

**ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**LÊ THỊ THU HUYỀN**

**NGHIÊN CỨU, TÌM HIỂU VỀ HỆ THỐNG  
CHỨNG THỰC SỐ VÀ ỨNG DỤNG**

**LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN**

**Hà Nội – 2016**

**ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**LÊ THỊ THU HUYỀN**

**NGHIÊN CỨU, TÌM HIỂU VỀ HỆ THỐNG  
CHỨNG THỰC SỐ VÀ ỨNG DỤNG**

Ngành: Công nghệ thông tin

Chuyên ngành: Hệ thống thông tin

Mã số:60480104

**LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN**

**NGƯỜI HƯỚNG DẪN KHOA HỌC CHÍNH  
TS. HỒ VĂN HƯƠNG**

**NGƯỜI HƯỚNG DẪN KHOA HỌC PHỤ  
TS. NGUYỄN VIỆT THỂ**

**Hà Nội – 2016**

## MỤC LỤC

DANH MỤC CÁC KÝ HIỆU VÀ TỪ VIẾT TẮT .....	4
MỞ ĐẦU .....	5
CHƯƠNG I TỔNG QUAN MẬT MÃ HỌC.....	6
1.1. Mật mã khóa bí mật .....	6
1.1.1. Giới thiệu về mật mã khóa bí mật và các khái niệm có liên quan.....	6
1.1.2. Một vài thuật toán sử dụng trong mật mã khóa đối xứng.....	6
1.2. Mật mã khóa công khai.....	6
1.2.1. Khái niệm.....	6
1.2.2. Các thuật toán sử dụng trong mật mã khóa công khai.....	7
1.3. Chữ ký số .....	7
1.3.1. Định nghĩa chữ ký số và các khái niệm .....	7
1.3.2. Tạo và kiểm tra chữ ký số.....	7
1.4. Hàm băm .....	8
1.4.1. Định nghĩa hàm băm.....	8
1.4.2. Ứng dụng của hàm băm .....	8
1.4.3. Một số hàm băm thông dụng .....	8
CHƯƠNG II CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI .....	9
2.1. Lịch sử phát triển PKI.....	9
2.2. Thực trạng PKI tại Việt Nam.....	9
2.3. Các định nghĩa về cơ sở hạ tầng khóa công khai và các khái niệm có liên quan .....	9
2.3.1. Định nghĩa về PKI .....	9
2.3.2. Các khái niệm liên quan trong PKI.....	10
2.3.3. Mục tiêu, chức năng.....	11
2.3.4. Các khía cạnh an toàn cơ bản mà PKI cung cấp.....	11
2.4. Các thành phần chính của PKI.....	11
2.4.1. Certification Authority (CA) – Tổ chức chứng thực .....	12
2.4.2.Registration Authority (RA) – Tổ chức đăng ký .....	12

2.4.3. Certificate – Enabled Client: Bên được cấp phát chứng thư số.....	12
2.4.4. Data Recipient: bên nhận dữ liệu.....	12
2.4.5. Chuỗi chứng thư số hoạt động như thế nào .....	12
2.5. Cách thức hoạt động của PKI .....	12
2.5.1. Khởi tạo thực thể cuối.....	12
2.5.2. Tạo cặp khóa công khai/ khóa riêng .....	12
2.5.3. Áp dụng chữ ký số để định danh người gửi.....	12
2.5.4. Mã hóa thông báo.....	12
2.5.5. Truyền khóa đối xứng.....	12
2.5.6. Kiểm tra danh tính người gửi thông qua một CA.....	12
2.5.7. Giải mã thông báo và kiểm tra nội dung thông báo.....	12
2.6. Các tiến trình trong PKI .....	12
2.6.1. Yêu cầu chứng thư số.....	12
2.7. Kiến trúc của hệ thống PKI.....	12
2.7.1. Mô hình phân cấp.....	13
2.7.2. Mô hình mạng lưới .....	13
2.7.3. Mô hình danh sách tin cậy .....	14
2.7.4. Mô hình Hub and Spoke .....	14
2.7.5. Mô hình CA đơn .....	14
2.8. Chứng thực chéo (Cross-certification).....	15
2.8.1. Tổng quan về chứng thực chéo.....	16
2.8.2. PKI Policy Networking.....	18
2.9. Ứng dụng của PKI.....	19
<b>CHƯƠNG III <u>ỨNG DỤNG</u> HỆ THỐNG CHỨNG THỰC PKI TRONG GIAO DỊCH ĐIỆN TỬ</b> .....	20
3.1. Giới thiệu về EJBCA .....	20
3.1.1. PKI – EJBCA.....	20
3.1.2. Đặc điểm kỹ thuật .....	20
3.1.3. Kiến trúc EJBCA .....	20
3.1.4. Chức năng .....	20

3.1.5. Đánh giá .....	20
3.2. Ứng dụng chứng thực chéo dựa trên EJBCA .....	20
3.2.1. Mô hình triển khai.....	20
3.2.2. Ứng dụng chứng thực chéo trên EJBCA .....	21
KẾT LUẬN .....	25
TÀI LIỆU THAM KHẢO.....	26

## DANH MỤC CÁC KÝ HIỆU VÀ TỪ VIẾT TẮT

Từ viết tắt	Từ viết đầy đủ
CSDL	Cơ sở dữ liệu
TCP/IP	Transmission Control Protocol /Internet Protocol
PKI	Public Key Infrastructure: Hạ tầng khóa công khai
CA	Certification Authority: Tổ chức chứng thực
RA	Rigistration Authority: Tổ chức đăng ký
EJBCA	Enterprise Java Beans Certificate Authority
CRL	Certificate Revocation List: Danh sách hủy bỏ chứng nhận
SHS	Secure Hash Standard: Chuẩn băm bảo mật
SHA	Secure Hash Algorithm: Thuật toán băm bảo mật
SSL	Secure Sockets Layer
VPN	Virtual Private Network
DN	Distinguished Name: Tên phân biệt
PKCS	Public Key Cryptography Standard: Chuẩn mật mã khóa công khai
PEM	Privacy-enhanced Electronic Mail: Thư điện tử bảo mật
CPS	Certification Prattice Statement
DNS	Domain Name System: Hệ thống tên miền

## MỞ ĐẦU

Nội dung luận văn được chia thành 3 chương, kết luận và tài liệu tham khảo:

### **Chương 1: Tổng quan về mật mã.**

Chương này tập trung tìm hiểu về mật mã học, hai loại mật mã thường được sử dụng là mật mã khóa bí mật và mật mã khóa công khai, chữ ký số và hàm băm. Hệ mã hóa, chữ ký số cũng như hàm băm chính là nền tảng để xây dựng hệ thống PKI sẽ được nêu tại chương tiếp theo.

### **Chương 2: Cơ sở hạ tầng khóa công khai.**

Chương này sẽ tìm hiểu về cơ sở hạ tầng khóa công khai, thực trạng về việc sử dụng hệ thống PKI, các thành phần chính của hệ thống PKI, kiến trúc một trung tâm chứng thực CA, các hoạt động chính trong hệ thống PKI, chứng thư số và chứng thực chéo để xác thực mối quan hệ giữa các PKI.

### **Chương 3: Một số ứng dụng của Hệ thống chứng thực điện tử PKI.**

Chương này xây dựng ứng dụng chứng thực chéo giữa các PKI sử dụng hệ thống phần mềm trung tâm CA mã nguồn mở EJBCA.

## CHƯƠNG I

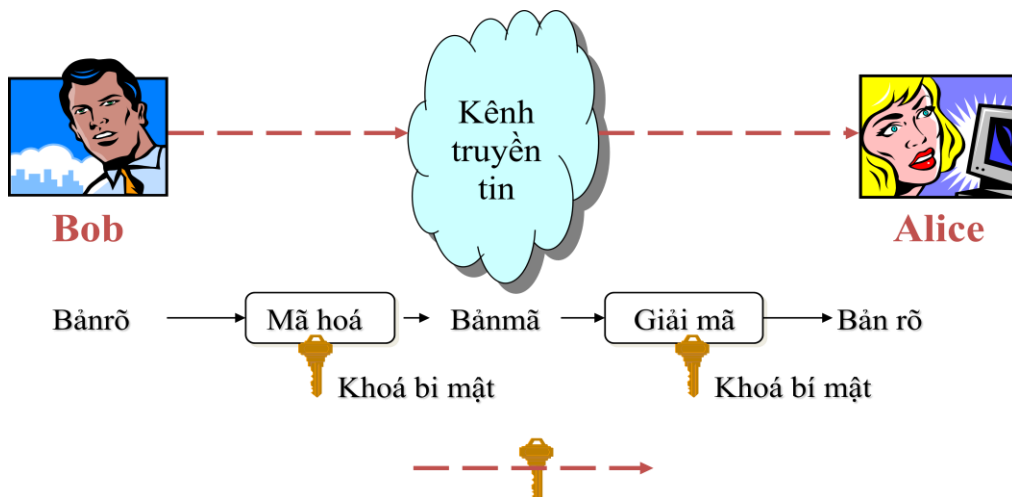
### TỔNG QUAN MẬT MÃ HỌC

Mật mã được chia làm hai loại chính là mật mã khóa bí mật (mật mã đối xứng) và mật mã hóa công khai (mật mã phi đối xứng).

#### 1.1. Mật mã khóa bí mật

##### 1.1.1. Giới thiệu về mật mã khóa bí mật và các khái niệm có liên quan

Mật mã khóa bí mật còn được gọi là mật mã khóa đối xứng. Đây là phương pháp mã hóa sử dụng cặp khóa đối xứng, người gửi và người nhận sẽ dùng chung một khóa để mã hóa và giải mã thông điệp.



