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

TÓM TẮT LUẬN VĂN THẠC SỸ

(Theo định hướng ứng dụng)

Hà Nội – 2023

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: PGS.TSKH HOÀNG VĂN HẢI

Phản biện 1: TS Vũ Văn Thoả

Phản biện 2: PGS.TS Đỗ Trung Tuấn

Luận văn này được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 09 giờ 00 ngày 17 tháng 02 năm 2023

Có thể tìm hiểu luận văn này tại:

Thư viện của Học viện Công nghệ Bưu chính Viễn thông

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

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.

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. 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

- 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.

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.

1.3. Tạo lập môi trường an ninh

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.

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.

1.3.3. Bảo mật

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.

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.

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.

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.

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.

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.

1.4.4. Chữ ký số

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.

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.

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.

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.

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.

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).

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

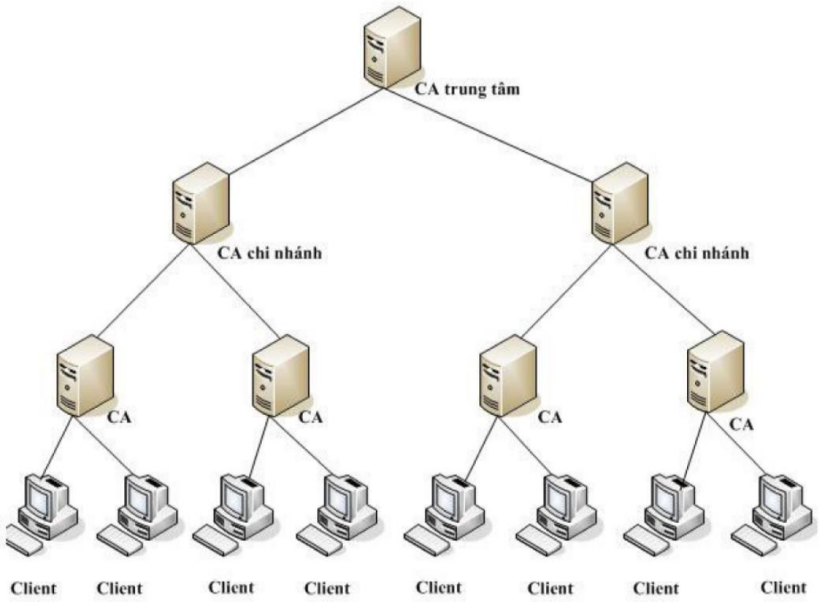
Hạ tầng khóa công khai PKI (Public Key Infrastructure) là một thuật ngữ dùng để mô tả một hệ thống hoàn thiện của một tập hợp các vai trò, chính sách, quy tắc, phần cứng, phần mềm và quy trình cần thiết để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi chứng chỉ kỹ thuật số cũng như quản lý mã hóa công khai.

2.2. Kiến trúc và chức năng của PKI

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. Một PKI bao gồm:

- Cơ quan cấp chứng chỉ (CA)
- Cơ quan đăng ký (RA
- Một thư mục trung tâm
- Một hệ thống quản lý chứng chỉ
- Chính sách về chứng chỉ
- Cơ quan xác thực bên thứ ba (VA)

