BAN CƠ YẾU CHÍNH PHỦ

BÁO CÁO ĐỀ TÀI NHÁNH

"NGHIÊN CỨU, XÂY DỰNG GIẢI PHÁP BẢO MẬT THÔNG TIN TRONG THƯƠNG MẠI ĐIỆN TỬ"

SẢN PHẨM SỐ 1: HỆ THỐNG CẤP PHÁT VÀ QUẢN LÝ CHỨNG CHỈ SỐ

Thuộc đề tài : "Nghiên cứu một số vấn đề kỹ thuật, công nghệ chủ yếu trong thương mại điện tử và triển khai thử nghiệm – Mã số KC.01.05"

6095-2

14/9/2006

Hà nội, tháng 9 năm 2004

Trong phần này chúng tôi sẽ giới thiệu sản phẩm hệ thống CA thử nghiệm tại Tổng cục thuế của đề tài ở dạng các mẫu thử sử dụng mục tiêu an toàn trong thương mại điện tử. Ứng ứng dụng này được phát triển trên cơ sở lý thuyết đã được trình bầy trong phần lý thuyết chung. Vì đây chỉ là những mẫu thử, nên khi áp dụng vào thực tế cần có những thay đổi về tham số để đảm bảo sự an toàn khi sử dụng. Tuỳ theo nhu cầu cụ thể mà chúng ta sẽ sử dụng những tham số phù hợp trong ứng dụng này.

NỘI DUNG

Mục tiêu 2
I. Mô hình hoạt động 3
II. Chu trình cấp phát chứng chỉ 4
A. Tổ chức cấp phát chứng chỉ tại các cục thuế 5
1. Khởi động chương trình 5
2. Đăng ký chứng chỉ 3
3. Ký nhận và gửi yêu cầu 6
4. Nhận yêu cầu chứng chỉ 7
5. Xuất yêu cầu chứng chỉ 9
6. Nhập các yêu cầu chứng chỉ 9
7. Xem, duyệt các yêu cầu chứng chỉ 10
8. Tạo chứng chỉ 11
9. Xuất chứng chỉ 12
10. Đưa chứng chỉ vào LDAP 12
11. Đưa chứng chỉ và RAServer 13
12. Chuyển chứng chỉ vào các vùng Client 14
13. Nhận chứng chỉ Vũ 15
14. Xuất chứng chỉ cho người dùng 16
15. Sửa đổi chứng chỉ 18
16. Quy trình cấp lại chứng chỉ 20
17. Quy trình huỷ bỏ chứng chỉ 22
B. Tổ chức cấp phát chứng chỉ tại Tổng cục thuế 24
C. Cài đặt chứng chỉ cho một trang Web 33

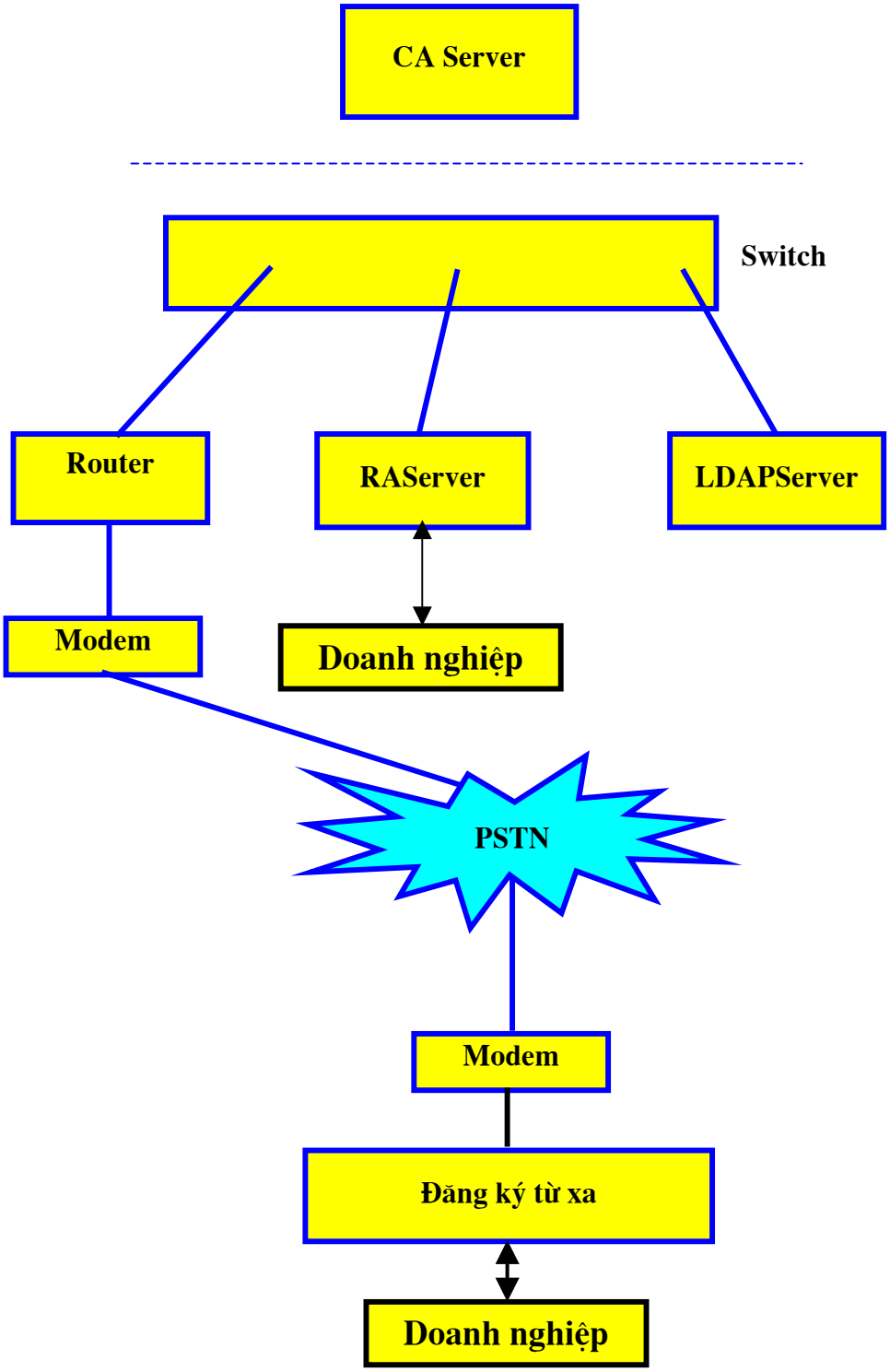
HỆ THỐNG CA THỬ NGHIỆM TẠI TỔNG CỤC THUẾ

Mục tiêu: Cung cấp cho tổng cục thuế một hệ thống quản lý và cấp phát chứng chỉ điện tử theo chuẩn X509 v3 phục vụ cho việc thử nghiệm kê khai thuế của các doanh nghiệp qua mạng.