**Hình 1.1. Mật mã khóa bí mật**

##### 1.1.2. Một vài thuật toán sử dụng trong mật mã khóa đối xứng

###### 1.1.2.1. Triple DES

###### 1.1.2.2. AES

##### Ưu nhược điểm của mật mã khóa bí mật

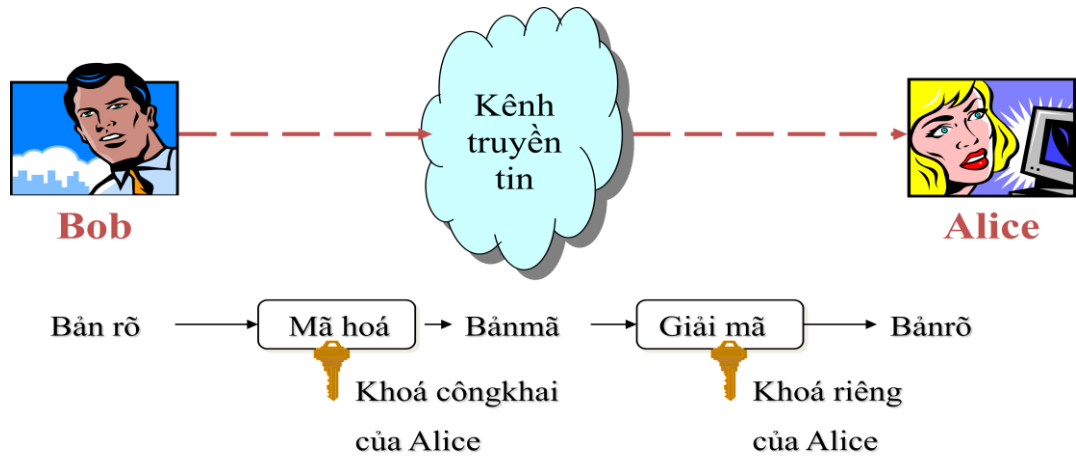
#### 1.2. Mật mã khóa công khai

##### 1.2.1. Khái niệm

Mật mã khóa công khai còn được gọi là mật mã phi đối xứng.

Mật mã khóa công khai cho phép người sử dụng trao đổi các thông tin mật mà không cần phải trao đổi các khóa bí mật trước đó. Trong mật mã khóa công khai sử dụng một cặp khóa có quan hệ toán học với nhau là khóa công khai (Public Key)/khóa riêng (Private Key) [2].





**Hình 1.2. Mật mã khóa công khai**

### 1.2.2. Các thuật toán sử dụng trong mật mã khóa công khai

#### 1.2.2.1. RSA

RSA là một thuật toán mã hóa khóa công khai.

RSA là thuật toán khởi đầu của lĩnh vực mật mã trong việc sử dụng khóa công khai và phù hợp để tạo ra chữ ký điện tử.

#### 1.2.2.2. Phương thức trao đổi khóa Diffie-Hellman

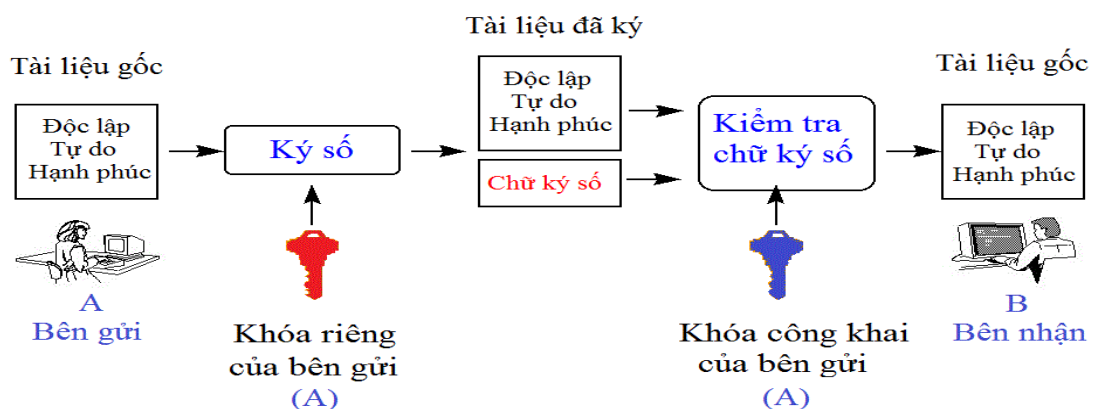
Trao đổi khóa Diffie–Hellman (D-H) là một phương pháp trao đổi khóa được phát minh sớm nhất trong mật mã học.

**Ưu nhược điểm của mật mã khóa công khai:**

### 1.3. Chữ ký số

#### 1.3.1. Định nghĩa chữ ký số và các khái niệm

#### 1.3.2. Tạo và kiểm tra chữ ký số



**Hình 1.3. Tạo và kiểm tra chữ ký**

### 1.3.3. Các thuật toán chữ ký số thông dụng

#### 1.3.3.1. Thuật toán chữ ký số RSA

Thuật toán chữ ký số RSA được xây dựng dựa trên thuật toán mã hóa khóa công khai RSA.

#### 1.3.3.2. Thuật toán chuẩn chữ ký số DSS

Chuẩn chữ ký số DSS (Digital Signature Standard) được đề xuất năm 1991, là cải biên của sơ đồ chữ ký ElGamal, và được chấp nhận là chuẩn vào năm 1994 để dùng trong một số lĩnh vực giao dịch ở USA.

Thông thường tài liệu số được mã hoá và giải mã 1 lần. Nhưng chữ ký lại liên quan đến pháp luật, chữ ký, có thể phải kiểm thử sau nhiều năm đã ký. Do đó chữ ký phải được bảo vệ cẩn thận.

### 1.4. Hàm băm

#### 1.4.1. Định nghĩa hàm băm

Hàm băm là thuật toán không dùng khóa để mã hóa, nó có nhiệm vụ “lọc” (băm) tài liệu và cho kết quả là một giá trị “băm” có kích thước cố định, còn gọi là “đại diện tài liệu” hay “đại diện bản tin”, “đại diện thông điệp” [1].

Hàm băm là hàm một chiều, theo nghĩa giá trị của hàm băm là duy nhất, và từ giá trị băm này, “khó thể” suy ngược lại được nội dung hay độ dài ban đầu của tài liệu gốc.

#### 1.4.2. Ứng dụng của hàm băm

Người ta dùng hàm băm  $h$  để tạo đại diện bản tin  $z = h(x)$ , nó có độ dài ngắn (ví dụ 128 bit). Sau đó ký trên  $z$ , như vậy chữ ký trên  $z$  sẽ nhỏ hơn rất nhiều so với chữ ký trên bản tin gốc  $x$ .

#### 1.4.3. Một số hàm băm thông dụng

SHS là chuẩn gồm tập hợp các thuật toán băm mật mã an toàn (Secure Hash Algorithm – SHA) như SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 do NIST và NSA xây dựng.

**Kết chương:** Chương này tập trung vào việc mã hóa dữ liệu, đưa ra được khái niệm về mã hóa dữ liệu và các hệ mã hóa trong đó có hệ mã hóa công khai. Nghiên cứu tổng quan về chữ ký số và hàm băm. Hệ mã hóa, chữ ký số cũng như hàm băm chính là nền tảng để xây dựng hệ thống cơ sở hạ tầng khóa công khai PKI sẽ được nêu tại chương tiếp theo.

## **CHƯƠNG II**

### **CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI**

#### **2.1. Lịch sử phát triển PKI**

Thị trường PKI thực sự đã tồn tại và phát triển nhưng không phải với quy mô đã được kỳ vọng từ những năm giữa của thập kỷ 1990. PKI chưa giải quyết được một số vấn đề mà nó được kỳ vọng. Những PKI thành công nhất tới nay là các phiên bản do các chính phủ thực hiện.

Quá trình nghiên cứu và phát triển PKI là một quá trình lâu dài và cùng với nó, mức độ chấp nhận của người dùng cũng tăng lên một cách khá chậm chạp.

#### **2.2. Thực trạng PKI tại Việt Nam**

##### **2.2.1. Văn bản quy phạm pháp luật**

Các Văn bản quy phạm pháp luật đã được ban hành:

Luật giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005.

Luật an toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015 chính thức có hiệu lực từ ngày 01/7/2016.

Nghị định số 26/2007/NĐ- CP.

Nghị định số 170/2013/NĐ-CP ngày 13 tháng 11 năm 2013.

Chỉ thị số 34/2008/CT-TTg ngày 03/12/2008 của Thủ tướng Chính phủ.

Nghị quyết 36a/NQ-CP ngày 14 tháng 10 năm 2015 về Chính phủ điện tử.

Nghị quyết số 26/NQ-CP ngày 15 tháng 4 năm 2015 của Chính phủ.

##### **2.2.2. Thực trạng triển khai PKI tại Việt Nam**

Hiện nay, Việt Nam có hai hệ thống PKI chính là: Dịch vụ chứng thực điện tử cho hoạt động của các cơ quan thuộc hệ thống chính trị (PKI Chính phủ) do Ban Cơ yếu Chính phủ đảm nhiệm và Dịch vụ chứng thực điện tử cho hoạt động công cộng do Bộ Thông tin và truyền thông quản lý.

