Chương trình KC-01:
Nghiên cứu khoa học phát triển công nghệ thông tin và truyền thông

Đề tài KC-01-01:
Nghiên cứu một số vấn đề bảo mật và an toàn thông tin cho các mạng dùng giao thức liên mạng máy tính IP

Báo cáo kết quả nghiên cứu

HỆ THỐNG PHẦN MỀM CUNG CẤP CHỨNG CHỈ SỐ

Quyển 6A: "Một hệ thống cung cấp chứng chỉ số theo mô hình sinh khoá tập trung"

HÀ NỘI-2003

Báo cáo kết quả nghiên cứu

HỆ THỐNG PHẦN MỀM CUNG CẤP CHỨNG CHỈ SỐ

Quyển 6A: "Một hệ thống cung cấp chứng chỉ số theo mô hình sinh khoá tập trung"

Chủ trì nhóm thực hiện:
TS. Trần Duy Lai

Mục lục

Chương I
CÀI ĐẶT THIẾT LẬP CẤU HÌNH CHO MÁY CA

1-Giới thiệu một số vấn đề liên quan đến cơ sở hạ tầng khóa công khai
1.1-Các giao thức quản lý cơ sở hạn tầng khóa công khai theo chuẩn X509
PKI được xây dựng bao gồm rất nhiều mô hình riêng biệt và việc quản trị các trong các mô hình đó là khác nhau. Management protocol được đưa ra bởi nó cần thiết để hỗ trợ các tương tác on-line giữa các thành phần PKI (giữa CA và hệ thống client, giữa các CA phát hành cross-certificates).

Trước khi xác định rõ riêng biệt các định dạng message và các thủ tục cho phần mềm PKI chúng ta phải đi xây dựng mô hình PKI Management: định nghĩa các thực thể trong PKI Management và tương tác của chúng. Sau đó chúng ta đi nhóm các tính năng này làm cho phù hợp các kiểu có thể định danh của các thực thể đầu cuối (end entity).

Các thực thể được đưa ra trong PKI Management bao gồm end entities (ví dụ, thực thể được đặt tên trong trường Subject của certificate) và CA (ví dụ, thực thể được đặt tên trong trường Issuer của certificate). Dưới đây một vài ví dụ về các định nghĩa trong PKI Management.

Subjects và End Entities
Như đã đề cập ở trên thì thuật ngữ "subject" được sử dụng ở đây để tham chiếu tới một thực thể được đặt tên trong trường Subject của một certificate, khi chúng ta muốn phân biệt giữa các công cụ hay giữa các phần mềm được sử dụng bởi subject đó (ví dụ, một module quản lý certificate cục bộ) được gọi là "subject equipment". Trong trường hợp tổng quát chúng ta sử dụng thuật ngữ "End Entity" (EE).

Tất cả các EEs yêu cầu bảo mật cục bộ truy cập tới một số thông tin tối thiểu: tên sở hữu và private key, tên của CA được tin cậy bởi thực thể và public key của CA (hoặc fingerprint của public key). Nơi lưu trữ các thông tin này có thể thay đổi, sự thay đổi này tuỳ thuộc vào cách cài đặt và ứng dụng (ví dụ, dạng file như cryptographic tokens), nơi này được gọi là Personal Security Environment (PSE) của EE, định dạng của PSE nằm ngoài phạm vi của RFC này.

Certificate Authority
Certificate Authority (CA) là một "third party" thực sự hoặc cũng có thể không phải là "third party" (điều này cho phép chúng ta phân biệt RootCA và Non-RootCA), CA thường thuộc về một tổ chức nào đó nhằm mục đích hỗ trợ các EEs. Một lần nữa chúng ta sử dụng thuật ngữ CA để chỉ thực thể được đặt tên trong trường Issuer của certificate, khi cần phân biệt các công cụ phần cứng hoặc phần mềm sử dụng bởi CA chúng ta đưa ra thuật ngữ "CA equipment". CA equipment bao gồm cả 2 thành phần: on-line và off-line (private key của CA được coi là thành phần off-line).

Các yêu cầu về PKI Management

Bao gồm 13 yêu cầu sau đây:

- Tương thích với chuẩn ISO 9594-8 và các phần certificate extensions.
- Tương thích giữa các thành phần trong các series.
- Đơn giản trong vấn đề cập nhật key pair mà không ảnh hưởng đến key pair khác (trong hệ thống).
- Sử dụng tính tin cậy trong PKI Management protocols phải dễ dàng các bài toán điều tiết.
- Phải tương thích với các thuật toán mã hoá (chuẩn công nghiệp): RSA, DSA, SHA-1,...
- Không loại trừ việc sinh cặp khoá bởi EEs, RAs, CAs.
- Hỗ trợ việc công khai các certificates (tuỳ thuộc vào các cài đặt khác nhau và các môi trường khác nhau).
- Hỗ trợ việc huỷ bỏ certificate của EEs (CRLs).
- Có thể sử dụng đa dạng "transport mechanisms": mail, http, TCP/IP và ftp.
- Chỉ có CA mới có thể thay đổi hoặc thêm giá trị trường trong certificate, xoá hoặc thay đổi extension dựa trên các chính sách hoạt động của nó.
- Hỗ trợ công việc cập nhật CA key cho các EEs.
- Các chức năng của RA phụ thuộc vào CA của nó (các cách cài đặt và các môi trường khác nhau).
- Khi EE yêu cầu một certificate bao gồm có cả giá trị public key, thì phải có một giá trị private key tương ứng (ký lên request - Proof of Possession of Private Key).

1.2-Hồ sơ chứng chỉ số và CRL cho cơ sở hạ tầng khóa công khai theo chuẩn X509

X.509 v3 certificate

Như đã biết, user có một public key sẽ có một private key được sở hữu bởi đúng subject (người dùng hoặc hệ thống) với một kỹ thuật mã hoá và chữ ký số được sử dụng. Tính tin cậy này được sử dụng trong các chứng chỉ public key (gọi là certificate), bị ràng buộc bởi chữ ký của CA (trusted CA) với một khoảng thời gian sử dụng xác định. Certificate có thể được phân phối qua các truyền thông không cần sự tin cậy và các hệ thống server khác nhau và có thể được lưu trong một kho không bảo mật trên hệ thống sử dụng certificate. ANSI X9 đã phát triển định dạng X.509 v3 dựa trên việc mở rộng một số trường dự trữ, các trường này bao gồm: thông tin định danh, thông tin về thuộc tính khoá, thông tin về chính sách (policy) hệ thống CA và các bắt buộc certification path (trường basicConstraints).

Certification paths and trust

Một user của một dịch vụ bảo mật có một public key (có hiệu lực) sẽ có một certificate được chứng nhận bởi một CA (ký lên public key), CA này cũng có thể được chứng nhận bởi một (hoặc nhiều) CA khác. Do vậy, nảy sinh khái niệm về

certification path. Trong RFC1422 đã định nghĩa một cấu trúc chuỗi các CAs một cách cứng nhắc, cấu trúc này tương thích với X.509 v1, gồm có 3 kiểu CA là: IPRA (Internet Policy Registration Authority), PCAs (Policy Certification Authorities) và CAs (Certification Authorities). Cấu trúc này có các hạn chế sau: cơ chế top-down tức là tất cả các certification paths phải bắt đầu từ IPRA, quy tắc đặt tên nhánh hạn chế subject của CA, sử dụng khái niệm PCA tức là yêu cầu phải biết từng PCAs được thiết lập trong logic kiểm tra chuỗi certificate. Với X.509 v3, thì hầu hết các yêu cầu trên được sử dụng trong certificate extension, mà không cần hạn chế các cấu trúc sử dụng CA. Với cấu trúc này, đưa ra kiến trúc hết sức mềm dẻo cho hệ thống CA.

Revocation

Khi phát hành ra một certificate, nó đã được định ra một khoảng thời hạn sử dụng nhất định. Tuy nhiên, vì một số lý do nào đó mà người sử dụng muốn huỷ bỏ certificate này khi chưa hết hạn sử dụng. X.509 định nghĩa một phương pháp huỷ bỏ certificate, phương pháp này cho phép các CAs chấp nhận huỷ bỏ certificate, được gọi là một CRL (Certificate Revocation List). Danh sách này liệt kê tất cả các certificate bị huỷ bỏ (theo số serial). Khi một hệ thống bảo mật sử dụng certificate, thì hệ thống này không những kiểm tra chữ ký của certificate và tính hiệu lực của nó mà còn kiểm tra sự có mặt của serial này trong CRL đó (tất nhiên là CRL này phải được cập nhật trên toàn bộ hệ thống theo một định kỳ nào đó). Nếu số serial này có trong CRL thì coi như certificate đó đã bị huỷ bỏ. CRL có thể được phân phối qua các truyền thông không bảo mật và các hệ thống server (repository). Một hạn chế của phương pháp CRL, đó là khoảng thời gian phát hành CRL là không liên tục. Có thể giải quyết hạn chế này bằng các phương pháp trực tuyến (on-line method), phương pháp này có thể áp dụng trong một số môi trường. Tuy nhiên, để sử dụng các phương pháp này sẽ phải đảm nhiệm thêm một số yêu cầu mới về bảo mật mới.

2-Cài đặt thiết lập cấu hình cho máy CA

Hệ thống cung cấp chứng chỉ số MyCA được xây dựng trên hệ điều hành RedHat Linux, gồm hai mô hình:

- Mô hình cấp phát, quản lý và huỷ bỏ chứng chỉ, do người sử dụng sinh khoá
- Mô hình cấp phát, quản lý và huỷ bỏ chứng chỉ do trung tâm sinh khoá (mô hình sinh khoá tập trung)

Trong tài liệu này chúng tôi trình bày việc cài đặt thiết lập,cấu hình và khởi tạo cho máy tính thực hiện chứng năng phát hành và huỷ bỏ chứng chỉ số theo mô hình tập trung đơn tầng (không có các CA cấp dưới). Để tiện trong việc trình bày, chúng tôi giả sử rằng máy Database server đã được cài đặt và thiết lập cấu hình (cụ thể được trình bày trong chương 2)

2.1-Cài đặt

Đối với các máy được thiết lập làm máy CA (Certificate Authority) trước khi thực hiện việc cài đặt cần kiểm tra một số yêu cầu về phần mềm dưới đây:

Hệ điều hành RedHat Linux 7.2
Perl phiên bản 5.6.0 hoặc cao hơn
Apache phiên bản 1.3.12 hoặc cao hơn

Toàn bộ phần mềm MyCA được lưu trên một đĩa CD ROM. Để cài đặt máy CA người thực hiện có thể tiến hành như sau:

-Copy tệp MayCA.tgz từ đĩa CD vào máy cần thiết lập làm máy CA.

-Gỡ nén tệp MayCA.tgz, bởi lệnh

tar -xvzf /đường dẫn/MayCA.tgz

được thư mục MayCA, trong đó có các thư mục: MyCA, và myca (trong thư mục này có các thư mục con: cgi-ca, htdocs-ca, cgi-print).

-Copy thư mục myca vào thư mục /home

-Copy thư mục MyCA ra ngoài cùng của hệ thống cây thư mục

2.2-Thiết lập cấu hình

Cấu hình Apache server

Giao diện giữa người quản trị và chương trình trên máy CA được thực hiện thông qua trình duyệt Netscape, do vậy sau khi cài đặt phần mềm CA để chương trình hoạt động cần thiết lập cấu hình cho chương trình CA trên Apache. Việc thiết lập cấu hình để CA sử dụng Apache được tiến hành như sau:

-Trong tệp cấu hình của Apache (tệp httpd.conf trong thư mục /etc/httpd/conf) cần bổ sung trang giao diện CA trong mục "VirtualHost" như sau:

```
<VirtualHost 200.1.1.2>
    DocumentRoot "/home/myca/cgi-print/"
    ServerName printcert
    Errorlog logs/print/error_log
    CustomLog logs/print/access_log common
    ScriptAlias /cgi-bin/ "/home/myca/cgi-print/"
    <Directory "/home/myca/cgi-print">
      AllowOverride None
      Options ExecCGI
      Order allow,deny
      Allow from all
    </Directory>
</VirtualHost>

<VirtualHost 200.1.1.2>
    DocumentRoot "/home/myca/htdocs-ca/"
    ServerName rootca
    Errorlog logs/ca/error_log
    CustomLog logs/ca/access_log common
    ScriptAlias /cgi-bin/ "/home/myca/cgi-ca/"
    <Directory "/home/myca/cgi-ca">
      AllowOverride None
      Options ExecCGI
      Order allow,deny
      Allow from all
    </Directory>
</VirtualHost>
```

Trong đó trang printcert được sử dụng để in giấy chứng nhận cấp chứng chỉ số cho người sử dụng, và trang rootca là giao diện chính để người quản trị thực hiện việc phát hành huỷ bỏ chứng chỉ.

-Trong tệp /etc/hosts bổ sung thêm các trang trên:

```
200.1.1.2 rootca printcert
```

-Cần tạo các thư mục: ca, print trong /etc/httpd/logs để lưu lại nhật ký, thông báo lỗi nếu chương trình xuất hiện lỗi.

-Sau khi thực hiện cấu hình xong cần khởi động lại Apache để các tham số mới được bổ sung có hiệu lực, bằng cách thực hiện lệnh sau:

```
/etc/init.d/httpd restart.
```

Cấu hình cho MySSL và MyCA

Tất cả các tham số cấu hình cho trình MySSL, MyCA tương ứng được để trong các tệp sau /MyCA/conf/myssl.cnf và /home/httpd/cgi-ca/ca.conf. Hầu hết các tham số trong hai tệp này có thể dùng chung cho toàn hệ thống, tuy nhiên trong đó có những tham số mà đối với mỗi máy CA (cả root hoặc nonroot) cần có sự thay đổi khi chúng được thiết lập.

Khi một máy CA được thiết lập, cần có một cặp khoá được sinh theo số ID đã được hệ thống chấp nhận, khi đó số ID dưới dạng thập phân sẽ được dùng làm phần chính của tên tệp khoá cũng như tên tệp chứng chỉ của CA đó (giả sử CA được cấp ID là 01 thì khi khởi tạo cho CA đó tệp khoá sẽ là 01.key, tệp chứng chỉ là 01.crt). Khi đó trong tệp cấu hình của MySSL (myssl.cnf) và MyCA (ca.conf) cần thay đổi các tham số sau:

-Trong tệp myssl.cnf vào phần [CA-default] thay đổi hai thuộc tính chứng chỉ và private_key thành:

```
certificate = $dir/01.crt
private_key=$dir/private/01.key
```

-Tương tự trong tệp ca.conf cần thay đổi hai thuộc tính cacert và cakey và thuộc tính chỉ địa chỉ của máy public database server:

```
cacert "/MyCA/01.crt"
cakey "/MyCA/private/01.key"
ldapserver 200.1.1.1
```

2.3- Mô tả các thư mục, tệp

2.3.1-Trong thư mục /MyCA

Trong thư mục /MyCA chứa cấu trúc thư mục để quản lý các yêu cầu cấp chứng chỉ, chứng chỉ và các tệp cơ sơ dữ liệu cho CA bao gồm một số thư mục con sau:

Tên thư mục/File	Mô tả
/MyCA/certs/new	Thư mục lưu các chứng chỉ vừa được phát hành

/MyCA/chain	Thư mục lưu tệp chain.crt
/MyCA/conf	Thư mục lưu tệp cấu hình cho trình MySSL
/MyCA/crl/new	Thư mục lưu tệp CRL khi CA phát hành
/MyCA/dB	Thư mục lưu các tệp dữ liệu trong đó lưu trữ các chứng chỉ (CA, User).
/MyCA/inbound/certs	Thư mục lưu các tệp chứng chỉ cấp cho CA
/MyCA/inbound/deleted	Thư mục lưu các yêu cầu của các CA tầng dưới trong quá trình cấp chứng chỉ cho CA tương ứng với tệp yêu cầu đó tiến hành không thành công.
/MyCA/inbound/processed	Thư mục lưu các tệp yêu cầu tương ứng với các chứng chỉ đã được cấp cho các CA cấp dưới.
/MyCA/inbound/reqs	Thư mục lưu các tệp yêu cầu của các CA cấp dưới.
/MyCA/private	Thư mục lưu tệp khoá của CA (đã được mã hoá)
/MyCA/reqs/pending	Thư mục lưu các tệp yêu cầu
/MyCA/reqs/processed	Thư mục lưu các chứng chỉ đã xử lý thành công
/MyCA/reqs/deleted	Thư mục lưu các tệp yêu cầu đã được xử lý nhưng không thành công.
/MyCA/tmp	Thư mục dùng để lưu các thông tin trung gian khi chương trình thực hiện.
/MyCA/stuff	Thư mục lưu các tệp thông tin liên quan đến quá trình CA phát hành chứng chỉ và CRL, gồm những tệp sau:
index.txt	Đây là tệp chứa một số thông tin tóm lược về các chứng chỉ đã được phát hành và trạng thái của nó (Nếu chứng chỉ nào có trạng thái là V (validate) thì nó đang có hiệu lực, ngược nếu là R (Revocation) thì chứng chỉ đó đã bị huỷ bỏ).
serial	Nội dung của tệp này là một số dưới dạng hexa, khi phát hành ra một chứng chỉ số serial của chứng chỉ đó sẽ là nội dung đọc ra từ tệp serial.
Thư mục /MyCA/user	Lưu khoá, chứng chỉ của người sử dụng (theo từng số ID)

2.3.2-Nội dung thư mục /home/myca/

Trong thư mục này lưu toàn bộ các tệp chương trình và các tiện ích chính thực hiện các chức năng của CA. Cụ thể dưới đây là bảng liệt kê danh sách các tệp và chức năng của chúng.

Tên thư mục và file	Chức năng
1. Thư mục /home/httpd/cgi-ca	
ca	Tệp chương trình chính để thực hiện các chức năng được gọi từ form chính của CA
ca.conf	Tệp cấu hình cho CA

2. Thư mục /home/httpd/cgi-ca/bin	
make	Tiện ích dùng để tạo các tệp link
myca-sign, myca-verify, myca-sv	Các tiện ích dùng để ký một chuỗi dữ liệu, kết quả đầu ra là một tệp PKCS#7, kiểm tra chữ ký trên tệp PKCS#7
myssl	Tiện ích thực hiện hầu hết các chức năng của CA
pvkh	Tiện ích dùng để mã hoá, giải mã tệp khoá bí mật của CA
3. Thư mục /home/httpd/cgi-ca/cmds	
genCADB	Tệp chương trình thực hiện khởi tạo cơ sở dữ liệu perl cho CA.
genCRL	Tệp chương trình tạo tệp CRL
initLDAP	Tệp chương trình khởi tạo entry lưu CRL và chứng chỉ của CA trên LDAP server
issueCerrtificate	Tệp chương trình phát hành đơn lẻ một chứng chỉ
revokeCertificate	Tệp chương trình thực hiện huỷ bỏ một chứng chỉ
SignCACerts	Tệp chương trình phát hành các chứng chỉ cho các CA tầng dưới
Signing	Tệp chương trình phát hành các chứng chỉ cho người sử dụng.
updateCRL	Tệp chương trình cập nhật CRL sang LDAP
4. Thư mục /home/httpd/cgi-ca/Convert và /home/httpd/cgi-ca/Net	
Thư mục lưu các module phục vụ cho các chức năng có liên quan đến LDAP	
5. Thư mục /home/httpd/cgi-ca/MainModule	
Thư mục lưu các module thuộc hệ thống MyCA	
6. Thư mục /home/httpd/cgi-ca/lib	
Thư mục lưu các thư viện gồm các hàm được xây dựng trên cơ sở hai module trên	
7. Thư mục /home/httpd/sheets	
Thư mục lưu các tệp html thực hiện việc hiển thị các form trong chương trình	
8. Thư mục /home/httpd/htdocs-ca	
index.html	Hiển thị giao diện chính của CA
init.html	Trang giao diện Initialzation
main.html, navbar.html và top.html	Các thành phần tạo nên giao diện chính (logo, menu chính, tiêu đề)
pwd.html	Giao diện nhận mật khẩu
sign.html	Trang giao diện phát hành các chứng chỉ
IssueCRL	Giao diện phát hành CRL mới
9. Thư mục /home/httpd/htdocs-ca/images	
Thư mục lưu các tệp ảnh.	
10. Thư mục /home/httpd/htdocs-ca/scripts	
Thư mục lưu các tệp javascript phục vụ cho việc thiết lập giao diện.	

