

Nhập môn an toàn thông tin

Đề tài: Xác thực X.509



Nhóm 21

Sinh viên thực hiện:

1. Bùi Hoàng Lộc: 20173237
2. Nguyễn Văn Lương: 20173249
3. Nguyễn Thị Thu Thành: 20173375
4. Mai Thị Thảo: 20173382

Mục lục

Định dạng X.509	4
1.1. Tổng quan về chứng chỉ số	4
1.1.1. Chứng chỉ số.	4
1.1.2. Lợi ích của chứng chỉ số	5
1.1.3. X.509	5
1.1.4. Các phiên bản của chứng chỉ số	6
1.2. Chứng chỉ X.509 version 1 và X.509 version 2	6
1.2.1. Chứng chỉ X.509 version 1	6
1.2.2. Chứng chỉ X.509 version 2	8
1.3. Chứng chỉ X.509 version 3 và các trường mở rộng	9
Hạ tầng PKI	13
2.1. Hạ tầng cơ sở khóa công khai	13
2.2 Vai trò và chức năng	15
2.3 Các thành phần của một hạ tầng cơ sở khóa công khai	15
2.4. Một số hệ thống PKI	18
Sản phẩm mã nguồn mở- EJBCA	20
3.1. Tổng quan về EJBCA	20
3.2. Đặc điểm kỹ thuật	21
3.3. Kiến trúc EJBCA	22
3.4. Chức năng	23
3.5. Đánh giá, so sánh.	23
Các pha làm việc	25
4.1. Nhận Chứng thư số	25
4.1.1. Giới thiệu chức năng:	25
4.1.2. Hướng dẫn nghiệp vụ :	26
4.2. Gia hạn Chứng thư số	26
4.2.1 Giới thiệu chức năng:	26
4.2.2 Hướng dẫn nghiệp vụ:	27
4.3. Gia hạn Khóa	28
4.3.1 Giới thiệu chức năng:	28
4.3.2 Hướng dẫn nghiệp vụ:	29
4.4. Cấp lại Chứng thư số	29
4.4.1 Giới thiệu chức năng:	29

4.4.2 Hướng dẫn nghiệp vụ:	29
4.5. Hủy Chứng thư số	30
4.5.1 Giới thiệu chức năng:	30
4.5.2 Hướng dẫn nghiệp vụ:	30
4.6. Thay đổi thiết bị lưu Chứng thư số	32
4.6.1 Giới thiệu chức năng:	32
4.6.2 Hướng dẫn nghiệp vụ:	32
4.7. Thay đổi mật khẩu Chứng thư số	34
4.7.1 Giới thiệu chức năng:	34
4.7.2 Hướng dẫn nghiệp vụ:	34
4.8. Xem nội dung thông tin Chứng thư số	35
4.8.1 Giới thiệu chức năng:	35
4.8.2 Hướng dẫn nghiệp vụ:	35
4.9. Kiểm tra mật khẩu Chứng thư số	36
4.9.1 Giới thiệu chức năng:	36
4.9.2 Hướng dẫn nghiệp vụ:	37
4.10. Cài đặt thủ công chương trình	38
4.10.1 Giới thiệu chức năng:	38
4.10.2 Hướng dẫn nghiệp vụ:	38
Ứng dụng chứng thực chéo dựa trên EJBCA	39
5.2.1. Mô hình triển khai	39
5.2.2. Ứng dụng chứng thực chéo trên EJBCA	39

1. Định dạng X.509

1.1. Tổng quan về chứng chỉ số

1.1.1. Chứng chỉ số.

Chứng chỉ số là thành phần làm nền tảng cho hoạt động của PKI. Nó là tài liệu điện tử để xác minh danh tính cho người dùng, tổ chức, máy tính, thiết bị mạng hoặc dịch vụ nào đó trên internet. Chứng chỉ số phải do một tổ chức đứng ra chứng nhận những thông tin của bạn là chính xác, được gọi là “nhà cung cấp chứng chỉ số” (CA:certificate authority) và được liên kết với một cặp khóa công khai và khóa bí mật. CA phải đảm bảo về độ tin cậy, chịu trách nhiệm về độ chính xác của chứng chỉ số mà mình cấp.

Một chứng chỉ là một tập tin được ký số, có kích thước từ 2KB đến 4KB và thường bao gồm các thông tin cơ bản sau:

- Thông tin về người dùng, máy tính, thiết bị mạng, v.v.. mà nắm giữ khóa bí mật tương ứng với chứng chỉ được cấp phát. Người dùng, máy tính hoặc thiết bị mạng này được nhắc tới như là chủ thể (subject) của chứng chỉ.
- Thông tin về CA phát hành chứng chỉ.
- Khóa công khai tương ứng với khóa bí mật được liên kết với chứng chỉ.
- Tên của các thuật toán để mã hóa và thuật toán tạo chữ ký số cho chứng chỉ.
- Một danh sách các phần mở rộng (extension) cho loại chứng chỉ X.509 version 3.
- Thông tin giúp xác định trạng thái thu hồi (revocation) và tính hiệu lực của chứng chỉ (như ngày phát hành và ngày hết hạn).

Trong đó thì 3 thành phần chính của một chứng chỉ số là:

- Thông tin cá nhân của người được cấp.
- Khóa công khai (Public Key) của người được cấp.
- Chữ ký số của cơ sở cấp chứng chỉ.

CA phải bảo đảm nhận dạng của đối tượng yêu cầu là xác thực trước khi cấp chứng chỉ. Việc xác minh nhận dạng có thể được thực hiện dựa trên các giấy phép an ninh (security credential) của đối tượng hoặc thông qua cuộc gặp mặt

và trao đổi trực tiếp với người yêu cầu. Sau khi nhận dạng được kiểm chứng là hợp lệ, CA sẽ cấp chứng chỉ được ký số bởi khóa bí mật của nó cho họ. Chữ ký số này cho biết nguồn gốc của chứng chỉ (do CA nào cấp), đảm bảo khóa công khai là thuộc về chủ thể của chứng chỉ và giúp phát hiện những thay đổi, giả mạo nếu có trong nội dung của chứng chỉ.

1.1.2. Lợi ích của chứng chỉ số

Mã hóa: Khi người gửi đã mã hóa thông tin bằng khóa công khai của bạn thì chắc chắn rằng chỉ có bạn mới giải mã được thông tin để đọc

Chống giả: Chứng chỉ số không thể làm giả nên việc trao đổi thông tin có kèm chứng chỉ số luôn đảm bảo an toàn.

Xác thực: Khi gửi một thông tin kèm chứng chỉ số, người nhận có thể là một đối tác kinh doanh, tổ chức hoặc cơ quan chính quyền....sẽ xác thực được danh tính của bạn.

Chống chối cãi nguồn gốc: Khi sử dụng chứng chỉ số, bạn phải chịu trách nhiệm hoàn toàn về những thông tin mà chứng chỉ số đi kèm.

Chữ ký điện tử : Với chứng chỉ số cá nhân, bạn có thể tạo thêm một chữ ký điện tử email như một bằng chứng xác nhận của mình.

Bảo mật website: sử dụng cho mục đích thương mại điện tử hay cho những mục đích quan trọng khác, những thông tin trao đổi giữa bạn và khách hàng có thể bị lộ.

Đảm bảo phần mềm: chứng chỉ số như là “những con tem chống hàng giả” cho phần mềm thông qua chứng chỉ số bạn sẽ đảm bảo tính hợp pháp cũng như nguồn gốc xuất xứ của sản phẩm.

1.1.3. X.509

X.509 là một đề nghị của **ITU** (International Telecommunication Union) định nghĩa một framework về chứng thực (certificate). X.509 dựa trên X.500, mà bản thân X.500 còn chưa được định nghĩa hoàn hảo. Kết quả là chuẩn X.509 đang được diễn giải theo một số cách, tùy theo công ty cung cấp quyết định sử dụng như thế nào. X.509 lần đầu tiên được công bố vào năm 1988, và các phiên bản tiếp theo đã được đưa ra để giải quyết các vấn đề an toàn, đây cũng là sự cố xảy ra bất ngờ ngay lần công bố đầu tiên. X.509 hỗ trợ cả hai mã bí mật (mã đơn) và mã công khai. X.509 định nghĩa các nội dung về một chứng thực, bao gồm số

phiên bản, số serial, ID chữ ký, tên công bố, thời điểm có hiệu lực, định nghĩa chủ đề, phần mở rộng và chữ ký trên các trường trên. Về cơ bản, một người có trách nhiệm chứng nhận sẽ đặt khóa công khai của một người nào đó có nhu cầu chứng thực vào thủ tục chứng thực và sau đó xác thực lại bằng khóa riêng. Điều này bắt buộc khóa và thủ tục chứng thực phải luôn đi kèm với nhau. Bất cứ ai cần dùng khóa công cộng của một đối tượng nào đó đều có thể mở thủ tục chứng thực bằng khóa công cộng của các đối tượng này do người có trách nhiệm chứng thực cung cấp (các khóa công cộng này được ký hoặc khóa bằng khóa riêng của người có trách nhiệm chứng thực). Vì vậy, người sử dụng phải tin rằng người có trách nhiệm chứng thực sẽ bảo đảm việc hợp lệ hóa người chủ của khóa công khai và thực sự khóa công khai ở đây chính là khóa công khai của người có trách nhiệm chứng thực. Đây chính là lãnh địa của các **PKI** (public-key infrastructures). PKI là một kiến trúc phân cấp những đối tượng có trách nhiệm xác minh các khóa công khai lẫn nhau.

1.1.4. Các phiên bản của chứng chỉ số

Có 3 phiên bản của chứng chỉ số được dùng trong một hệ tầng PKI là:

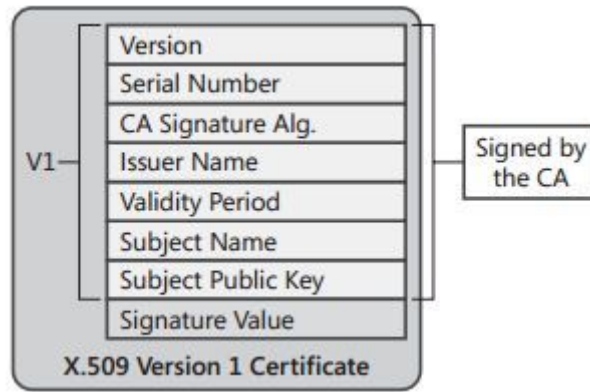
- Chứng chỉ X.509 version 1
- Chứng chỉ X.509 version 2
- Chứng chỉ X.509 version 3

1.2. Chứng chỉ X.509 version 1 và X.509 version 2

1.2.1. Chứng chỉ X.509 version 1

X.509 version 1

Được định nghĩa vào năm 1988, X.509 version 1 giờ đây hầu như không còn được sử dụng nữa. Định dạng của loại chứng chỉ này được thể hiện như hình dưới đây:



Một chứng chỉ X.509 version 1 bao gồm các trường sau:

Version: chứa giá trị cho biết đây là chứng chỉ X.509 version 1

Serial Number: cung cấp một mã số nhận dạng duy nhất cho mỗi chứng chỉ được phát hành bởi CA

CA Signature Algorithm: tên của thuật toán mà CA sử dụng để ký lên nội dung của chứng chỉ số.

Issuer Name: tên phân biệt (distinguished name) của CA phát hành chứng chỉ. Thường thì tên phân biệt này được biểu diễn theo chuẩn X.500 hoặc định dạng theo đặc tả của X.509 và RFC 3280.

Validity Period: khoảng thời gian mà chứng chỉ được xem là còn hiệu lực, bao gồm 2 trường là: Valid From và Valid To.

Subject Name: tên của máy tính, người dùng, thiết bị mạng sở hữu chứng chỉ. Thường thì tên chủ thể này được biểu diễn theo chuẩn X.500 hoặc định dạng theo đặc tả của X.509, nhưng cũng có thể bao gồm các định dạng tên khác như được mô tả trong RFC 822.

Subject Public Key Info: khóa công khai của đối tượng nắm giữ chứng chỉ. Khóa công khai này được gửi tới CA trong một thông điệp yêu cầu cấp chứng chỉ (certificate request) và cũng được bao gồm trong nội dung của chứng chỉ được phát hành sau đó. Trường này cũng chứa nhận dạng của thuật toán được dùng để tạo cặp khóa công khai và khóa bí mật được liên kết với chứng chỉ.

Signature Value: chứa giá trị của chữ ký.

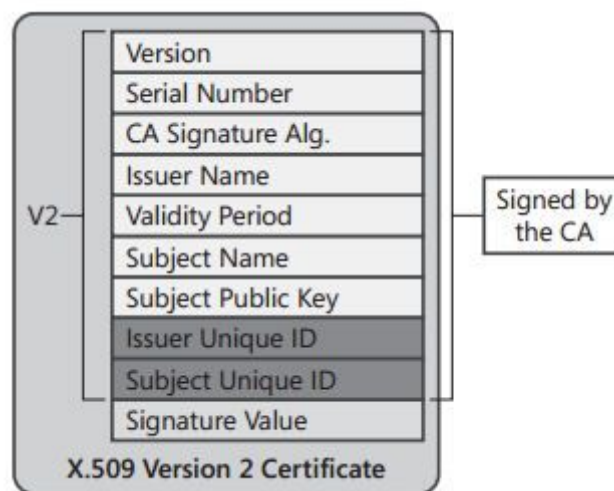
Các trường Issuer Name và Subject Name được cấu trúc để các chứng chỉ có thể được tổ chức thành một chuỗi các chứng chỉ mà bắt đầu bằng chứng chỉ được cấp cho người dùng, máy tính, thiết bị mạng, hoặc dịch vụ và kết thúc bằng chứng chỉ gốc của CA.

1.2.2. Chứng chỉ X.509 version 2

X.509 version 2

Mặc dù chứng chỉ X.509 version 1 cung cấp khá đầy đủ những thông tin cơ bản về người nắm giữ chứng chỉ nhưng nó lại có ít thông tin về tổ chức cấp phát chứng chỉ khi chỉ bao gồm Issuer Name, CA Signature Algorithm và Signature Value. Điều này không giúp dự phòng trong trường hợp CA được thay mới.

Khi chứng chỉ của CA được thay mới, trường Issuer Name trong cả 2 chứng chỉ mới và cũ đều như nhau. Tương tự, có thể có một tổ chức khác muốn tạo một CA có trường Issuer Name trong chứng chỉ giống như vậy. Giải quyết vấn đề này để có thể sử dụng lại Issuer Name thì chứng chỉ X.509 version 2 đã được giới thiệu vào năm 1993. Trong định dạng của nó có thêm 2 trường mới như được thể hiện trong hình dưới đây:



Hai trường mới được bổ sung là:

Issuer Unique ID: là một trường không bắt buộc, chứa chuỗi giá trị ở hệ 16, mang tính duy nhất và dành để nhận dạng CA. Khi CA thay mới chứng chỉ của chính nó, một Issuer Unique ID mới được khởi tạo cho chứng chỉ đó.