- Đối với dịch vụ chứng thực điện tử cho hoạt động của cơ quan thuộc hệ thống chính trị (PKI Chính phủ):

- Đối với dịch vụ chứng thực điện tử cho hoạt động công cộng:

#### **2.3. Các định nghĩa về cơ sở hạ tầng khóa công khai và các khái niệm có liên quan**

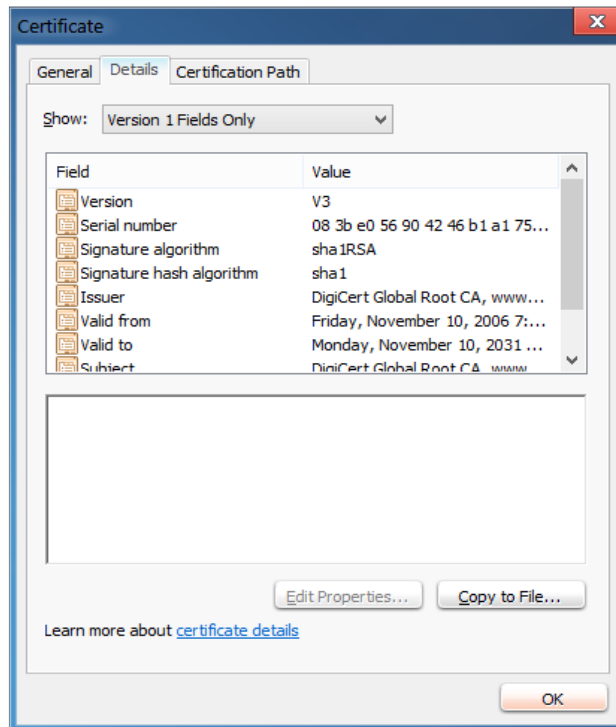
##### **2.3.1. Định nghĩa về PKI**

PKI là một tập hợp phần cứng, phần mềm, con người, các chính sách và các thủ tục cần thiết để tạo, quản lý, lưu trữ, phân phối và thu hồi các chứng chỉ khóa công khai dựa trên mật mã khóa công khai.

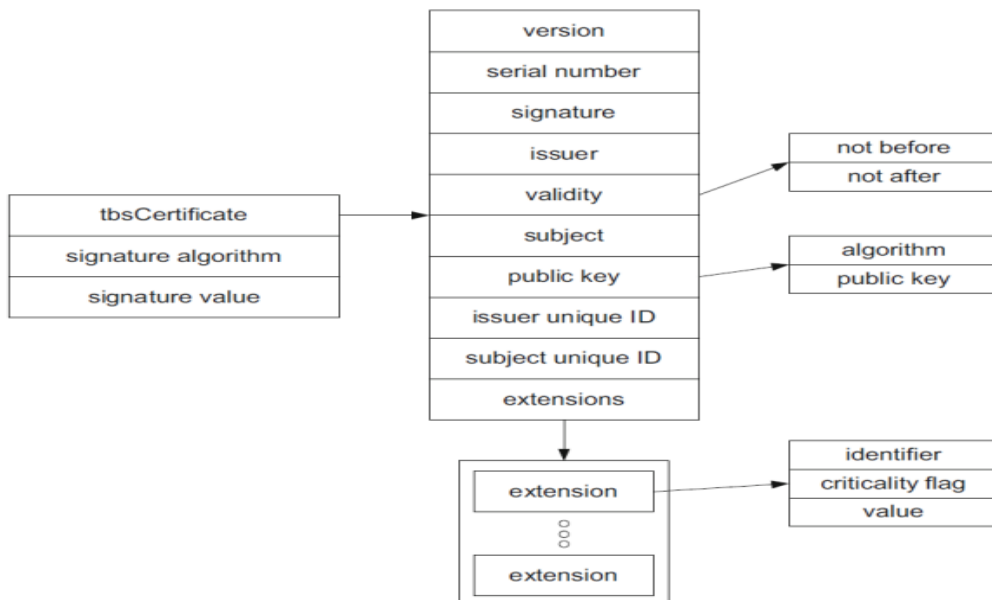
## 2.3.2. Các khái niệm liên quan trong PKI

### 2.3.2.1. Chứng thư số

Chứng thư số là một dạng chứng thư điện tử, nó được cung cấp bởi tổ chức cung cấp dịch vụ chứng thực số. Chứng thư số được xem như là thẻ căn cước sử dụng trên môi trường mạng máy tính.



Hình 2.1. Ví dụ về chứng thư số



Hình 2.2. Cấu trúc chung chứng thư số X.509 v3

#### 2.3.2.2. Kho chứng thư số

#### 2.3.2.3. Thu hồi chứng thư số

#### 2.3.2.4. Danh sách thu hồi chứng thư số

#### 2.3.2.5. Sao lưu và phục hồi khóa

#### 2.3.2.6. Cập nhật khóa

#### 2.3.2.7. Lịch sử khóa

#### 2.3.2.8. Hỗ trợ chống chối bỏ

#### 2.3.2.9. Tem thời gian

#### 2.3.2.10. Phần mềm phía Client

### 2.3.3. Mục tiêu, chức năng

#### 2.3.3.1. Xác thực

Về cơ bản, tính xác thực cung cấp 2 khía cạnh ứng dụng chính đó là định danh thực thể và định danh nguồn gốc dữ liệu.

- Định danh thực thể
- Định danh nguồn gốc dữ liệu

#### 2.3.3.2. Bí mật

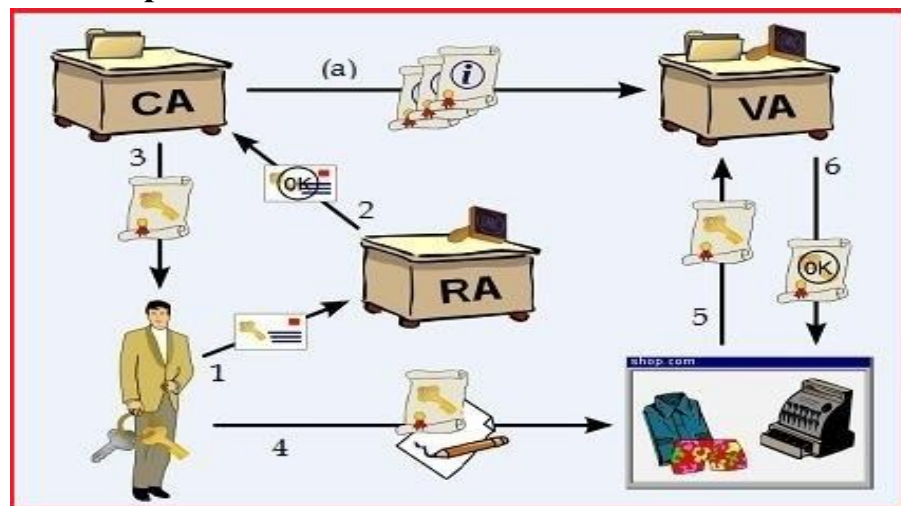
#### 2.3.3.3. Toàn vẹn dữ liệu

#### 2.3.3.4. Chống chối bỏ

### 2.3.4. Các khía cạnh an toàn cơ bản mà PKI cung cấp

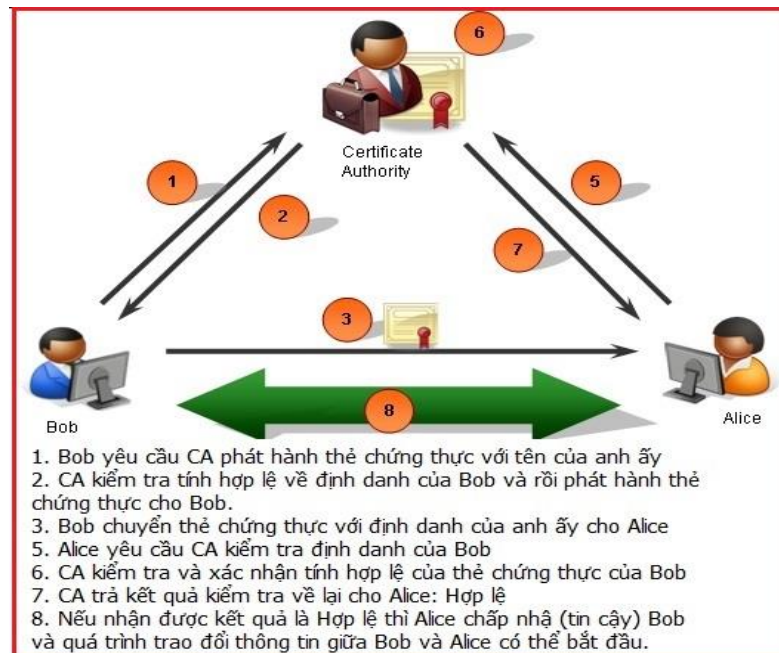
- Đăng nhập an toàn
- Đăng nhập một lần an toàn
- Trong suốt với người dùng cuối
- An ninh toàn diện