MÔ HÌNH QUẢN LÝ VÀ CẤP PHÁT CHỨNG CHỈ

I. MÔ HÌNH HOẠT ĐỘNG

Hệ thống CA hoạt động theo mô hình sau:



Trong đó:

CAServer là thành phần quan trọng nhất trong hệ thống. Nó được cài đặt phần mềm CA và lưu giữ khoá riêng của CA. Chính vì vậy, cần phải đảm bảo an toàn tuyệt đối cho CAServer.

RAServer cài đặt chương trình quản lý các đăng ký và các chứng chỉ. RAServer thực hiện kiểm tra các yêu cầu đăng ký chứng chỉ, chấp nhận hoặc huỷ bỏ các yêu cầu đăng ký chứng chỉ trước khi chúng được CA ký, đồng thời gửi chứng chỉ đã được CA phát hành xuống các điểm đăng ký từ xa để chuyển cho doanh nghiệp, hoặc cũng có thể chuyển trực tiếp cho doanh nghiệp.

LDAP Server là một máy chủ chứa tất cả các chứng chỉ đã được phát hành, cho phép các doanh nghiệp sử dụng dịch vụ thư mục để tra cứu thông tin về các chứng chỉ.

Điểm đăng ký từ xa có nhiệm vụ kiểm tra thông tin đăng ký (chẳng hạn như xin cấp mới, huỷ bỏ, hoặc cấp lại chứng chỉ) của doanh nghiệp và ký xác nhận trước khi chuyển cho RAServer. Tất cả quá trình truyền thông giữa RAServer và điểm đăng ký từ xa được thực hiện thông qua những phiên liên lạc an toàn.

* Để thiết lập mạng cấp phát chứng chỉ, các điểm đặng ký từ xa được thiết lập trước và được cấp chứng chỉ trong quá trình thiết lập mạng cấp phát. Khoá công khai của CA và khoá riêng của các điểm đăng ký từ xa được CA cấp theo một kênh an toàn.

II. CHU TRÌNH CẤP PHÁT CHỨNG CHỈ

Khi một doanh nghiệp muốn đăng ký một chứng chỉ, doanh nghiệp đến gặp người quản trị tại điểm đăng ký từ xa hoặc người quản trị RAServer, đưa ra yêu cầu và điền các thông tin cần thiết chẳng hạn tên, số chứng minh thư, địa chỉ thư điện tử, kích thước khoá yêu cầu, ... theo một mẫu đăng ký. Khi xác minh thông tin, nếu thông tin không chính xác người quản trị yêu cầu doanh nghiệp điền lại, ngược lại nếu thông tin chính xác, yêu cầu sẽ được nhập vào cơ sở dữ liệu để quản lý, đồng thời chuyển cho RAServer. Sau khi nhận và kiểm tra yêu cầu, người quản trị trên RAServer sẽ chuyển yêu cầu cho CAServer theo một kênh an toàn.

Tại CAServer, các yêu cầu về chứng chỉ được nhập vào. Nếu thông tin đăng ký là hợp lệ, CAServer sẽ sinh cặp khoá và tạo chứng chỉ cho doanh nghiệp với khoá công khai vừa tạo. Các chứng chỉ được CAServer chuyển cho RAServer theo một kênh an toàn. RAServer sẽ chuyển chứng chỉ cho doanh nghiệp, đồng thời cũng chuyển chúng vào LDAP Server để các doanh nghiệp khác có thể tra cứu.

Chứng chỉ, khoá riêng của doanh nghiệp và khoá công khai của CA được RAServer chuyển trực tiếp cho doanh nghiệp, hoặc chuyển cho điểm đăng ký từ xa (nơi doanh nghiệp đến đăng ký) thông qua phiên liên lạc an toàn, sau đó doanh nghiệp đến điểm đăng ký từ xa để nhận trực tiếp. Doanh nghiệp có thể lưu chứng chỉ trong máy tính của mình và lưu khoá riêng trong các thiết bị ngoài an toàn (chẳng hạn như smart card, đĩa mềm ...).