Subject Unique ID: là một trường không bắt buộc, chứa chuỗi giá trị ở hệ 16, mang tính duy nhất và dùng để nhận dạng chủ thể của chứng chỉ. Nếu chủ thể này cũng chính là CA thì trường này sẽ giống với Issuer Unique ID.

Ngoài việc đưa vào 2 trường mới ở trên thì trường Version trong chứng chỉ X.509 version 2 có giá trị là 2 để chỉ ra phiên bản của chứng chỉ.

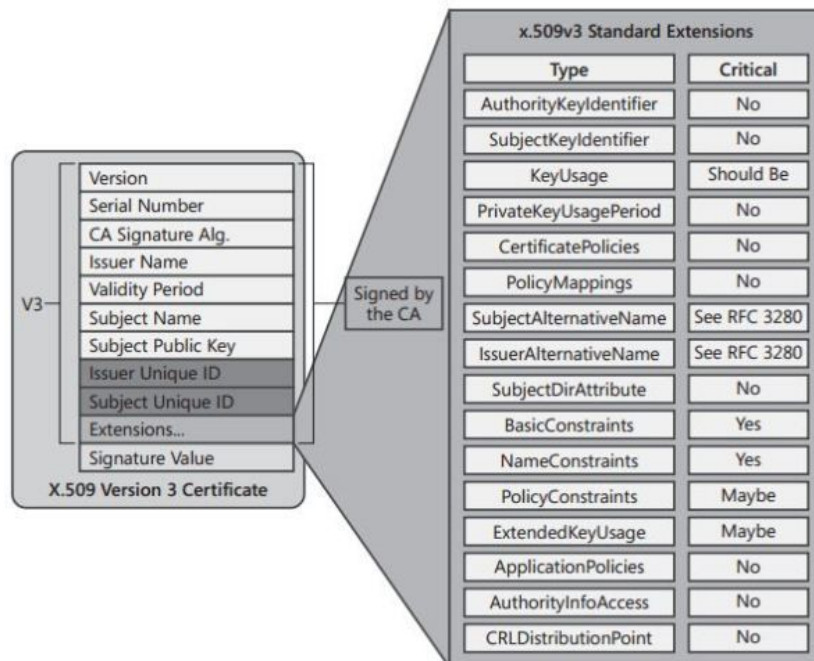
Các trường Issuer Unique ID và Subject Unique ID đã cải tiến quá trình xây chuỗi chứng chỉ. Giờ đây việc tìm kiếm chứng chỉ của CA sẽ là so khớp Issuer Name trong chứng chỉ được cấp phát với Subject Name trong chứng chỉ của CA và thực hiện thêm một bước kiểm tra thứ hai là so khớp Issuer Unique ID trong chứng chỉ được cấp phát với Subject Unique ID trong chứng chỉ của CA.

Bước so khớp thứ hai này cho phép phân biệt giữa các chứng chỉ của cùng một CA khi CA đó làm mới lại chứng chỉ của chính nó. Cách này cũng giúp phân biệt giữa các CA khác nhau nhưng trùng Subject Name.

Mặc dù định dạng X.509 version có cải tiến hơn version 1 nhưng chuẩn này cũng không còn được áp dụng rộng rãi. Và thực tế thì trong RFC 3280 đã khuyến cáo là bỏ qua việc sử dụng 2 trường mới trên của X.509 version 2 do lo ngại có thể có sự xung đột xảy ra nếu như hai chứng chỉ có cùng Subject Name và Subject Unique ID.

1.3. Chứng chỉ X.509 version 3 và các trường mở rộng

Được ra đời vào năm 1996, định dạng X.509 version 3 được bổ sung thêm các phần mở rộng (extension) để khắc phục các vấn đề liên quan tới việc so khớp Issuer Unique ID và Subject Unique ID cũng như là các vấn đề về xác thực chứng chỉ. Một chứng chỉ X.509 version 3 có thể chứa một hoặc nhiều extension, như được thể hiện trong hình dưới đây:



Mỗi extension trong chứng chỉ X.509 version 3 gồm 3 phần:

Extension Identifier: là một mã nhận dạng đối tượng (Object Identifier – OID) cho biết kiểu định dạng và các định nghĩa của extension.

Criticality Flag: là một dấu hiệu cho biết thông tin trong extension có quan trọng (critical) hay không. Nếu một ứng dụng không thể nhận diện được trạng thái critical của extension hoặc extension không hề chứa giá trị nào thì chứng chỉ đó không thể được chấp nhận hoặc được sử dụng. Nếu mục criticality flag này không được thiết lập thì một có thể sử dụng chứng chỉ ngay cả khi ứng dụng đó không nhận diện được extension.

Extension Value: là giá trị được gán cho extension. Nó phụ thuộc vào từng extension cụ thể.

Trong một chứng chỉ X.509 version 3, các extension sau có thể có là:

Authority Key Identifier: extension này có thể chứa một hoặc hai giá trị, chúng có thể là:

- Subject Name của CA và Serial Number của chứng chỉ của CA mà đã cấp phát chứng chỉ này.
- Giá trị băm của khóa công khai của chứng chỉ của CA mà đã cấp phát chứng chỉ này.

Subject Key Identifier: extension này chứa giá trị băm của khóa công khai của chứng chỉ.

Key Usage: một CA, người dùng, máy tính, thiết bị mạng hoặc dịch vụ có thể sở hữu nhiều hơn một chứng chỉ. Extension này định nghĩa các dịch vụ bảo mật mà một chứng chỉ có thể cung cấp như:

Digital Signature: khóa công khai có thể được dùng để kiểm tra chữ ký. Khóa này cũng được sử dụng để xác thực máy khách và xác minh nguồn gốc của dữ liệu.

Non-Repudiation: khóa công khai có thể được dùng để xác minh nhận dạng của người ký, ngăn chặn người ký này từ chối rằng họ không hề ký lên thông điệp hoặc đối tượng nào đó.

Key Encipherment: khóa công khai có thể được dùng để trao đổi khóa, ví dụ như đối xứng (hoặc khóa phiên). Giá trị này được dùng khi một khóa RSA được dùng cho việc quản lý khóa.

Data Encipherment: khóa công khai có thể được dùng để mã hóa dữ liệu một cách trực tiếp thay vì phải trao đổi một khóa đối xứng (hay khóa phiên) để mã hóa dữ liệu.

Key Agreement: khóa công khai có thể được dùng để trao đổi khóa, ví dụ như khóa đối xứng. Giá trị này được dùng khi một khóa Diffie-Hellman được dùng cho việc quản lý khóa.

Key Cert Sign: khóa công khai có thể được dùng để kiểm tra chữ ký của chứng chỉ số.

CRL Sign: khóa công khai có thể được dùng để kiểm tra chữ ký của CRL (danh sách chứa các chứng chỉ bị thu hồi).

Encipher Only: giá trị này được dùng kết hợp với các extension Key Agreement và Key Usage. Kết quả là khóa đối xứng chỉ có thể được dùng để mã hóa dữ liệu.

Decipher Only: giá trị này được dùng kết hợp với các extension Key Agreement và Key Usage. Kết quả là khóa đối xứng chỉ có thể được dùng để mã hóa dữ liệu.

Private Key Usage Period: extension này cho phép khóa bí mật có khoảng thời gian hiệu lực khác so với khoảng thời gian hiệu lực của chứng chỉ. Giá trị này có thể được đặt ngắn hơn so với khoảng thời gian hiệu lực của chứng chỉ. Điều này giúp khóa bí mật có thể được dùng để ký lên các tài liệu trong một khoảng thời gian ngắn (ví dụ, một năm) trong khi khóa công khai có thể được dùng để xác minh chữ ký trong khoảng thời gian hiệu lực của chứng chỉ là 5 năm.

Certificate Policies: extension này mô tả các chính sách và thủ tục được dùng để xác minh chủ thể của chứng chỉ trước khi chứng chỉ được cấp phát. Các chính sách chứng chỉ được đại diện bởi các OID. Ngoài ra, một chính sách chứng chỉ có thể bao gồm một đường dẫn (URL) tới trang web mô tả nội dung của chính sách và thủ tục.

Policy Mappings: extension này cho phép chuyển dịch thông tin về chính sách giữa hai tổ chức. Ví dụ, thử tưởng tượng rằng một tổ chức định nghĩa một chính sách chứng chỉ có tên là Management Signing mà trong đó các chứng chỉ được dùng để ký lên một lượng lớn các đơn đặt hàng. Một tổ chức khác có thể có một chính sách chứng chỉ tên là Large Orders mà cũng được dùng để ký lên một

lượng lớn các đơn đặt hàng. Khi đó, Policy Mapping cho phép hai chính sách chứng chỉ này được đánh giá ngang nhau.

Subject Alternative Name: extension này cung cấp một danh sách các tên thay thế cho chủ thể của chứng chỉ. Trong khi định dạng cho Subject Name thường tuân theo chuẩn X.500 thì Subject Alternative Name cho phép thể hiện theo các dạng khác như User Principal Name (UPN), địa chỉ email, địa chỉ IP hoặc tên miền (DNS).

Issuer Alternative Name: extension này cung cấp một danh sách các tên thay thế cho CA. Mặc dù thường không được áp dụng nhưng extension này có thể chứa địa chỉ email của CA.

Subject Dir Attribute: extension này có thể bao gồm bất kỳ thuộc tính nào từ danh mục LDAP hoặc X.500 của tổ chức, ví dụ, thuộc tính country. Extension này có thể chứa nhiều thuộc tính và với mỗi thuộc tính phải gồm OID và giá trị tương ứng của nó.

Basic Constraints: extension này cho biết chứng chỉ có phải của CA hay của các chủ thể như người dùng, máy tính, thiết bị, dịch vụ. Ngoài ra, extension này còn bao gồm một ràng buộc về độ dài của đường dẫn mà giới hạn số lượng các CA thứ cấp (subordinated CA) có thể tồn tại bên dưới CA mà cấp phát chứng chỉ này.

Name Constraints: extension này cho phép một tổ chức chỉ định không gian tên (namespace) nào được phép hoặc không được phép sử dụng trong chứng chỉ.

Policy Constraints: extension này có thể có trong các chứng chỉ của CA. Nó có thể ngăn cấm Policy Mapping giữa các CA hoặc yêu cầu mỗi chứng chỉ trong chuỗi chứng chỉ phải bao gồm một OID của chính sách chứng chỉ.

Enhanced Key Usage: extension này cho biết khóa công khai của chứng chỉ có thể được sử dụng như thế nào. Những cái này không có trong extension Key Usage. Ví dụ: Client Authentication (có OID là 1.3.6.1.5.5.7.3.2), Server Authentication (có OID là 1.3.6.1.5.5.7.3.1), và Secure Email (có OID là 1.3.6.1.5.5.7.3.4). Khi ứng dụng nhận được một chứng chỉ, nó có thể yêu cầu sự có mặt của một OID trong các OID kể trên.

CRL Distribution Points: extension này chứa một hoặc nhiều URL dẫn tới tập tin chứa danh sách các chứng chỉ đã bị thu hồi (CRL) được phát hành bởi CA. Nếu việc kiểm tra trạng thái thu hồi của chứng chỉ được cho phép thì một ứng

dụng sẽ sử dụng các URL này để tải về phiên bản cập nhật của CRL. Các URL có thể sử dụng một trong các giao thức như HTTP, LDAP, FTP, File.

Authority Information Access: extension này có thể chứa một hoặc nhiều URL dẫn tới chứng chỉ của CA. Một ứng dụng sử dụng URL này để tải về chứng chỉ của CA khi xây dựng chuỗi chứng chỉ nếu như nó không có sẵn trong bộ nhớ đệm của ứng dụng.

Freshest CRL: extension này chứa một hoặc nhiều URL dẫn tới delta CRL do CA phát hành. Delta CRL chỉ chứa các chứng chỉ bị thu hồi kể từ lần cuối base CRL được phát hành. Nếu việc kiểm tra trạng thái thu hồi của chứng chỉ được cho phép thì một ứng dụng sẽ sử dụng các URL này để tải về phiên bản cập nhật của delta CRL. Các URL có thể sử dụng một trong các giao thức như HTTP, LDAP, FTP, File.

Subject Information Access: extension này chứa thông tin cho biết cách thức để truy cập tới các chi tiết khác về chủ thể của chứng chỉ. Nếu đây là chứng chỉ của CA thì thông tin này có thể bao gồm các chi tiết về các dịch vụ xác minh chứng chỉ hay chính sách của CA. Nếu chứng chỉ được cấp cho người dùng, máy tính, thiết bị mạng, hoặc dịch vụ thì extension này có thể chứa thông tin về các dịch vụ được các chủ thể này cung cấp và cách thức để truy cập tới các dịch vụ đó.

2. Hạ tầng PKI

2.1. Hạ tầng cơ sở khóa công khai

Trong mật mã học, hạ tầng cơ sở khóa công khai PKI (Public Key Infrastructure) là một cơ chế để cho một bên thứ 3 (thường là cơ quan cấp chứng thực số) cung cấp và xác thực định danh các bên tham gia vào quá trình trao đổi thông tin. Cơ chế này cũng cho phép gán cho mỗi người sử dụng trong hệ thống một cặp khóa công khai/khóa bí mật. Các quá trình này thường được thực hiện bởi một phần mềm đặt tại trung tâm và các phần mềm phối hợp khác tại các địa điểm của người dùng.

Khóa công khai thường được phân phối trong chứng thực điện tử. Khái niệm hạ tầng khóa công khai thường được dùng để chỉ toàn bộ hệ thống bao gồm cơ quan cấp chứng thực số (CA) cùng các cơ chế liên quan đồng thời với toàn bộ

việc sử dụng các thuật toán mật mã hóa khóa công khai trong trao đổi thông tin. Tuy nhiên phần sau được bao gồm không hoàn toàn chính xác bởi vì các cơ chế trong PKI không nhất thiết sử dụng các thuật toán mã hóa khóa công khai.

PKI cho phép những người tham gia xác thực lẫn nhau và sử dụng thông tin từ các chứng thực khóa công khai để mã hóa và giải mã thông tin trong quá trình trao đổi. Thông thường, PKI bao gồm phần mềm máy khách (client), phần mềm máy chủ (server), phần cứng (như thẻ thông minh) và các quy trình hoạt động liên quan. Người sử dụng cũng có thể ký các văn bản điện tử với khóa bí mật của mình và mọi người đều có thể kiểm tra với khóa công khai của họ. PKI cho phép các giao dịch điện tử được diễn ra đảm bảo tính bí mật, toàn vẹn và xác thực lẫn nhau mà không cần phải trao đổi các thông tin mật từ trước.