2.4 Các chức năng trên máy CA

Trên máy CA gồm có các chức năng chính sau:

- **Mục Initilization:**

Tên mục, chức năng	**Mô tả chức năng chính**
1.Initilize local perl Database	Khởi tạo cơ sở dữ liệu trên máy CA để lưu các chứng chỉ đã phát hành, đã huỷ bỏ
2.Generate Root CA Key Pair and Selft Sign Certificate	Sinh cặp khoá và chứng chỉ tự ký cho Root CA
3.Export Root CA certificate and empty CRL to LDAP	Tạo CRL rỗng (chưa có chứng chỉ bị huỷ bỏ), export CRL rỗng và chứng chỉ của Root CA ra LDAP

- **Mục Process Cert Request**

Tên mục,chức năng	**Mô tả chức năng chính**
Input User's Data	Nhập thông tin về người sử dụng được cấp chứng chỉ
Signing certificate requests gồm các chức năng sau:	
1.Sign nonRoot CA request files	Phát hành các chứng chỉ sử dụng cho nonRoot CA trong hệ thống (trong trường hợp hệ thông áp dụng Ca nhiều cấp).
2.Sign user's request files	Phát hành các chứng chỉ cho người sử dụng
Create PKCS#12 Certificate	Chuyển đổi định dạng chứng chỉ và khoá của người sử dụng sang dạng PKCS12
Pending Requests List	Hiển thị danh sách các yêu cầu cấp chứng chỉ của người sử dụng chua được ký.

- **Mục Certificates**

Tên mục, chức năng	**Mô tả chức năng chính**
Issued Certificates	Hiển thị danh sách các chứng chỉ đã được phát hành
Export Certificates to LDAP	Cập nhật các chứng chỉ đã được phát hành lên LDAP server.

- **Mục CRL**

Tên mục, chức năng	**Mô tả chức năng chính**
Revoke a certificate by administrator	Thực hiện huỷ bỏ một chứng chỉ số
Issue New CRL	Phát hành CRL mới.
Udate current CRL to LDAP server	Cập nhật CRL hiện hành ra LDAP server

3-Khởi tạo cho CA

Sau khi thực hiện và thiết lập cấu hình cho máy CA, để kích hoạt giao diện của chương trình MyCA, người quản trị chạy trình duyệt Netscape, mở trang rootca, giao diện chính xuất hiện như hình 1

Hình 1

Để thực hiện khởi tạo cho máy CA chọn chức năng **Root CA initilization**, trên màn hình Netscape xuất hiện trang MyCA RootCA Init gồm ba chức năng như hình 2.

Hình 2

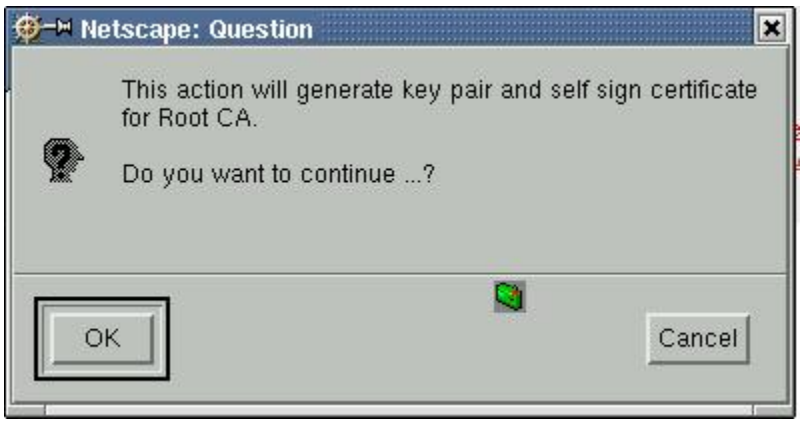
- ***Bước 1: "Initialize local perl Database"***

Khởi tạo cơ sở dữ liệu dùng để lưu các chứng chỉ trên chính máy máy CA, khi chọn chức năng này các tệp dữ liệu dùng để lưu trữ các chứng chỉ của người sử dụng được khởi tạo. Quá trình khởi tạo kết thúc khi trên màn hình xuất hiện thông báo:

Hình 3

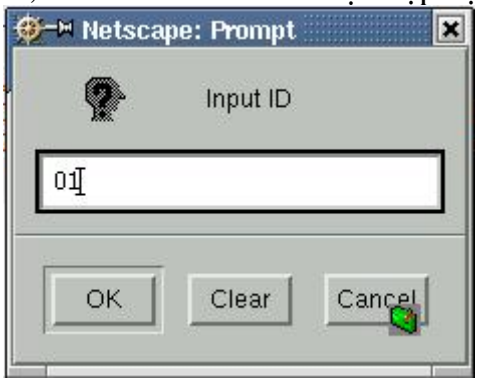
- ***Bước 2: "Generate Root CA key pair and self sign certificate"***

Thực hiện sinh tệp khoá và tệp chứng chỉ tự ký (self sign certificate) cho máy CA. Khi chọn chức năng này trên màn hình xuất hiện hộp hội thoại khuyến cáo như hình 4.



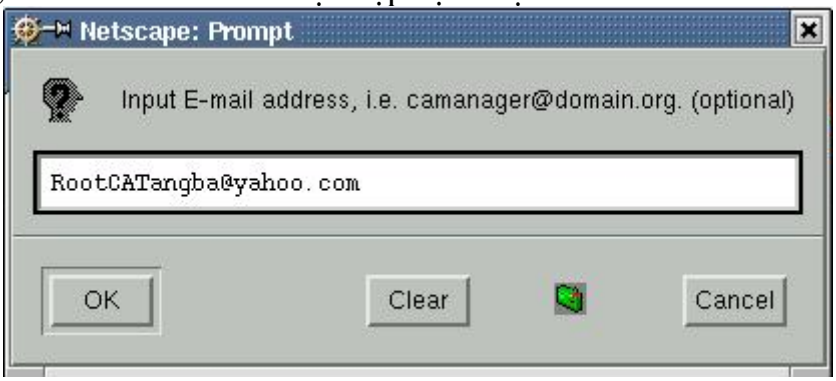
Hình 4

Người quản trị chọn "OK", trên màn hình xuất hiện hộp hội thoại như hình 5



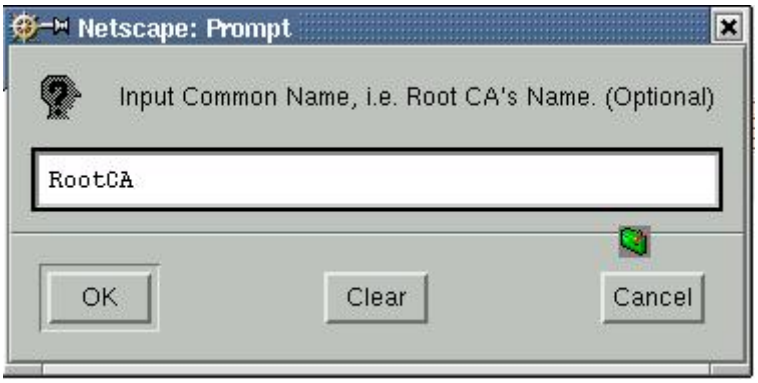
Hình 5

Người quản trị nhập số ID hệ thống MyCA cấp cho máy CA đang thiết lập, rồi nhấn "OK", trên màn hình xuất hiện hộp hội thoại như hình 6.



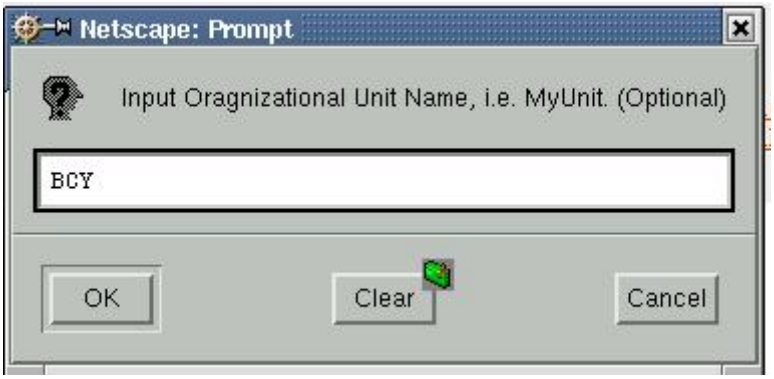
Hình 6

Người quản trị nhập vào địa chỉ Email (cũng có thể để trống), nhấn "OK", trên màn hình xuất hiện hộp hội thoại như hình 7.



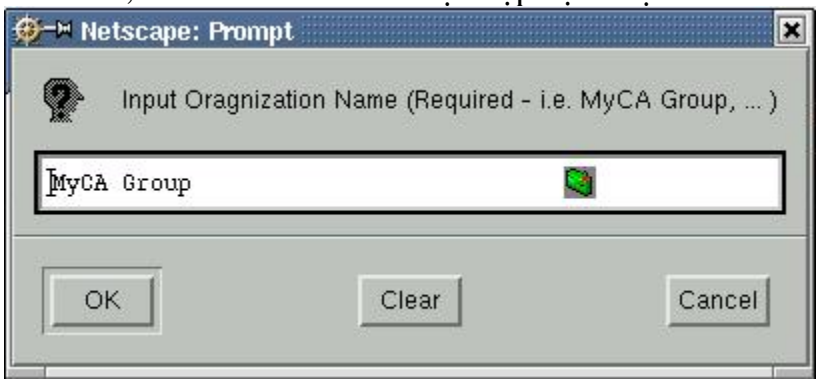
Hình 7

Người quản trị nhập tên của CA (cũng có thể để trống), nhấn “OK”, trên màn hình xuất hiện hộp hội thoại như hình 8.



Hình 8

Người quản trị nhập tên của ngành đang được thiết lập hệ thống CA (chẳng hạn Root CA đang được thiết lập cho Ban Cơ Yếu chẳng hạn), trường này cũng có thể bỏ trống, nhấn "OK", trên màn hình xuất hiện hộp hội thoại như hình 9.



Hình 9

Trường Organization Name bắt buộc phải có và giá trị mặc định của trường này là MyCA Group, nếu người quản trị muốn thay đổi trường này (hoặc trường Country) thì khi thiết lập tệp cấu hình cho LDAP server cần thay đổi hai trường này trong thuộc tính suffix cho tương ứng. Tốt nhất là người quản trị giữ nguyên giá trị mặc định, nhấn "OK", hộp hội thoại nhận trường country xuất hiện với giá trị mặc định của trường này là VN.

Hình 10

Cũng tương tự như trường Organization Name, trường Country cũng là trường yêu cầu phải có, với giá trị mặc định là "VN" người quản trị có thể nhấn "OK", trên màn hình xuất hiện hộp hội thoại như hình 11.

Hình 11

Người quản trị nhập một chuỗi có độ dài tối thiểu là 8 ký tự, để làm mầm khoá khi thực hiện mã hoá tệp khoá của CA bằng thuật toán mã dòng. Chú ý, người quản trị cần nhớ kỹ chuỗi đã nhập vào, vì mỗi khi CA cần phát hành một chứng chỉ hay một CRL mới thì người quản trị cần nhập khoá này vào để chương trình thực hiện việc giải mã tệp khoá của CA. Sau khi nhập khoá, nhấn "OK" quá trình sinh tệp khoá và tệp chứng chỉ tự ký bắt đầu, quá trình này sẽ kết thúc khi trên màn hình hiển thị nội dung của chứng chỉ vừa được sinh.

Hình 12

Sau khi thực hiện quá trình khởi tạo cho Root CA, sẽ xuất hiện tệp khoá 01.key (trong thư mục /MyCA/private) đã được mã hoá bằng thuật toán mã dòng, và tệp chứng chỉ 01.crt (trong thư mục /MyCA) nếu người quản trị hiển thị tệp này trên màn hình text nó sẽ có dạng dưới đây (định dạng PEM):

```
-----BEGIN CERTIFICATE-----
MIICazCCAdSgAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMSUwIwYJKoZIhvcNAQkB
FhZSb290Q0FUYW5nYmFAeWFob28uY29tMQ8wDQYDVQQDEwZSb290Q0ExDDAKBgNV
```

```
BAsTA0JDWTETMBEGA1UEChMKTXlDQSBHcm91cDELMAkGA1UEBhMCVk4wHhcNMDIw
OTA1MDIwNzE4WhcNMDQwOTA0MDIwNzE4WjBoMSUwIwYJKoZIhvcNAQkBFhZSb290
Q0FUYW5nYmFAeWFob28uY29tMQ8wDQYDVQQDEwZSb290Q0ExDDAKBgNVBAsTA0JD
WTETMBEGA1UEChMKTXlDQSBHcm91cDELMAkGA1UEBhMCVk4wgZ4wDQYJKoZIhvcN
AQEBBQADgYwAMIGIAoGAQAAIAADgAAoAAGABkBmaBuw0As8qi6ToubbX58N3Zmf4
0Kf6QVylmxKkHhNx/jZ7nYAmJEAAep4ugZz3XHebDym5Pi9vjLCEfTc7fg3796WY
qlgjDqTD+tmQEAhorN0jv4E4qhW9rjqBPNAf5cdzRpSjh+tfibbDCUE6RkR2SJsC
AwEAAaMmMCQwDwYDVR0TAQH/BAUwAwEB/zARBglghkgBhvhCAQEEBAMCAAcwDQYJ
KoZIhvcNAQEFBQADgYEAPmDw/qn2T7G9mx/w2QqCWq5ga+bJsVodcnzRCrgJ9Cq2
lja5SugyDG/t8vW5sb+zBj609ayZY+CzRb7qhddy3tdoDP1Z7pSt9aS1eSeWC6Jb
WC5l57o2myromOCitcQBoGR1TrLeEGYwvoZ1BCjer2/ksLm15qyWed6d79+IqDc=
-----END CERTIFICATE-----
```