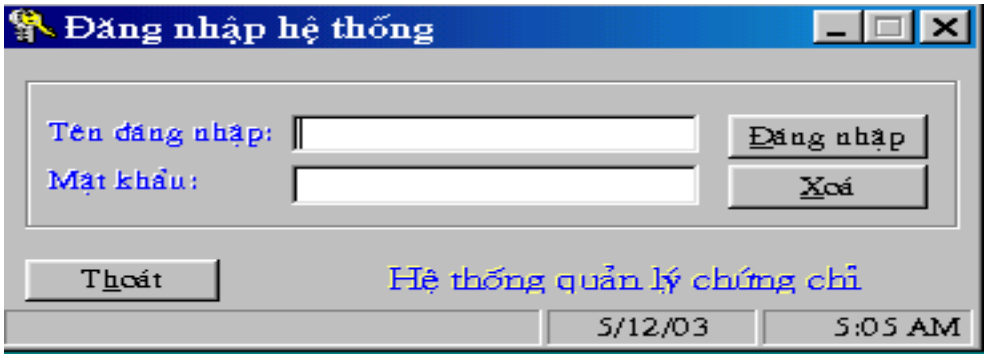
A. TỔ CHỨC CẤP PHÁT CHỨNG CHỈ TẠI CÁC CỤC THUẾ

QUI TRÌNH CẤP PHÁT CHỨNG CHỈ

1. KHỞI ĐỘNG CHƯƠNG TRÌNH

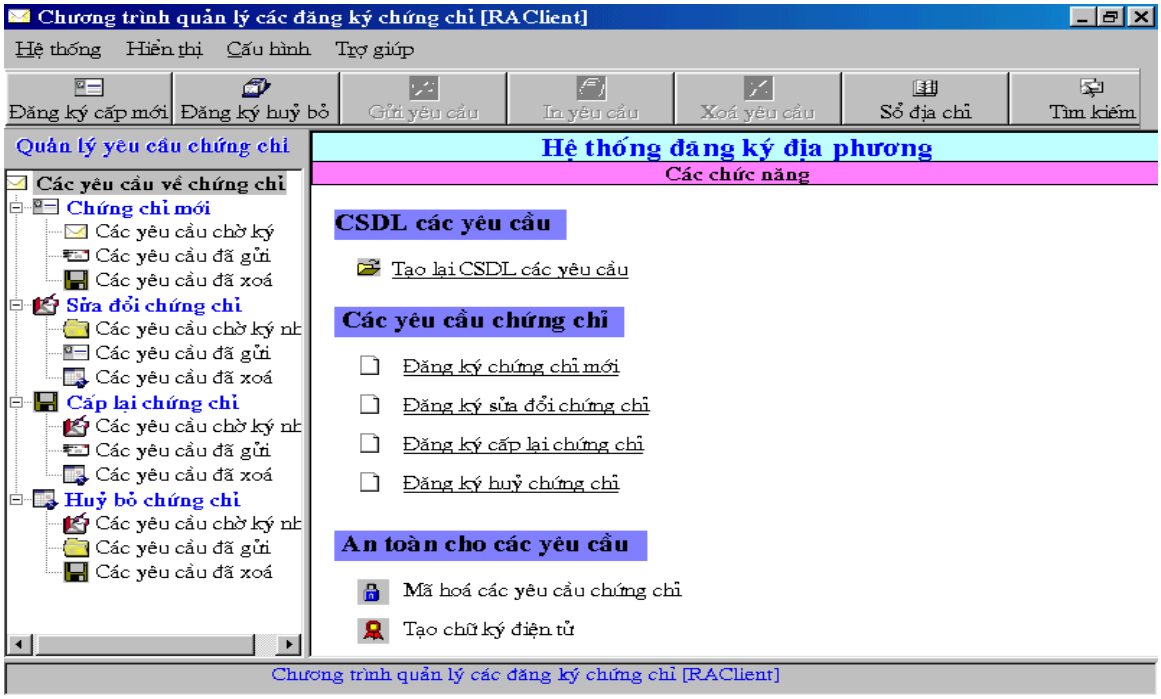
Điểm đăng ký địa phương chạy chương trình đăng ký chứng chỉ (RAClient) bằng cách vào **Start-> Program -> KC01-05 RAClient -> Đăng ký chứng chỉ**.

Mỗi lần chạy, chương trình đều yêu cầu nhập mật khẩu đăng nhập.



Hình 1: Màn hình đăng nhập hệ thống

user name và mật khẩu mặc định là **"admin"**. Sau đó người quản trị hệ thống có thể cấu hình lại để thay đổi.

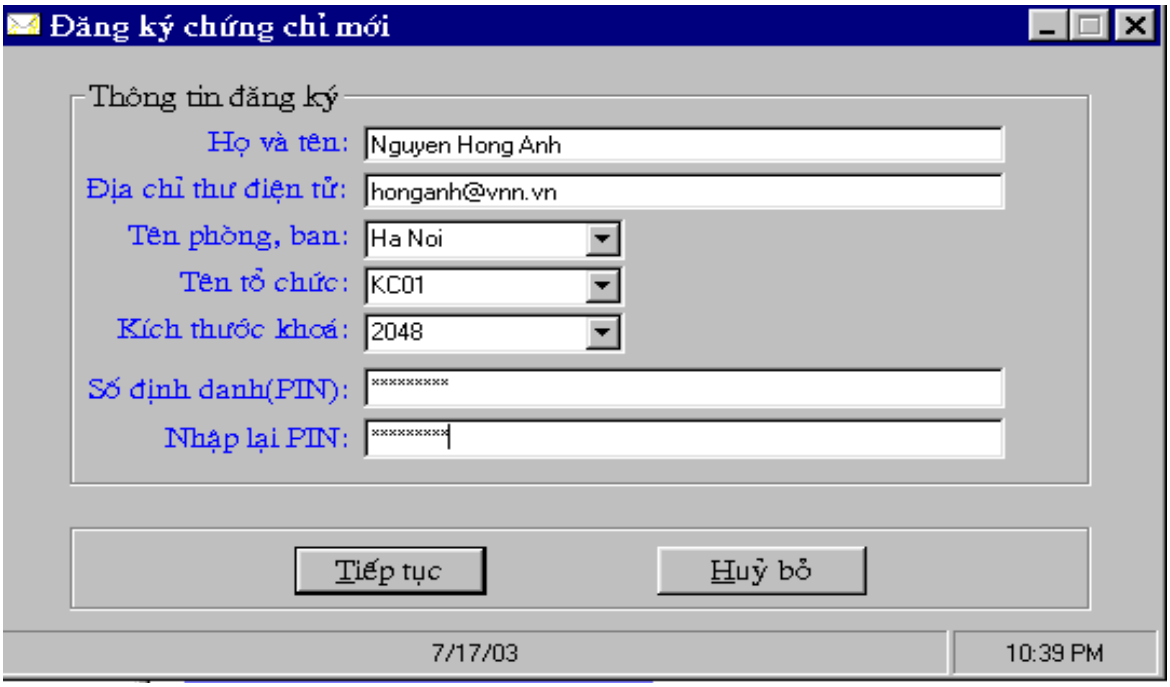


Hình 2: Chương trình quản lý đăng ký tại RAClient

2. ĐĂNG KÝ CHỨNG CHỈ

Trình tự đăng ký và cấp phát chứng chỉ cho người dùng được thực hiện như sau:

Người dùng đến gặp người quản trị tại điểm đăng ký địa phương xin đăng ký chứng chỉ và điền các thông tin cần thiết vào mẫu đăng ký. Sau khi người dùng đăng ký chứng chỉ và điền các thông tin cần thiết, người quản trị tại điểm đăng ký địa phương xác minh lại các thông tin. Nếu thông tin nào chưa chính xác thì yêu cầu người dùng đăng ký lại, nếu các thông tin là chính xác thì vào chương trình quản lý các đăng ký dành cho các RAClient, chọn mục **"Đăng ký chứng chỉ mới"** và điền các thông tin của người dùng vào Form đăng ký rồi chọn **"Tiếp tục"**