Hầu hết các hệ thống PKI quy mô doanh nghiệp đều dựa trên các chuỗi chứng thực để xác thực các thực thể. Chứng thực của người dùng sẽ được một cơ quan cấp chứng thực số cấp, đến lượt nhà cung cấp này lại có chứng thực được một nhà cung cấp khác ở cấp cao hơn tạo ra... (hình cây). Hệ thống sẽ bao gồm nhiều máy tính thuộc nhiều tổ chức khác nhau với các gói phần mềm tương thích từ nhiều nguồn khác nhau. Vì vậy, các tiêu chuẩn là yếu tố rất quan trọng đối với hoạt động của các PKI. Hầu hết các tiêu chuẩn về PKI hiện tại được soạn thảo bởi nhóm làm việc PKIX của IETF.

Các hệ thống PKI doanh nghiệp thường được tổ chức theo mô hình danh bạ trong đó khóa công khai của mỗi người dùng được lưu trữ (bên trong các chứng thực số) kèm với các thông tin cá nhân (số điện thoại, E-mail, địa chỉ, nơi làm việc...). Hiện nay, công nghệ danh bạ tiên tiến nhất là LDAP và định dạng chứng thực phổ biến nhất

X.509 cũng được phát triển từ mô hình trước đó của LDAP là X.500. Mục tiêu chính của PKI là cung cấp khóa công khai và xác định mối liên hệ giữa khóa và định dạng người dùng. Nhờ vậy người dùng có thể sử dụng trong một số ứng dụng như:

- Mã hóa E-mail hoặc xác thực người gửi E-mail (OpenPGP hay S/MIME).
- Mã hóa hoặc nhận thực văn bản (Các tiêu chuẩn chữ ký XML hoặc mã hóa XML khi văn bản được thể hiện dưới dạng XML).

- Xác thực người dùng ứng dụng (Đăng nhập bằng thẻ thông minh nhận thực người dùng trong SSL).
- Các giao thức truyền thông an toàn dùng kỹ thuật Bootstrapping (IKE, SSL): trao đổi khóa bằng khóa bất đối xứng, còn mã hóa bằng khóa đối xứng.

2.2 Vai trò và chức năng

PKI cho phép những người tham gia xác thực lẫn nhau. Mục tiêu chính của PKI là cung cấp khóa công khai và xác định mối liên hệ giữa khóa và định danh người dùng. Nhờ vậy người dùng có thể sử dụng trong một số ứng dụng như:

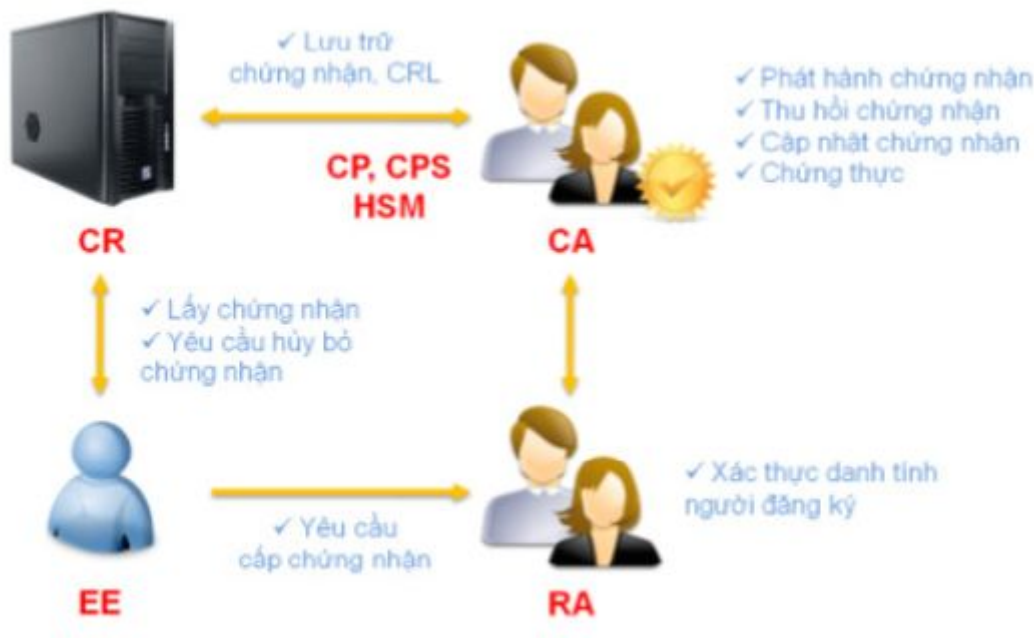
- Mã hóa, giải mã văn bản;
- Xác thực người dùng ứng dụng;
- Mã hóa email hoặc xác thực người gửi email;
- Tạo chữ ký số trên văn bản điện tử.

Một PKI phải đảm bảo được các tính chất sau trong một hệ thống trao đổi thông tin:

- Tính bí mật (Confidentiality): PKI phải đảm bảo tính bí mật của dữ liệu.
- Tính toàn vẹn (Integrity): PKI phải đảm bảo dữ liệu không thể bị mất mát hoặc chỉnh sửa và các giao tác không thể bị thay đổi.
- Tính xác thực (Authentication): PKI phải đảm bảo danh tính của thực thể được xác minh.
- Tính không thể chối từ (Non-Repudiation): PKI phải đảm bảo dữ liệu không thể bị không thừa nhận hoặc giao tác bị từ chối.

2.3 Các thành phần của một hạ tầng cơ sở khóa công khai

PKI là cơ cấu tổ chức gồm con người, tiến trình, chính sách, thủ tục, phần cứng và phần mềm dùng để phát sinh, quản lý, lưu trữ, triển khai và thu hồi các chứng nhận khóa công khai



PKI gồm các thành phần chính sau:

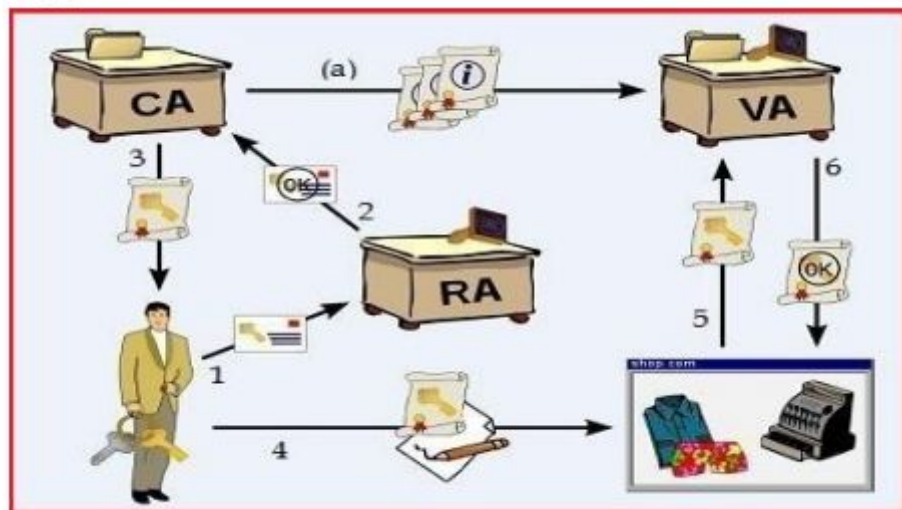
- Thực thể cuối (End Entity – EE): Đối tượng sử dụng chứng nhận (chứng thư số): có thể là một tổ chức, một người cụ thể hay một dịch vụ trên máy chủ, ...
- Tổ chức chứng nhận (Certificate Authority – CA): Có nhiệm vụ phát hành, quản lý và hủy bỏ các chứng thư số. Là thực thể quan trọng trong một PKI mà được thực thể cuối tin nhiệm. Gồm tập hợp các con người và các hệ thống máy tính có độ an toàn cao.
- Chứng nhận khóa công khai (Public Key Certificate): Một chứng nhận khóa công khai thể hiện hay chứng nhận sự ràng buộc của danh tính và khóa công khai của thực thể cuối. Chứng nhận khóa công khai chứa đủ thông tin cho những thực thể khác có thể xác nhận hoặc kiểm tra danh tính của chủ nhận chứng nhận đó.

Định dạng được sử dụng rộng rãi nhất của chứng nhận số dựa trên chuẩn IETF X.509.

- Tổ chức đăng ký chứng nhận (Registration Authority – RA):

- Mục đích chính của RA là để giảm tải công việc của CA.
- Xác thực cá nhân, chủ thể đăng ký chứng thư số.
- Kiểm tra tính hợp lệ của thông tin do chủ thể cung cấp.

- Xác nhận quyền của chủ thể đối với những thuộc tính chứng thư số được yêu cầu.
 - Kiểm tra xem chủ thể có thực sự sở hữu khóa riêng đang được đăng ký hay không (chứng minh sở hữu).
 - Tạo cặp khóa bí mật, công khai. (nếu chủ thể yêu cầu)
 - Phân phối bí mật được chia sẻ đến thực thể cuối (ví dụ khóa công khai của CA).
 - Thay mặt chủ thể thực thể cuối khởi tạo quá trình đăng ký với CA.
 - Lưu trữ khóa riêng.
 - Khởi sinh quá trình khôi phục khóa
 - Phân phối thẻ bài vật lý (thẻ thông minh)
- Kho lưu trữ chứng nhận (Certificate Repository – CR):
- Hệ thống (có thể tập trung hoặc phân tán) lưu trữ chứng thư và danh sách các chứng thư bị thu hồi
 - Cung cấp cơ chế phân phối chứng thư và danh sách thu hồi chứng thư (CRLs - Certificate Revocation Lists).



- (1) : Người dùng gửi yêu cầu phát hành thẻ chứng thư số và khóa công khai của nó đến RA;
- (2) : Sau khi xác nhận tính hợp lệ định danh của người dùng thì RA sẽ chuyển yêu cầu này đến CA;
- (3) : CA phát hành thẻ chứng thư số cho người dùng;
- (4) : Sau đó người dùng “ký” thông điệp trao đổi với thẻ chứng thư số mới vừa nhận được từ CA và sử dụng chúng (thẻ chứng thực số + chữ ký số) trong giao dịch;

- (5) : Định danh của người dùng được kiểm tra bởi đối tác thông qua sự hỗ trợ của VA;

VA (validation authority) : Cơ quan xác thực của bên thứ ba có thể cung cấp thông tin thực thể này thay mặt cho CA.)

- (6) : Nếu chứng thư số của người dùng được xác nhận tính hợp lệ thì đối tác mới tin cậy người dùng và có thể bắt đầu quá trình trao đổi thông tin với nó (VA nhận thông tin về thẻ chứng thư số đã được phát hành từ CA (a))

2.4. Một số hệ thống PKI

Việc Diffie, Hellman và Rivest, Shamir, Adleman công bố công trình nghiên cứu về trao đổi khóa an toàn và thuật toán mật mã hóa khóa công khai vào năm 1976 đã làm thay đổi hoàn toàn cách thức trao đổi thông tin mật. Cùng với sự phát triển của các hệ thống truyền thông điện tử tốc độ cao (Internet và các hệ thống trước nó), nhu cầu về trao đổi thông tin bí mật trở nên cấp thiết.

Thêm vào đó một yêu cầu nữa phát sinh là việc xác định định dạng của những người tham gia vào quá trình thông tin. Vì vậy ý tưởng về việc gắn định dạng người dùng với chứng thực được bảo vệ bằng các kỹ thuật mật mã đã được phát triển một cách mạnh mẽ. Các nhà doanh nghiệp kỳ vọng vào một thị trường hứa hẹn mới đã thành lập những công ty hoặc dự án mới về PKI và bắt đầu vận động các chính phủ để hình thành nên khung pháp lý về lĩnh vực này.

Một dự án của American Bar Association đã xuất bản một nghiên cứu tổng quát về những vấn đề pháp lý có thể nảy sinh khi vận hành PKI. Không lâu sau đó, một vài tiểu bang của Hoa Kỳ mà đi đầu là Utah (năm 1995) đã thông qua những dự luật và quy định đầu tiên.

Các nhóm bảo vệ quyền lợi người tiêu dùng thì đặt ra các vấn đề về bảo vệ quyền riêng tư và các trách nhiệm pháp lý. Tuy nhiên, các luật và quy định đã được thông qua lại không thống nhất trên thế giới. Thêm vào đó là những khó khăn về kỹ thuật và vận hành khiến cho việc thực hiện PKI khó khăn hơn rất nhiều so với kỳ vọng ban đầu.

Tại thời điểm đầu thế kỷ XXI, người ta nhận ra rằng các kỹ thuật mật mã cũng như các quy trình/giao thức rất khó được thực hiện chính xác và các tiêu chuẩn hiện tại chưa đáp ứng được các yêu cầu đề ra. 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 người ta đã đặt hy vọng vào nó. Những PKI thành công nhất tới nay là các phiên bản do các chính phủ thực hiện.

Dưới đây là danh sách một số hệ thống PKI, trong đó một số cơ quan cấp chứng thực số hàng đầu (ví dụ VeriSign) không được liệt kê vì các phần mềm của họ không được công bố công khai.

- Hệ thống quản lý chứng thực Red Hat
- Computer Associates eTrust PKI
- Entrust
- Microsoft
- US Government External Certificate Authority (ECA)
- Nexus
- OpenCA (Một mô hình PKI mã nguồn mở)
- RSA Security
- phpki
- GenCerti
- ejbca
- newpki
- Papyrus CA Software
- pyCA
- IDX-PKI

- TinyCA
- ElyCA
- SimpleCA
- SeguriData
- Safelayer Secure Communication

3. Sản phẩm mã nguồn mở- EJBCA

3.1. Tổng quan về EJBCA

EJBCA là sản phẩm mã nguồn mở của hãng Primekey. Đây là một CA được xây dựng dựa trên công nghệ Java J2EE, nhờ đó hiệu suất hoạt động cũng như khả năng tùy biến của CA là tương đối cao so với các hệ thống mã nguồn mở khác. Bên cạnh đó, EJBCA còn cung cấp các tính năng và thành phần (OCSP, RA Service, Publisher,...) giúp cấu thành một hệ thống PKI tương đối đầy đủ và hoàn thiện.