### 2.4. Các thành phần chính của PKI



Hình 2.3. Các thành phần trong hệ thống PKI

### 2.4.1. Certification Authority (CA) – Tổ chức chứng thực



**Hình 2.4. Quá trình xác thực dựa trên CA**

### 2.4.2. Registration Authority (RA) – Tổ chức đăng ký

### 2.4.3. Certificate – Enabled Client: Bên được cấp phát chứng thư số

### 2.4.4. Data Recipient: bên nhận dữ liệu

### 2.4.5. Chuỗi chứng thư số hoạt động như thế nào

## 2.5. Cách thức hoạt động của PKI

### 2.5.1. Khởi tạo thực thể cuối

### 2.5.2. Tạo cặp khóa công khai/ khóa riêng

### 2.5.3. Áp dụng chữ ký số để định danh người gửi

### 2.5.4. Mã hóa thông báo

### 2.5.5. Truyền khóa đối xứng

### 2.5.6. Kiểm tra danh tính người gửi thông qua một CA

### 2.5.7. Giải mã thông báo và kiểm tra nội dung thông báo

## 2.6. Các tiến trình trong PKI

### 2.6.1. Yêu cầu chứng thư số

#### 2.6.1.1. Gửi yêu cầu

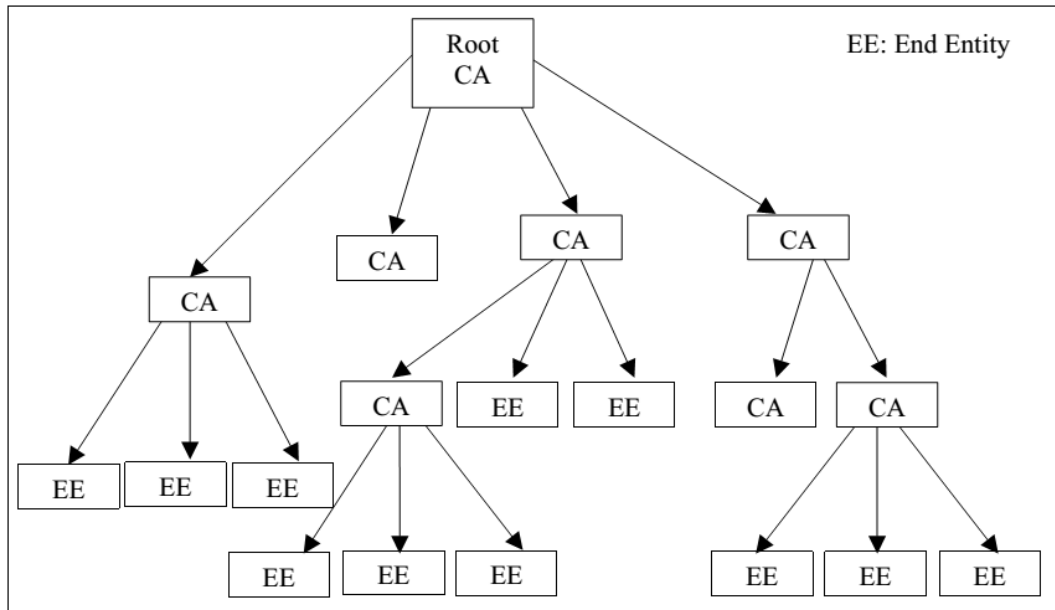
#### 2.6.1.2. Các chính sách

## 2.7. Kiến trúc của hệ thống PKI

Hiện nay PKI được triển khai trong nhiều tổ chức như là một công cụ đảm bảo những nguồn tài nguyên nhạy cảm an toàn. Tuy nhiên, với nhiều mục đích khác nhau, tiến trình khác nhau nên khó có thể đưa ra một tiêu chuẩn thiết kế

chung. Về cơ bản có các mô hình kiến trúc PKI có dựa trên các mô hình chính [9], [13]: mô hình phân cấp, mô hình mạng lưới, mô hình danh sách tin cậy,...

### 2.7.1. Mô hình phân cấp

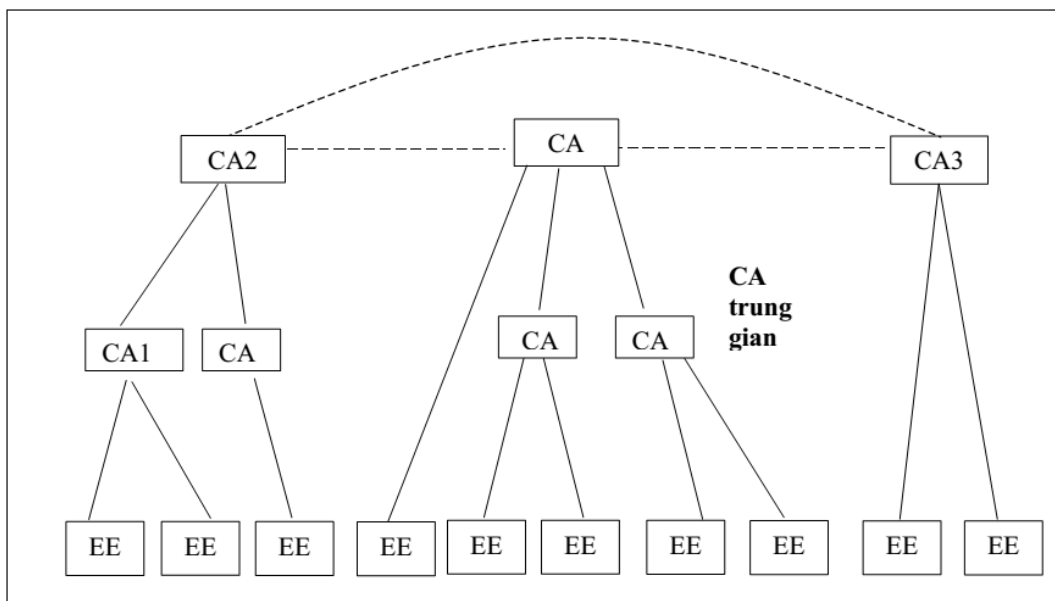


**Hình 2.5. Mô hình phân cấp**

**Ưu điểm:**

**Nhược điểm:**

### 2.7.2. Mô hình mạng lưới



**Hình 2.6. Mô hình mạng lưới**

**Ưu điểm:**

**Nhược điểm:**

### 2.7.3. Mô hình danh sách tin cậy

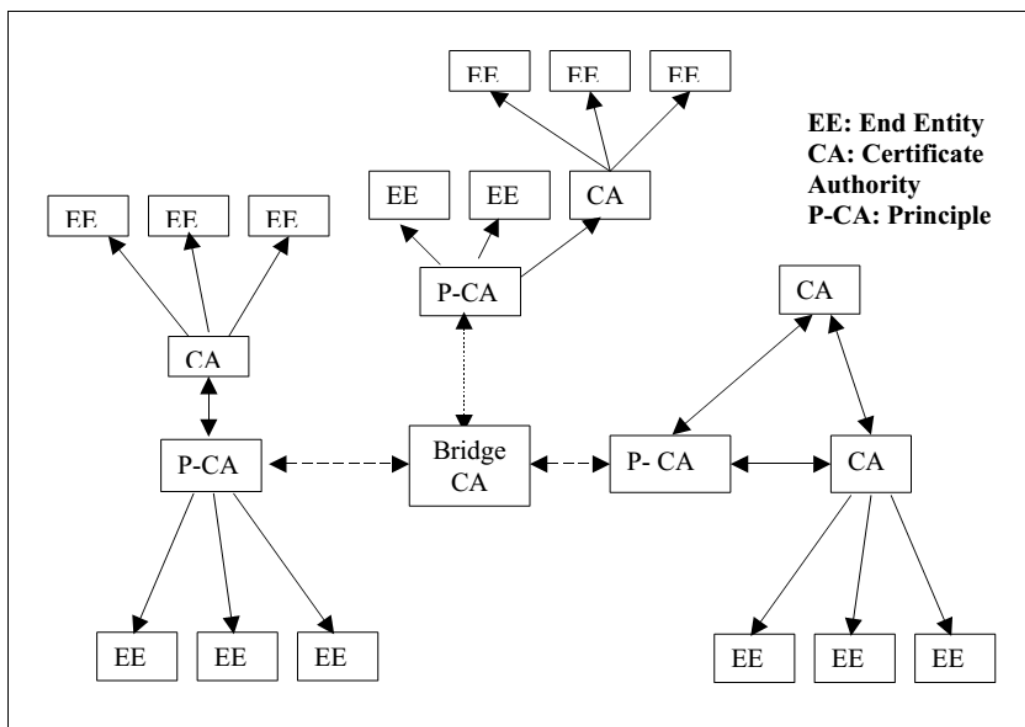
Trong mô hình này các ứng dụng duy trì một danh sách các RootCA được tin cậy. Đây là kiến trúc được áp dụng rộng rãi với các dịch vụ Web, các trình duyệt và các máy chủ là những đối tượng sử dụng tiêu biểu nhất.

**Ưu điểm:**

**Nhược điểm:**

### 2.7.4. Mô hình Hub and Spoke

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



**Hình 2.7. Mô hình Hub and Spoke (Bridge CA)**

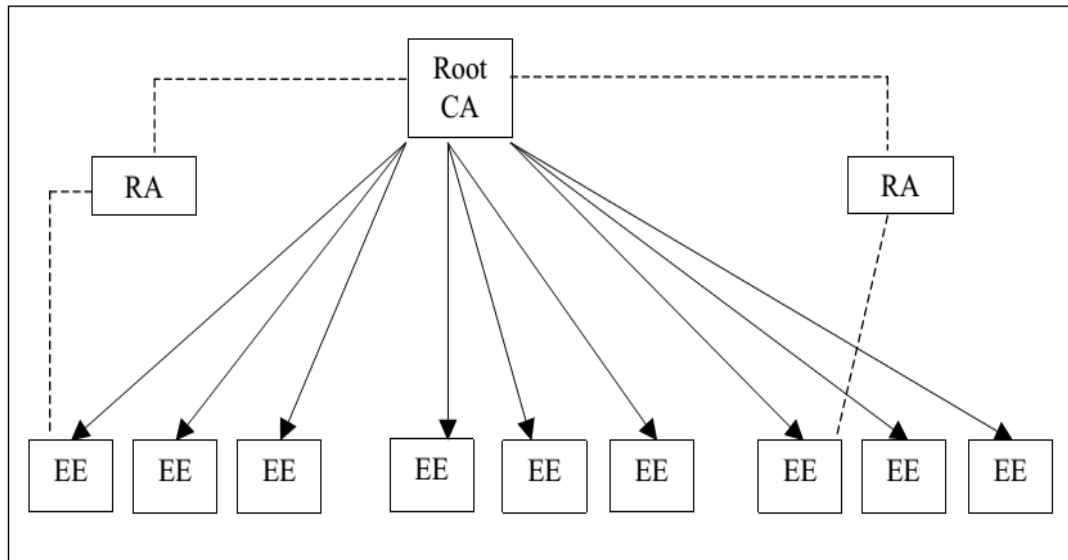
**Ưu điểm:**

**Nhược điểm**

### 2.7.5. Mô hình CA đơn

Đây là mô hình tổ chức CA cơ bản và đơn giản nhất. Trong mô hình CA đơn chỉ có một CA xác nhận tất cả các thực thể cuối trong miền PKI. Mỗi người sử dụng trong miền nhận khoá công khai của CA gốc (Root CA) theo một số cơ chế nào đó.