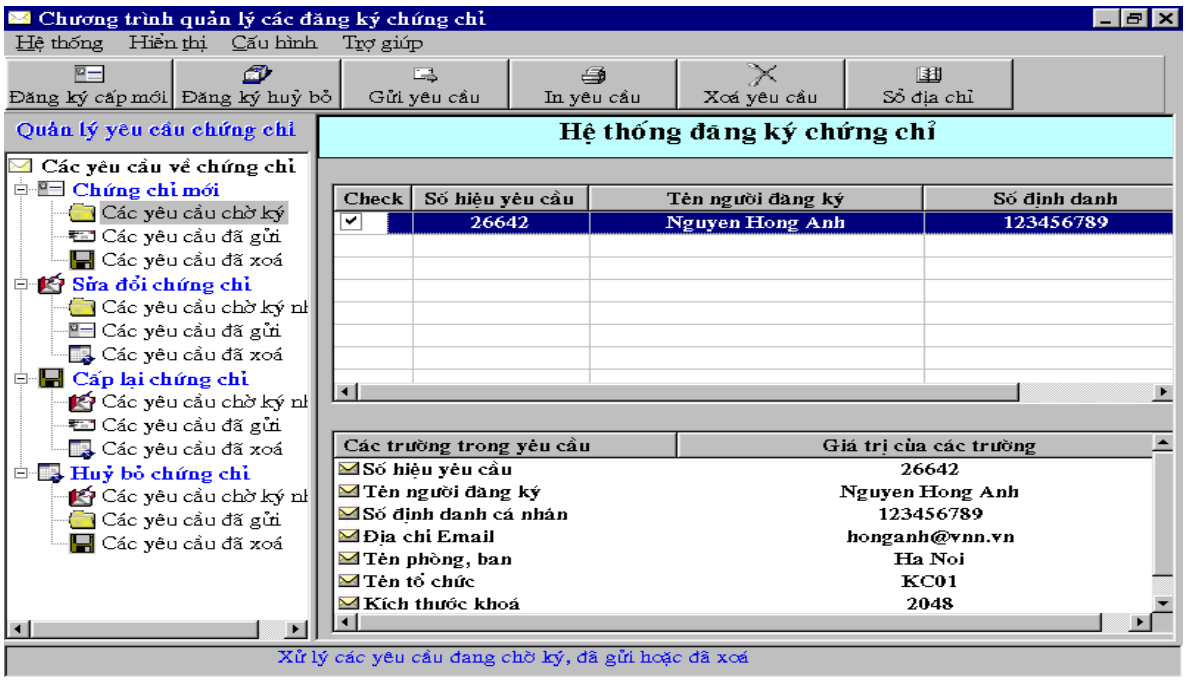
Hình 3: Màn hình nhập thông tin đăng ký chứng chỉ mới

Người quản trị kiểm tra lại các thông tin đã nhập, nếu chưa đúng thì chọn **"Huỷ bỏ"** để về Form nhập dữ liệu ban đầu sửa đổi lại, nếu đúng thì chọn **"Chấp nhận"** để đưa yêu cầu vào CSDL chờ ký nhận và gửi đi.

Hình 4: Màn hình xác nhận lại thông tin đăng ký đã nhập

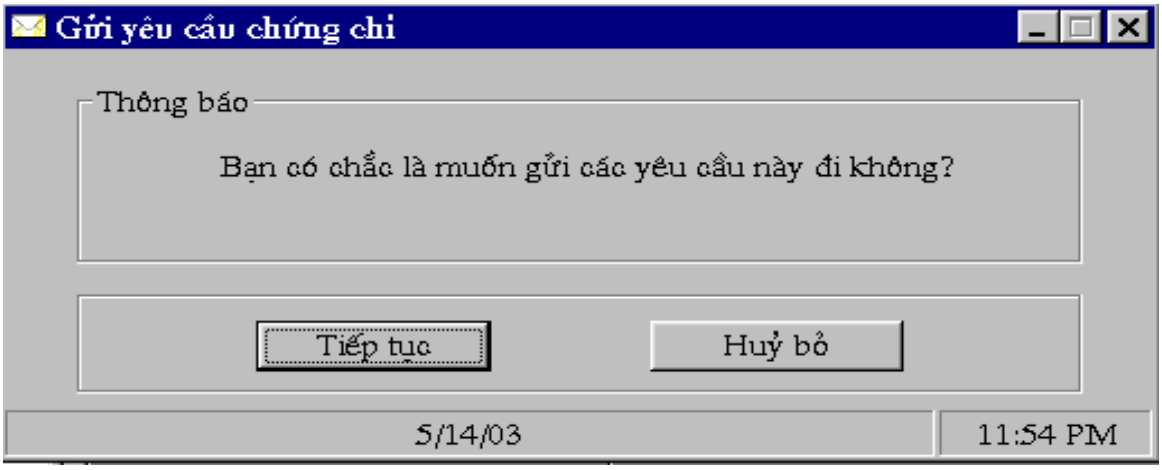
3. KÝ NHẬN VÀ GỬI YÊU CẦU

Để yêu cầu có thể chuyển sang CA ký tạo chứng chỉ thì trước đó yêu cầu phải được ký nhận bởi các RAClient Cục thuế và gửi lên RAServer Tổng cục. Người quản trị tại RAClient Cục thuế thực hiện việc này bằng cách chọn mục **"Các yêu cầu chờ ký"** trong phần **"Chứng chỉ mới"** để xem danh sách các yêu cầu cấp chứng chỉ đang chờ ký nhận, chọn các yêu cầu sẽ ký nhận để gửi đi.



Hình 5: RAClient xem và chọn các yêu cầu để gửi đi

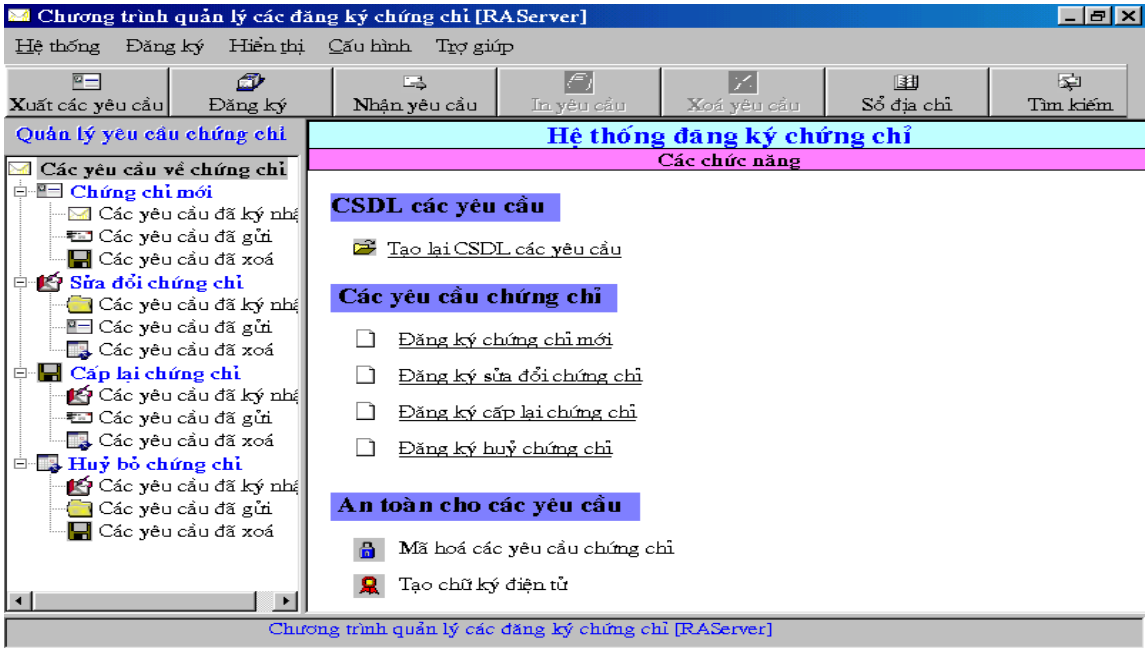
Sau khi chọn các yêu cầu, RAClient chọn chức năng **"Gửi yêu cầu"** trên thanh công cụ và chọn nút **"Tiếp tục"** để xác nhận việc gửi các yêu cầu. Khi đó các yêu cầu được chọn sẽ được mã hoá và ký nhận bởi RAClient.