EJBCA trải qua các giai đoạn phát triển như sau:

- Phiên bản 1.x bắt đầu như một bản beta trên SourceForge vào tháng 11/2001. Ý tưởng của EJBCA là thực thi một CA bên trong một máy chủ ứng dụng J2EE. Phiên bản 1.0-1.4 cung cấp các hỗ trợ đối với Jboss, WebLogic, CRL, LDAP, MySQL, PostgreSQL, Oracle.
- Phiên bản 2.x lấy kinh nghiệm từ phiên bản 1.x và được bắt đầu từ tháng 3/2003. Phiên bản này cung cấp các hỗ trợ đối với thẻ từ, PIN/PUK, phục hồi khóa, trạng thái chứng nhận, OCSP, SCEP, các tính năng đặc biệt cho AD và Outlook, OpenLDAP.
- Phiên bản 3.x bắt đầu từ tháng 6/2004, cung cấp các hỗ trợ đối với CA ảo, kiểm tra JUnit, hỗ trợ HSM (nCipher, Luna/Eracom/SafeNet), ngôn ngữ (Tây Ban nha, Pháp, Ý, Trung Quốc, Thụy Điển, Đức), OCSP Responder bên ngoài, Informix, OpenVPN, RA API ngoài, CMP, XKMSv2, các dịch vụ theo dõi, ECDSA, các mở rộng chứng nhận tùy thích, DN và alt Name OIDs. EJBCA là phần mềm mở nguồn mở, hỗ trợ rất nhiều chức năng. Tính đến 6/10/2008, phiên bản 3.x đã có hơn 47.600 lượt tải về . EJBCA

thực sự đã trở thành một sản phẩm toàn diện cho các giải pháp PKI/CA thay thế cho mọi ứng sản phẩm khác.

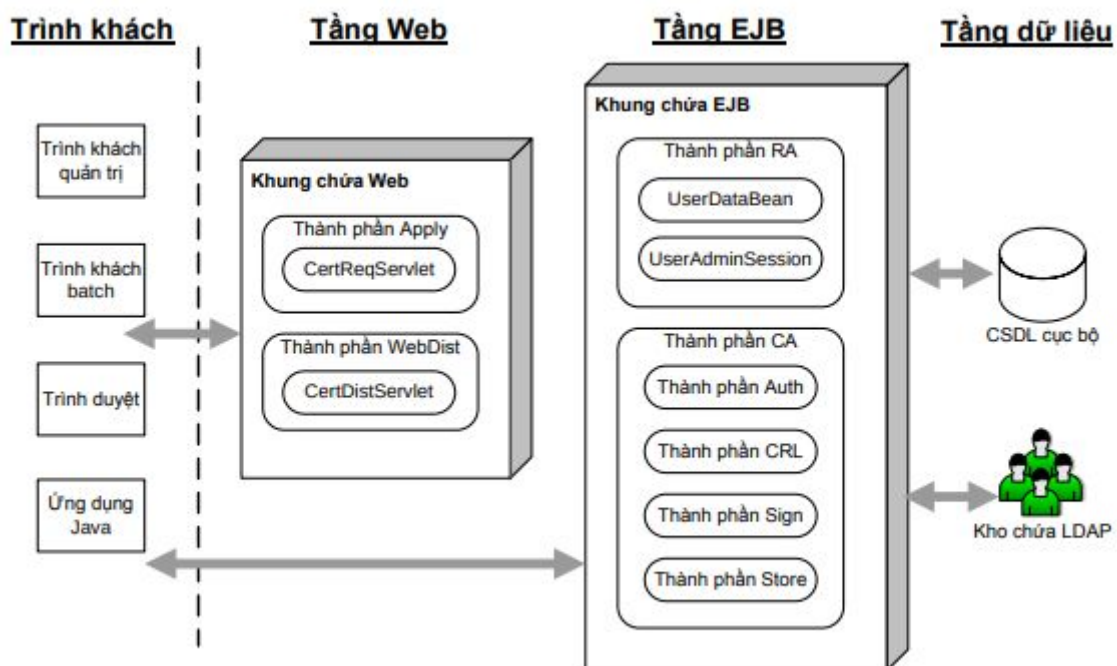
3.2. Đặc điểm kỹ thuật

Được xây dựng dựa trên Java, EJBCA thực sự là một nền tảng độc lập, chạy trên hầu như toàn bộ các phần cứng phổ biến cũng như các hệ điều hành thông dụng như: Windows, Linux. Để có thể hoạt động, EJBCA cần chạy trên một nền tảng máy chủ ứng dụng (Application Server) cũng như một hệ thống Cơ sở dữ liệu nhất định. Về mặt này, EJBCA cũng hỗ trợ hầu hết các nền tảng App Server phổ biến hiện nay như: JBOSS – Oracle, Weblogic – IBM Websphere ... cũng như các hệ cơ sở dữ liệu từ miễn phí đến trả phí: MySQL, Oracle, IBM DB2, MS SQL,...

Bên cạnh đó, EJBCA còn có một số điểm đặc trưng sau:

- Cung cấp khả năng xây dựng CA theo nhiều mức, không giới hạn số lượng CA.
- Hỗ trợ thuật toán RSA với độ dài khóa lên tới 4096 bits.
- Hỗ trợ các thuật toán DSA với độ dài khóa lên tới 1024 bits.
- Hỗ trợ các hàm băm như MD5, SHA-1, SHA-256.
- Chứng thư được phát hành tuân thủ nghiêm ngặt chuẩn X509.

3.3. Kiến trúc EJBCA



Hình 3.1: Kiến trúc EJBCA

EJBCA được xây dựng với kiến trúc phân tầng, cụ thể như sau:

- Tầng dữ liệu (Data Tier): Tầng dữ liệu lưu trữ các chứng nhận, CRL cũng như các thực thể cuối. EJBCA sử dụng một cơ sở dữ liệu mặc định để lưu trữ các thực thể cuối. Các chứng nhận được lưu trữ trong một kho chứa LDAP (Lightweight Directory Access Protocol).
- Thành phần CA: Thành phần có chức năng tạo các CA gốc, CA con, chứng nhận, CRL và giao tiếp với kho chứa LDAP để lưu trữ thông tin chứng nhận.
- Thành phần RA: Thành phần có chức năng tạo, xóa và hủy bỏ người dùng. Nó giao tiếp với cơ sở dữ liệu cục bộ để chứa thông tin người dùng.
- Tầng Web: Đây là giao diện (điển hình là giao diện người – máy bằng đồ họa) để trình khách tương tác với hệ thống EJBCA, đồng thời quy định các cấp độ và phạm vi truy cập thông tin khác nhau cho thực thể cuối.
- Trình khách: Trình khách là thực thể cuối hay người sử dụng như trình khách thư điện tử, máy chủ web, trình duyệt web hay cổng VPN. Các thực thể cuối không được phép phát hành chứng nhận đến các thực thể khác, nói cách khác chúng là các nút lá trong PKI.

3.4. Chức năng

- EJBCA là một tổ chức chứng nhận rất phổ biến hiện đang được sử dụng, một trong những CA được ưa thích hiện nay. Các đặc trưng cơ bản của CA này bao gồm sự lựa chọn của thuật toán ta cần như tùy chọn chọn giữa các thuật toán SHA1 hay SHA256 với RSA và với các kích thước khóa khác nhau như 1024, 2048 và 4096.
- Cung cấp một số tính năng nổi bật về lựa chọn ngôn ngữ trong quá trình cấu hình hệ thống.
- Ngoài ra cũng có thể chọn loại publisher mình muốn như LDAP, thư mục động (AD – Active Directory) hay một kết nối publisher tự làm.
- Sự phát hành của chứng nhận luôn luôn thuộc chuẩn X509. Cũng có một tùy chọn được cung cấp để chọn loại khóa ký – soft hay hard. Việc ký

chứng nhận có thể là tự ký (self-signed), CA bên ngoài (external CA) hay CA quản trị (admin CA).

- CA gốc có khóa RSA độ dài mặc định là 2048 bit và có hiệu lực 10 năm. Việc đăng ký chứng nhận trong EJBCA cung cấp cho người sử dụng nhiều lựa chọn như người sử dụng có thể chọn nhà cung cấp dịch vụ mã hóa (Cryptographic Service Provider – CSP22) mà họ thích và có thể chọn kích thước khóa khác nhau được cung cấp như 512, 1024 và 2048. Nó cũng cung cấp cho người sử dụng những tùy chọn của việc thêm chứng nhận vào thẻ nhận dạng điện tử (Electronic Identity Card)

3.5. Đánh giá, so sánh.

Ngoài EJBCA còn có các sản phẩm khác có thể triển khai hệ thống PKI hoàn chỉnh như OpenCA và Windows 2003 Server CA. Do Windows 2003 Server CA không phải là sản phẩm mã nguồn mở, không thể tự do phát triển cũng như kiểm soát được quá trình phát triển và độ an toàn nên không được quan tâm tìm hiểu.

EJBCA và OpenCA đều là các dự án PKI mã nguồn mở mạnh và hiện cũng có nhiều phát triển đang được thực hiện trên cả hai phần mềm này.

EJBCA là một CA và là một hệ thống quản lý PKI hoàn chỉnh, là một giải pháp PKI rất mạnh, độc lập môi trường, hiệu suất cao, có thể mở rộng và dựa trên thành phần. Ngoài ra, EJBCA rất linh hoạt trong việc cung cấp các cách thức hoạt động tùy chọn như một CA độc lập hoặc được tích hợp hoàn toàn trong ứng dụng thương mại bất kỳ. Hơn nữa, tuy việc cấu hình hệ thống EJBCA phức tạp hơn OpenCA rất nhiều nhưng hệ thống EJBCA khi đã đi vào hoạt động lại mang đến rất nhiều tiện lợi và đơn giản cho người sử dụng trong việc phát sinh và quản lý chứng nhận. Ngoài ra, khác với OpenCA, việc cập nhật CRL trong EJBCA hoàn toàn tự động.

Ngoài ra, EJBCA được phát triển và cung cấp bởi PrimeKey, một công ty PKI mã nguồn mở đứng đầu trên thế giới nên với việc sử dụng EJBCA ta có thể thừa hưởng từ năng lực phát triển của công ty và hoàn toàn yên tâm về tính an toàn luôn có trong mã nguồn.

Bảng so sánh một số đặc điểm giữa EJBCA và OpenCA

Đặc điểm	EJBCA	OpenCA
Độ khó khi cấu hình	Rất phức tạp	Phức tạp
Tính cân 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 không thể chối từ	Có	Có
Khả năng chọn thuật toán để sử dụng	Có	Có
OCSP ²³	Có	Không
Khả năng chọn CSP	Có	Không
Cập nhật CRL	Tự động	Bằng tay
Hỗ trợ thẻ thông minh	Có	Không
Chi phí	Miễn phí	Miễn phí
Các mở rộng	Có	Có
Môi trường nền	Java J2EE (độc lập nền)	Perl CGI trên Unix
Cơ sở dữ liệu	Hypersonic, PostgreSQL, MySQL, MS SQL, Oracle, Sybase, Informix, DB2	MySQL
Hỗ trợ LDAP	Có	Có
Môđun	EJB	Perl
Dựa trên thành phần	Có	Có
Khả năng mở rộng	Được thiết kế tổ và có thể mở rộng	Mở rộng khó với độ phức tạp tăng rất nhiều
Thành phần độc lập	PKI có thể được quản trị hoàn toàn thông qua dòng lệnh	Chỉ có một cách quản trị PKI là thông qua giao diện web
Các trình duyệt được hỗ trợ	Nhiều	Nhiều

Lý do chọn gói phần mềm mã nguồn mở EJBCA

- EJBCA đảm bảo tất cả các tiêu chí trong bảng trên
- Là một CA và là một hệ thống quản lý PKI hoàn chỉnh, là một giải pháp PKI rất mạnh, độc lập môi trường, hiệu suất cao, có thể mở rộng và dựa trên thành phần.
- Linh hoạt trong việc cung cấp các cách thức hoạt động tùy chọn như một CA độc lập hoặc được tích hợp hoàn toàn trong ứng dụng thương mại bất kỳ
- Việc cập nhật CRL trong EJBCA hoàn toàn tự động.
- Tuy việc cấu hình hệ thống EJBCA phức tạp hơn OpenCA rất nhiều nhưng hệ thống EJBCA khi đã đi vào hoạt động lại mang đến rất nhiều tiện lợi và đơn giản cho người sử dụng trong việc phát sinh và quản lý chứng nhận.

4. Các pha làm việc

4.1. Nhận Chứng thư số

4.1.1. Giới thiệu chức năng:

Chức năng này dùng cho người dùng đã có Mã phê duyệt chứng nhận số và số tham chiếu.

Chức năng này dùng thay thế Bước: Nhận Chứng thư số của quy trình đăng ký người dùng BMT/NT

4.1.2. Hướng dẫn nghiệp vụ :

Quản lý Chứng thư số	
1	<p>Nhận Chứng thư số Nhập Mã phê duyệt CTS và Số tham chiếu để nhận CTS.</p> <p>Gia hạn Chứng thư số Kéo dài thời gian sử dụng CTS khi CTS đã hết hạn. Việc gia hạn CTS chỉ được thực hiện 30 ngày trước khi hết hạn và chức năng này không làm thay đổi khóa đang dùng.</p> <p>Gia hạn khóa Giữ khóa đang dùng.</p> <p>Cấp lại Chứng thư số Khi CTS hết hạn, người dùng cần nhập số và theo các bước như sau để cấp lại.</p>
2	<p>Hủy Chứng thư số Thực hiện hủy CTS này sẽ xóa tất cả thông tin liên quan đến CTS.</p>
3	<p>Thay đổi thiết bị lưu Chứng thư số Là hình thức sao chép CTS. Bạn có thể di chuyển CTS lưu trên đĩa cứng, đĩa mềm, USB-khóa hoặc thẻ thông minh và lưu nó sang các phương tiện thông tin lưu trữ khác.</p>
4	<p>Thay đổi mật khẩu Chứng thư số Đây là chức năng thay đổi mật khẩu CTS được sử dụng khi tham gia vào Hệ thống.</p>
5	<p>Xem nội dung Chứng thư số Sử dụng chức năng này để xem chi tiết thông tin chứng nhận số của bạn. Có thể xác nhận nội dung thông tin chứng nhận số bao gồm thời hạn sử dụng, nơi cấp v...</p> <p>Kiểm tra mật khẩu Chứng thư số Nếu có thông báo "Mật khẩu bạn nhập vào không chính xác." Hãy nhấn vào đây rồi chọn phương tiện lưu giữ tương ứng. Sau khi nhấn vào chứng nhận số và nhập mật khẩu hãy xác nhận công việc này.</p> <p>Cài đặt thủ công chương trình Chương trình quản lý chứng thư số sẽ tự động cài đặt. Khi một cửa sổ pop-up xuất hiện, bấm vào OK để hoàn tất việc cài đặt. Nếu cài đặt không thành công thì bấm vào nút này sau đó tải file xuống. Đóng tất cả các cửa sổ rồi thực hiện run file 98install.bat nếu là window 95, 98, và NTinstall.bat nếu là window NT, 2000 trong C:\SignGATE.</p>

Đây là màn hình nhận Chứng thư số, sau khi đã nhận được Mã phê duyệt Chứng nhận số và số tham chiếu ở Bước 2 của quy trình đăng ký BMT/NT.