Nếu chuyển đổi sang dạng text nội dung của chứng chỉ có dạng như sau:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: Email=RootCATangba@yahoo.com, CN=RootCA, OU=BCY, O=MyCA
Group, C=VN
        Validity
            Not Before: Sep  5 02:07:18 2002 GMT
            Not After : Sep  4 02:07:18 2004 GMT
        Subject: Email=RootCATangba@yahoo.com, CN=RootCA, OU=BCY,
O=MyCA Group, C=VN
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1023 bit)
                Modulus (1023 bit):
                    40:00:08:00:00:e0:00:0a:00:00:60:01:90:19:9a:
                    06:ec:34:02:cf:2a:8b:a4:e8:b9:b6:d7:e7:c3:77:
                    66:67:f8:d0:a7:fa:41:5c:a5:9b:12:a4:1e:13:71:
                    fe:36:7b:9d:80:26:24:40:00:7a:9e:2e:81:9c:f7:
                    5c:77:9b:0f:29:b9:3e:2f:6f:8c:b0:84:7d:37:3b:
                    7e:0d:fb:f7:a5:98:aa:58:23:0e:a4:c3:fa:d9:90:
                    10:08:68:ac:dd:23:bf:81:38:aa:15:bd:ae:3a:81:
                    3c:d0:1f:e5:c7:73:46:94:a3:87:eb:5f:89:b6:c3:
                    09:41:3a:46:44:76:48:9b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
    Signature Algorithm: sha1WithRSAEncryption
        3e:60:f0:fe:a9:f6:4f:b1:bd:9b:1f:f0:d9:0a:82:5a:ae:60:
        6b:e6:c9:b1:5a:1d:72:7c:d1:0a:b8:09:f4:2a:b6:96:36:b9:
        4a:e8:32:0c:6f:ed:f2:f5:b9:b1:bf:b3:06:3e:b4:f5:ac:99:
        63:e0:b3:45:be:ea:85:d7:72:de:d7:68:0c:fd:59:ee:94:ad:
        f5:a4:b5:79:27:96:0b:a2:5b:58:2e:65:e7:ba:36:9b:2a:e8:
        98:e0:a2:b5:c4:01:a0:64:75:4e:b2:de:10:66:30:be:86:75:
        04:28:de:af:6f:e4:b0:b9:b5:e6:ac:96:79:de:9d:ef:df:88:
        a8:37
```

Nội dung của một chứng chỉ gồm hai phần như sau.

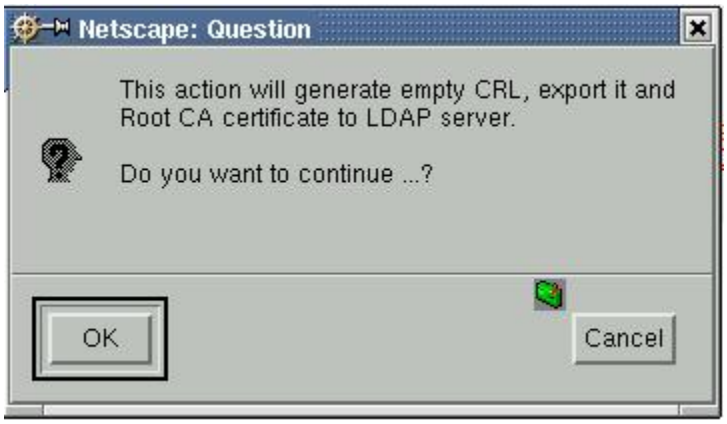
-Phần data gồm các trường chính sau:

- *Version*: phiên bản chuẩn X509.
- *Serial Number*: Số serial của chứng chỉ, đối với chứng chỉ của Root CA (silf sign certificate) trường này bao giờ cũng có giá trị là 0. (Để chỉnh lại đặc điểm này phụ thuộc vào trình myssl)
- *Signature Algorithm*: Tên hàm băm và thuật toán ký (ở đây là SHA1 và RSA)
- *Issuer*: Trường này chứa Distinguished Name (Email, CN, OU...) của đối tượng ký chứng chỉ này, ở đây ta thấy nội dung của Issuer hoàn toàn giống nội dung trong trường Subject là bởi vì chứng chỉ này được ký bởi chính nó.
- *Validity*: Trường này chứa khoảng thời gian mà chứng chỉ này có hiệu lực
- *Subject*: Distinguished Name của đối tượng được cấp chứng chỉ.
- *X509v3 extentions*: phần mở rộng theo chuẩn x509V3.

-Phần chữ ký: gồm có thông tin về thuật toán hàm băm và thuật toán ký cùng nội dung của chữ ký số.

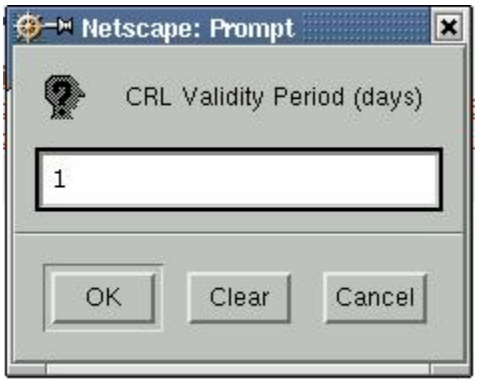
- ***Bước 3: "Export Root CA certificate and empty CRL to LDAP"***

Sau khi thực hiện sinh xong chứng chỉ tự ký cho CA, bước cuối cùng trong qui trình khởi tạo cho CA là: sinh ra một tệp "empty" CRL, đây là tệp CRL đầu tiên khởi tạo cho toàn bộ hệ thống thuộc CA này quản lý, gửi "empty" CRL và chứng chỉ tự ký của CA lên LDAP server. Khi sử dụng chức năng "Export Root CA certificate and empty CRL to LDAP", hộp hội thoại xuất hiện như hình 13.



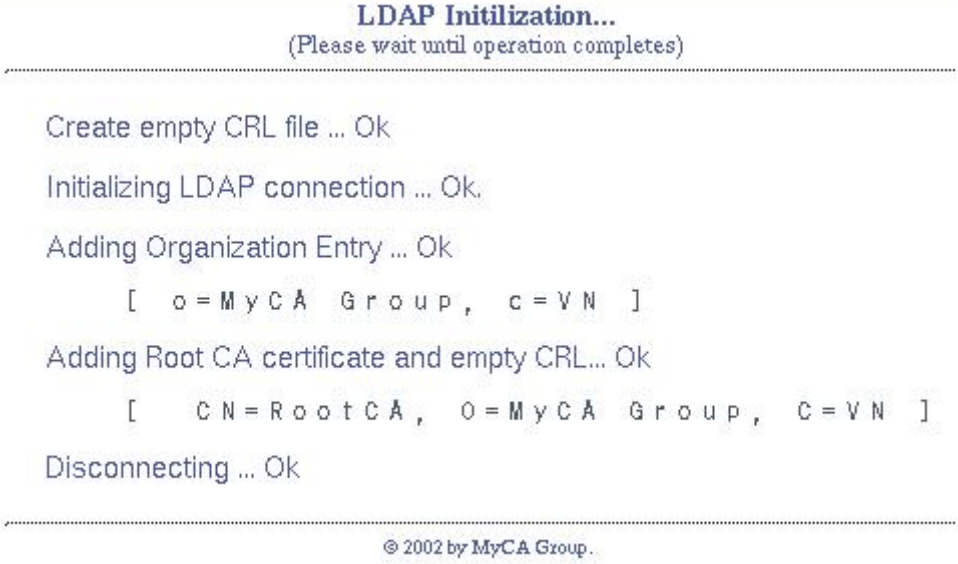
Hình 13

Chọn "OK" trên màn hình xuất hiện hộp hội thoại yêu cầu nhập thời hạn cần cập nhật CRL tiếp theo như hình 14



Hình 14

Sau khi nhập thời gian (đơn vị là ngày) nhấn "OK", trên màn hình xuất hiện hộp hội thoại yêu cầu nhập mật khẩu dùng làm khoá giải mã tệp khoá của CA xuất hiện như hình 11, người quản trị nhập mật khẩu và nhấn "OK", tiến trình thực hiện sẽ kết thúc khi trên màn hình có thông báo như hình 15 dưới đây.



Hình 15

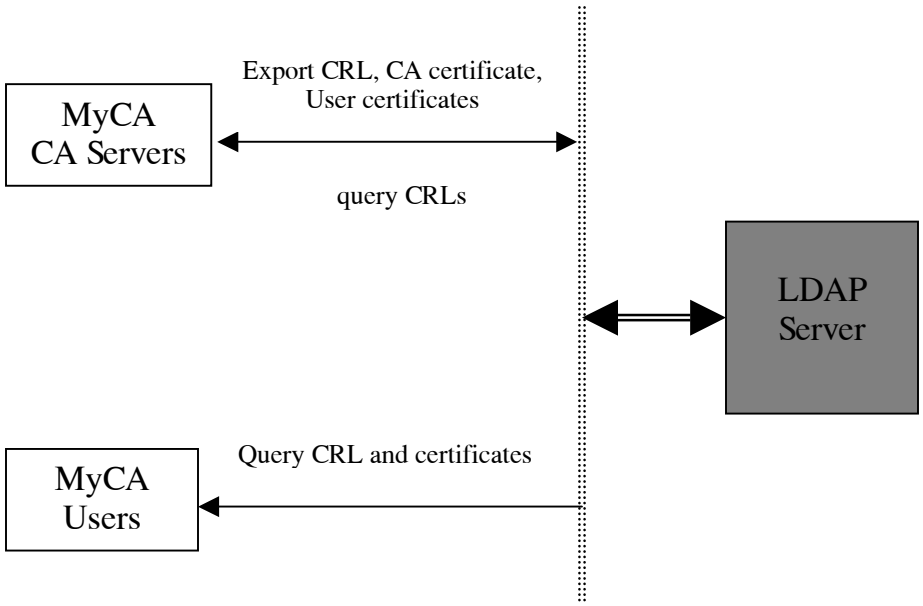
Quá trình khởi tạo cho máy máy CA kết thúc. Sau khi quá trình khởi tạo kết thúc, ngoài tệp khoá đã được mã hoá và tệp chứng chỉ của CA như chúng tôi đã trình bày ở trên, chương trình còn tạo ra các tệp chain.crt, RootCA.crt trong /MyCA/chain để phục vụ cho việc xây dựng chuỗi chứng chỉ trong trường hợp thiết lập hệ thống gồm nhiều cấp CA và tệp CRL 01_cacrlpem.crl (trong thư mục /MyCA/crl/new) là tệp "empty" CRL (chưa hề có một chứng chỉ nào bị huỷ bỏ).

Chương II
LDAP VÀ PUBLIC DATABASE TRONG HỆ THỐNG MYCA

Trong hệ thống MyCA các CRL và các chứng chỉ của người sử dụng đã được các trung tâm phát hành cần được lưu giữ trên một cơ sở dữ liệu công khai, để người sử dụng có thể tải các chứng chỉ hoặc cập nhật CRL từ cơ sở dữ liệu đó. Với yêu cầu việc cập nhật dữ liệu từ các máy server (CA server) và được query dữ liệu từ các máy client phải nhanh chóng, chính xác, phù hợp với kiểu dữ liệu có cấu trúc như các chứng chỉ. Để đạt được mục tiêu này hiện tại có rất nhiều hệ quản trị cơ sở dữ liệu có thể đáp ứng, tuy nhiên theo các thông tin chúng tôi tìm hiểu thông qua các tài liệu của những nhà khoa học có kinh nghiệm trong lĩnh vực thiết kế các hệ thống PKI thì LDAP hiện nay được dùng phổ biến nhất trong các hệ thống PKI. Do đó cơ sở dữ liệu chúng tôi chọn để lưu trữ các CTL, CRL trong hệ thống MyCA là LDAP, LDAP database server được lưu trên một (hoặc nhiều) máy server riêng. Mối quan hệ giữa LDAP server với các máy khác trong toàn hệ thống có thể phân làm hai loại sau:

- Máy CA trong hệ thống khi phát hành CRL sẽ cập nhật CRL này ra LDAP server. Khi người sử dụng đến trung tâm nhận chứng chỉ, đồng thời với việc cấp chứng chỉ cho người sử dụng, chứng chỉ đó cũng được export ra LDAP từ máy CA, ngược lại khi chứng nhận cho việc chứng chỉ của người sử dụng đã được huỷ bỏ, từ máy CA người quản trị cần truy cập tới LDAP để query CRL.
- Người sử dụng có thể dùng một trang web riêng có thể truy nhập đến LDAP database server bất cứ lúc nào để tải các chứng chỉ cũng như cập nhật các CRL.

Mô hình dưới đây có thể mô phỏng hai mối quan hệ và trao đổi dữ liệu trên:



1- LDAP
1.1- Giới thiệu chung về LDAP

LDAP là một giao thức Client/Server để truy nhập đến một Directory Service. Có thể xem Driectory như một cơ sở dữ liệu, tuy nhiên đối với các directory thường việc đọc dữ liệu hiệu quả hơn việc ghi dữ liệu. Có nhiều cách khác nhau để thiết lập một Directory Service, và cũng có nhiều phương pháp để tham chiếu, query, và truy nhập đến dữ liệu trong directory. LDAP directory service dựa trên mô hình Client/Server. Một hoặc nhiều LDAP server lưu trữ dữ liệu tạo nên các cây thư mục LDAP hoặc các backend database. LDAP client kết nối tới LDAP server, đưa ra yêu cầu để LDAP server thực hiện và trả lại kết quả cho client.

Dữ liệu khi lưu trên LDAP server có thể được lưu dưới ba loại backend database khác nhau trên LDAP server mà người sử dụng có thể lựa chọn: LDBM, SHELL, PSSWD. Đối với hệ thống MyCA chúng ta chỉ quan tâm đến loại thứ nhất.

Để truy xuất (tạo, sửa đổi, bổ sung, ...) đối với một LDBM chúng ta sử dụng các trình tiện ích như ldapmodify, ldapreplace, với dữ liệu đầu vào lưu trong các tệp LDIF (LDAP Interchange Format), hoặc cũng có thể nhập trực tiếp thông qua các tham số của các lệnh.

1.2-Cài đặt và thiết lập cấu hình cho LDAP server
1.2.1 Cài đặt LDAP server

Đối với các máy server của hệ thống MyCA chạy trên phiên bản RedHat Linux 7.2, khi thiết lập một máy làm LDAP server để lưu trữ các CTL và các CRL cần cài đặt các packege sau:

```
openLDAP-2.0.11-13
openLDAP-servers-2.0.11-13
openLDAP-devel-2.0.11-13
```

Sau khi LDAP server được cài đặt, trong thư mục /etc xuất hiện thư mục openldap trong đó cần chú ý các tệp sau:
-Tệp thiết lập cấu hình cho LDAP server /etc/openldap/slapd.conf (Stand-alone LDAP Deamon).
-Các tệp qui định tên các thuộc tính, kiểu dữ liệu của các thuộc tính, ... được lưu trên LDAP server trong thư mục /etc/openldap/schema.

1.2.2-Tệp cấu hình LDAP server

Tệp thiết lập các tham số cấu hình cho LDAP server là tệp slapd.conf (Stand-alone LDAP Daemon). Sau khi cài đặt (theo đường dẫn mặc định) tệp này được đặt trong /etc/openldap/slapd.conf, nội dung gồm các phần chính sau:

```
<Global config options>
Database <backend 1 type>
<config options specific to backend 1>
```

```
Database <backend 2 type>
<config options specific to backend 2>
....
```

Global options dùng để thiết lập các lựa chọn cấu hình chung cho LDAP server (cho tất cả các loại backend database):

+defaultaccesss quyền truy nhập mặc định (read, write)

+Includefile thiết lập các option cho các objectclass, attributes

+schemacheck thiết lập (on) hoặc huỷ bỏ (off) việc kiểm tra schem (mặc định là off)

+sizelimit chỉ ra không gian nhớ được dùng lưu trữ dữ liệu.

Backend database options (có các options chỉ dùng cho LDBM)

+database <type> (ở đây dùng ldbm)

+rootdn (root distinguished name)

+rootpw<password>

+suffix <dn suffix> (chỉ ra các dn có hậu tố như dn suffix sẽ chuyển qua database)

+cachesize

+directorry <batch> (nơi lưu dữ liệu)

.....

Để start, stop hoặc biết thông tin về trạng thái của LDAP server sử dụng tệp script ldap. Ví dụ để start LDAP server sử dụng lệnh:

/etc/rc.d/init.d/ldap start

2- Cài đặt và thiết lập cấu hình cho Public Database Server.

2.1-Cài đặt Public Database Server

Yêu cầu:

- MySSL phiên bản 0.9 hoặc cao hơn.
- Perl phiên bản 5.6.0 hoặc cao hơn.
- Apache phiên bản 1.3.12 hoặc cao hơn.
- Các module LDAP đã trình bày ở trên.

Cài đặt:

Bộ cài đặt Public Database Server lưu trong đĩa CD MyCA, để cài đặt người thực hiện các lệnh sau:

-Cài đặt Apache server trên máy LDAP server (đối với Linux 7.2 khi thực hiện cài đặt hệ điều hành Apache server đã được cài đặt luôn)

-Cho CD MyCA vào ổ CD Rom.

-Thực hiện lệnh: mount /mnt/cdrom.

-Copy tệp Database.tgz vào máy cần cài đặt và thực hiện lệnh gỡ nén:

tar -xvzf Database.tgz, được thư mục Database trong đó có các thư mục con là cgi-database và htdocs-database.

-Tạo thư mục httpd trong thư mục /home và copy hai thư mục trên vào thư mục vừa tạo.

2.2-Thiết lập cấu hình Public Database Server.

2.2.1-Thiết lập cấu hình LDAP server.

Để thiết lập cấu hình LDAP sử dụng cho MyCA cần chỉnh sửa các mục sau trong tệp slapd.conf:

-Các thuộc tính của dữ liệu cần lưu:

```
database ldbm
suffix "o=MyCA Group, c=VN"
rootdn "cn=root, o=MyCA Group, c=VN"
rootpw passwd
directory /ldap-db
```

Trên đây là những thuộc tính thiết lập cho LDAP Server, để CA server, RAOs server và người sử dụng thông qua trang publicdatabase có thể kết nối và đọc ghi dữ liệu vào LDAP trong các tệp thiết lập cấu hình cho CA server và RAOs server (ca.conf và secure.cnf) cần thiết lập các thuộc tính tương ứng với các thuộc tính trên. Cụ thể trong tệp ca.conf và secure.cnf cần bổ sung nội dung như sau:

```
## LDAP Section:
## =============
 ldapserver 200.1.1.1
 ldapport 389
 ldaplimit 100
 basedn "o=MyCA Group, c=VN"
 ldaproot "cn=root, o=MyCA Group, c=VN"
 ldappwd  "passwd"
 ldapbasedir "/ldap-db"
 ##End LDAP section
```

Với tất cả các thuộc tính cấu hình trên, LDAP server cho phép lưu các CRL và các chứng chỉ do hệ thống MyCA cấp. Tuy nhiên điều này chỉ đúng khi các trường trong chứng chỉ được nhập vào dưới dạng tiếng Anh (ví dụ các trường họ tên, quê quán, ...). Nếu muốn sử dụng tiếng Việt cho các trường này, riêng việc lưu trữ vào LDAP cũng đã là một vấn đề phức tạp chưa nói đến chuyện có thể đưa ra giải pháp tìm kiếm theo giao diện tiếng Việt. Hiện tại chúng tôi thực hiện theo giải pháp như sau: Chấp nhận việc tìm kiếm theo một trường nào đấy không liên quan đến tiếng Việt mà vẫn đảm bảo được tính duy nhất đối với từng chứng chỉ (cụ thể ở đây chúng tôi dùng trường Email của người sử dụng), khi đó chúng ta chỉ cần thực hiện làm sao lưu được các chứng chỉ có sử dụng tiếng Việt và khi query các chứng chỉ đó về vẫn giữ nguyên định dạng tiếng Việt là được.

Trong tệp /home/httpd/cgi-database/database.conf cần sửa mục ldapserver trong phần LDAP section thành địa chỉ IP của máy LDAP server. Ví dụ ở đây máy LDAP server có địa chỉ IP là 200.1.1.1 thì cần sửa thành:

ldapserver 200.1.1.1

2.2.2-Thiết lập cấu hình trang publicdatabase trên Apache

Sau khi cài đặt xong người thực hiện cần thực hiện việc thiết lập cấu hình thông qua một vài thao tác sau.

-Trong tệp cấu hình của Apache server cần bổ sung trang publicdatabase như sau:

```
<VirtualHost 200.1.1.1>
    DocumentRoot "/home/httpd/htdocs-database/"
    ServerName publicdatabase
    Errorlog logs/database/error_log
    CustomLog logs/database/access_log common
    ScriptAlias /cgi-bin/ "/home/httpd/cgi-database/"
    <Directory "/home/httpd/cgi-database">
      AllowOverride None
      Options ExecCGI
      Order allow,deny
      Allow from all
    </Directory>
</VirtualHost>
```

Sau khi thiết lập cấu hình xong cần tạo các thư mục sau:

- /ldap-db để LDAP server lưu dữ liệu.
-Tạo thư mục database trong thư mục /etc/httpd/logs

Khởi động lại LDAP để các thuộc tính vừa được cấu hình có hiệu lực bởi lệnh:

/etc/init.d/ldap restart

2.3-Mô tả các tệp thư mục trên Public Database Server

Sau khi cài đặt xong trên máy Public Database server xuất hiện hai thư mục: /home/httpd/cgi-database và /home/httpd/htdocs-database với các tệp và thư mục chính sau:

- **Trong thư mục /home/httpd/cgi-database:**

Tên tệp, thư mục	**Chức năng**
Thư mục Convert	Module chuyển đổi dữ liệu thành dạng chuẩn ANS1
Thư mục lib	Các thư viện sử dụng cho LDAP
Thư mục MailModule	Các module gồm các hàm xử lý cho MyCA
Thư mục Net	Các module xây dựng trước bao gồm các hàm làm việc với LDAP
Tệp database.cnf	Tệp cấu hình cho Public Database Server
Tệp Search	Chương trình phục vụ việc tìm kiếm (theo Email) và tải chứng chỉ từ Database server về cho người sử dụng dùng Linux
Tệp SearchIE	Chương trình phục vụ việc tìm kiếm (theo Email) và tải chứng chỉ từ Database server về cho người sử dụng dùng Windows
Tệp SearchCAlinux	Chương trình tìm kiếm (theo tên của CA) và tải các chứng chỉ của CA về cho người sử dụng dùng Linux
Tệp SearchCAwindows	Chương trình tìm kiếm (theo tên của CA) và tải các

	chứng chỉ của CA về cho người sử dụng dùng Windows
Tệp SearchCRLApa	Chương trình tìm kiếm (theo tên CAphát hành) và tải CRL về cho người sử dụng dùng Apache
Tệp SearchCRLNet	Chương trình tìm kiếm (theo tên CAphát hành) và tải CRL về cho người sử dụng dùng Netscape
Tệp SearchCRLwin	Chương trình tìm kiếm (theo tên CAphát hành) và tải CRL về cho người sử dụng dùng IE, IIS

- **Trong thư mục /home/httpd/htdocs-database:**

Tên tệp, thư mục	**Chức năng**
Tệp Index.html	Giao diện chính của trang publicdatabase
Tệp getcacert.html	Giao diện của trang "Get CA certficates"
Tệp getcacertlinux.html	Giao diện tìm kiếm, tải chứng chỉ của CA cho người sử dụng dùng Linux
Tệp getcacertwindows.html	Giao diện tìm kiếm, tải chứng chỉ của CA cho người sử dụng dùng Windows
Tệp getusercert.html	Giao diện của trang "Get a certificate"
Tệp getcertlinux.html	Giao diện tìm kiếm, tải chứng chỉ từ database server về cho người sử dụng dùng Windows
Tệp getcertwindows.html	Giao diện tìm kiếm, tải chứng chỉ từ database server về cho người sử dụng dùng Windows
Tệp getcrl.html	Giao diện trang "Dowload CRL Page"
Tệp getcrlforapache.html	Giao diện tìm kiếm và tải CRL từ database server về cho người sử dụng dùng để thiết lập Apache
Tệp getcrlfornet.html	Giao diện tìm kiếm và cập nhật CRL từ database server cho người sử dụng dùng trình duyệt Netscape
Tệp getcrlforwin.html	Giao diện tìm kiếm và tải CRL từ database server về cho người sử dụng dùng để cài đặt cho IE & IIS

2.4-Các chức năng trên trang publicdatabase

Dưới đây là bảng các chức năng chính của trang publicdatabase

Tên mục, chức năng	**Mô tả chức năng chính**
Chức năng "Download CA certificates chain from LDAP" gồm có hai mục sau:	
1."Get CA certificate for IE & IIS"	Người sử dụng dùng chức năng để tìm kiếm và tải chứng chỉ của Root CA từ database server về cho người sử dụng dùng Windows. (Trong trường hợp CA nhiều cấp tìm kiếm theo tên của CA bậc thấp nhất trong các CA có các chứng chỉ trong chuỗi các chứng chỉ cần tìm).
2. "Get CA certificate for Apache & Netscape"	Người sử dụng dùng chức năng để tìm kiếm và tải chứng chỉ của Root CA từ database

	server về cho người sử dụng dùng Netscape và Apache trên môi trường Linux. (Trong trường hợp CA nhiều cấp tìm kiếm theo tên của CA bậc thấp nhất trong các CA có các chứng chỉ trong chuỗi các chứng chỉ cần tìm).
Chức năng "Download Certificate from LDAP" gồm 2 mục sau:	
1."Get Certificate for Netscape Browser, Apache server"	Người sử dụng dùng chức năng để tìm kiếm (theo Email được đăng ký trong chứng chỉ cần tìm) và tải chứng chỉ từ database server về cho người sử dụng dùng Linux
2."Get Certificate for IE & IIS"	Người sử dụng dùng chức năng để tìm kiếm (theo Email được đăng ký trong chứng chỉ cần tìm) và tải chứng chỉ từ database server về cho người sử dụng dùng Windows
Chức năng "Update CRLs" gồm có ba mục sau:	
1. "Update current CRLs for Netscape"	Người sử dụng dùng chức năng để tìm kiếm (theo tên của CA phát hành ra CRL cần tìm) và cập nhật CRL đó cho Netscape trên Linux
2."Get current CRLs for Apache Server"	Người sử dụng dùng chức năng để tìm kiếm (theo tên của CA phát hành ra CRL cần tìm) và tải CRL đó về cho người sử dụng dùng để thiết lập cấu hình cho Apache trên Linux
3."Get current CRLs for IE & IIS"	Người sử dụng dùng chức năng để tìm kiếm (theo tên của CA phát hành ra CRL cần tìm) và tải CRL đó về cho người sử dụng dùng để cài đặt cho IE và IIS trên Windows.

3-Sử dụng các chức năng của trang giao diện Public Database Server

Để cập nhật CRL, tải các CTL của người khác (để sử dụng cho mục đích bảo mật Mail chẳng hạn), hoặc tải chuỗi các chứng chỉ của các CA, người sử dụng có thể dùng trang publicdatabase.

Để truy cập được tới publicdatabase người sử dụng cần thiết lập cấu hình trên máy của mình như sau:

-Đối với trường hợp người sử dụng dùng môi trường Linux cần bổ sung thêm dòng:

200.1.1.1 publicdatabase

vào tệp /etc/hosts

-Đối với người sử dụng dùng môi trường Windows cần bổ sung dòng :

200.1.1.1 publicdatabase

vào tệp c:\Windows\hosts

Trong đó 200.1.1.1 là địa chỉ IP của máy Public Database Server.

Khi truy cập tới trang http://publicdatabase, giao diện chính của trang publicdatabase xuất hiện như hình 1

Hình 1

3.1-Tải các chứng chỉ của CA từ Public Database Server

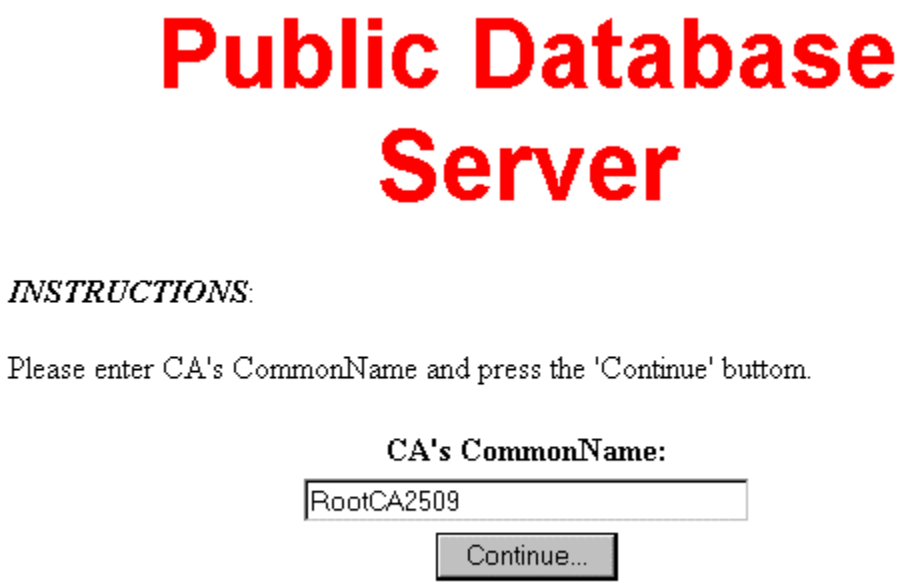
Việc tải chuỗi các chứng chỉ của các CA (CA certificates chain), phục vụ cho việc thiết lập cấu hình Apache server để xác thực các Web browser, hoặc trong trường hợp người sử dụng các trình duyệt làm mất tệp RootCA.crt đã được cấp.

Để thực hiện chọn chức năng "Dowload CA certificates chain from LDAP", khi đó trên màn hình xuất hiện giao diện như hình 2.

Hình 2

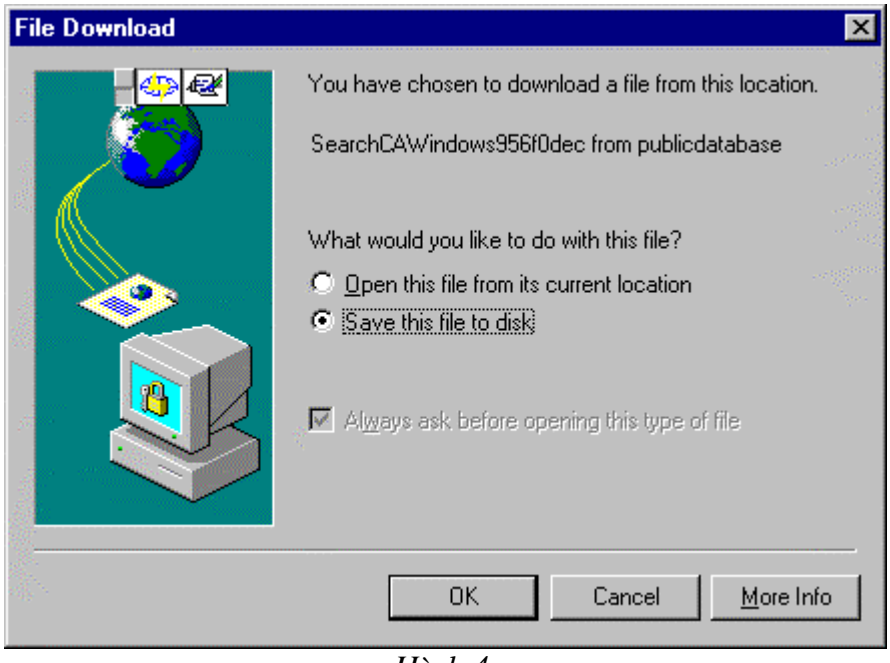
Trên đó có hai sự lựa chọn tương ứng với hai môi trường mà người sử dụng có thể đang dùng ("Get CA certificates chain for Linux's users" cho môi trường Linux và

"Get CA certificates chain for Windows's Users" cho môi trường Windows). Khi chọn một trong hai chức năng này trên màn hình xuất hiện form như hình 3.



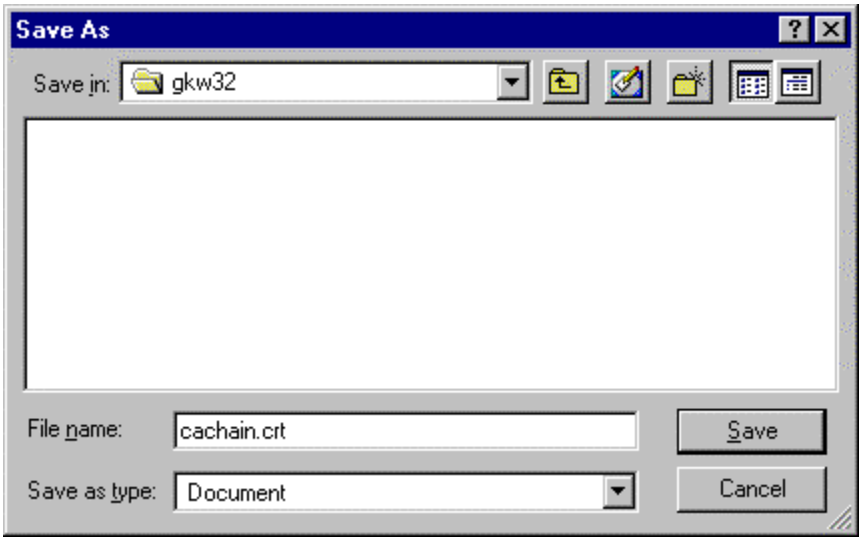
Hình 3.

Người sử dụng nhập tên CA đã cấp chứng chỉ cho người sử dụng vào mục "CA's CommonName", rồi chọn "Continue...". Trên màn hình xuất hiện hộp hội thoại như hình 4.



Hình 4.

ở đây chúng tôi trình bày cho người sử dụng dùng Windows, đối với trường hợp người sử dụng dùng môi trường Linux hoàn toàn tương tự. Người sử dụng chọn "OK", trên màn hình xuất hiện hộp hội thoại yêu cầu người sử dụng chọn tên và đường dẫn tệp lưu các chứng chỉ của CA.

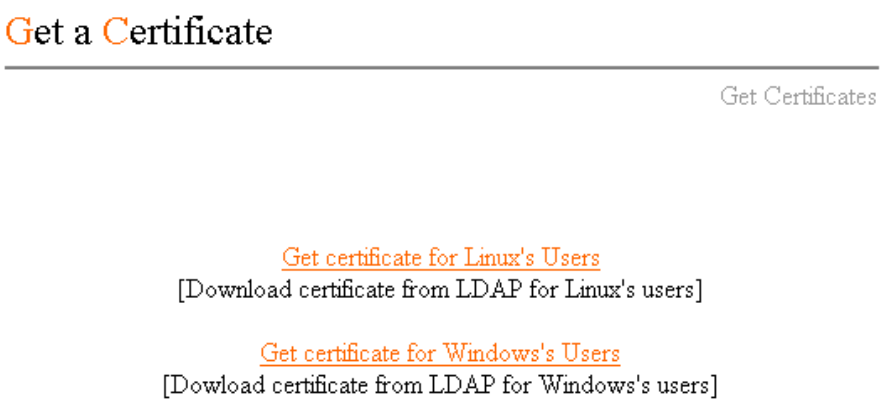


Hình 5.

Sau khi chọn đường dẫn và tên tệp người sử dụng chọn "Save", quá trình tải và lưu tệp chứng chỉ của CA vào máy của người sử dụng được tiến hành.

3.2-Tải chứng chỉ của người khác từ Public Database Server

Người sử dụng chọn chức năng *"Download certificate from LDAP"* khi muốn tải một chứng chỉ của một người khác từ Public Database Server về sử dụng (chẳng hạn sử dụng cho mục đích bảo mật Mail). Khi chọn chức năng này trên màn hình xuất hiện giao diện như hình 6.



Hình 6

Tương tự như trường hợp người sử dụng muốn tải các chứng chỉ của CA, ở đây cũng có hai sự lựa chọn dành cho hai môi trường mà người sử dụng có thể dùng. Khi chọn một trong hai lựa chọn này trên màn hình xuất hiện form như hình 7.

Hình 52

Người sử dụng nhập địa chỉ E-mail của người có chứng chỉ cần tải về vào mục "E-Mail address", rồi nhấn "Continue". Trên màn hình lần lượt xuất hiện các hộp hội thoại như hình 4, 5 người sử dụng thực hiện tương tự như đối với trường hợp lưu tệp các chứng chỉ của CA.