Hình 6: Xác nhận lại việc gửi các yêu cầu chứng chỉ

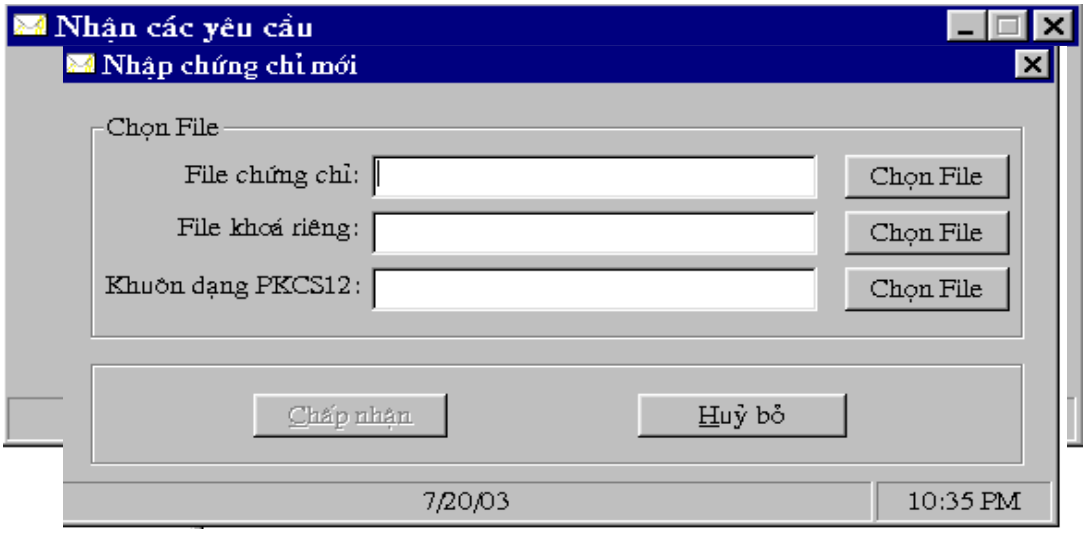
4. NHẬN YÊU CẦU CHỨNG CHỈ

Trên RAServer, người quản trị chạy chương trình quản lý các đăng ký bằng cách vào **Start-> Program -> KC01-05 RAServer-> Quản lý đăng ký chứng chỉ** và đăng nhập với **user name** và mật khẩu mặc định là **"admin".**



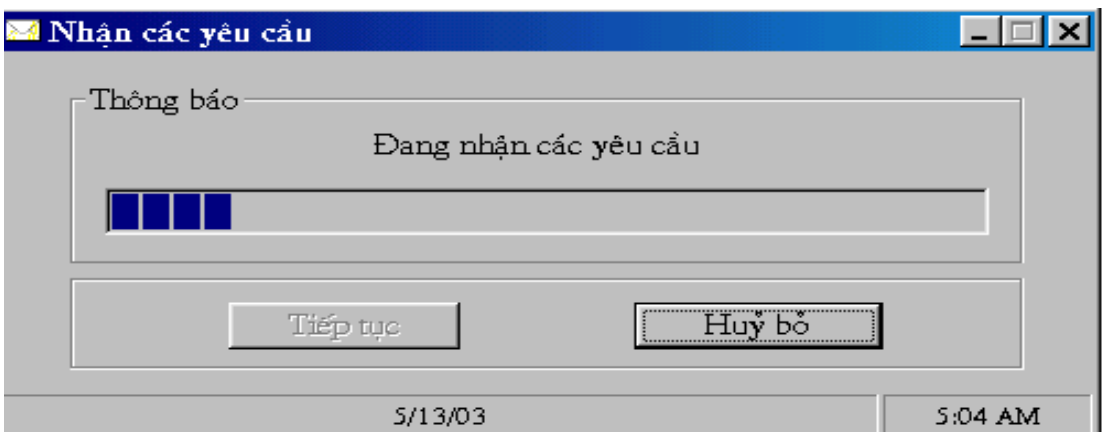
Hình 7: Chương trình quản lý đăng ký trên RAServer

Để nhận các yêu cầu từ các RAClient, người quản trị chọn chức năng **"Nhận yêu cầu"** trên thanh công cụ.



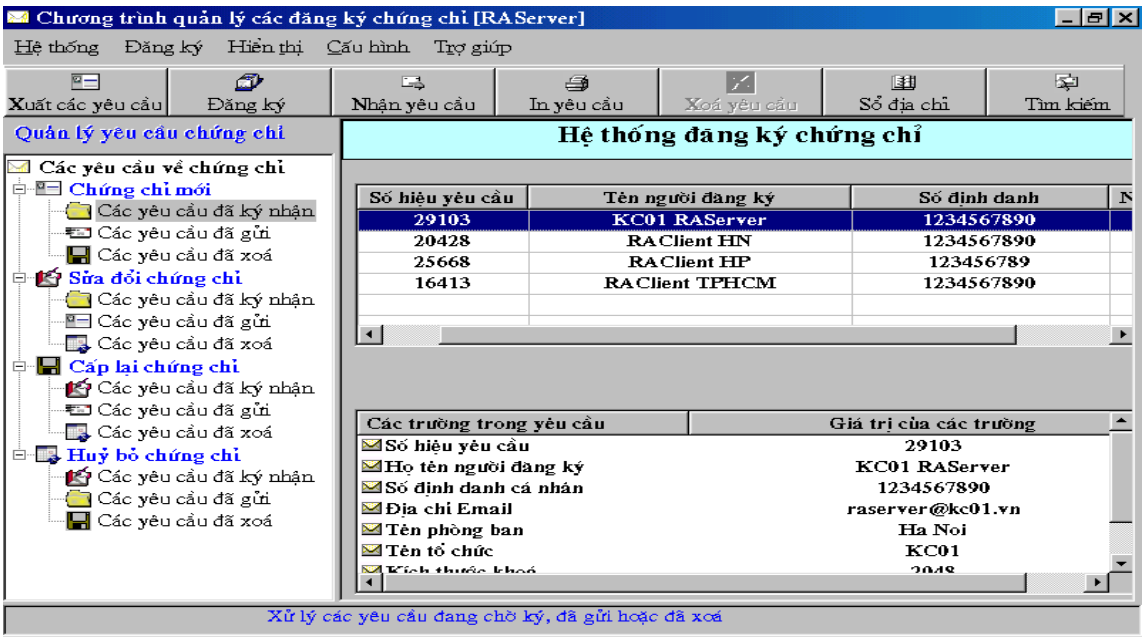
Hình 21 - Chọn File chứng chỉ và File khoá riêng để nhập

Khi đó các yêu cầu chứng chỉ được nhận về, phân tích, giải mã và cập nhật vào CSDL trên RAServer.