Sau khi đã nhập 2 thông số trên, người dùng thực hiện các bước làm tương tự như Bước 3: Nhận Chứng thư số của quy trình đăng ký người dùng BMT/NT. Sau khi thực hiện xong các bước như nói trên, người dùng nhận được Chứng thư số của mình.

4.2. Gia hạn Chứng thư số

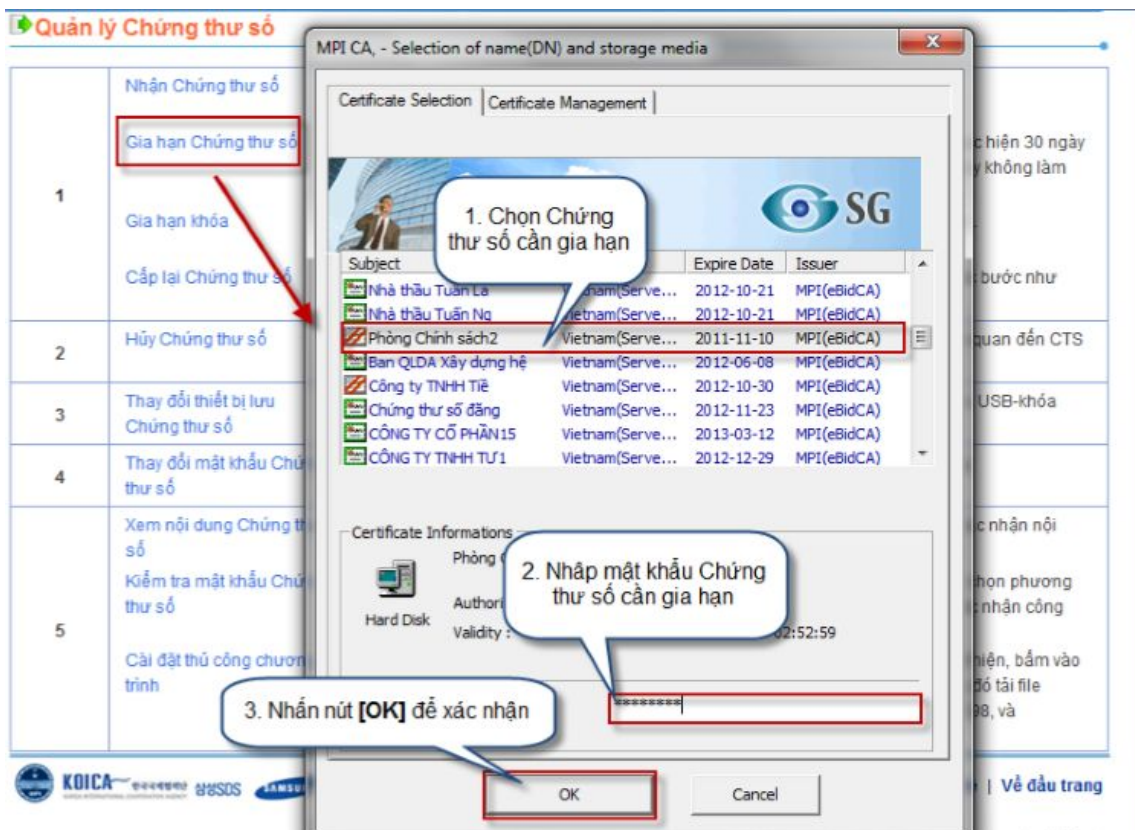
4.2.1 Giới thiệu chức năng:

Chức năng này được sử dụng khi chứng thư số của người dùng (Bên mời thầu, nhà thầu) hết hạn, người dùng vào chức năng này để gia hạn mà không cần gửi công văn đến Cơ quan vận hành hệ thống xin gia hạn.

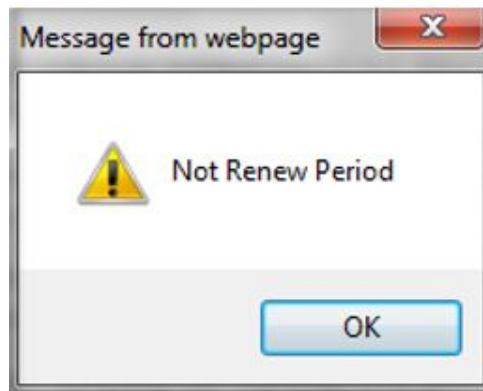
Chứng thư số chỉ được gia hạn trong vòng 30 ngày trước khi hết hạn.

4.2.2 Hướng dẫn nghiệp vụ:

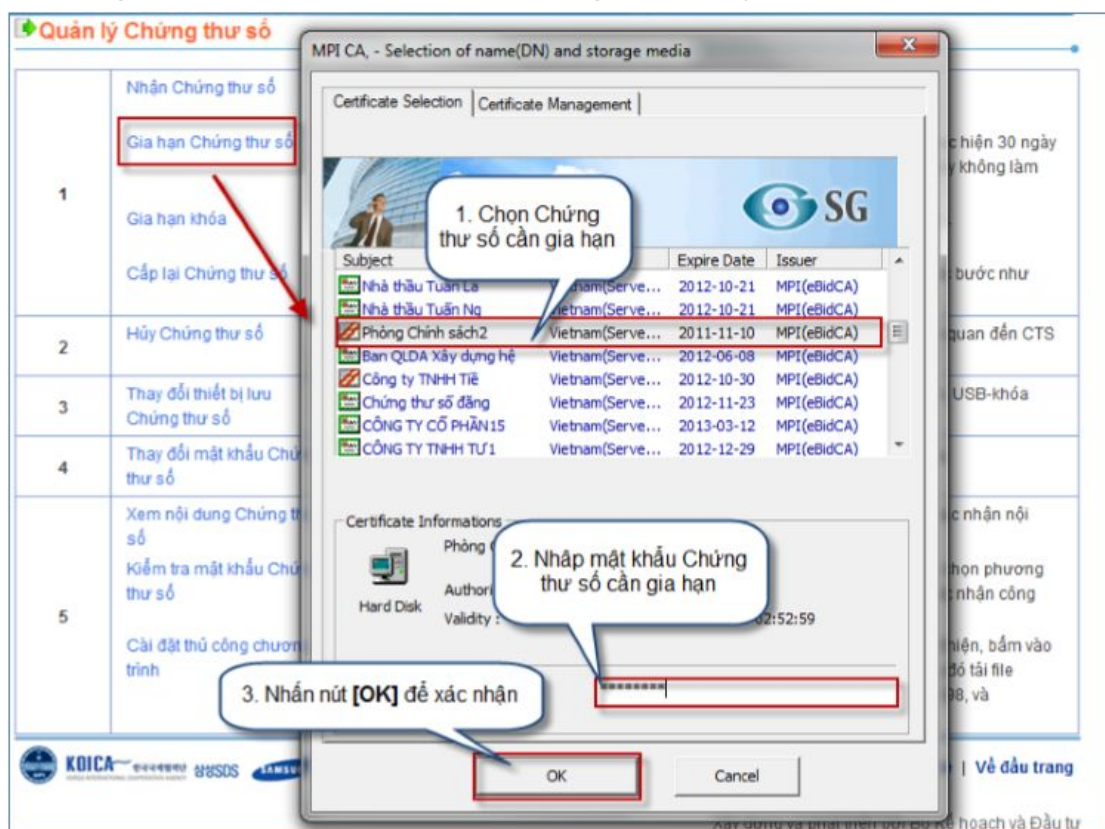
Bước 1: Người dùng chọn Chứng thư số cần gia hạn, nhập mật khẩu và nhấn nút [OK]



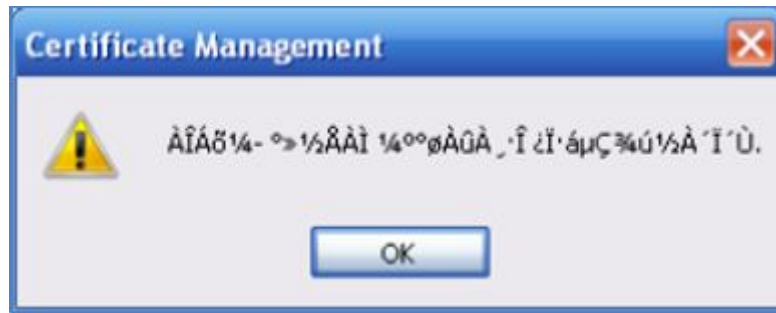
Bước 2.1: Nếu xuất hiện thông điệp như hình dưới đây thì hệ thống không cho phép gia hạn Chứng thư số này vì đã hết thời hạn để gia hạn



Bước 2.2: Nếu Hệ thống xuất hiện màn hình như ở Bước 1, là do hệ thống muốn người dùng xác nhận lại một lần nữa việc gia hạn này.



Bước 3: Người dùng nhập lại thông tin như Bước 1, sau đó hệ thống báo là người dùng đã gia hạn thành công. Xuất hiện màn hình như sau:



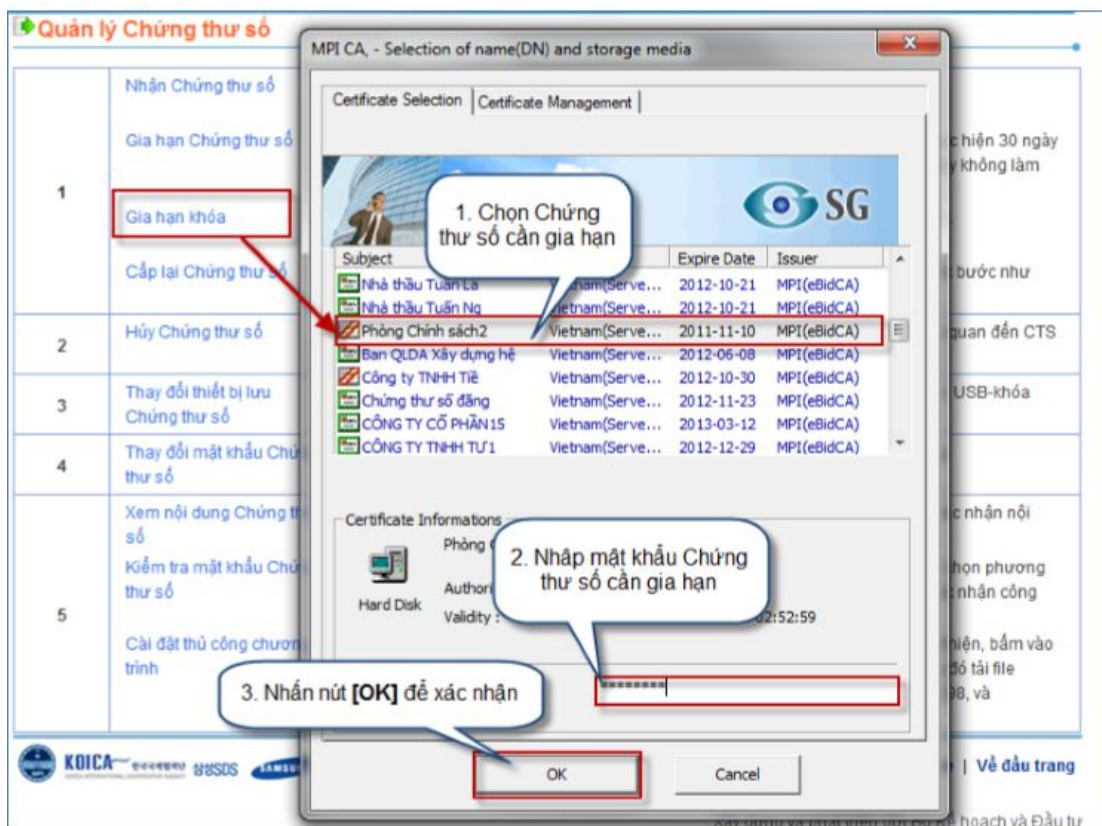
4.3. Gia hạn Khóa

4.3.1 Giới thiệu chức năng:

Về mặt giao diện, chức năng này giống với chức năng gia hạn chứng thư số. Về mặt nội dung, chức năng này làm thay đổi khóa đang dùng.

4.3.2 Hướng dẫn nghiệp vụ:

Tương tự như phần Gia hạn Chứng thư số.



4.4. Cấp lại Chứng thư số

4.4.1 Giới thiệu chức năng:

- Chức năng này dùng để cấp lại Chứng thư số khi người dùng đánh mất Chứng thư số đã được cấp, hoặc Chứng thư số đó đã bị hủy.
- Khi sử dụng chức năng này, người dùng không phải đăng ký lại thông tin, mà chỉ cần có sự đồng ý cấp lại hai số (Số tham chiếu và mã phê duyệt đăng ký) của người quản trị hệ thống.
- Điều kiện để xin cấp lại: Là phải có đơn xin cấp lại, gửi đến Cục QLĐT.

4.4.2 Hướng dẫn nghiệp vụ:

Tương tự như phần Nhận Chứng thư số

Quản lý Chứng thư số		
	Nhận Chứng thư số	Nhập Mã phê duyệt CTS và Số tham chiếu để nhận CTS.
	Gia hạn Chứng thư số	Kéo dài thời gian sử dụng CTS khi CTS đã hết hạn. Việc gia hạn CTS chỉ được thực hiện 30 ngày trước khi hết hạn. Chức năng này không làm thay đổi thông tin của CTS.
1	Gia hạn khóa	Giống như gia hạn CTS.
	Cấp lại Chứng thư số	Chức năng này dùng để cấp lại CTS khi người dùng đánh mất CTS đã được cấp, hoặc CTS đó đã bị hủy. Khi sử dụng chức năng này, người dùng không phải đăng ký lại thông tin, mà chỉ cần có sự đồng ý cấp lại hai số (Số tham chiếu và mã phê duyệt đăng ký) của người quản trị hệ thống. Điều kiện để xin cấp lại: Là phải có đơn xin cấp lại, gửi đến Cục QLĐT.
2	Hủy Chứng thư số	Thực hiện hủy CTS. Khi hủy CTS, tất cả thông tin liên quan đến CTS sẽ bị xóa.
3	Thay đổi thiết bị lưu Chứng thư số	Là hình thức sao chép CTS. Bạn có thể di chuyển CTS lưu trên đĩa cứng, đĩa mềm, USB-khóa hoặc thẻ thông minh và lưu nó sang các phương tiện thông tin lưu trữ khác.
4	Thay đổi mật khẩu Chứng thư số	Đây là chức năng thay đổi mật khẩu CTS được sử dụng khi tham gia vào Hệ thống.
5	Xem nội dung Chứng thư số	Sử dụng chức năng này để xem chi tiết thông tin chứng nhận số của bạn. Có thể xác nhận nội dung thông tin chứng nhận số bao gồm thời hạn sử dụng, nơi cấp v.v...
	Kiểm tra mật khẩu Chứng thư số	Nếu có thông báo "Mật khẩu bạn nhập vào không chính xác." Hãy nhấn vào đây rồi chọn phương tiện lưu giữ tương ứng. Sau khi nhấn vào chứng nhận số và nhập mật khẩu hãy xác nhận công việc này.
	Cài đặt thủ công chương trình	Chương trình quản lý chứng thư số sẽ tự động cài đặt. Khi một cửa sổ pop-up xuất hiện, bấm vào OK để hoàn tất việc cài đặt. Nếu cài đặt không thành công thì bấm vào nút này sau đó tải file xuống. Đóng tất cả các cửa sổ rồi thực hiện run file 98install.bat nếu là window 95,98, và NTinstall.bat nếu là window NT, 2000 trong C:\SignGATE.