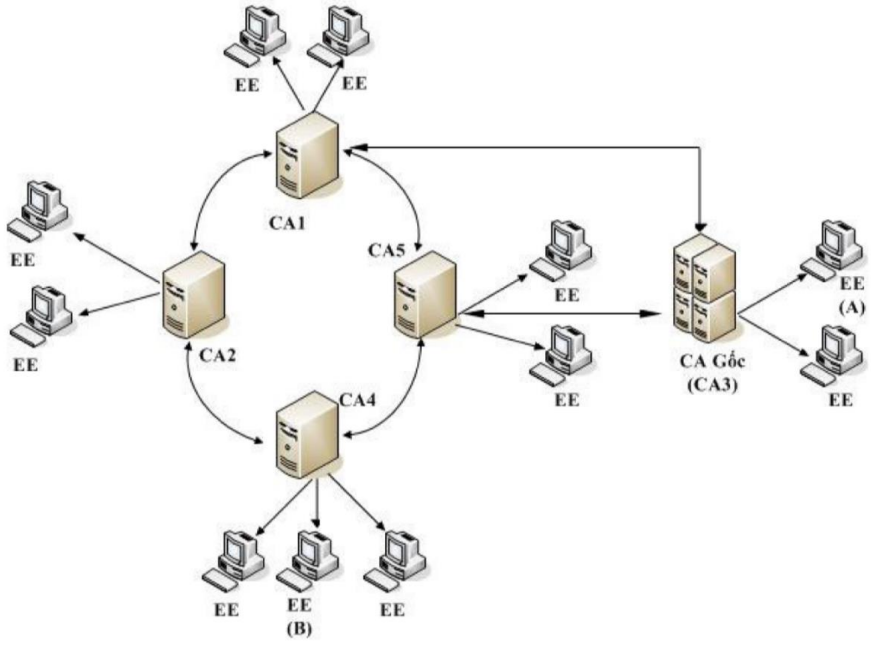
2.2.1. Mô hình phân cấp



Hình 1 Mô hình phân cấp

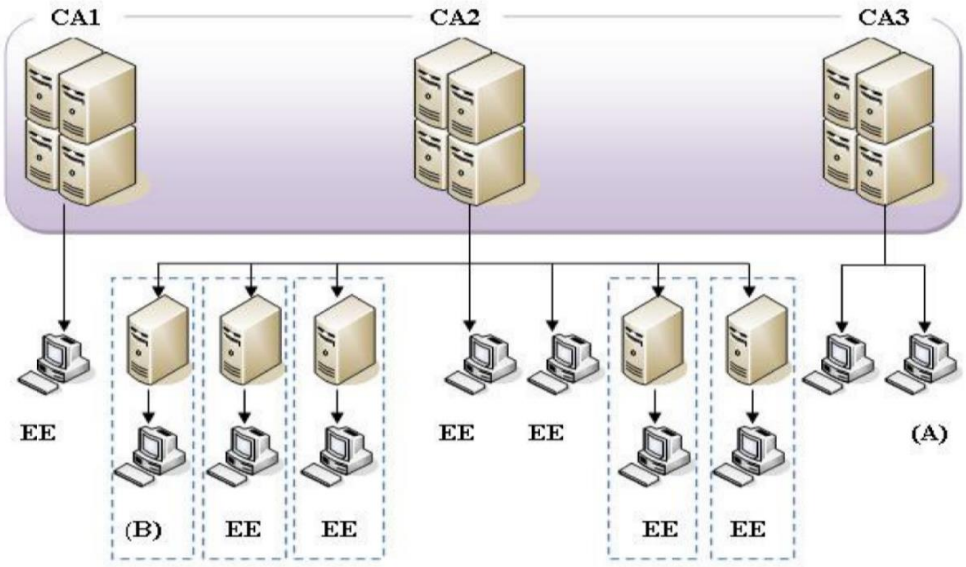
Đây là mô hình được sử dụng phổ biến rộng rãi nhất hiện nay.

2.2.2. Mô hình mạng lưới



Hình 2 Mô hình mạng lưới

2.2.3. Mô hình danh sách tin cậy



Hình 3 Mô hình danh sách tin cậy

2.3. Ưu điểm và nhược điểm của PKI

Hạ tầng khóa công khai PKI có một số ưu điểm như sau: Tính không từ chối, hiệu quả về chi phí, mức độ bảo mật cao, được các chính phủ chấp nhận. Cùng với các ưu điểm của PKI thì hạ tầng này cũng có một số nhược điểm như sau: Chi phí triển khai cao, chi phí phát sinh, cần đội ngũ quản trị viên được đào tạo bài bản.

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.

2.4.2. EJBCA

EJBCA là một hệ thống CA mã nguồn mở được phát triển bằng Java.

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.

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.

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.

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.

2.5. So sánh đặc điểm giữa 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.

3.2. Kiến trúc của hệ thống PKI sử dụng EJBCA

3.2.1. Standalone CA/RA/VA

Một bản cài đặt EJBCA độc lập hoạt động như CA, RA và VA.

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.

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.

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.

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).

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.

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.