5. XUẤT YÊU CẦU VÀ TẠO CHỨNG CHỈ

Sau khi các đăng ký cấp chứng chỉ đã được nhận về, người quản trị trên RAServer xem lại các đăng ký bằng cách chọn mục **"Các yêu cầu đã ký nhận"** trong phần **"Chứng chỉ mới"**, chọn các đăng ký sau đó chọn chức năng **"Xuất các yêu cầu"** trên thanh công cụ và chọn thiết bị lưu trữ để xuất các yêu cầu là đĩa mềm.



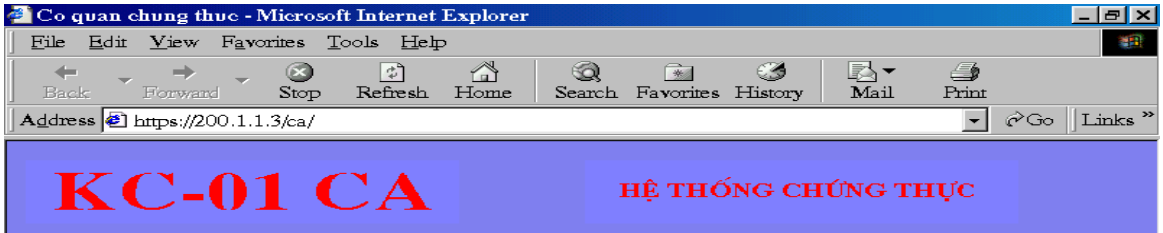
Hình 10: Xem và xuất các yêu cầu sang CA

Khi đó các đăng ký chứng chỉ sẽ được chuyển vào thư mục **requests** trên đĩa mềm.

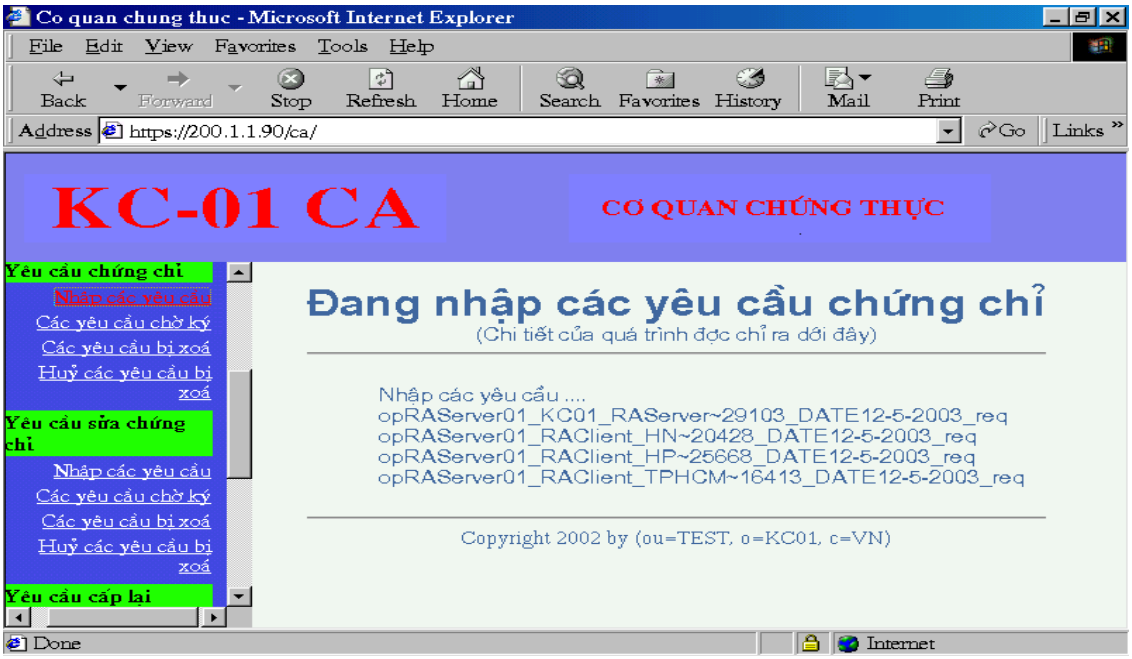
6. NHẬP CÁC YÊU CẦU ĐĂNG KÝ CHỨNG CHỈ

Vào trang Web của CA bằng cách khởi động **Netscape**, nhập địa chỉ Web có dạng: **https://tên_máy (hoặc địa chỉ IP)/tên trang Web CA/** . Ví dụ: **https://linux/ca/** hoặc **https://10.64.0.251/ca/**

Màn hình CA có dạng:



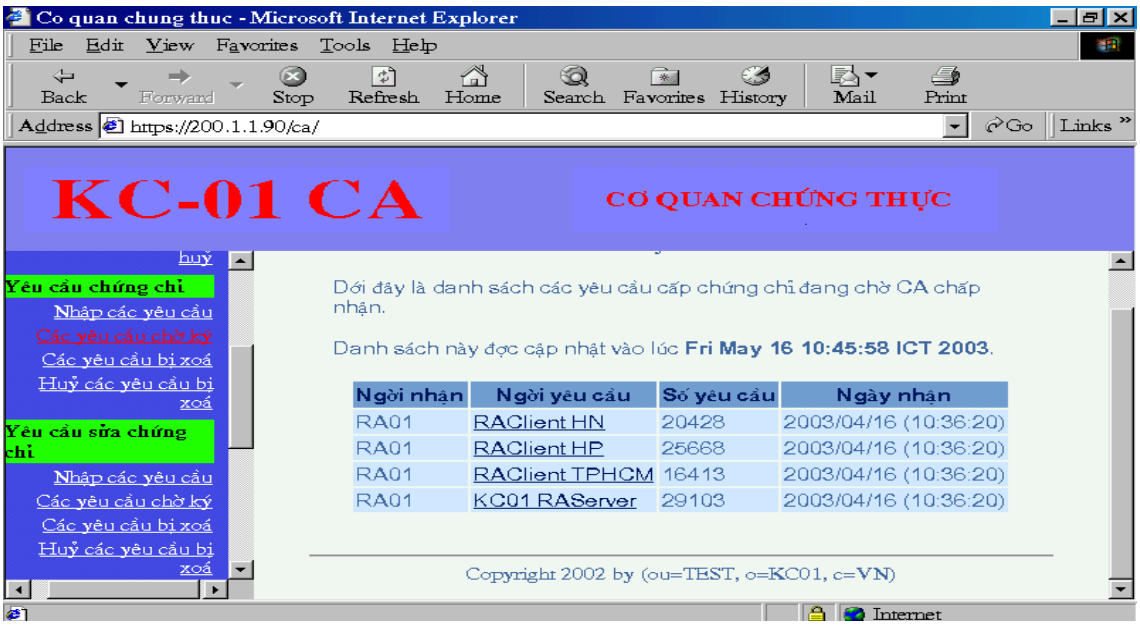
Cho đĩa mềm vào ổ A, trên trang Web của CA chọn mục **"Nhập các yêu cầu"** trong phần **"Yêu cầu chứng chỉ"**