4.5. Hủy Chứng thư số

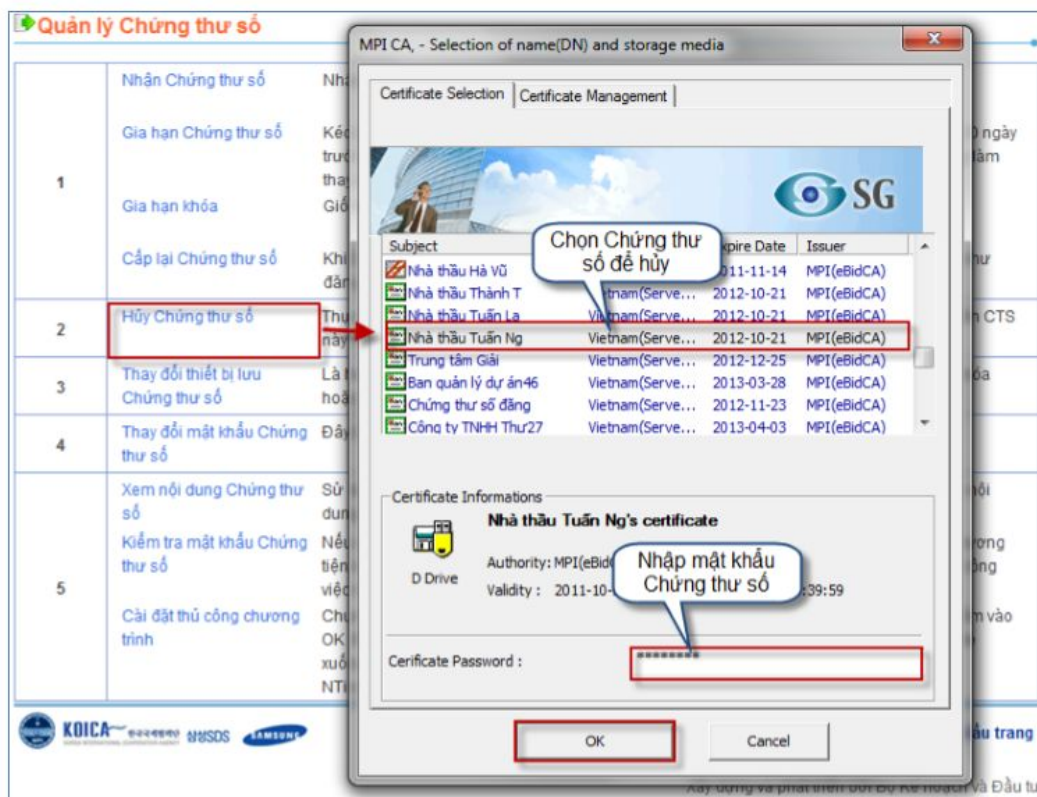
4.5.1 Giới thiệu chức năng:

Chức năng này có nhiệm vụ Hủy Chứng thư số đã được cấp.

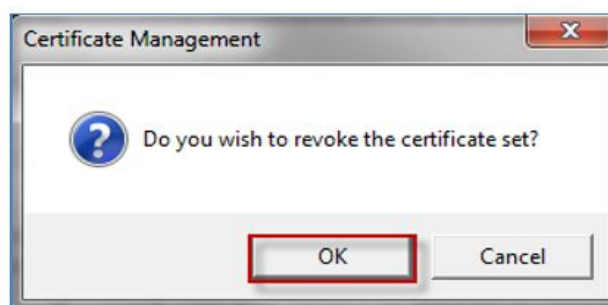
Sau khi hủy Chứng thư số này thì Chứng thư số này không sử dụng lại được nữa và các thông tin liên quan đến Chứng thư số này sẽ bị mất.

4.5.2 Hướng dẫn nghiệp vụ:

Bước 1: Chọn Chứng thư số, nhập mật khẩu Chứng thư số cần hủy và nhấn nút [OK]

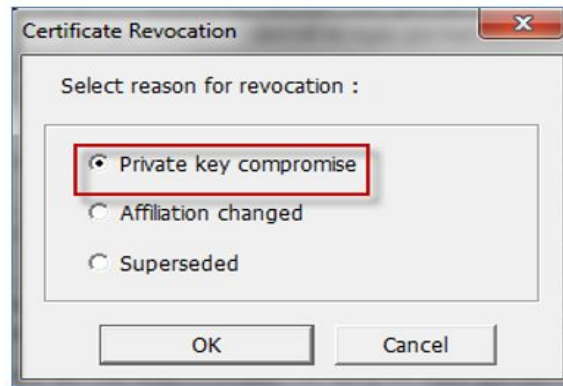


Bước 2: Xuất hiện thông điệp để xác nhận cho việc làm này.

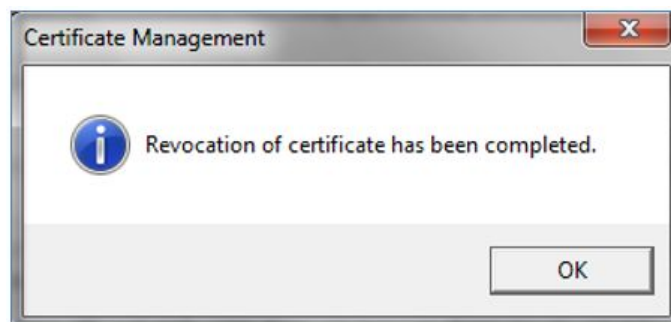


Bước 3: Lựa chọn lý do cho việc Hủy Chứng thư số này. Có 3 lý do để người dùng lựa chọn cho việc Hủy Chứng thư số.

- Khóa Chứng thư số bị hỏng.
- Thay đổi người đại diện pháp luật hoặc tư cách pháp lý của Chứng thư số.
- Sử dụng Chứng thư số khác.



Bước 4: Hệ thống xuất hiện thông báo là đã Hủy thành công.



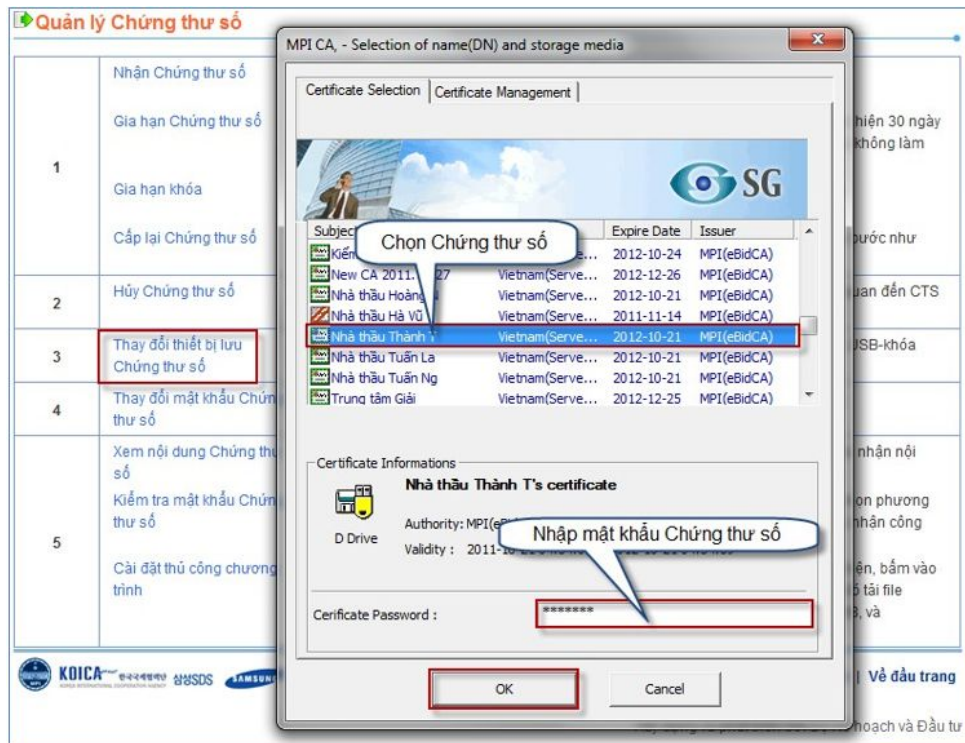
4.6. Thay đổi thiết bị lưu Chứng thư số

4.6.1 Giới thiệu chức năng:

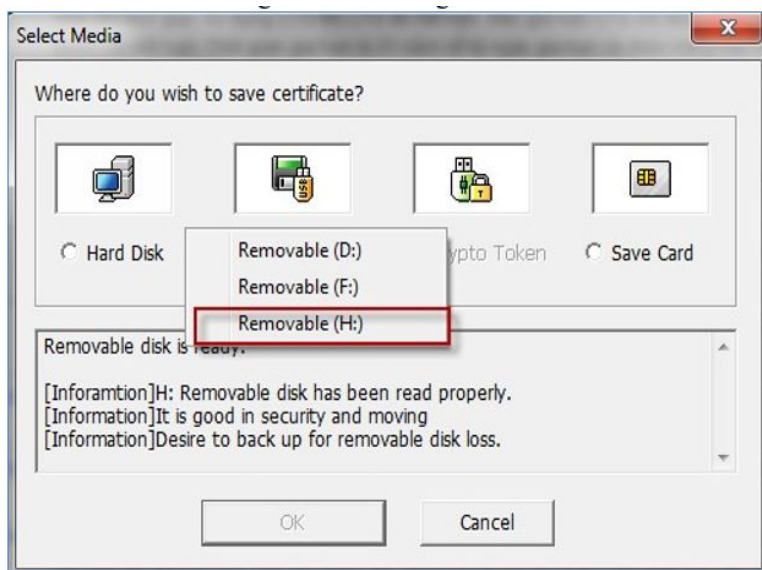
Đây là chức năng thay đổi thiết bị lưu/ Đường dẫn Chứng thư số khi người dùng muốn lưu Chứng thư số vào ổ đĩa cứng khác hoặc USB...

4.6.2 Hướng dẫn nghiệp vụ:

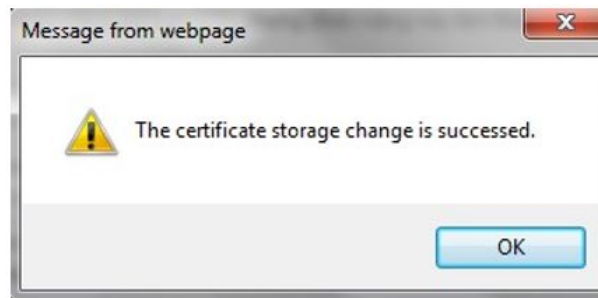
Bước 1: Chọn Chứng thư số cần lưu, sau đó nhập mật khẩu và nhấn nút [OK] để xác nhận.



Bước 2: Chọn thiết bị/đường dẫn lưu Chứng thư số



Bước 3: Hiện thị thông báo đã thực hiện thành công.



4.7. Thay đổi mật khẩu Chứng thư số

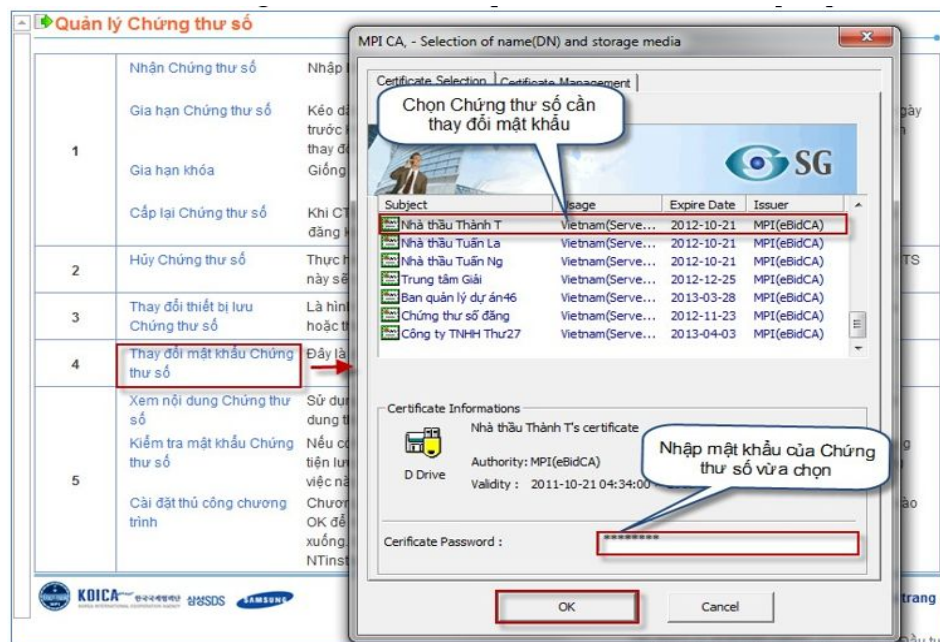
4.7.1 Giới thiệu chức năng:

Đây là chức năng thay đổi mật khẩu Chứng thư số. Việc thiết lập mật khẩu mới cũng phải theo những quy định bắt buộc sau:

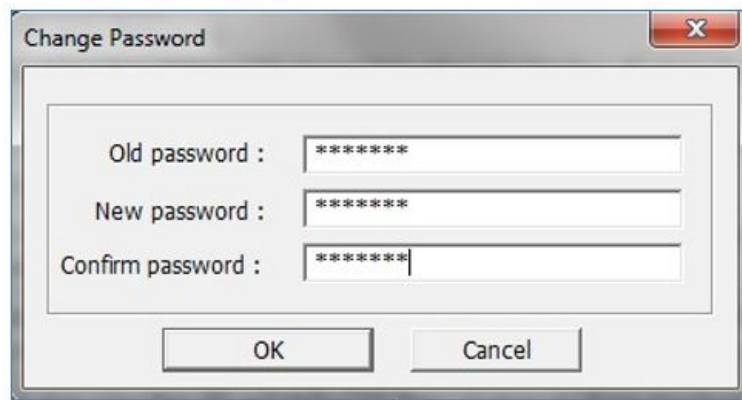
- Mật khẩu dài ít nhất 8 ký tự
- Bao gồm cả ký tự số lẫn chữ
- Không được dùng quá 3 ký tự trùng nhau trong khi đặt mật khẩu.