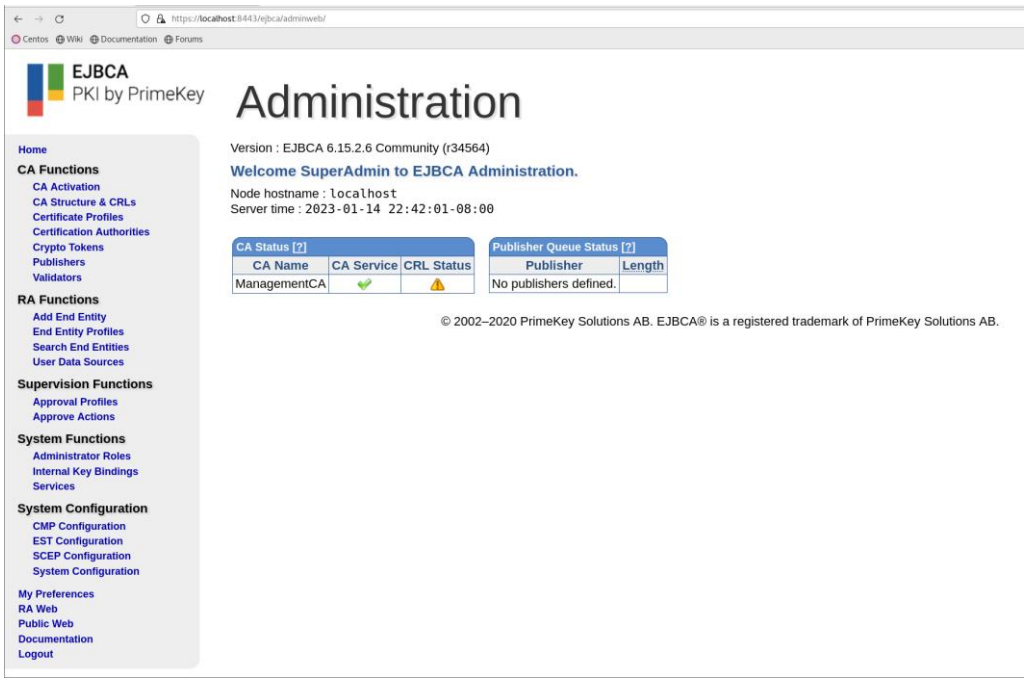
3.4. Mô hình triển khai

- 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

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

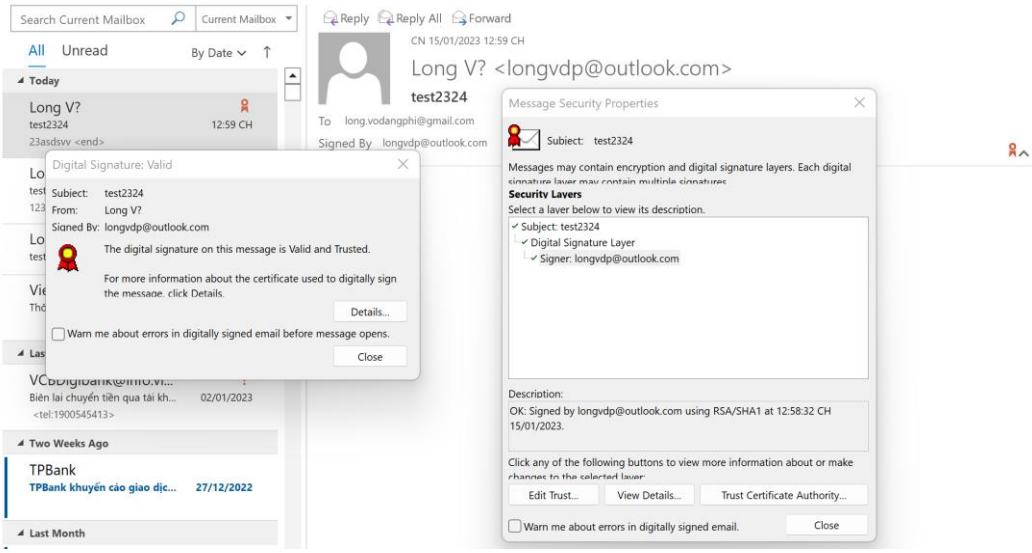
Tại đây, chọn **Import** rồi chọn file **superadmin.p12** tại thư mục ***/opt/ejbca/ejbca_ce_6_15_2_6/p12*** rồi chọn OK, sau đó truy cập vào giao diện quản trị web bằng đường dẫn: ***https://localhost:8443/ejbca***



Hình 4 Giao diện quản trị của EJBCA

3.6. Kịch bản ứng dụng vào thực tiễn

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 5 Thông tin về chứng thư đã ký vào email

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

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./