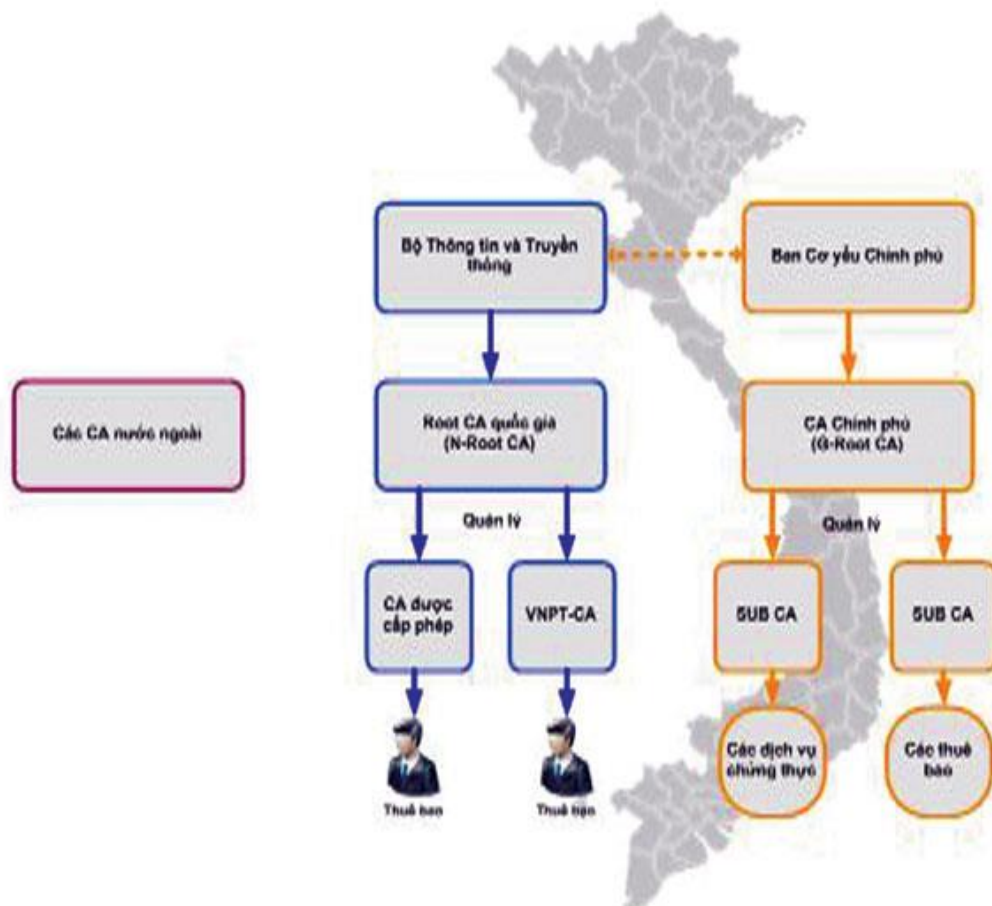


Hình 2.8. Mô hình CA đơn

**Ưu điểm**

**Nhược điểm**

## 2.8. Chứng thực chéo (Cross-certification)

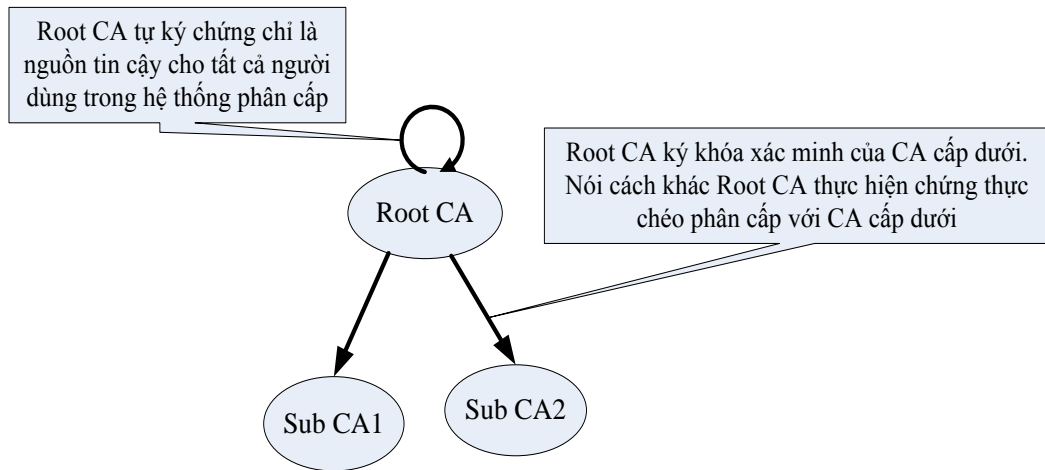


Hình 2.9. Sơ đồ hệ thống chứng thực điện tử tại Việt Nam

Đây là vấn đề rất cấp thiết hiện nay. Vì vậy, cần phải thiết lập một môi trường tác để xây dựng cơ chế tin cậy lẫn nhau giữa hệ thống CA chuyên dùng Chính phủ và hệ thống CA công cộng. Để giải quyết vấn đề này chúng ta đi nghiên cứu và xây dựng giải pháp chứng thực chéo.

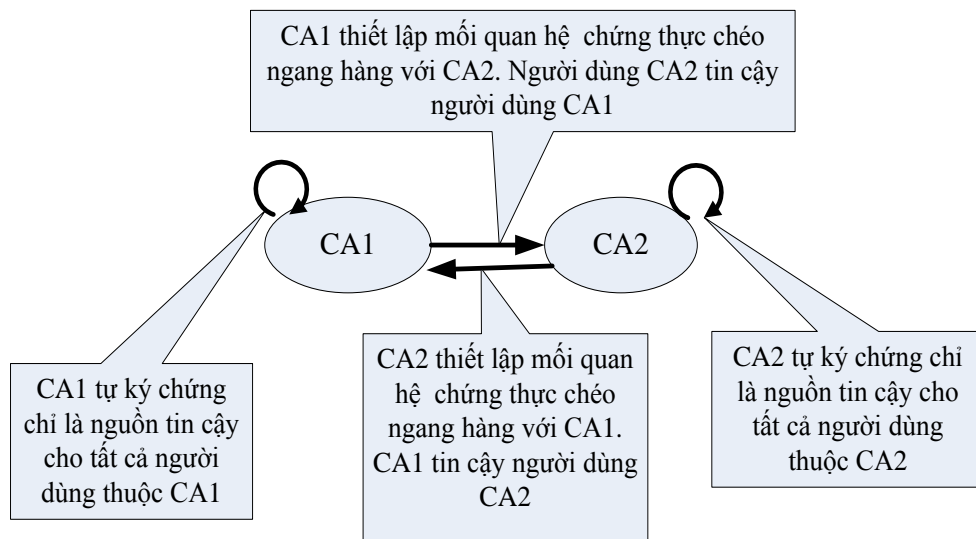
### 2.8.1. Tổng quan về chứng thực chéo

Thuật ngữ chứng thực chéo nói đến 2 hoạt động [11]:



**Hình 2.10 : Chứng thực chéo phân cấp giữa một Root CA (tự trị) và các CA cấp dưới phụ thuộc**

Nếu nguồn tin cậy của người dùng là CA cục bộ của người dùng, thì CA cục bộ của người dùng là một CA tự trị. Tự trị dùng để chỉ các CA không dựa trên một CA cấp trên trong hệ thống phân cấp.



**Hình2.11. Chứng thực chéo ngang hàng**

### 2.8.1.1. Lợi ích của chứng thực chéo phân cấp

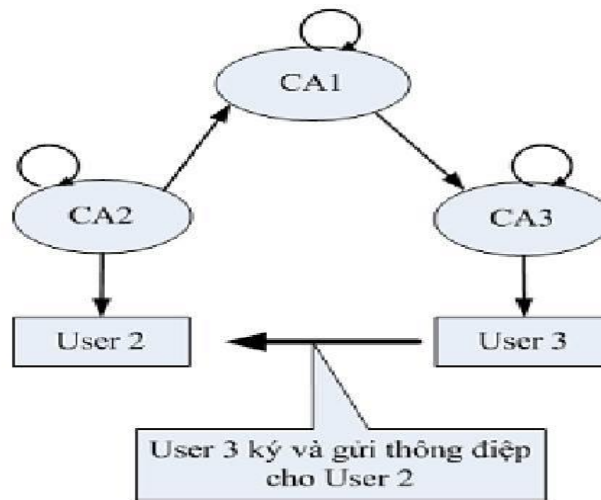
Chứng thực chéo phân cấp là ý tưởng trong tổ chức có nhiều các CA đây là điều cần thiết và đòi hỏi tổ chức phải kiểm soát tối đa trên tất cả các CA trong hệ thống phân cấp.