4.7.2 Hướng dẫn nghiệp vụ:

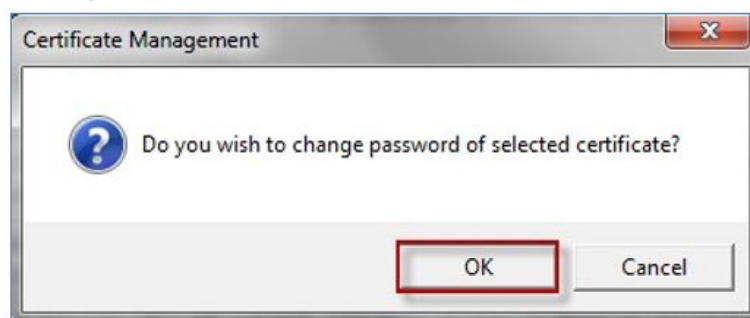
Bước 1: Chọn Chứng thư số, sau đó nhập mật khẩu và nhấn nút [OK]



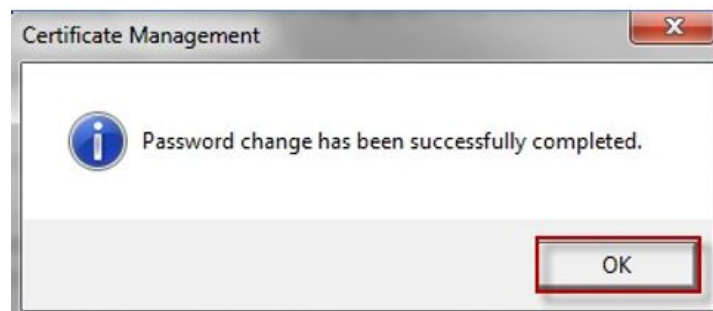
Bước 2: Xuất hiện màn hình, người dùng phải nhập lại mật khẩu cũ, nhập mật khẩu mới, và nhập lại lần nữa mật khẩu mới, mà người dùng muốn thay đổi.



Bước 3: Sau khi nhấn nút [OK], Xuất hiện màn hình xác nhận người dùng có muốn thay đổi không.



Bước 4: Sau khi nhấn nút [OK], Xuất hiện màn hình xác nhận người dùng đã thay đổi thành công.



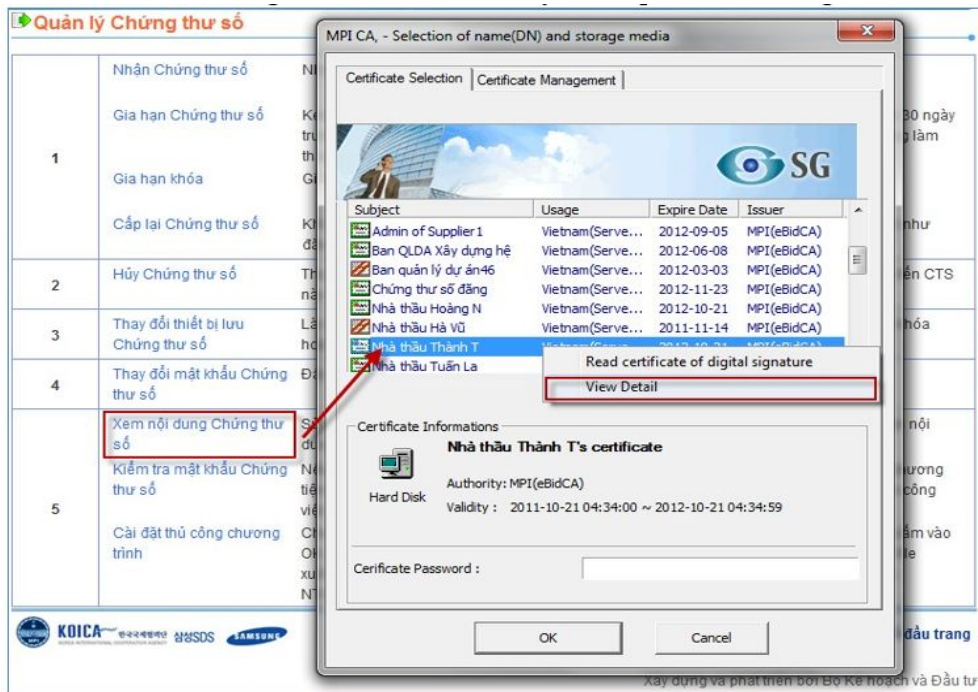
4.8. Xem nội dung thông tin Chứng thư số

4.8.1 Giới thiệu chức năng:

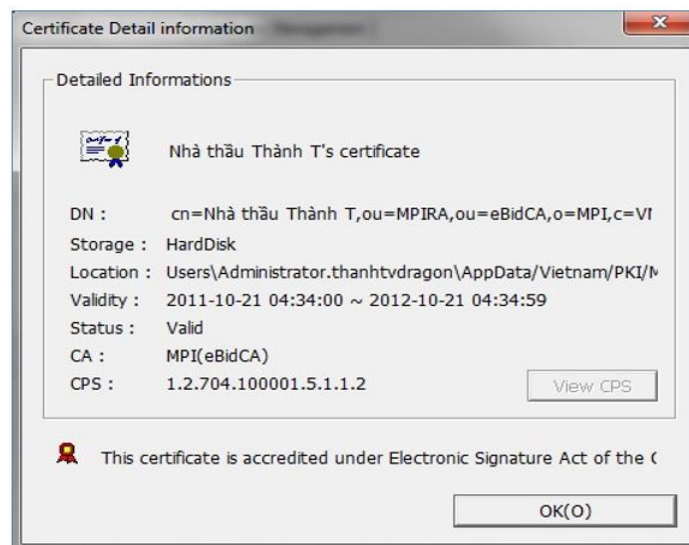
Chức năng này cho phép người dùng xem thông tin chi tiết Chứng thư số của mình bao gồm: tên Chứng thư số, đường dẫn lưu Chứng thư số, thời hạn sử dụng...

4.8.2 Hướng dẫn nghiệp vụ:

Bước 1: Chọn Chứng thư số được lưu, nhấp chuột phải vào Chứng thư số vừa chọn.



Bước 2: Chọn “View Detail”, người dùng có thể xem thông tin chi tiết Chứng thư số này.



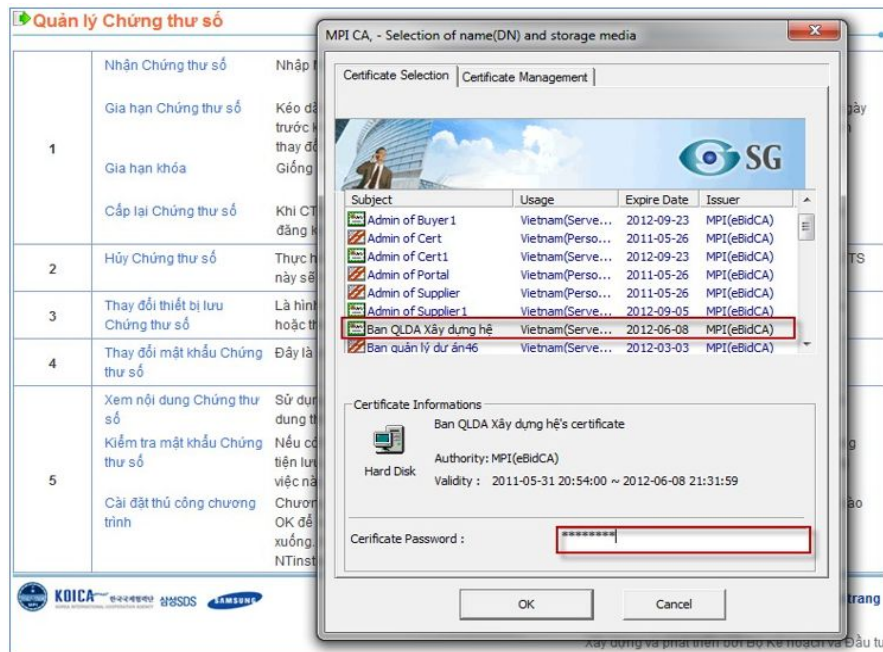
4.9. Kiểm tra mật khẩu Chứng thư số

4.9.1 Giới thiệu chức năng:

Nếu bạn không nhớ chính xác mật khẩu Chứng thư số của mình, bạn có thể kiểm tra điều đó bằng chức năng này. Chức năng này cho phép mật khẩu bạn đang sử dụng có đúng hay không.

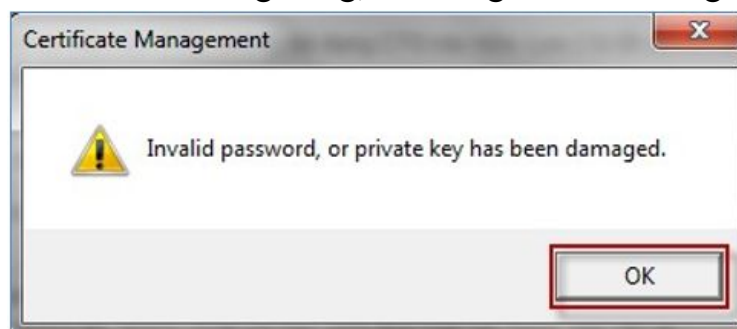
4.9.2 Hướng dẫn nghiệp vụ:

Bước 1: Chọn và nhập mật khẩu Chứng thư số người dùng muốn kiểm tra.

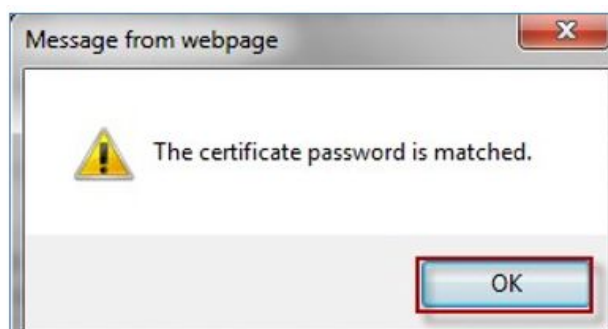


Bước 2: Nhấn nút [OK]

- Nếu Mật khẩu không đúng, hệ thống hiển thị thông báo:



- Nếu Mật khẩu nhập vào đúng, hệ thống hiển thị thông báo:



4.10. Cài đặt thủ công chương trình

4.10.1 Giới thiệu chức năng:

Đây là chức năng cài đặt các gói phần mềm ActiveX SG trên hệ thống đầu thầu điện tử.

- Nếu người dùng chưa cài đặt các gói ActiveX SG, thì người dùng có thể sử dụng chức năng này để cài đặt nó.
- Chức năng này cho phép bạn Download về máy mình rồi cài đặt như các phần mềm khác.

4.10.2 Hướng dẫn nghiệp vụ:

Quản lý Chứng thư số

1	Nhận Chứng thư số	Nhập Mã	0% of AxSignGatePSetup.exe from muasamcong.mpi.gov...
	Gia hạn Chứng thư số	Kéo dài t	30 ngày
	Gia hạn khóa	thay đổi k	g làm
	Cấp lại Chứng thư số	Giống ch	như
2	Hủy Chứng thư số	Khi CTS t	đến CTS
		đăng ký n	khóa
3	Thay đổi thiết bị lưu Chứng thư số	Thực hiện	
		này sẽ bị	
4	Thay đổi mật khẩu Chứng thư số	Là hình th	
		hoặc thể	
5	Xem nội dung Chứng thư số	Đây là c	
	Kiểm tra mật khẩu Chứng thư số	Sử dụng chức năng này để xem chi tiết thông tin chứng nhận số của bạn. Có thể xác nhận nội dung thông tin chứng nhận số bao gồm thời hạn sử dụng, nơi cấp w...	
	Cài đặt thủ công chương trình	Nếu có thông báo "Mật khẩu bạn nhập vào không chính xác." Hãy nhấn vào đây rồi chọn phương tiện lưu giữ tương ứng. Sau khi nhấn vào chứng nhận số và nhập mật khẩu hãy xác nhận công việc này.	
		Chương trình quản lý chứng thư số sẽ tự động cài đặt. Khi một cửa sổ pop-up xuất hiện, bấm vào OK để hoàn tất việc cài đặt. Nếu cài đặt không thành công thì bấm vào nút này sau đó tải file xuống. Đóng tất cả các cửa sổ rồi thực hiện run file 98install.bat nếu là window 95,98, và NTinstall.bat nếu là window NT, 2000 trong C:\SignGATE.	

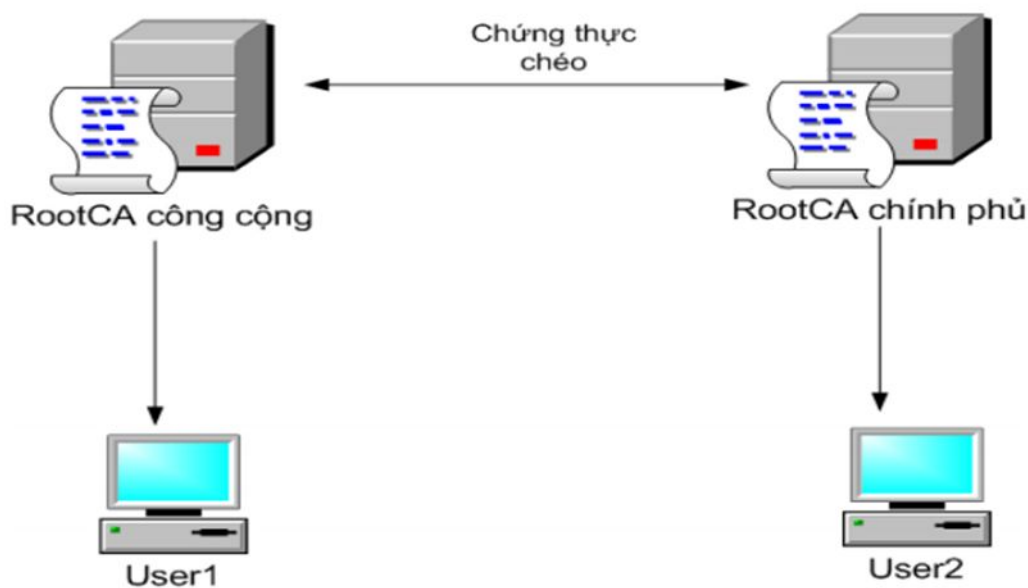
Trang chủ | Giới thiệu | Hướng dẫn sử dụng | Liên hệ | Về đầu trang

5. Ứng dụng chứng thực chéo dựa trên EJBCA

5.2.1. Mô hình triển khai

Triển khai cài đặt EJBCA trên 2 máy khác nhau nhằm tạo hai hệ thống PKI khác nhau: hệ thống PKI Chính phủ và hệ thống PKI công cộng như hình 3.2.