3.3-Cập nhật CRLs

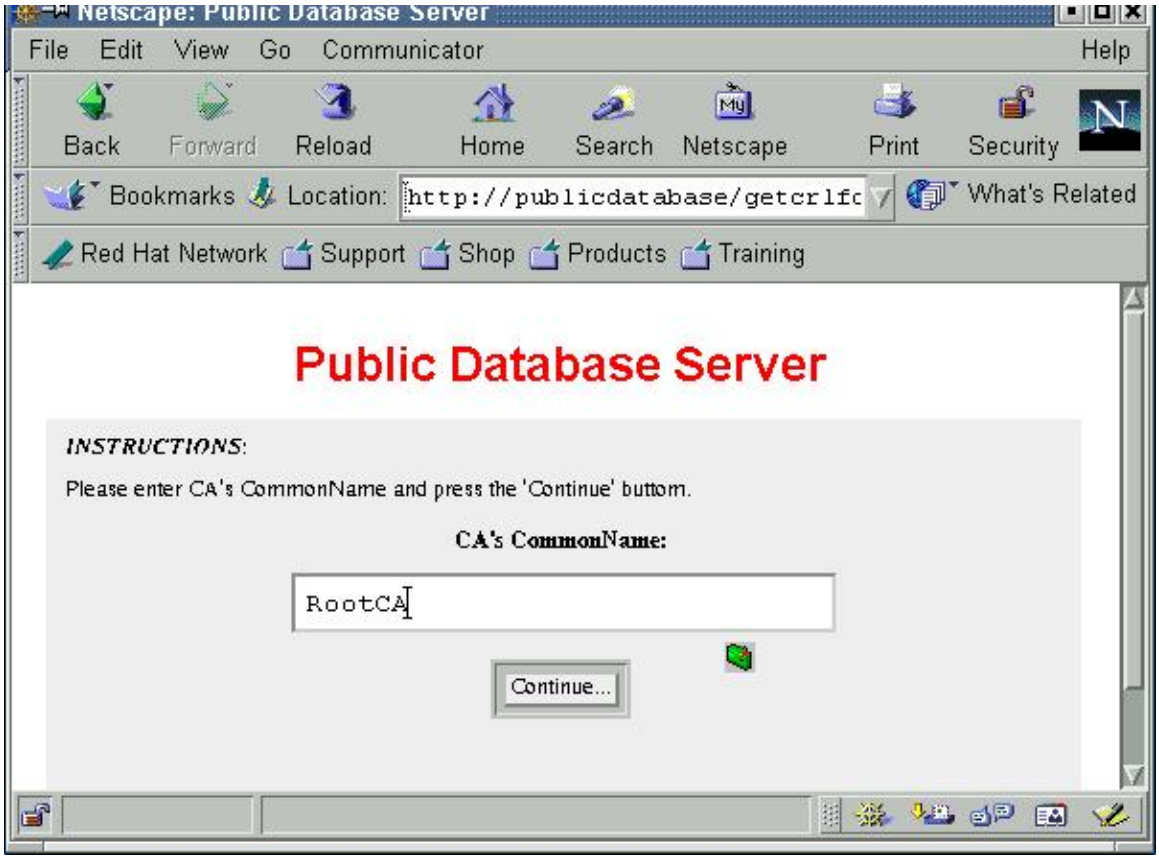
Công việc cập nhật CRL phải được thực hiện thường xuyên trên toàn hệ thống (kể cả người sử dụng). Công việc này rất quan trọng, nếu bạn không cập nhật CRL thường xuyên thì có thể bạn phải làm việc với một đối tác dùng chứng chỉ đã đã bị huỷ bỏ, điều này sẽ bất lợi cho bạn (hoặc với cả đối tác đã huỷ chứng chỉ).
Để thực hiện việc cập nhật CRLs người sử dụng chọn chức năng "*Update CRLs*", khi đó trên màn hình xuất hiện giao diện như hình dưới.

Hình 8

Đến đây chúng ta phải lựa chọn một trong 3 chức năng, việc lựa chọn tuỳ thuộc vào hệ thống của bạn. Trong mục này chúng tôi đi trình bày chi tiết cách cập nhật CRL của từng hệ thống: Netscape Browser, Apache Server, IE và IIS.

3.3.1 Cập nhật CRL cho trình duyệt Netscape

Để cập nhật CRL cho Netscape Browser chúng ta phải chọn chức năng thứ nhất **Update curren CRLs for Netscape**, trên màn hình xuất hiện hộp thoại yêu cầu nhập Common Name của CA phát hành ra CRL mà người sử dụng cần cập nhật.

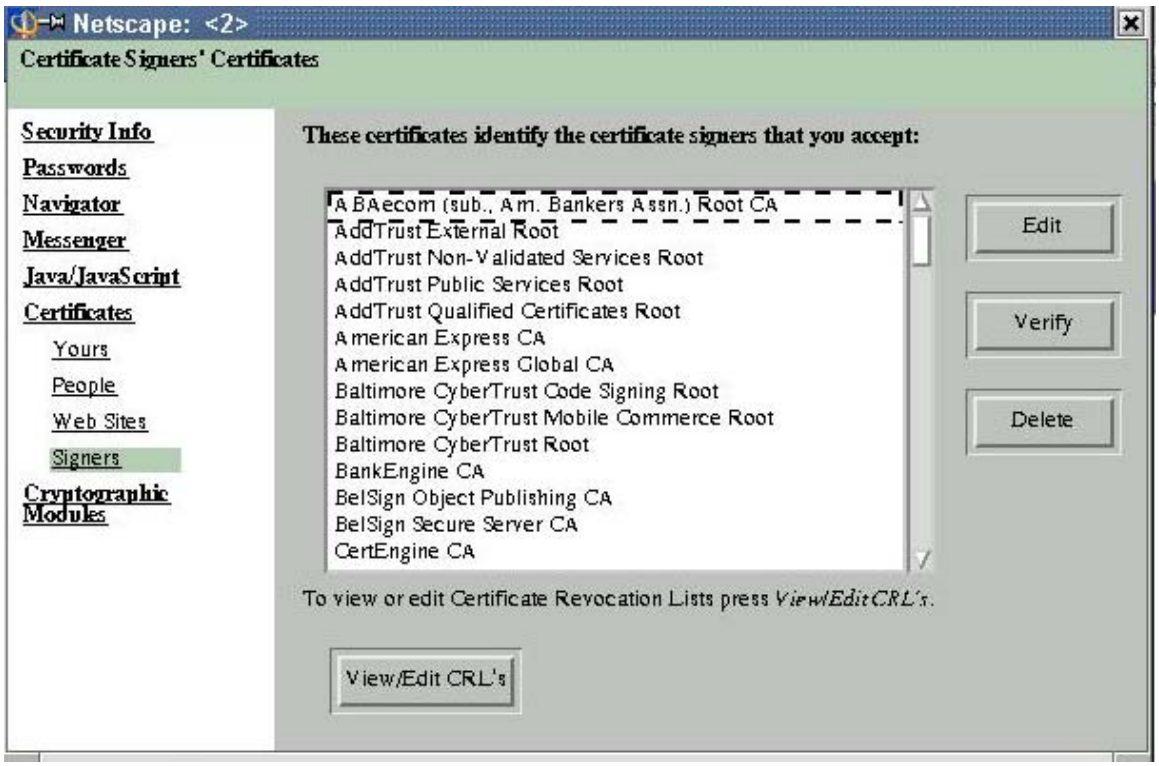


Hình 9

Sau khi nhập Common Name của CA (ở đây là RootCA), chọn **Continue...**, Quá trình tải và cập nhật CRLs cho Netscape se tự động được tiến hành. Để kiểm tra, bạn vào hộp **Security** của trình duyệt, xuất hiện hộp thoại:

Hình 10

Chọn **Signers** trong mục **Certificates**, xuất hiện hộp thoại đưa ra danh sách tất cả các CA bạn đang sử dụng:



Hình 11

Trong hộp thoại này, chọn tên CA phát hành ra CRL chúng ta vừa cập nhật rồi chọn hộp **View/Edit CRL's**, xuất hiện hộp thoại hiển thị danh sách các CRLs (ứng với CA đã phát hành) đã cập nhật vào Netscape:

Hình 12

Trong hộp thoại trên danh sách các CRL (trong mục CRL List) đã cập nhật chỉ có CRL phát hành của RootCA. Để hiển thị thông tin các chứng chỉ đã huỷ bỏ do một CA nào đó phát hành thì bạn chọn CA đó và chọn hộp More Info..., ở đây chọn RootCA, khi đó xuất hiện hộp thoại:

Hình 13

Giải thích:

- Netscape cập nhật CRL qua trang http://publicdatabase.
- Cập nhật lần cuối cùng vào thứ tư ngày 11 tháng 9 năm 2002.
- Cập nhật lần tiếp theo muộn nhất vào thứ tư ngày 18 tháng 9 năm 2002 (được thiết lập ở CA trong trường CRL Validity Period (days) của mục Issue New CRL).
- CRL được phát hành bởi RootCA.
- Danh sách các chứng chỉ đã huỷ bỏ do CA đó phát hành, ở đây chỉ có 1 chứng chỉ bị huỷ bỏ với số ID là 1e8484 (2000004) dạng hexa.

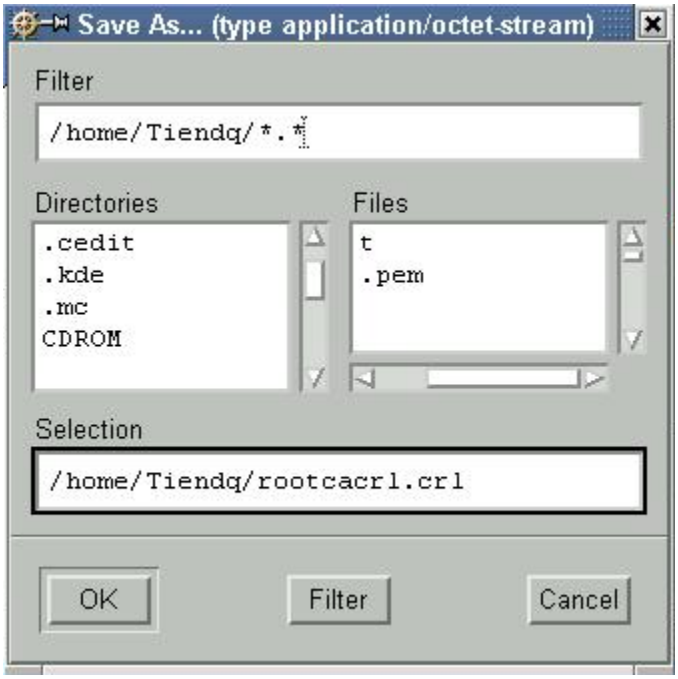
Sau khi đã cập nhật CRL thì những chứng chỉ trong danh sách đã huỷ bỏ sẽ không thể thực hiện kết nối bảo mật với hệ thống của bạn nữa và ngược lại.

3.3.2- Cập nhật CRL cho Apache Server

Để Cập nhật CRL cho Apache Server người quản trị Apache chọn chức năng thứ 2 **Get current CRLs for Apache Server**, xuất hiện hộp thoại yêu cầu vào Common Name của CA cần cập nhật CRL (CA của đối tác), ở đây chúng tôi chọn RootCA.

Hình 14

Chọn "**Continue...**" trên màn hình xuất hiện hộp thoại yêu cầu chỉ ra đường dẫn và tên tệp lưu CRL cần tải về:



Hình 15

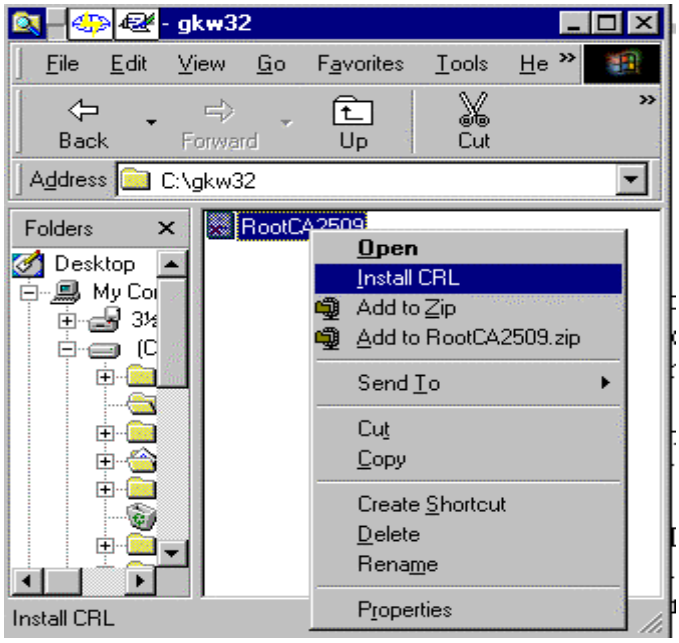
Trong hộp thoại trên lưu CRL vào tệp có tên rootcacrl.crl đặt trong thư mục /home/Tiendq.

3.3.3 Cập nhật CRL cho trình duyệt Internet Explorer

Để Cập nhật CRL cho IE **Get current CRLs for IE& IIS**, khi chọn chức năng này trên màn hình trình duyệt IE xuất hiện form như hình 3. Người sử dụng nhập tên của CA phát hành ra CRL cần tải về vào mục CA's CommonName, rồi nhấn "Continue...", khi đó trên màn hình lần lượt xuất hiện các hộp hội thoại như hình 4, hình 5, Người sử dụng chọn tên tệp lưu CRL khi tải về (ở đây chúng tôi chọn luôn tên là RootCA2509.crl), và thực hiện việc tải CRL về tương tự như việc tải CA certificate chúng tôi đã trình bày ở trên.

Sau khi đã tải CRL về người sử dụng cần cập nhật CRL đó cho trình duyệt IE và IIS. Trong mục này chúng tôi chỉ trình bày việc cập nhật CRL cho trình duyệt IE còn việc cập nhật CRL cho IIS chúng tôi sẽ trình bày trong mục sau. Các bước cập nhật được tiến hành như sau:

-Mở Windows Explorer, chọn tên tệp lưu CRL vừa tải về, nhấn nút phải chuột.

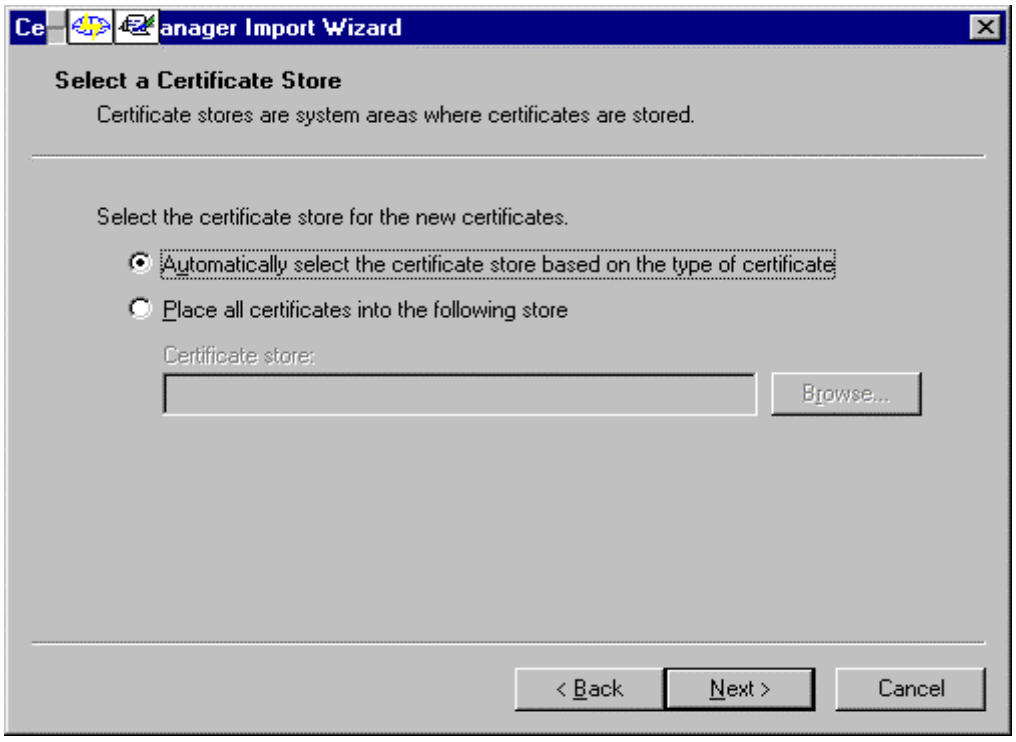


Hình 16

-Trên menu popup chọn mục "Install CRL", trên màn hình xuất hiện hộp hội thoại như hình 17.

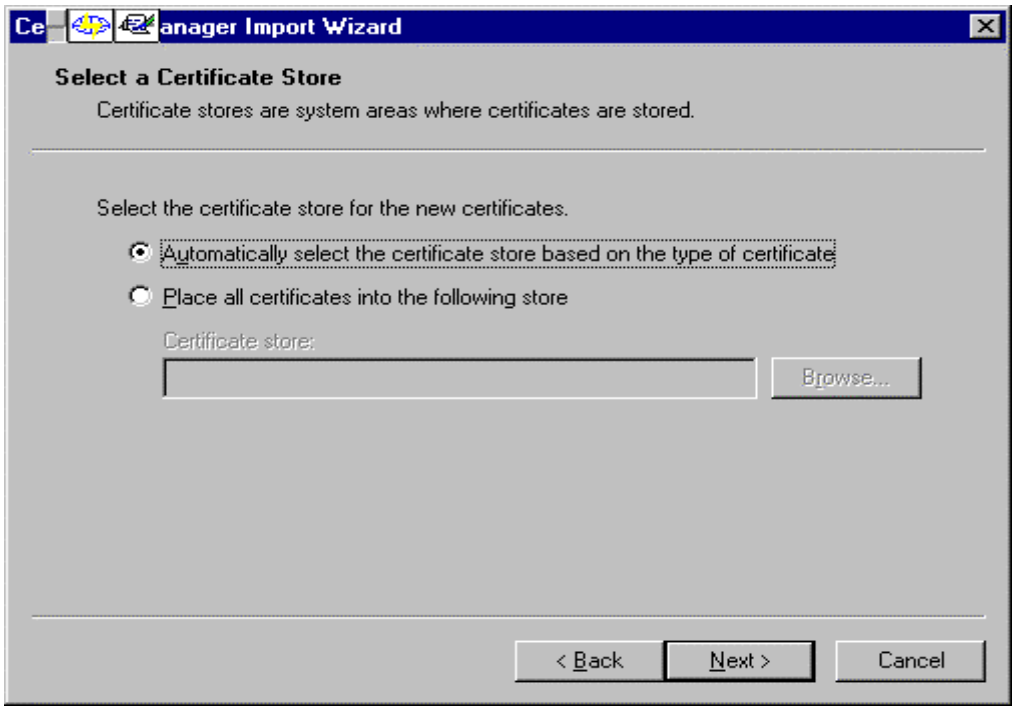
Hình 17

-Người sử dụng chọn "Next", trên màn hình xuất hiện hộp hội thoại như hình 18.



Hình 18

-Người sử dụng chọn "Next", trên màn hình xuất hiện hộp hội thoại như hình 19.



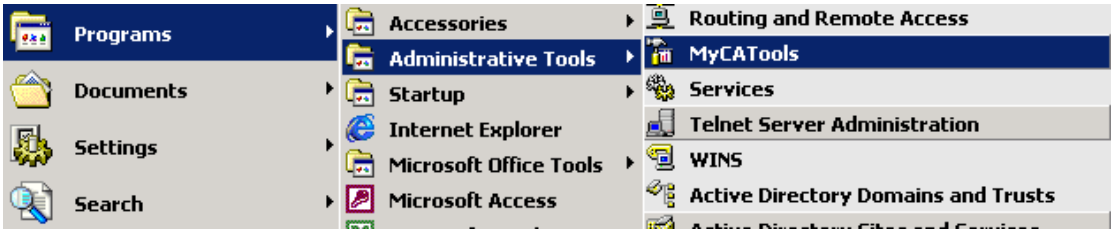
Hình 19

-Người sử dụng chọn "Next", quá trình cài đặt CRL cho IE kết thúc khi trên màn hình hộp hội thoại thông báo như hình 20.

Hình20

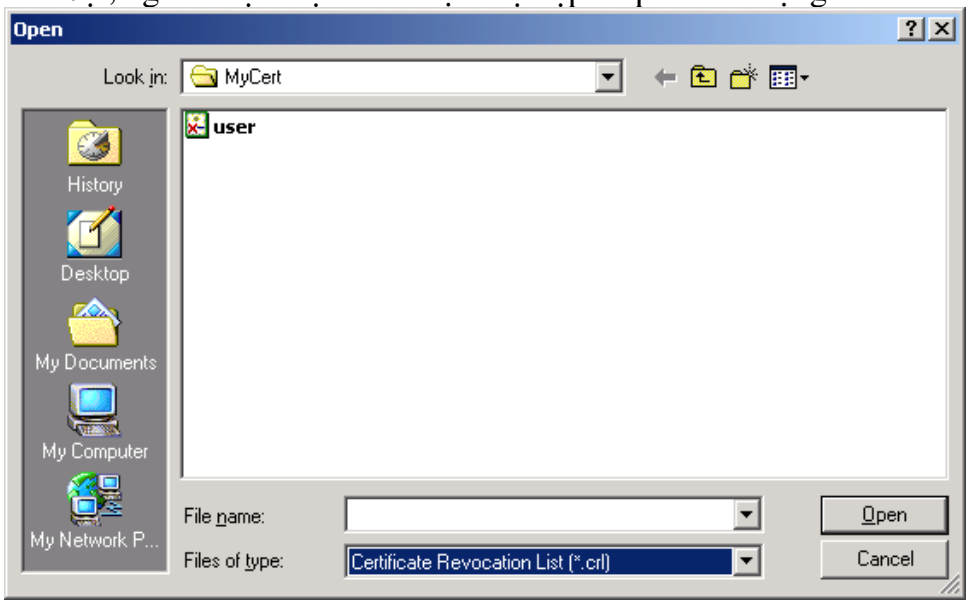
3.3.4-Cập nhật CRL cho IIS

Để cập nhật CRL cho IIS, người quản trị chạy tiện ích MyCATool trên Start menu theo đường dẫn như hình dưới đây:



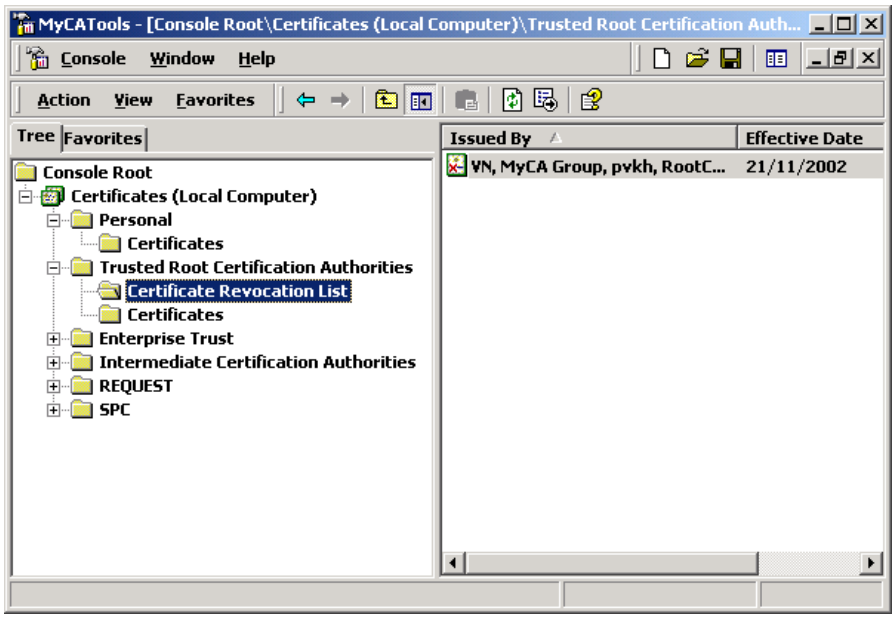
Hình 21

Sau khi chạy MyCATool, màn hình Console xuất hiện như hình 22, để cập nhật CRL do Root CA người quản trị chọn mục Trusted Root Certification Authorities", nhấn chuột phải, chọn All Tasks/import..., quá trình thực hiện việc cập nhật CRL tương tự như khi cài đặt chứng chỉ, chỉ chú ý rằng khi hộp hội thoại yêu cầu chọn tệp cần cài đặt, người thực hiện cần chọn loại tệp có phần mở rộng là ".crl".



Hình 22

-Sau khi thực hiện việc cập nhật CRL, nếu chọn "Trusted Root Certification Authorities"/"Certificates Revocation List", sẽ thấy CRL vừa được cập nhật trong danh sách.



Hình 23

Chương III
QUI TRÌNH PHÁT HÀNH CHỨNG CHỈ SỐ

Phần mềm cấp chứng chỉ số chạy trên môi trường Linux 7.2, giao diện thực hiện các thao tác cấp chứng chỉ được thực hiện thông qua trình duyệt Web, cụ thể trong tài liệu này chúng tôi sử dụng giao diện của trình duyệt Netscape.

Giao diện chính của phần mềm cung cấp chứng chỉ số như hình 1.

Hình 1.

Để sinh một chứng chỉ số cho một người sử dụng, chúng ta chỉ cần thực hiện ba chức năng trên giao diện chính của phần mềm, đó là: Input User's Data, Sign Certificate Requests và Generate PKCS12 Certificate. Dưới đây lần lượt là các bước thực hiện việc cấp một chứng chỉ số.

1. Bước 1: Nhập thông tin về người được cấp (Input User's Data)

Khi chọn chức năng này trên màn hình xuất hiện giao diện như hình 2.

Hình 2

Người thực hiện lần lượt nhập các thông tin của người được cấp chứng chỉ vào các mục trên giao diện.

-Họ và tên (Fullname)

-Số chứng minh nhân dân (ID Card Number)

-Ngày cấp chứng minh (ID Card Issued Date)

-Ngày tháng năm sinh (Date of Birth)

-Phòng ban (Office)

-Địa chỉ Email (Email)

-Chức năng của chứng chỉ được cấp (Certificate Type), đối với ứng dụng Mail kiểu chứng chỉ bao giờ cũng phải chọn là "User Certificate".

-Số PIN, số PIN sẽ tự động được tăng lên khi thông tin một người được chấp nhận.

Sau khi nhập đầy đủ các thông tin trên, người thực hiện chọn nút lệnh "Accept". Khi đó trên màn hình xuất hiện hộp hội thoại như hình 3

Hình 3

Chương trình sẽ tự động sinh yêu cầu cấp chứng chỉ số (Certificate Request) với các thông tin trên. Quá trình sinh yêu cầu kết thúc khi trên màn hình xuất hiện thông báo như hình 4.

Hình 4

Sau khi thực hiện xong bước 1, trong thư mục /MyCA/user sẽ xuất hiện thêm thư mục mang tên là số ID của người sử dụng, trong đó có lưu tệp khoá bí mật và tệp yêu cầu cấp chứng chỉ của người sử dụng dưới định dạng PKCS#10

Ví dụ định dạng tệp khoá bí mật của người sử dụng:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgEAAAL2/IIyjw/DAAOnaBlaeiWRU5hyYgwylsGPxC6tqOBJaHyxo
Ddl6OWTKqB0hJb6qLVTMrGBlF7CikN8Ut5ymS3+Nl1FfRMNTAgKIWbGGYzppT3z/
62pJdObH3Eju/HYAkauMySo6MZiyu2BuH7riRLi8x9iTn180uqOa1+nbAgMBAAEC
gYAicl3zww135SUvTYiwVYMX2BjHAdMhDQ1sHzoDcNgBGRi49/zTX+Ykad6+Wz2F
ADRanSns/ITDFWZc0gL7ryDsC+OSJZeMfCR8pQ7s5k5LEymuAWEjUFuwzstcm4bK
mztiVwxjVor4hfU1nukj0ZqFLMY7zZek52qDb2flDFX10QJBAIAAAL2/QAAAAAAA
ASxwanoUTHEoOmcc/yhXCDtcsWFCbL5aVEmIkSc3OAE92ADmQ2nKHcB3o0CYgkW5
eLMfc00CQQCAAAC9vwAAAAAAACnQ5991rVWwOGY4tjYImNIEJhlM3ikprYRSifS
Y3RUxyW783hRTrGLBzk8VGVJnJccw+3HAkAePuHt9EktNtLJLTcZxx6B5lYBzx2t
y95HK/mX/Vk0wDtt525PSePyvkuPj4uA+ugnEUlid2KuGtt9mkv5F49pAkBNT7Mi
6Fp3pYhad6XtYUrUFvswiw+36ExRP3P38w4ZEh2sVYVirAeha7C4BBEmlMf3VDCo
aJSJe/AxpgMfvLfBAkB4RpdFbJREFkXlozJRSbWPyWc3jGh5axkKQHwIOYbqwaFc
SIaD+vA2CUCpxdczfOBae4GqNRZdFW0sPqb6JIb7
-----END RSA PRIVATE KEY-----
```