Hình 12: Nhập các yêu cầu vào CA

7. XEM CÁC YÊU CẦU CẤP CHỨNG CHỈ ĐÃ NHẬP

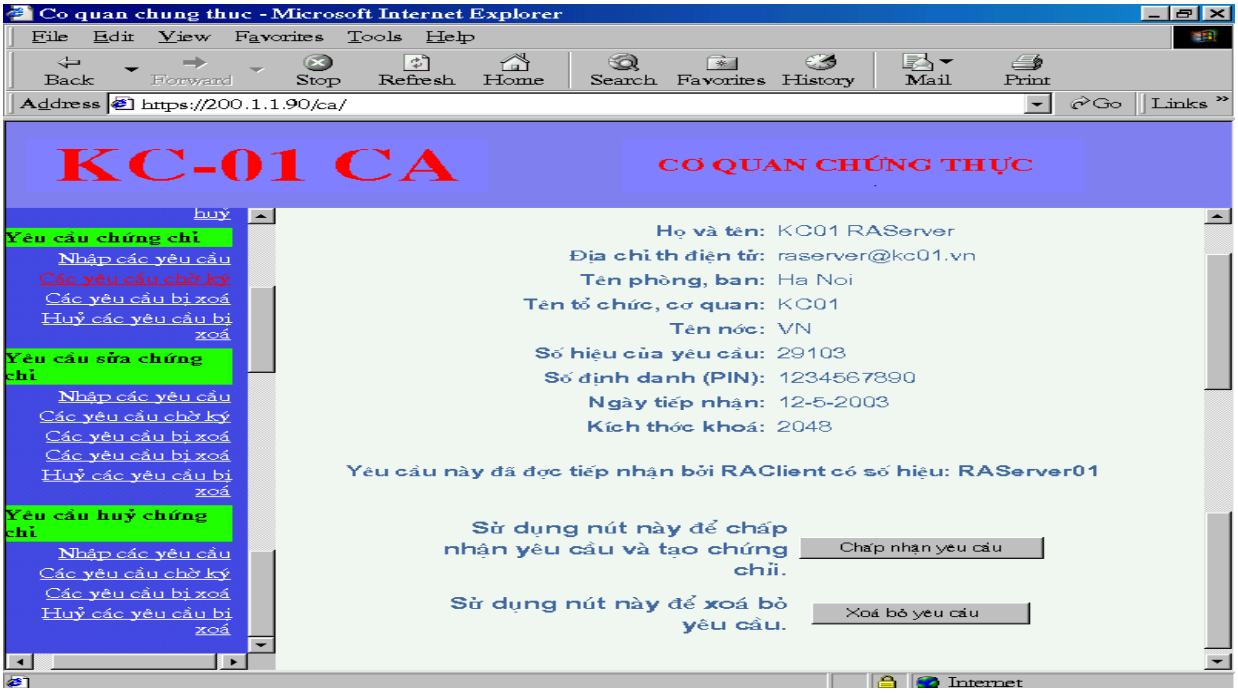
Chọn mục **"Các yêu cầu chờ ký"** trong phần **"Yêu cầu chứng chỉ",** chương trình cho phép xem danh sách các yêu cầu cấp chứng chỉ đang chờ CA chấp nhận.



Hình 13: Các yêu cầu cấp chứng chỉ chờ ký

8. TẠO CHỨNG CHỈ

Chọn yêu cầu cần tạo chứng chỉ trong danh sách các yêu cầu chờ ký, kiểm tra thông tin đăng ký. Nếu thông tin chưa chính xác, CA có thể xoá bỏ yêu cầu. Nếu thông tin là chính xác, CA chấp nhận yêu cầu để sinh cặp khoá và chứng chỉ cho người dùng.



Hình 14: Xem thông tin đăng ký trước khi tạo chứng chỉ

Hình 15: Các chứng chỉ đã phát hành

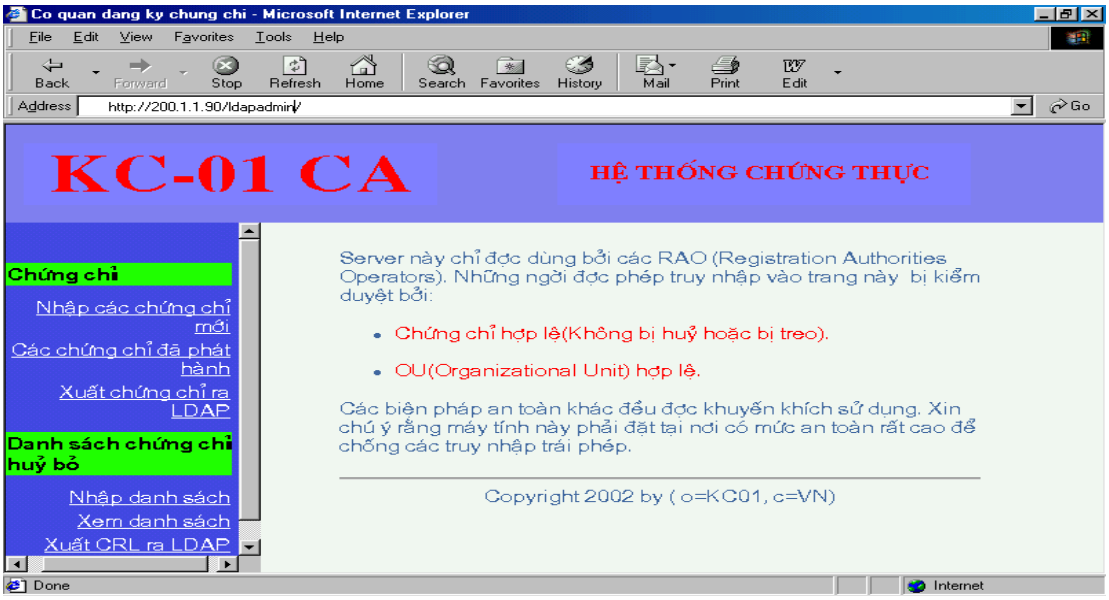
9. XUẤT CHỨNG CHỈ

Sau khi được tạo ra trên CA các chứng chỉ phải được xuất ra thiết bị lưu trữ để đưa vào RAServer và LDAPServer. Thực hiện xuất các chứng chỉ bằng cách cho đĩa vào ổ mềm, chọn mục **"Xuất các chứng chỉ"** trên màn màn hình CA. Khi đó các chứng chỉ sẽ được đưa vào thư mục