Tính năng và lợi ích của chứng thực chéo phân cấp:

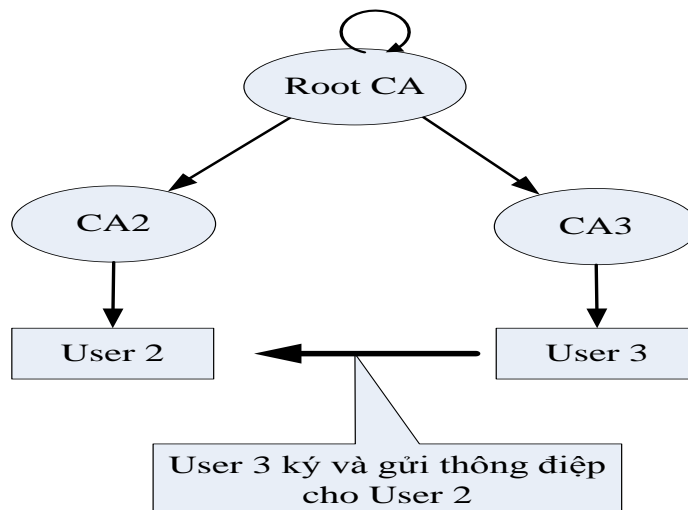
### 2.8.1.2. Lợi ích của chứng thực chéo ngang hàng

Chứng thực chéo ngang hàng là ý tưởng giữa các tổ chức nơi mà chỉ tổ chức đó muốn kiểm soát tối đa tổ chức riêng của mình. Chứng thực chéo ngang hàng phải xảy ra giữa các CA tự trị, nơi mà một CA tự trị có thể là root CA trong hệ thống phân cấp của các CA hoặc ngược lại một CA độc lập.

### 2.8.1.3. Ví dụ về chứng thực chéo



Hình 2.12. Hình minh họa 1

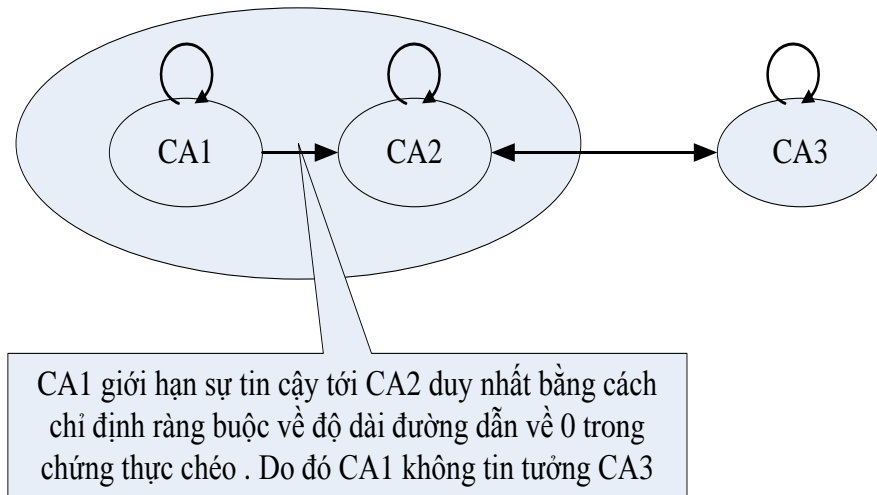


Hình 2.13. Hình minh họa 2

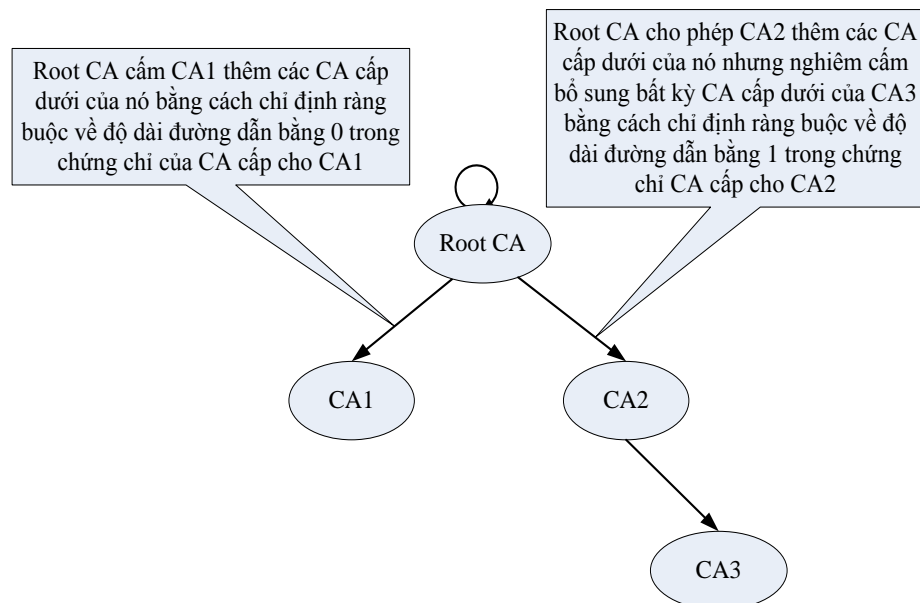
### 2.8.2. PKI Policy Networking

Có 3 cách cơ bản để ràng buộc sự tin tưởng giữa các CA: độ dài đường dẫn (path length), tên (name) và chính sách (policy). Chứng thực chéo giữa hai CA (chứng thực chéo ngang hàng) hoặc chứng thư CA cấp dưới (chứng thực chéo phân cấp) được sử dụng để truyền tải những hạn chế, và các ứng dụng khách tự động thực thi các ràng buộc khi xác nhận chứng thư số.

#### 2.8.2.1. Ràng buộc về độ dài đường dẫn (Path Length Constraints)

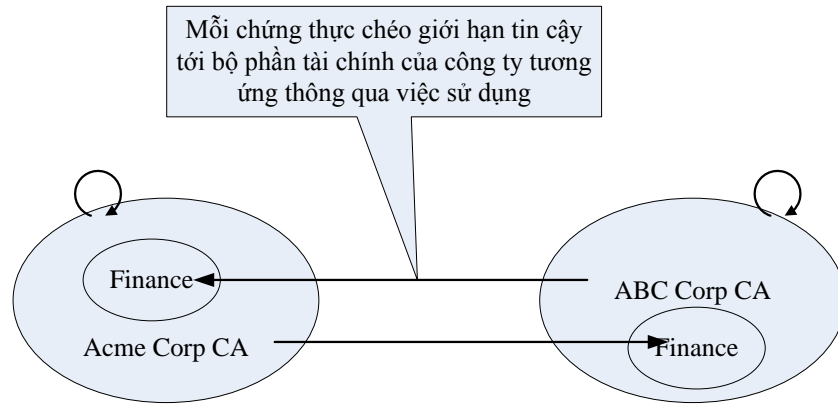


**Hình 2.14. Ràng buộc về đường dẫn giữa các CA trong chứng thực chéo ngang hàng**



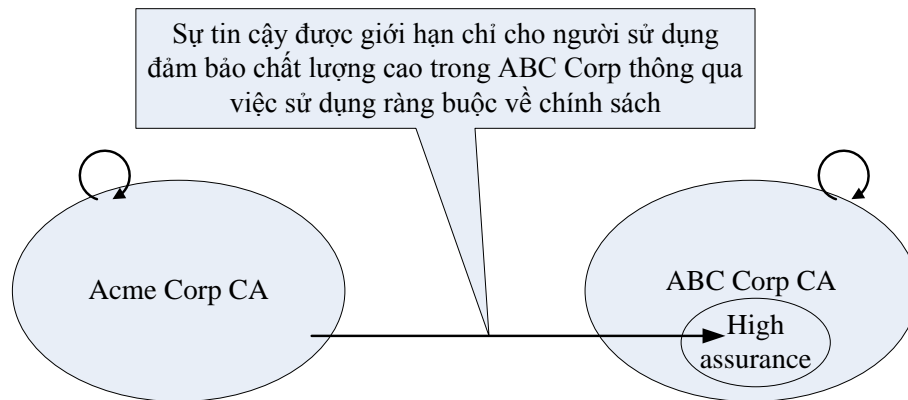
**Hình 2.15. Ràng buộc về đường dẫn giữa các CA trong chứng thực chéo phân cấp**

#### 2.8.2.2. Ràng buộc về tên (Name constraints)



**Hình 2.16. Ràng buộc về tên trong chứng thực chéo**

### 2.8.2.3. Ràng buộc về chính sách (Policy Constraints)



**Hình 2.17. Ràng buộc về chính sách trong chứng thực chéo**

### 2.8.2.4. Bản đồ chính sách

## 2.9. Ứng dụng của PKI

**Kết chương:** Nội dung chương này sẽ tìm hiểu về cơ sở hạ tầng khóa công khai. Trong đó, trước tiên phải khái quát được cơ sở hạ tầng khóa công khai, thực trạng về việc sử dụng hệ thống PKI, các thành phần chính của hệ thống PKI, kiến trúc một trung tâm chứng thực CA. Tìm hiểu các hoạt động chính trong hệ thống PKI. Đặc biệt, trong chương này tập trung nghiên cứu, tìm hiểu về chứng thực chéo để giải quyết các vấn đề chứng thực trong PKI.