Triển khai chứng thực chéo giữa hai hệ thống PKI này bằng cách: trên mỗi hệ thống khởi tạo RootCA và khởi tạo các thực thể cuối sau đó tiến hành xác thực chéo lẫn nhau.



Hình 3.2. Mô hình triển khai

5.2.2. Ứng dụng chứng thực chéo trên EJBCA

Triển khai chứng thực chéo ngang hàng trên phần mềm nguồn mở EJBCA.

Vào trang quản trị EJBCA



Hình 3.3. Trang quản trị EJBCA

- Tạo hai RootCA là RootCA1 và RootCA2.
- Trên trang quản trị chọn Certification Authorities để tạo ra các các RootCA:



Hình 3.4. Tạo các RootCA

Tạo RootCA1 và RootCA2 bằng cách Add CA

EJBCA
PKI by PrimeKey

Administration

Home

- CA Functions**
 - CA Activation
 - CA Structure & CRLs
 - Certificate Profiles
 - Certification Authorities
 - Crypto Tokens
 - Publishers
- RA Functions**
 - Add End Entity
 - End Entity Profiles
 - Search End Entities
 - User Data Sources
- Supervision Functions**
 - Approve Actions
 - View Log
- System Functions**
 - Administrator Roles
 - Internal Key Bindings
 - Services
- System Configuration**

Create CA

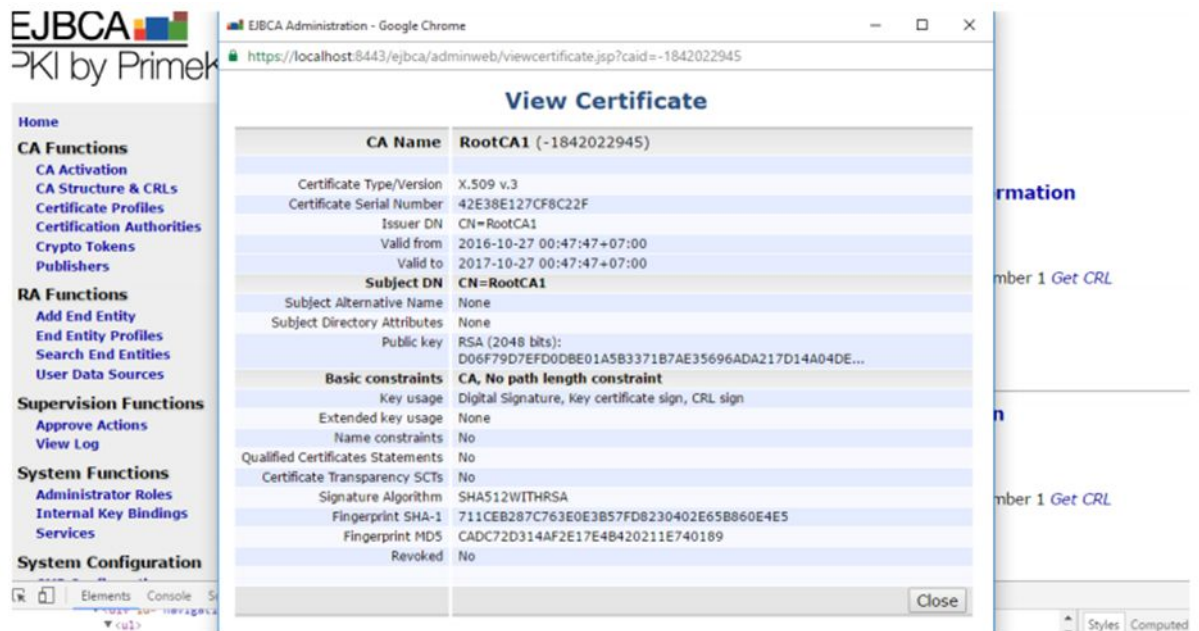
CA Name : RootCA1

[Back to Certificate Aut](#)

Type of CA [?]	X509 ▼
Signing Algorithm	SHA1WithRSA ▼
Crypto Token [?]	- Create a new soft Crypto Token with recommended key pair
Key sequence format [?]	numeric [0-9] ▼
Key sequence [?]	00000
Description	<input type="text"/>
Directives	
Enforce unique public keys [?]	<input checked="" type="checkbox"/> Enforce
Enforce unique DN [?]	<input checked="" type="checkbox"/> Enforce
Enforce unique Subject DN SerialNumber [?]	<input type="checkbox"/> 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

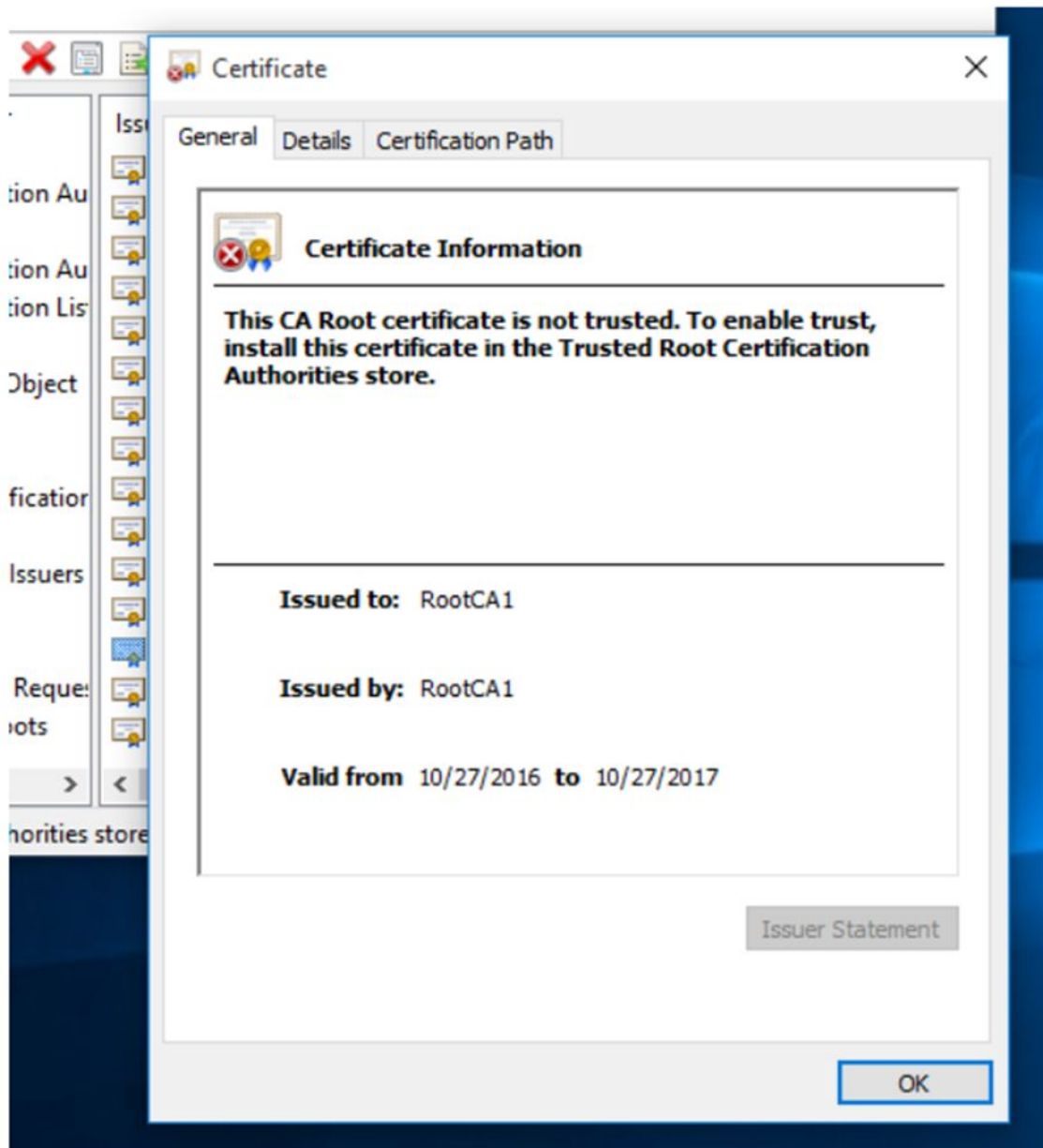


Hình 3.6. Thông tin đầy đủ khi một RootCA được tạo



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 bằng cách chạy Run → certmgr.msc → chọn Action → All Tasks → Import → thực hiện các bước để Import file “.pem” để tạo chứng chỉ RootCA1 (RootCA2). (Các RootCA tự ký).



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.



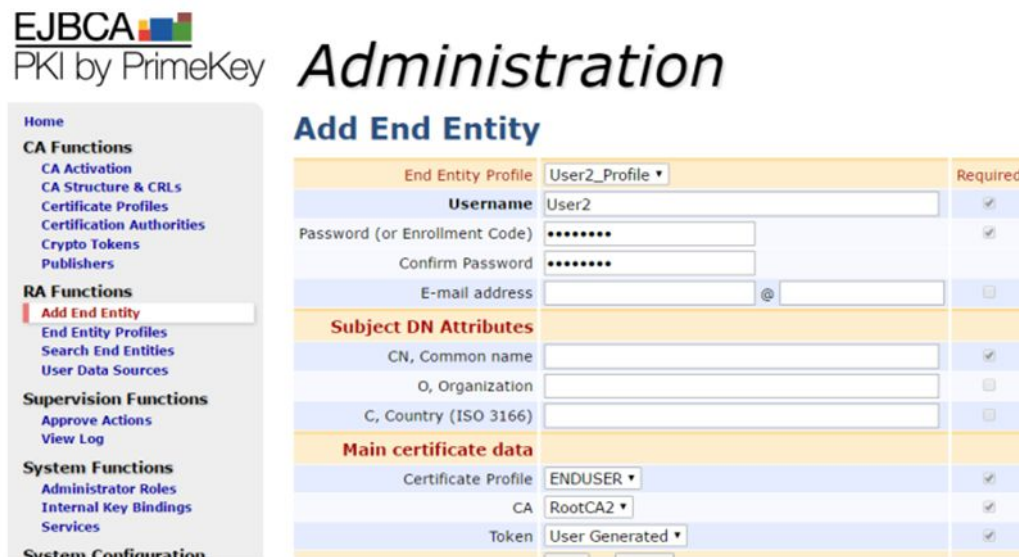
Hình 3.9. Tạo người dùng End Entity

Đối với RootCA1 ta Add Profile User1_Profile Đối với RootCA2 ta Add Profile User2_Profile Sau đó, chọn Edit End Entity Profile để cập nhật thông tin của từng User1_Profile và User2_Profile (User name, Password, thêm Subject DN Attributes, được chứng thực bởi RootCA1 đối với User1_Profile, RootCA2 đối với User2_Profile), chọn Save để lưu các thông tin.



Hình 3.10. Điền đầy đủ thông tin cho các User

Sau đó Add lại các thông tin của End Entity.



EJBCA
PKI by PrimeKey

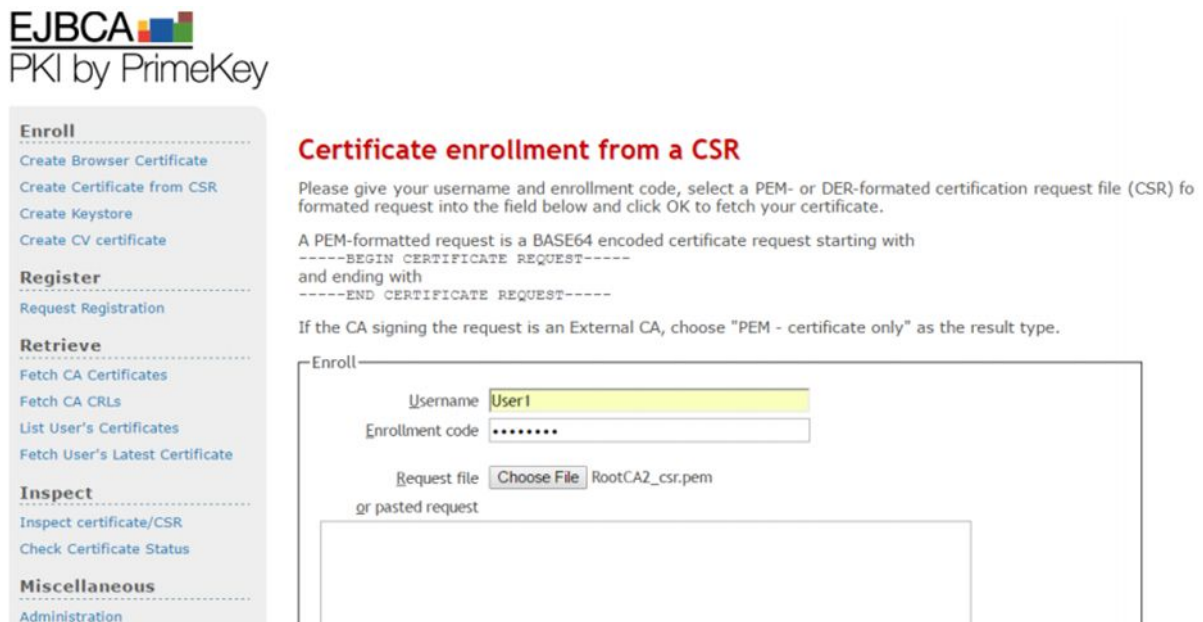
Administration

Add End Entity

End Entity Profile	User2_Profile ▾	Required
Username	User2	<input checked="" type="checkbox"/>
Password (or Enrollment Code)	*****	<input checked="" type="checkbox"/>
Confirm Password	*****	
E-mail address	<input type="text"/> @ <input type="text"/>	<input type="checkbox"/>
Subject DN Attributes		
CN, Common name	<input type="text"/>	<input checked="" type="checkbox"/>
O, Organization	<input type="text"/>	<input type="checkbox"/>
C, Country (ISO 3166)	<input type="text"/>	<input type="checkbox"/>
Main certificate data		
Certificate Profile	ENDUSER ▾	<input checked="" type="checkbox"/>
CA	RootCA2 ▾	<input checked="" type="checkbox"/>
Token	User Generated ▾	<input checked="" type="checkbox"/>

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

Certificate enrollment from a CSR

Please give your username and enrollment code, select a PEM- or DER-formatted certification request file (CSR) 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: RootCA2_csr.pem

or pasted request

Hình 3.12. Các User gửi request để thực hiện xác thực chéo

Xác thực chéo thành công:



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



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

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.