin/jboss-cli.sh --connect :reload

```
ExecStop=/opt/ejbca/wildfly/bin/jboss-cli.sh --connect :shutdown
Restart=on-failure
TimeoutStopSec=300
[Install]
WantedBy=multi-user.target
```

Khởi động lại tiến trình hệ thống để thay đổi có thể hoạt động:

$ sudo systemctl daemon-reload

$ sudo systemctl enable --now ejbca

Chạy lệnh dưới để xem trạng thái của chương trình EJBCA. Nếu status là running có màu xanh lá có nghĩa là dịch vụ đang hoạt động.

$ systemctl status ejbca