Ví dụ định dạng tệp yêu cầu của người sử dụng dưới dạng text

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: Email=thuchv@yahoo.com, CN=Hoàng Văn Thức-2000001-
123456789-123456789-12-12-1990, ST=Thanh Hoá, OU=MyCA User, O=MyCA
Group, C=VN
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1023 bit)
                Modulus (1023 bit):
                    40:00:00:bd:bf:a0:8c:a4:81:b0:20:01:c2:32:b9:
```

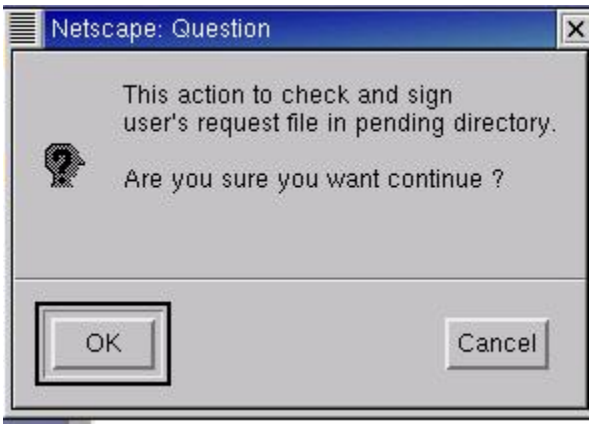
```
                    d0:84:56:5e:df:d0:9c:33:e3:1e:b7:80:4d:60:9a:
                    87:33:85:c6:3c:5e:47:22:d1:5e:76:62:9a:f6:50:
                    ae:a8:a3:51:e7:ff:c6:5f:c1:aa:88:da:06:42:0f:
                    df:a0:de:e4:00:15:30:27:54:2d:07:ee:ed:80:e1:
                    61:3d:e7:16:af:a7:fd:d5:2d:3f:40:34:8e:c5:c8:
                    e4:3e:c6:1d:99:88:20:f2:c5:84:26:92:9f:a4:62:
                    67:cb:9a:16:f5:78:9c:9f:82:9c:ff:37:0d:ce:ce:
                    af:89:fb:7a:07:31:89:c5
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        0a:27:1d:84:a0:52:54:67:cf:70:e1:08:54:9e:6c:cf:92:59:
        4b:cf:5d:61:f0:f8:7f:86:7d:ad:cc:15:4e:e7:d0:1c:00:e8:
        ac:da:85:56:2d:b6:f3:3d:07:f3:f3:ae:70:37:9b:63:55:12:
        ce:be:2f:1e:d4:95:b2:f1:f9:7b:5d:26:22:37:c2:7c:78:91:
        48:09:2a:9e:f5:46:de:e4:a7:f1:82:41:ee:a7:6a:51:4c:31:
        16:55:b6:3f:2d:f1:04:eb:b0:2a:c3:6e:64:f3:6a:ef:4e:da:
        49:fd:3e:2b:3a:58:44:48:ac:ed:9d:a2:81:48:96:a3:c6:54:
        dc:da
-----BEGIN CERTIFICATE REQUEST-----
MIIB6zCCAVQCAQAwgasxHzAdBgkqhkiG9w0BCQEWEHRodWNodkB5YWhvby5jb20x
PjA8BgNVBAMUNUhvtW5nIFaobiBUaPhjLTIwMDAwMDEtMTIzNDU2Nzg5LTEyMzQ1
Njc4OS0xMi0xMi0xOTkwMRIwEAYDVQQIFAlUaGFuaCBIb7gxEjAQBgNVBAsTCU15
Q0EgVXNlcjETMBEGA1UEChMKTXlDQSBHcm91cDELMAkGA1UEBhMCVk4wgZ4wDQYJ
KoZIhvcNAQEBBQADgYwAMIGIAoGAQAAAvb+gjKSBsCABwjK50IRWXt/QnDPjHreA
TWCahzOFxjxeRyLRXnZimvZQrqijUef/xl/BqojaBkIP36De5AAVMCdULQfu7YDh
YT3nFq+n/dUtP0A0jsXI5D7GHZmIIPLFhCaSn6RiZ8uaFvV4nJ+CnP83Dc7Or4n7
egcxicUCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAAonHYSgUlRnz3DhCFSebM+S
WUvPXWHw+H+Gfa3MFU7n0BwA6KzahVYttvM9B/PzrnA3m2NVEs6+Lx7UlbLx+Xtd
JiI3wnx4kUgJKp71Rt7kp/GCQe6nalFMMRZVtj8t8QTrsCrDbmTzau9O2kn9Pis6
WERIrO2dooFIlqPGVNza
-----END CERTIFICATE REQUEST-----
```

2. Bước 2: Ký yêu cầu cấp chứng chỉ số (Sign Certificate Requests)

Khi chọn chức năng này trên màn hình xuất hiện giao diện như hình 5

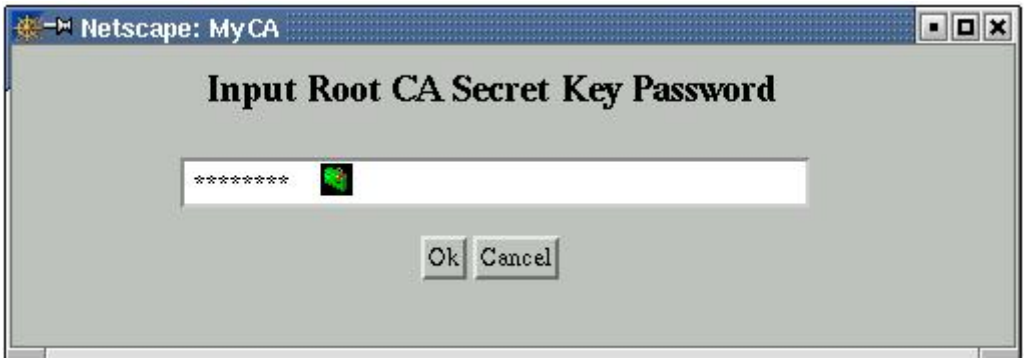
Hình 5

Người thực hiện chọn chức năng "Sign User's Request Files", khi đó trên màn hình xuất hiện hộp hội thoại như hình 6.



Hình 6

Người quản trị chọn "OK", trên màn hình xuất hiện hộp hội thoại như hình 7.



Hình 7

Người sử dụng nhập mật khẩu dùng để giải mã khóa bí mật của CA (mật khẩu này được đặt khi thực hiện thiết lập hệ thống), rồi chọn "OK". Quá trình phát hành chứng chỉ số cho người sử dụng sẽ được thực hiện .

Hình 8

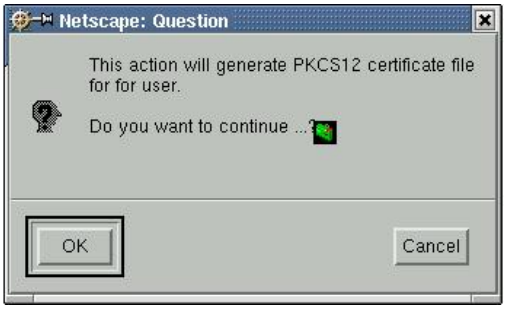
Trong ví dụ trên người được cấp chứng chỉ số có số PIN là 2000202. Quá trình phát hành chứng chỉ thành công khi có thông báo "Ok!" (như ở hình 8), việc phát hành là không thành công nếu thay bởi thông báo "Ok!" chương trình thông báo "Failed!".

3. Bước 3: Chuyển đổi định dạng của chứng chỉ (Generate PKCS12 Certificate)

Sau khi đã phát hành chứng chỉ số, để cài đặt được chứng chỉ cho ứng dụng Mail hoặc lưu vào thiết bị IKey, thì chứng chỉ số cần được chuyển đổi định dạng thành dạng PKCS12, để thực hiện sử dụng chức năng "Generate PKCS12 Certificate", khi đó trênn màn hình xuất hiện giao diện như hình 9.

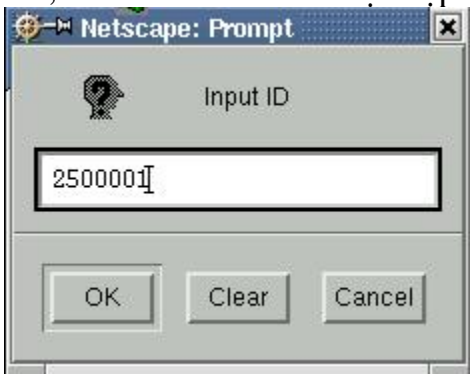
Hình 9.

Người thực hiện chọn "Generate User's PKCS12 files", trên màn hình xuất hiện hopp hội thoại như hình 10.



Hình 10

Người thực hiện chọn "OK", trên màn hình xuất hiện hộp hội thoại như hình 11.

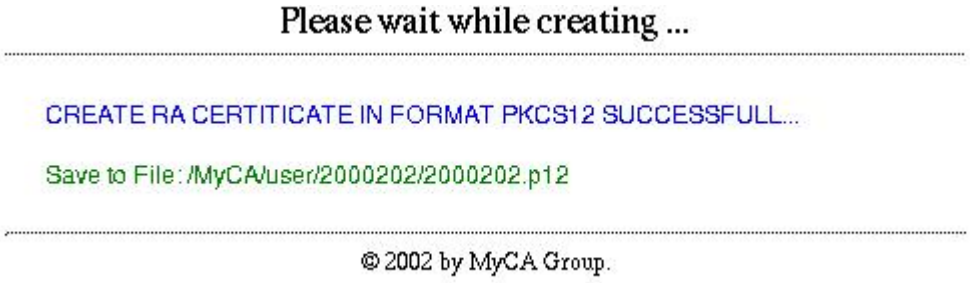


Hình 11

Người thực hiện nhập số PIN của người được cấp chứng chỉ rồi chọn "OK", trên màn hình xuất hiện hộp hội thoại như hình 12.

Hình 12

Người quản trị nhập mật khẩu mã hoá khoá bí mật trong tệp pkcs#12 rồi chọn "OK", quá trình chuyển đổi được thực hiện như thông báo trên màn hình.

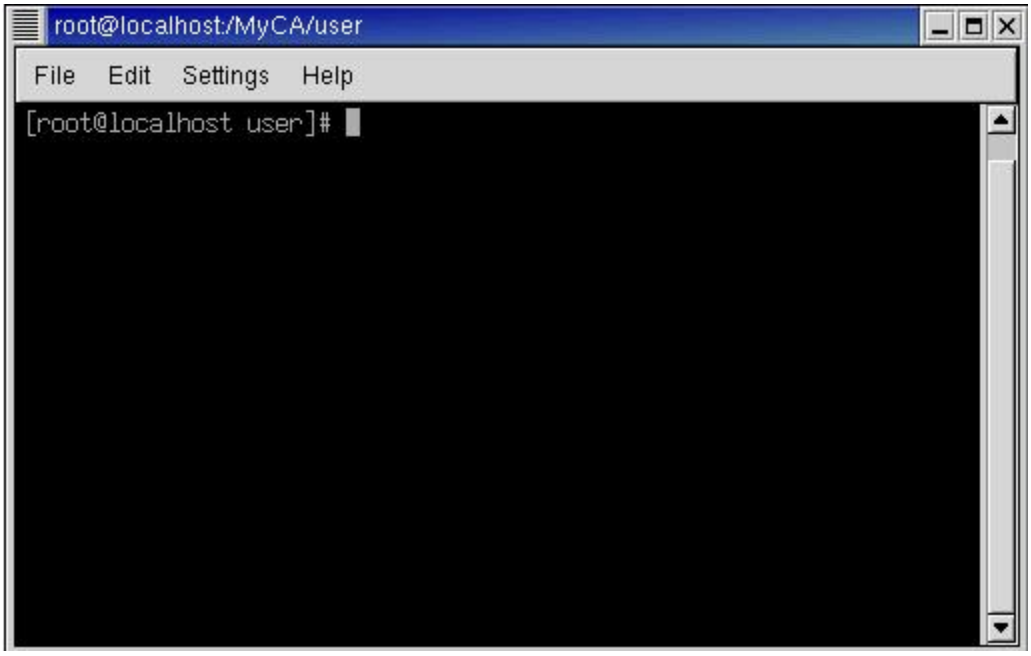


Hình 13

Quá trình sinh chứng chỉ kết thúc.

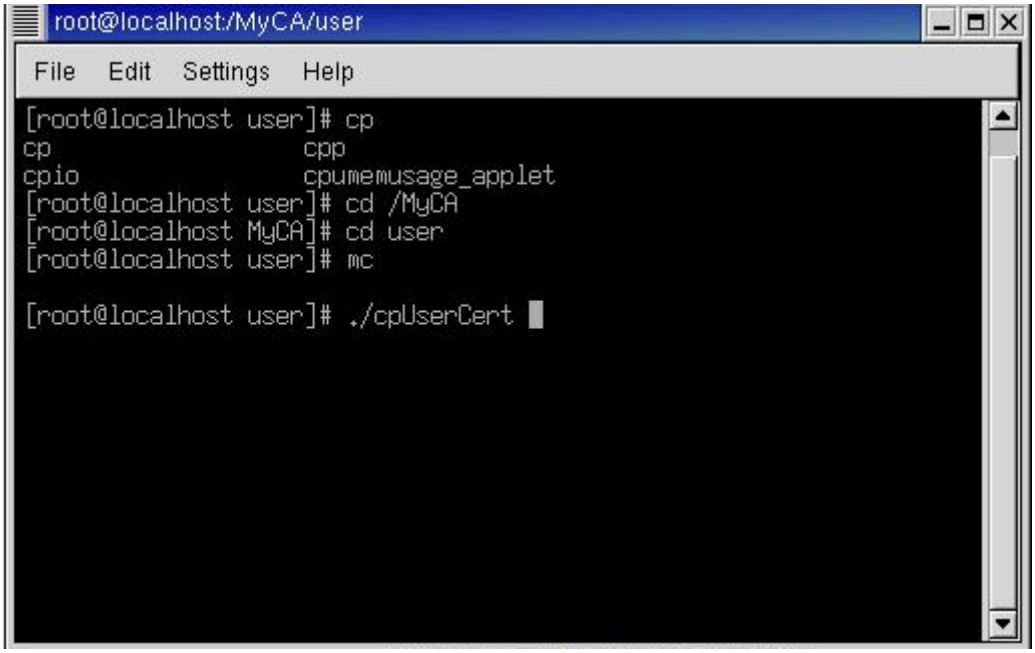
4. Bước 4: Cấp chứng chỉ cho người dùng

Bản chất của bước này là copy chứng chỉ vào đĩa mềm cho người sử dụng. Để thực hiện mở màn hình commandline, chuyển thư mục hiện hành thành /MyCA/user, như hình 14



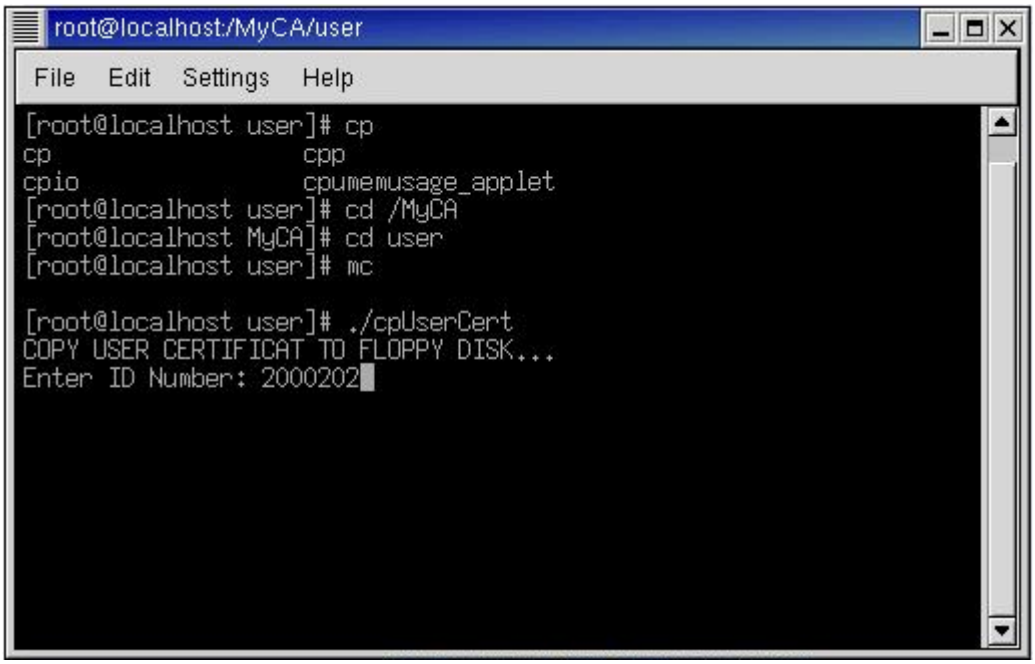
Hình 14

Cho đĩa mềm vào ổ và thực hiện lệnh "./copyUserCert" như hình 15



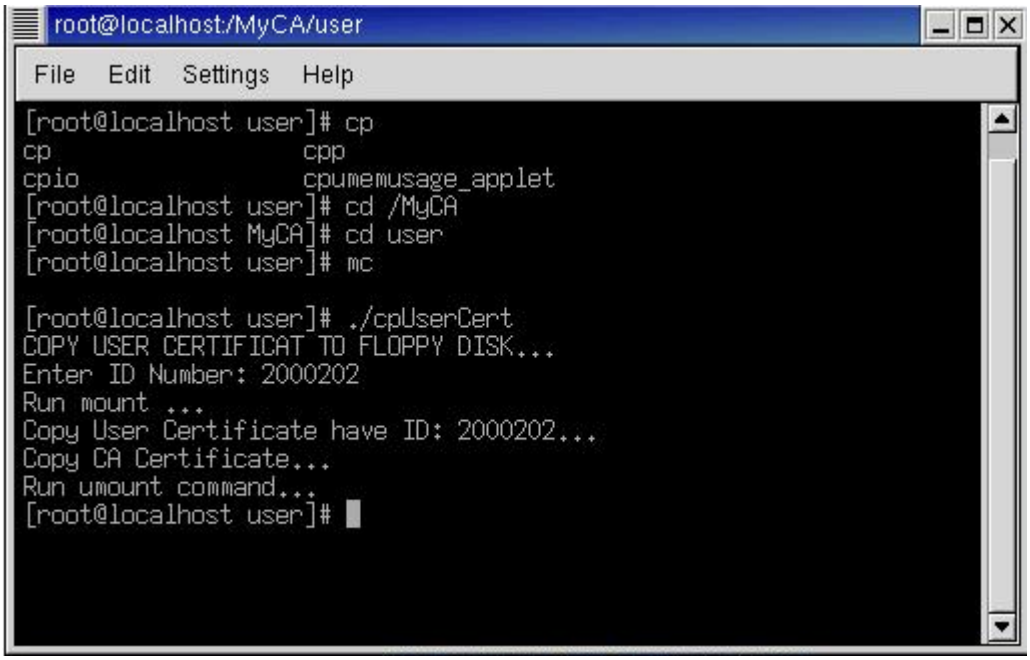
Hình 15