## CHƯƠNG III

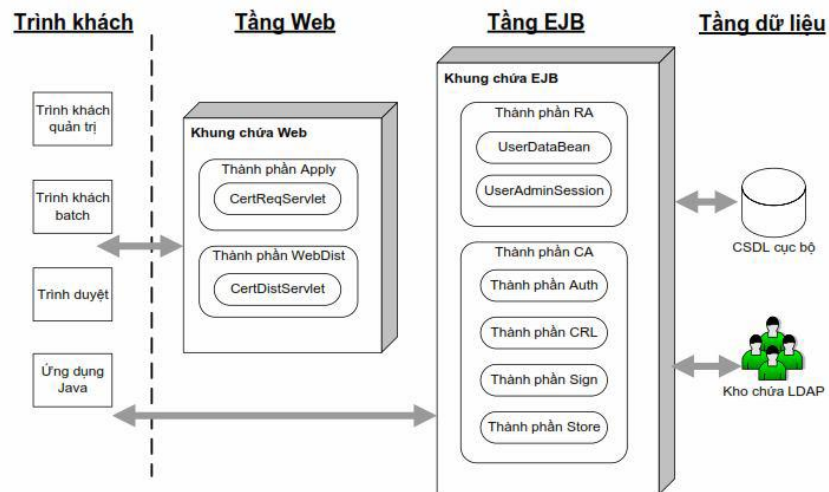
### ỨNG DỤNG HỆ THỐNG CHỨNG THỰC PKI TRONG GIAO DỊCH ĐIỆN TỬ

#### 3.1. Giới thiệu về EJBCA

##### 3.1.1. PKI – EJBCA

##### 3.1.2. Đặc điểm kỹ thuật

##### 3.1.3. Kiến trúc EJBCA



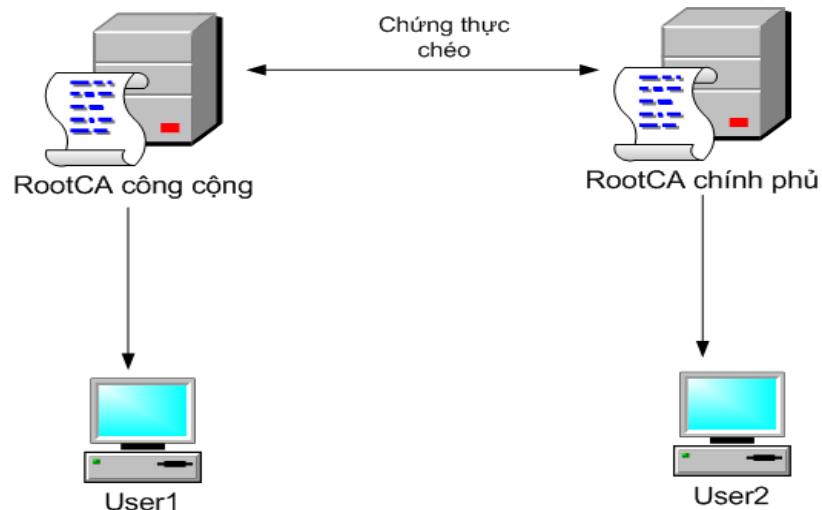
**Hình 3.1. Kiến trúc EJBCA**

##### 3.1.4. Chức năng

##### 3.1.5. Đánh giá

#### 3.2. Ứng dụng chứng thực chéo dựa trên EJBCA

##### 3.2.1. Mô hình triển khai



**Hình 3.2. Mô hình triển khai**

### 3.2.2. Ứng dụng chứng thực chéo trên EJBCA

Vào trang quản trị EJBCA

**EJBCA**  
PKI by PrimeKey *Administration*

Version : EJBCA 6.3.1.1 (

Welcome SuperAdmin to EJBCA Administration.

Node hostname : nguyenthanson  
Server time : 2016-10-27 00:34:10+07:00

CA health state [?]			Publish queue status [?]	
CA Name	CA Service	CRL Status	Publisher	Length
ManagementCA	✓	⚠	No publishers defined.	

© 2002-2015 PrimeKey Solutions AB. EJBCA® is a registered trademark of PrimeKey Solutions AB.

Hình 3.3. Trang quản trị EJBCA

Tạo hai RootCA là RootCA1 và RootCA2.

**EJBCA**  
PKI by PrimeKey *Administration*

**Manage Certification Authorities**

List of Certification Authorities

ManagementCA, (Active)

Edit CA Delete CA Import CA keystore... Import CA certificate...

Create Authenticated Certificate Signing Request [?]

Add CA

Create... Rename

Hình 3.4. Tạo các RootCA

**EJBCA**  
PKI by PrimeKey *Administration*

**Create CA**

CA Name : RootCA1

Back to Certificate Aut

Type of CA [?] X509

Signing Algorithm SHA1WithRSA

Crypto Token [?] - Create a new soft Crypto Token with recommended key pairs

Key sequence format [?] numeric [0-9]

Key sequence [?] 00000

Description

**Directives**

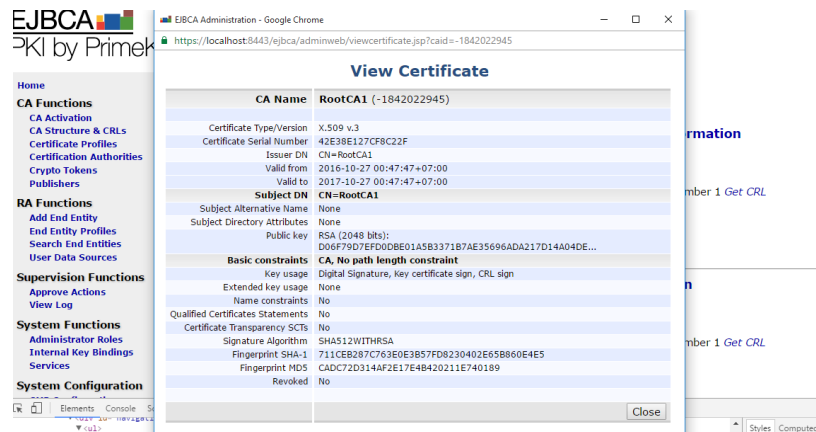
Enforce unique public keys [?] ☒ Enforce

Enforce unique DN [?] ☒ Enforce

Enforce unique Subject DN SerialNumber [?] ☐ Enforce

Hình 3.5. Điền thông tin cơ bản cho một RootCA

Điền thông tin cơ bản của RootCA1 và RootCA2 (chọn thuật toán ký, Subject DN, số ngày hết hạn của chứng chỉ) → Create ta tạo được 2 RootCA



Hình 3.6. Thông tin đầy đủ khi một RootCA được tạo



Hình 3.7. Download PEM file của RootCA

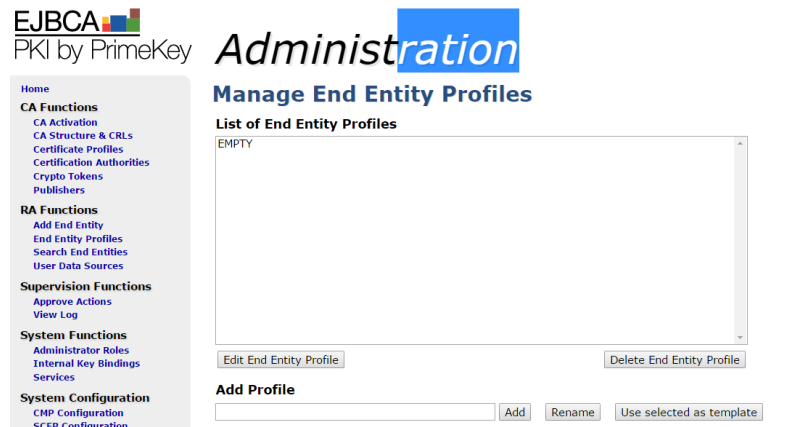
Download PEM file của RootCA1 (tương tự đối với RootCA2), sau đó nhập chứng chỉ RootCA1.cacert.pem (RootCA2. cacert.pem) vào Trusted Root Certification Authorities trong hệ quản lý chứng chỉ của windows.



Hình 3.8. Chứng thư số của RootCA



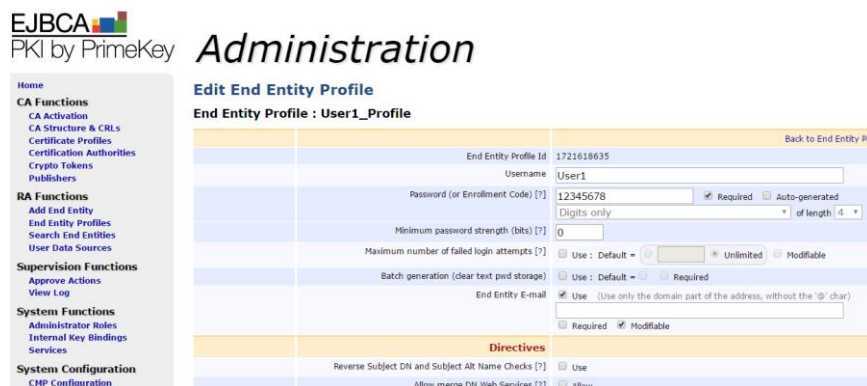
Tiếp theo, tạo các thực thể cuối cho 2 RootCA  
Chọn End Entity Profiles sau đó add các thực thể.