Người thực hiện nhập số PIN của người sử dụng cần copy chứng chỉ số như hình 16.



Hình 16

Quá trình copy chứng chỉ số của người sử dụng và chứng chỉ của CA lên đĩa mềm được thực hiện và thông báo như trên hình 17.



Hình 17

Quá trình cấp chứng chỉ số kết thúc. Người sử dụng được cấp một đĩa mềm trên đó có chứng chỉ số của họ dưới định dạng PKCS12 và chứng chỉ của CA. Người sử dụng sẽ thực hiện cài đặt các chứng chỉ này cho ứng dụng Mail.

5- Bước 5: Cập nhật chứng chỉ vừa phát hành lên LDAP server

Để thực hiện, người quản trị chọn chức năng "Export Certificates to LDAP server", khi đó trên màn hình xuất hiện thông báo như hình 18.

Hình 18

Ngoài các chức năng trên, trên giao diện chính còn hai chức năng nữa nhưng đây chỉ là các chức năng phụ không cần quan tâm.

-Chức năng "Pending Requests List": hiển thị các yêu cầu chưa được ký. Khi chọn chức năng này trên màn hình xuất hiện danh sách các request chưa được ký như hình 19.

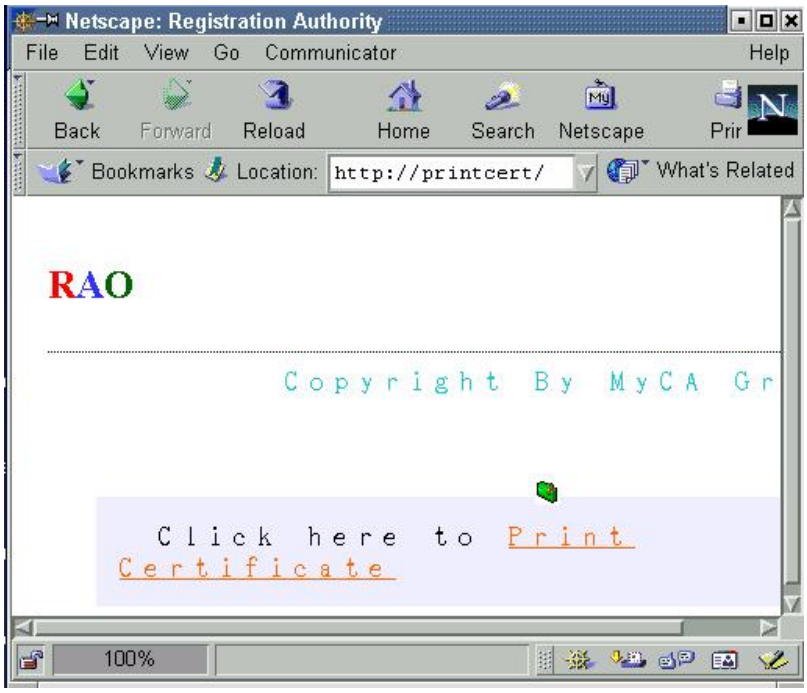
Hình 19

-Chức năng "Issue Certificate": hiển thị danh sách các chứng chỉ đã cấp như hình 20

Hình 20

6- Bước 6: In nội dung chứng chỉ

Sử dụng trang http://printcert khi đó trên màn hình Netscape xuất hiện giao diện như hình 21.

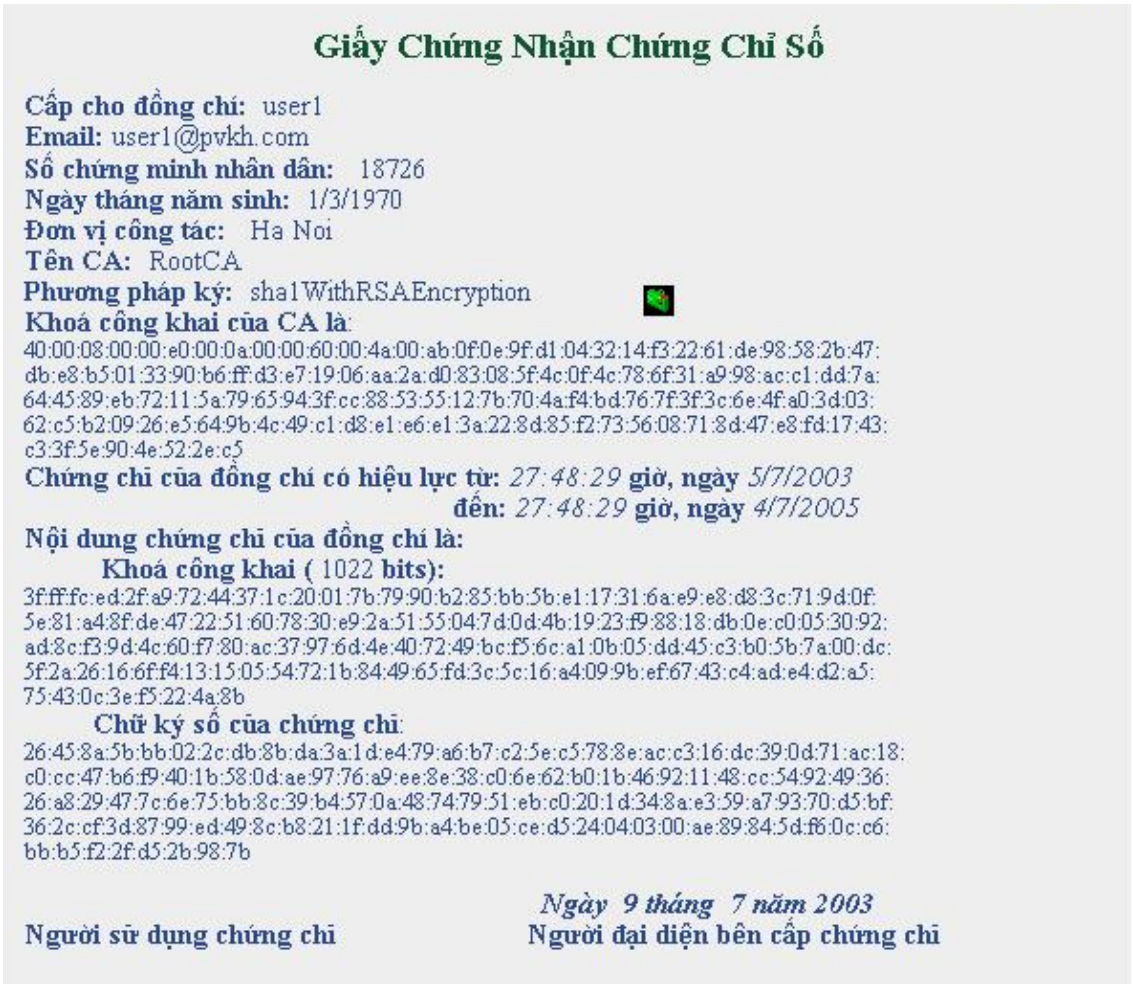


Hình 21

Nhấp chuột vào "Print Certificate", trên màn hình xuất hiện form như hình 22.

Hình 22

Người thực hiện gõ số PIN của chứng chỉ cần in, rồi nhấn "Continue...", trên màn hình xuất hiện nội dung cần in như hình 23.



Giấy Chứng Nhận Chứng Chỉ Số

Cấp cho đồng chí: user1
Email: user1@pvkh.com
Số chứng minh nhân dân: 18726
Ngày tháng năm sinh: 1/3/1970
Đơn vị công tác: Ha Noi
Tên CA: RootCA
Phương pháp ký: sha1WithRSAEncryption
Khoá công khai của CA là:
40:00:08:00:00:e0:00:0a:00:00:60:00:4a:00:ab:0f:0e:9f:d1:04:32:14:f3:22:61:de:98:58:2b:47:
db:e8:b5:01:33:90:b6:ff:d3:e7:19:06:aa:2a:d0:83:08:5f:4c:0f:4c:78:6f:31:a9:98:ac:c1:dd:7a:
64:45:89:eb:72:11:5a:79:65:94:3f:cc:88:53:55:12:7b:70:4a:f4:bd:76:7f:3f:3c:6e:4f:a0:3d:03:
62:c5:b2:09:26:e5:64:9b:4c:49:c1:d8:e1:e6:e1:3a:22:8d:85:f2:73:56:08:71:8d:47:e8:fd:17:43:
c3:3f:5e:90:4e:52:2e:c5
Chứng chỉ của đồng chí có hiệu lực từ: *27:48:29* **giờ, ngày** *5/7/2003*
đến: *27:48:29* **giờ, ngày** *4/7/2005*
Nội dung chứng chỉ của đồng chí là:
Khoá công khai (1022 **bits):**
3f:ff:fc:ed:2f:a9:72:44:37:1c:20:01:7b:79:90:b2:85:bb:5b:e1:17:31:6a:e9:e8:d8:3c:71:9d:0f:
5e:81:a4:8f:de:47:22:51:60:78:30:e9:2a:51:55:04:7d:0d:4b:19:23:f9:88:18:db:0e:c0:05:30:92:
ad:8c:f3:9d:4c:60:f7:80:ac:37:97:6d:4e:40:72:49:bc:f5:6c:a1:0b:05:dd:45:c3:b0:5b:7a:00:dc:
5f:2a:26:16:6f:f4:13:15:05:54:72:1b:84:49:65:fd:3c:5c:16:a4:09:9b:ef:67:43:c4:ad:e4:d2:a5:
75:43:0c:3e:f5:22:4a:8b
Chữ ký số của chứng chỉ:
26:45:8a:5b:bb:02:2c:db:8b:da:3a:1d:e4:79:a6:b7:c2:5e:c5:78:8e:ac:c3:16:dc:39:0d:71:ac:18:
c0:cc:47:b6:f9:40:1b:58:0d:ae:97:76:a9:ee:8e:38:c0:6e:62:b0:1b:46:92:11:48:cc:54:92:49:36:
26:a8:29:47:7c:6e:75:bb:8c:39:b4:57:0a:48:74:79:51:eb:c0:20:1d:34:8a:e3:59:a7:93:70:d5:bf:
36:2c:cf:3d:87:99:ed:49:8c:b8:21:1f:dd:9b:a4:be:05:ce:d5:24:04:03:00:ae:89:84:5d:f6:0c:c6:
bb:b5:f2:2f:d5:2b:98:7b

Ngày 9 tháng 7 năm 2003
Người sử dụng chứng chỉ **Người đại diện bên cấp chứng chỉ**

Hình 23

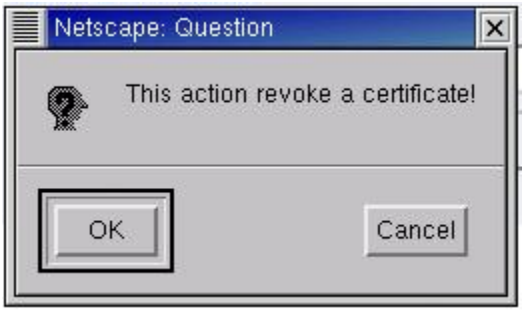
Vào menu File của trình duyệt Netscape, chọn chức năng Print để in nội dung của chứng chỉ cấp cho người sử dụng.

Chương IV
QUI TRÌNH HUỶ BỎ CHỨNG CHỈ SỐ

1-Qui trình huỷ bỏ chứng chỉ
1.1-Huỷ bỏ một chứng chỉ
Chọn chức năng "Revoke a certificate by Administrator" trên giao diện chính của CA, khi đó trên màn hình xuất hiện giao diện như hình 1.

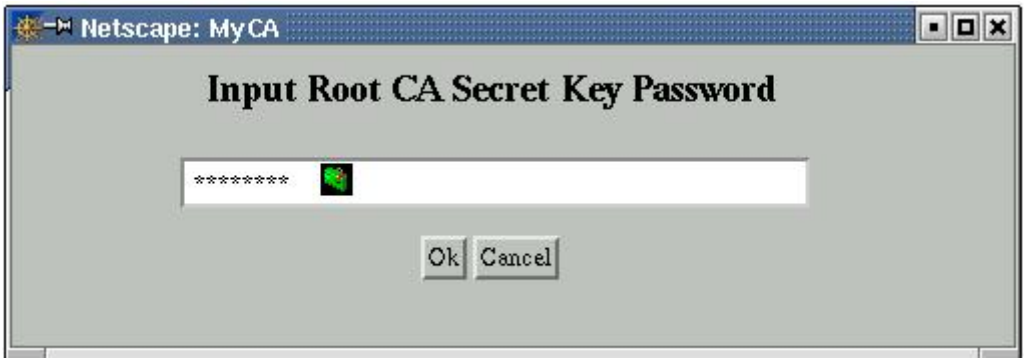
Hình 1

Người quản trị thực hiện gõ ID của chứng chỉ cần huỷ bỏ vào mục "Input ID", rồi chọn "Continue". Trên màn hình xuất hiện hộp hội thoại như hình 2



Hình 2

Người quản trị chọn "OK", trên màn hình xuất hiện hộp hội thoại như hình 3



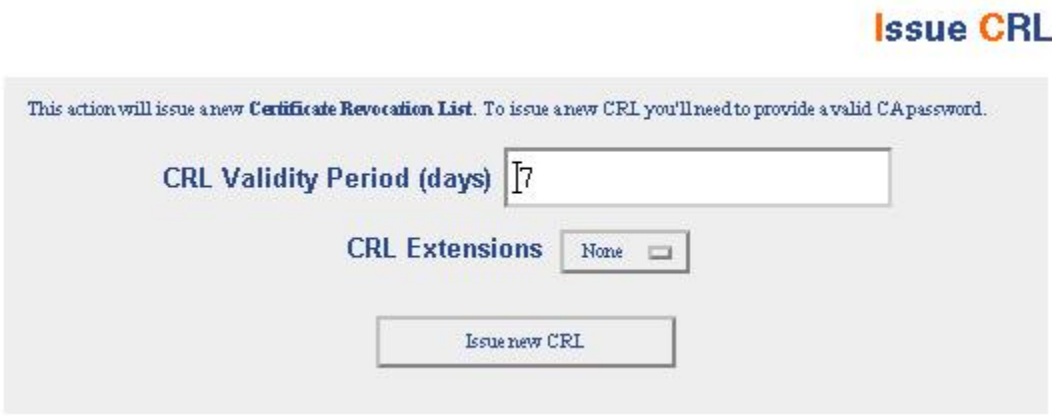
Hình 3

Người quản trị nhập mật khẩu được sử dụng để làm khoá giải mã khoá bí mật của CA, sau đó chọn "OK", quá trình huỷ bỏ chứng chỉ có ID được nhập ở trên được thực hiện.

Hình 4

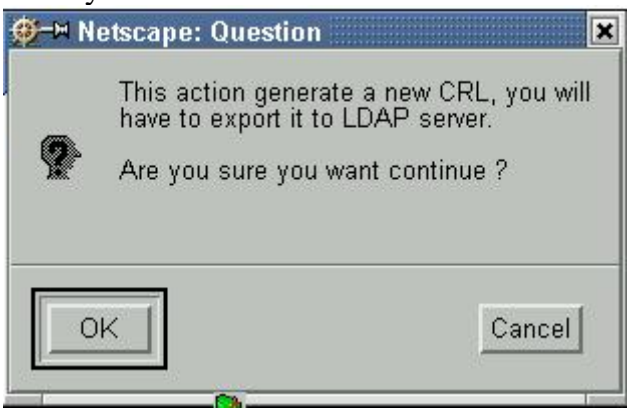
1.2-Phát hành CRL và cập nhật lên LDAP

Trên máy CA người quản trị chọn mục **Issue New CRL**, xuất hiện hộp thoại như hình 5.



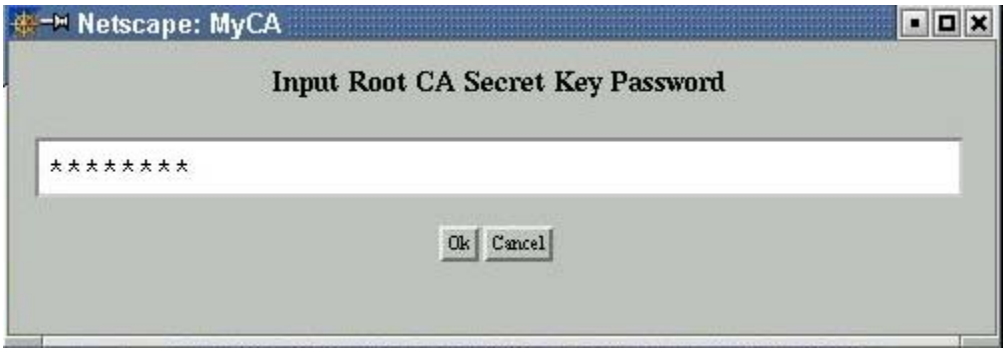
Hình 5

Ngầm định hiệu lực của danh sách các chứng chỉ huỷ bỏ sẽ là 7 ngày (có thể thay đổi), chọn **Issue new CRL**, xuất hiện cảnh báo bạn sẽ phải đưa danh sách này công khai trên toàn hệ thống CA, tức là đưa ra máy LDAP server sau khi phát hành, như hình 6 dưới đây.



Hình 6

Chọn **OK** để tiếp tục, xuất hiện hộp thoại như hình 7 yêu cầu vào mật khẩu của CA:

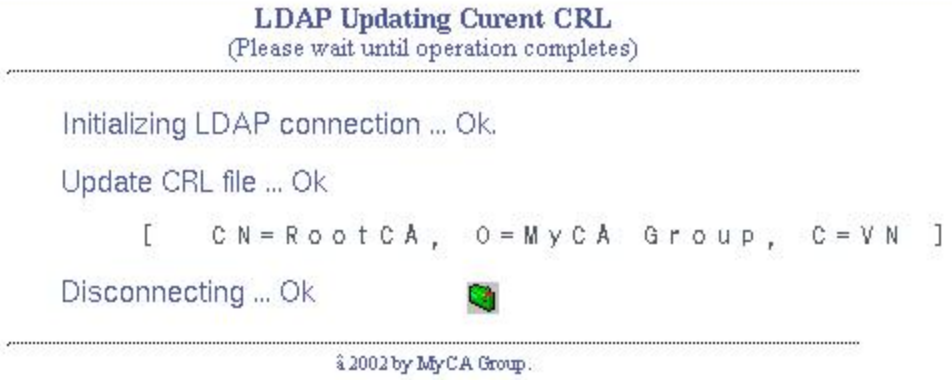


Hình 7

Chọn **OK**, để thực hiện công việc phát hành danh sách các chứng chỉ huỷ bỏ như hình 8 dưới đây.

Hình 8

Công việc cuối cùng mà người quản trị CA phải thực hiện đó là đưa danh sách này công khai trên toàn hệ thống, chọn mục **Update current CRL to LDAP server**, nếu thành công sẽ xuất hiện thông báo như hình 9 dưới đây.



Hình 9

Sau bước này thì chứng chỉ của các người sử dụng có yêu cầu huỷ bỏ đã được phát hành và đưa lên LDAP Server. Tất cả các máy trên hệ thống CA phải cập nhật danh sách này vào hệ thống của mình thông qua trang **publicdatabase** đặt trên máy LDAP (việc cập nhật CRL cho người sử dụng trên các môi trường làm việc khác nhau chúng tôi đã trình bày trong chương 2).

2-Cấp chứng nhận huỷ bỏ chứng chỉ cho người sử dụng

2.1-Tải CRL từ LDAP server về máy CA

Để tải CRL hiện tại từ LDAP server, phục vụ cho việc in chứng nhận huỷ bỏ, người quản trị trên máy Ca thực hiện:

Trong tệp /etc/hosts bổ sung dòng:

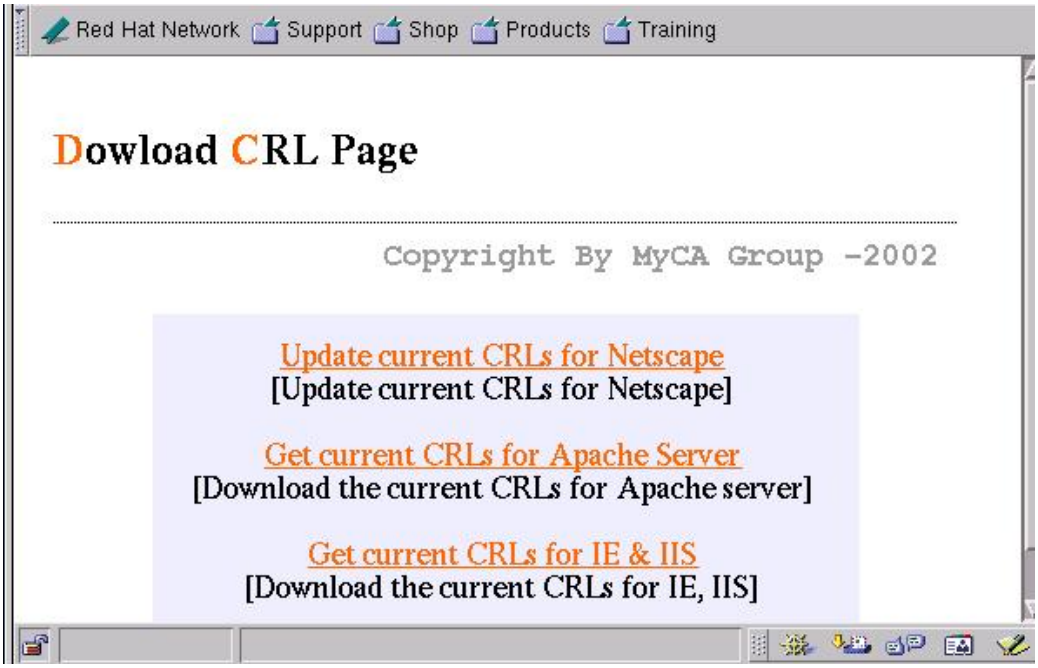
200.1.1.1 publicdatabase

(Trong đó địa chỉ IP 200.1.1.1 là địa chỉ của máy LDAP server)

Mở trang http://publicdatabase, giao diện trang này xuất hiện như hình 10

Hình 10

Sử dụng chức năng "Update CRLs", trên màn hình xuất hiện giao diện như hình 11



Hình 11

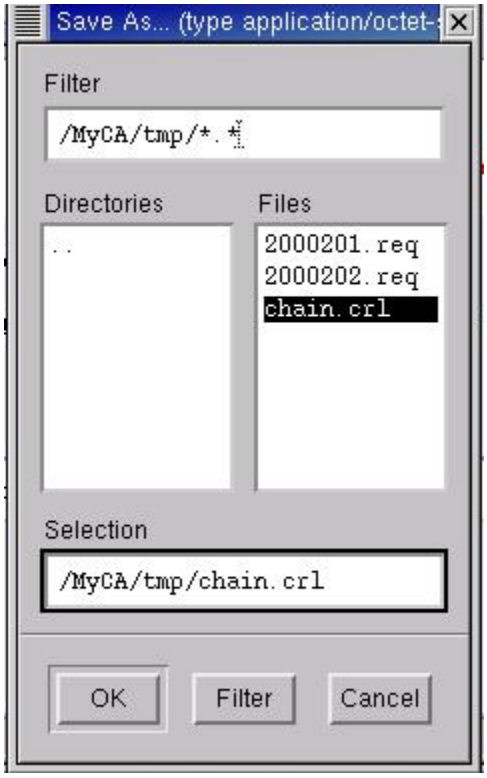
Chọn "Get Current CRLs for Apache Server", trên màn hình xuất hiện giao diện như hình 12

Hình 12

Người quản trị gõ tên của CA vào mục "CA's Common Name", rồi chọn "Continue...", trên màn hình xuất hiện hộp hội thoại như hình 13

Hình 13

Người quản trị chọn "Continue Submission", trên màn hình xuất hiện hộp hội thoại như hình 14

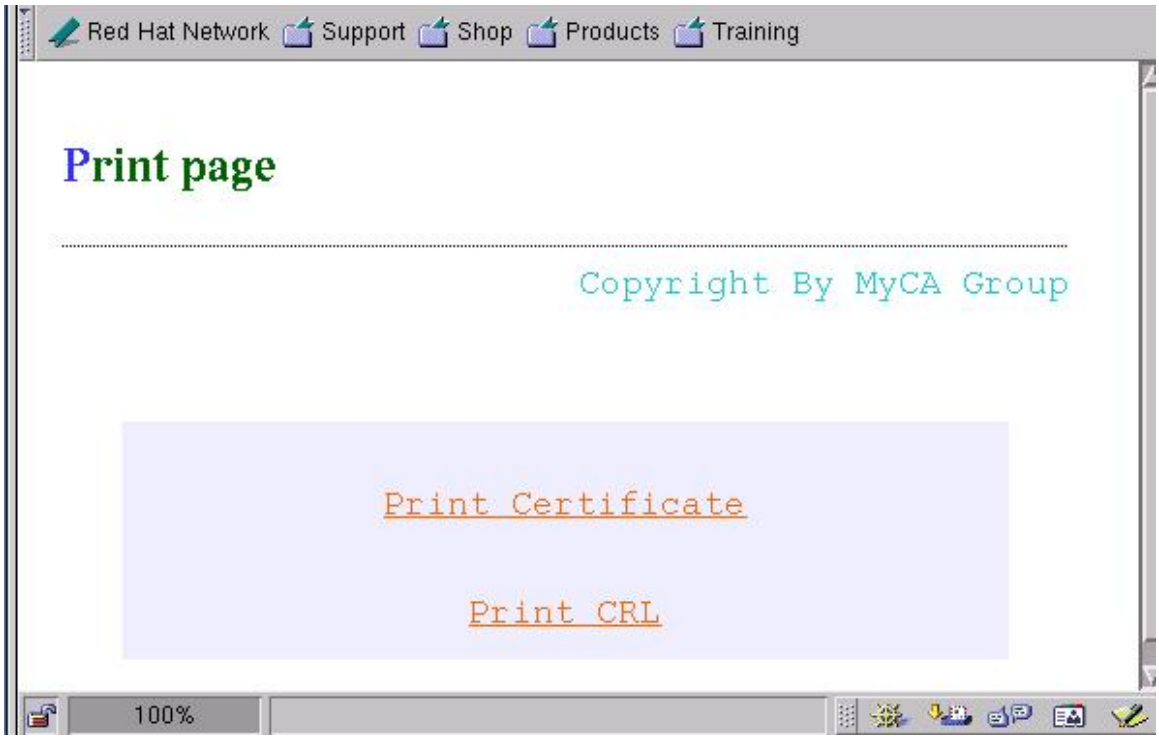


Hình 14

Người quản trị chọn nơi lưu tệp CRL được tải về theo đường dẫn /MyCA/tmp/chain.crl và chọn OK.
Quá trình tải tệp CRL kết thúc,

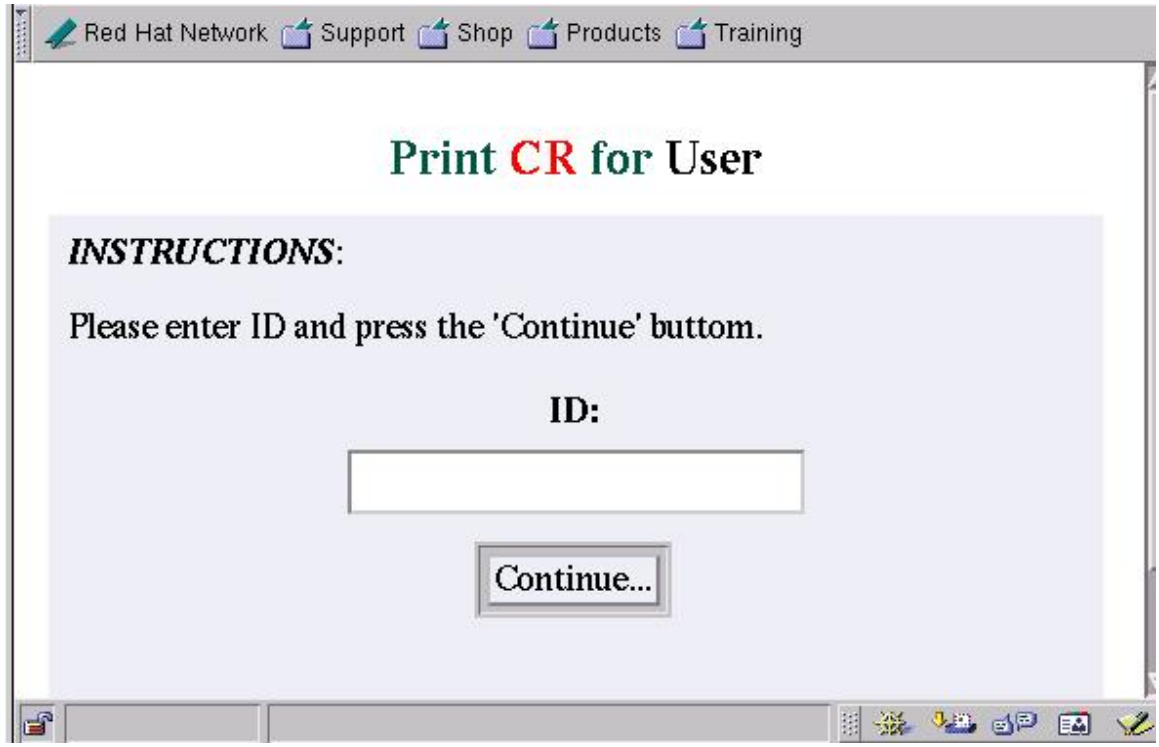
2.2-In chứng nhận huỷ bỏ cho người sử dụng

Để thực hiện việc in chứng nhận chứng chỉ số của một người sử dụng nàô đấy đã bị huỷ bỏ, người quản trị thực hiện các bước dưới đây:
Mở trang http://printcert, trên màn hình xuất hiện hộp hội thoại như hình 15



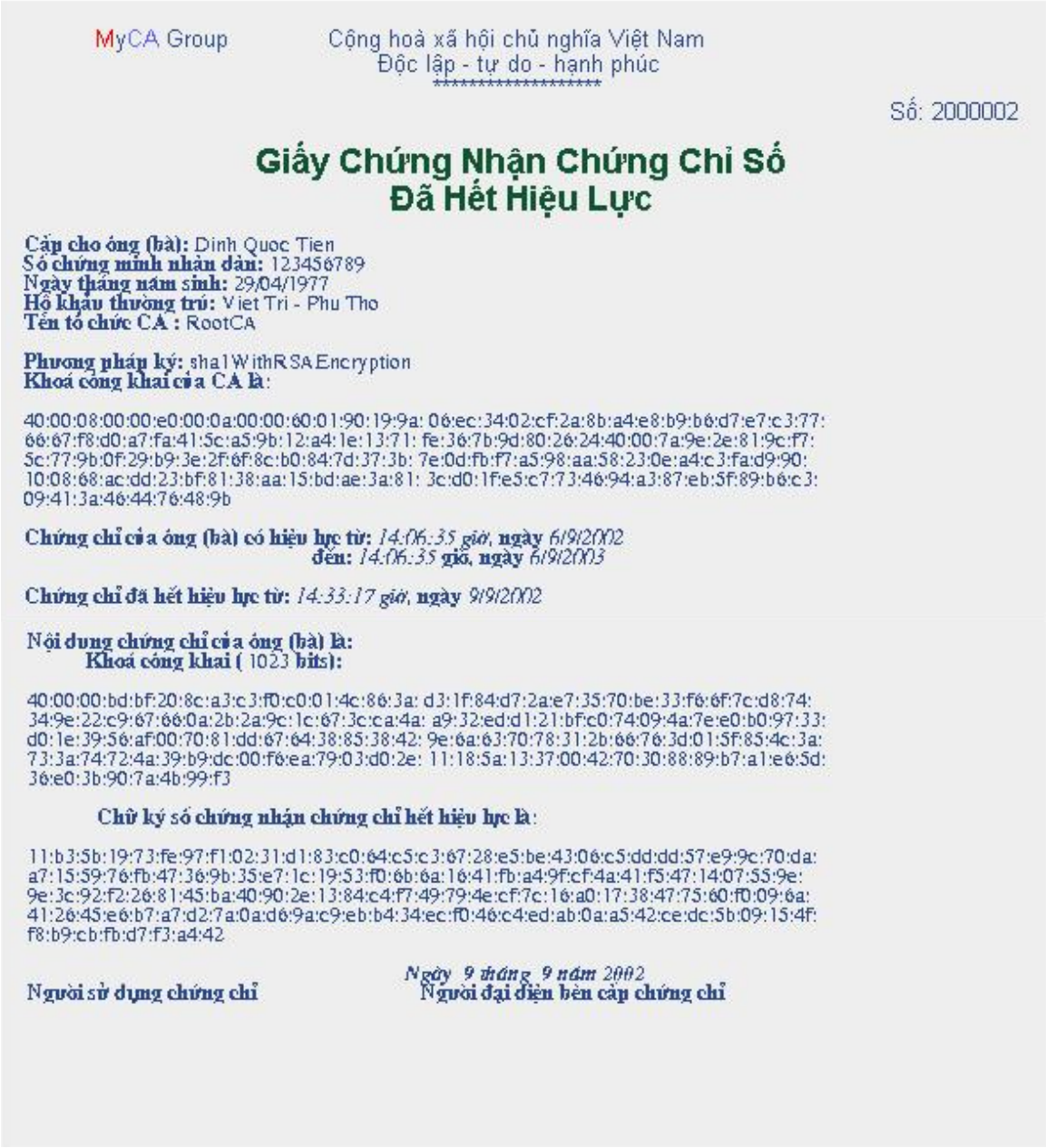
Hình 15

Người quản trị chọn chức năng "Print CRL", trên màn hình xuất hiện giao diện như hình 16.



Hình 16

Người quản trị nhập số ID của chứng chỉ đã bị huỷ bỏ vào mục "ID" rồi chọn "Continue", trên màn hình xuất hiện form hiển thị nội dung giấy chứng nhận huỷ bỏ chứng chỉ như hình 17.



MyCA Group

Cộng hoà xã hội chủ nghĩa Việt Nam
Độc lập - tự do - hạnh phúc
****

Số: 2000002

Giấy Chứng Nhận Chứng Chỉ Số Đã Hết Hiệu Lực

Cấp cho ông (bà): Dinh Quoc Tien
Số chứng minh nhân dân: 123456789
Ngày tháng năm sinh: 29/04/1977
Hộ khẩu thường trú: Viet Tri - Phu Tho
Tên tổ chức CA : RootCA

Phương pháp ký: sha1WithRSAEncryption
Khoá công khai của CA là:

40:00:08:00:00:e0:00:0a:00:00:60:01:90:19:9a: 06:ec:34:02:cf:2a:8b:a4:e8:b9:b6:d7:e7:c3:77:
66:67:f8:d0:a7:fa:41:5c:a5:9b:12:a4:1e:13:71: fe:36:7b:9d:80:26:24:40:00:7a:9e:2e:81:9c:f7:
5c:77:9b:0f:29:b9:3e:2f:6f:8c:b0:84:7d:37:3b: 7e:0d:fb:f7:a5:98:aa:58:23:0e:a4:c3:fa:d9:90:
10:08:68:ac:dd:23:bf:81:38:aa:15:bd:ae:3a:81: 3c:d0:1f:e5:c7:73:46:94:a3:87:eb:5f:89:b6:c3:
09:41:3a:46:44:76:48:9b

Chứng chỉ của ông (bà) có hiệu lực từ: *14:06:35 giờ*, **ngày** *6/9/2002*
đến: *14:06:35* **giờ, ngày** *6/9/2003*

Chứng chỉ đã hết hiệu lực từ: *14:33:17 giờ*, **ngày** *9/9/2002*

Nội dung chứng chỉ của ông (bà) là:
Khoá công khai (1023 bits):

40:00:00:bd:bf:20:8c:a3:c3:f0:c0:01:4c:86:3a: d3:1f:84:d7:2a:e7:35:70:be:33:f6:6f:7c:d8:74:
34:9e:22:c9:67:66:0a:2b:2a:9c:1c:67:3c:ca:4a: a9:32:ed:d1:21:bf:c0:74:09:4a:7e:e0:b0:97:33:
d0:1e:39:56:af:00:70:81:dd:67:64:38:85:38:42: 9e:6a:63:70:78:31:2b:66:76:3d:01:5f:85:4c:3a:
73:3a:74:72:4a:39:b9:dc:00:f6:ea:79:03:d0:2e: 11:18:5a:13:37:00:42:70:30:88:89:b7:a1:e6:5d:
36:e0:3b:90:7a:4b:99:f3

Chữ ký số chứng nhận chứng chỉ hết hiệu lực là:

11:b3:5b:19:73:fe:97:f1:02:31:d1:83:c0:64:c5:c3:67:28:e5:be:43:06:c5:dd:dd:57:e9:9c:70:da:
a7:15:59:76:fb:47:36:9b:35:e7:1c:19:53:f0:6b:6a:16:41:fb:a4:9f:cf:4a:41:f5:47:14:07:55:9e:
9e:3c:92:f2:26:81:45:ba:40:90:2e:13:84:c4:f7:49:79:4e:cf:7c:16:a0:17:38:47:75:60:f0:09:6a:
41:26:45:e6:b7:a7:d2:7a:0a:d6:9a:c9:eb:b4:34:ec:f0:46:c4:ed:ab:0a:a5:42:ce:dc:5b:09:15:4f:
f8:b9:cb:fb:d7:f3:a4:42

Ngày 9 tháng 9 năm 2002

Người sử dụng chứng chỉ **Người đại diện bên cấp chứng chỉ**

Hình 17

Văn bản trên được in ra ít nhất là 2 bản, người sử dụngr và người đại diện xác nhận phải thực hiện ký vào biên bản đó. Đến đây kết thúc việc huỷ bỏ một chứng chỉ (người sử dụng hết trách nhiệm đối với chứng chỉ đó).