**Hình 3.9. Tạo người dùng End Entity**

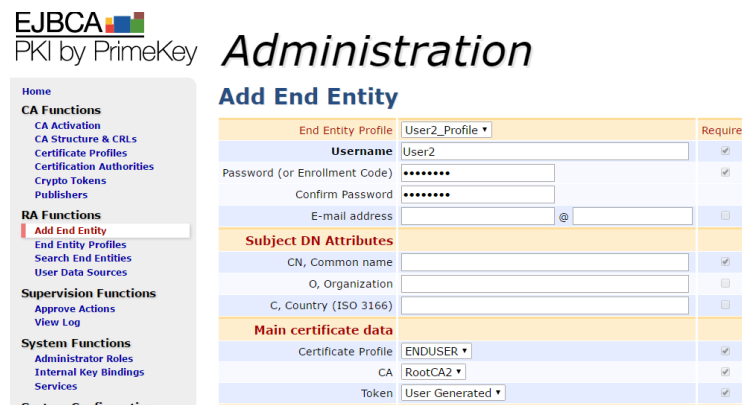
Đối với RootCA1 ta Add Profile User1\_Profile

Đối với RootCA2 ta Add Profile User2\_Profile



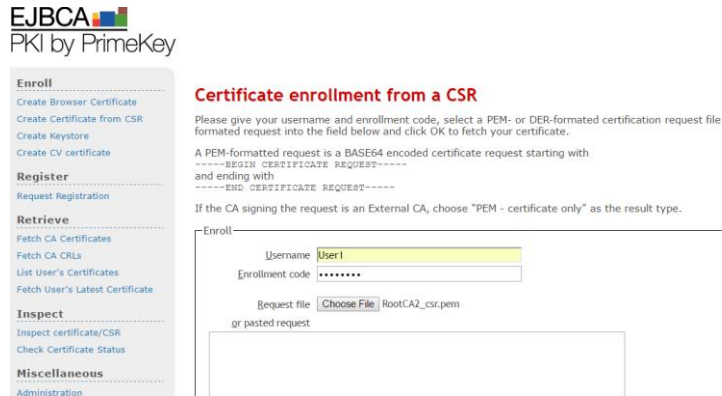
**Hình 3.10. Điền đầy đủ thông tin cho các User**

Sau đó Add lại các thông tin của End Entity



**Hình 3.11. Add lại thông tin của các User**

Tiến hành chứng thực chéo bằng cách: User1 gửi request đến RootCA2 và User2 gửi request đến RootCA1 để xác thực.



**EJBCA**  
PKI by PrimeKey

**Enroll**  
Create Browser Certificate  
Create Certificate from CSR  
Create Keystore  
Create CV certificate

**Register**  
Request Registration

**Retrieve**  
Fetch CA Certificates  
Fetch CA CRLs  
List User's Certificates  
Fetch User's Latest Certificate

**Inspect**  
Inspect certificate/CSR  
Check Certificate Status

**Miscellaneous**  
Administration

**Certificate enrollment from a CSR**

Please give your username and enrollment code, select a PEM- or DER-formatted certification request file (CSR) to formatted request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded certificate request starting with  
-----BEGIN CERTIFICATE REQUEST-----  
and ending with  
-----END CERTIFICATE REQUEST-----

If the CA signing the request is an External CA, choose "PEM - certificate only" as the result type.

Enroll

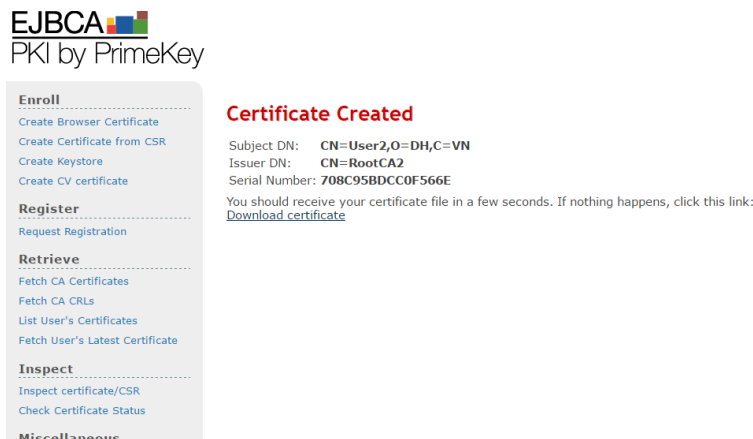
Username:

Enrollment code:

Request file:  [Choose File](#)

or pasted request

**Hình 3.12. Các User gửi request để thực hiện xác thực chéo**  
Xác thực chéo thành công:



**EJBCA**  
PKI by PrimeKey

**Enroll**  
Create Browser Certificate  
Create Certificate from CSR  
Create Keystore  
Create CV certificate

**Register**  
Request Registration

**Retrieve**  
Fetch CA Certificates  
Fetch CA CRLs  
List User's Certificates  
Fetch User's Latest Certificate

**Inspect**  
Inspect certificate/CSR  
Check Certificate Status

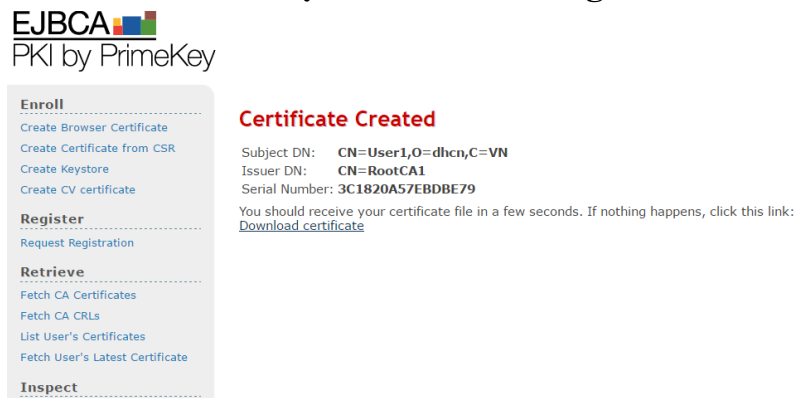
**Miscellaneous**

**Certificate Created**

Subject DN: CN=User2,O=DH,C=VN  
Issuer DN: CN=RootCA2  
Serial Number: 708C95BDCC0F566E

You should receive your certificate file in a few seconds. If nothing happens, click this link: [Download certificate](#)

**Hình 3.13. Xác thực chéo thành công cho User1**



**EJBCA**  
PKI by PrimeKey

**Enroll**  
Create Browser Certificate  
Create Certificate from CSR  
Create Keystore  
Create CV certificate

**Register**  
Request Registration

**Retrieve**  
Fetch CA Certificates  
Fetch CA CRLs  
List User's Certificates  
Fetch User's Latest Certificate

**Inspect**

**Certificate Created**

Subject DN: CN=User1,O=dhcn,C=VN  
Issuer DN: CN=RootCA1  
Serial Number: 3C1820A57EBDBE79

You should receive your certificate file in a few seconds. If nothing happens, click this link: [Download certificate](#)

**Hình 3.14. Xác thực chéo thành công cho User2**

**Kết chương:** Nội dung chương này đã xây dựng được ứng dụng PKI sử dụng giải pháp chứng thực chéo dựa trên phần mềm mã nguồn mở EJBCA.

## KẾT LUẬN

### **Kết quả đạt được:**

Trong thời gian tìm hiểu, xây dựng ứng dụng, luận văn đã hoàn thành được các nhiệm vụ đặt ra, cụ thể là:

*Về mặt lý thuyết:* Luận văn nghiên cứu tìm hiểu hệ thống chứng thực điện tử gồm:

- Cơ sở lý thuyết về mật mã khóa bí mật, mật mã khóa công khai, chữ ký số và hàm băm làm cơ sở cho việc tìm hiểu hạ tầng khóa công khai PKI.
- Hạ tầng khóa công khai PKI tìm hiểu về khái niệm PKI, các thành phần cũng như cách thức hoạt động, chức năng của PKI, các mô hình kiến trúc PKI.
- Thực trạng ứng dụng PKI tại Việt nam.
- Luận văn đi sâu vào nghiên cứu tìm hiểu về chứng thực chéo trong PKI để giải quyết bài toán xây dựng cơ chế tin cậy lẫn nhau giữa các hệ thống chứng thực điện tử khác nhau.
- Các ứng dụng của PKI.

*Về ứng dụng:* Kết quả triển khai chứng thực chéo trên hệ thống phần mềm nguồn mở EJBCA.

### **Hướng phát triển:**

Ứng dụng được phát triển để xây dựng chứng thực chéo trong hệ thống chứng thực điện tử tại Việt Nam để giải quyết các vấn đề chứng thực giữa các hệ thống chứng thực khác nhau mà cần liên thông với nhau làm cơ sở để xây dựng Chính phủ điện tử.

Em xin chân thành cảm ơn!

## **TÀI LIỆU THAM KHẢO**

### **Tài liệu tiếng Việt**

- [1] Trịnh Nhật Tiến, "An toàn dữ liệu" Đại học Công Nghệ- ĐHQGHN
- [2] Bùi Doãn Khanh, Nguyễn Đình Thúc (2004), Giáo trình mã hóa thông tin – Lý thuyết và ứng dụng, NXB LĐXH.
- [3] Hồ Văn Hương, Đào Thị Ngọc Thùy, Cơ sở hạ tầng khóa công khai sinh trắc BioPKI, tạp chí An toàn thông tin, 2009.
- [4] Hồ Văn Hương, Đào Thị Ngọc Thùy, Một số ứng dụng của cơ sở hạ tầng khóa công khai sinh trắc, tạp chí An toàn thông tin, 2010.
- [5] Hồ Văn Hương, Hoàng Chiến Thắng, Ký số và xác thực trên nền tảng Web, tạp chí An toàn thông tin, 2013.
- [6] Lê Quang Tùng, Giải pháp liên thông hệ thống chứng thực điện tử tại Việt Nam, tạp chí An toàn thông tin, 2015.

### **Tài liệu tiếng Anh**

- [7] A.I. Ghorl, A. Parveen (2006), "PKI Administration Using EJBCA and OpenCA", George Mason University.
- [8] Andrew Nash, William Duane, Celia Joseph and Derek Brink (2001), "PKI: Implementing and Managing E-security", RSA Press.
- [9] Carlisle Adams, Steve Lloyd, (November 06, 2002), "Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition"
- [10] IETF Public-Key Infrastructure X.509 (PKIX) Working Group.
- [11] Jim Turnbull (2000), Cross-Certification and PKI Policy Networking.
- [12] Suranjan Choudhury, Kartik Bhatnagar, and Wasim Haque (2001), "Public Key Infrastructure Implementation and Design", M&T Books.
- [13] Z. Guo, T. Okuyama, M.R. Finley. Jr (2005), "A New Trust Model for PKI Interoperability".
- [14] <http://www.ejbca.org>.