certificates trên đĩa mềm, khoá riêng được đưa vào thư mục **keys**, các chứng chỉ ở khuôn dạng PKCS12 được đưa vào thư mục **pkcs12** trên đĩa mềm.

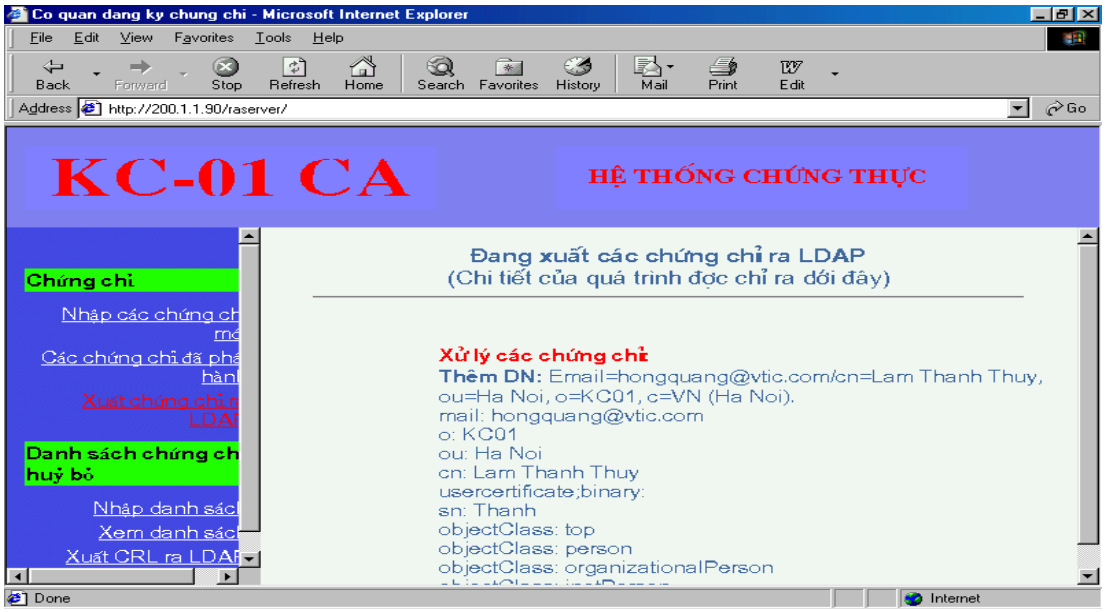
10. ĐƯA CHỨNG CHỈ VÀO LDAPSERVER

Vào trang Web quản trị LDAPServer bằng cách khởi động **Netscape**, nhập địa chỉ Web có dạng: **https://tên_máy (hoặc địa chỉ IP)/tên trang Web quản trị LDAP/** . Ví dụ: **https://hanoi/ldapadmin/** hoặc **https://10.64.0.252/ldapadmin**



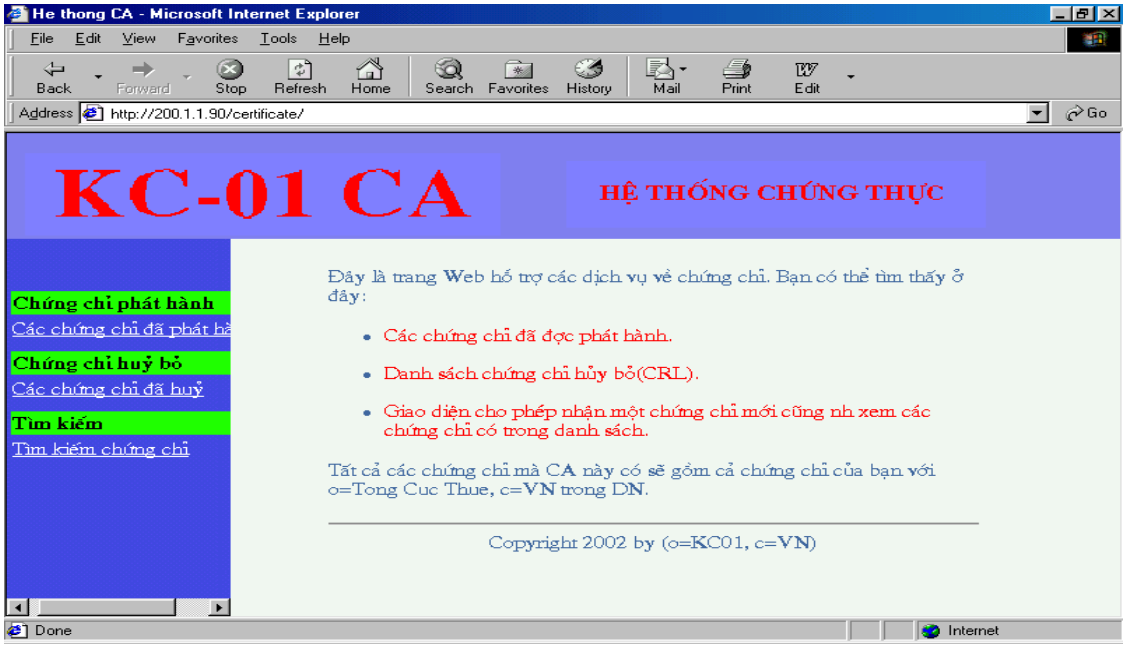
Hình 16: Trang Web quản trị LDAPServer

Đưa đĩa mềm chứa các chứng chỉ vừa xuất từ CA vào ổ mềm của LDAPserver, chọn chức năng **"Nhập các chứng chỉ mới"**, chọn tiếp chức năng **"Xuất chứng chỉ ra LDA"**. Khi đó các chứng chỉ sẽ được đưa lên LDAP Server để mọi người có thể tìm kiếm và download về.

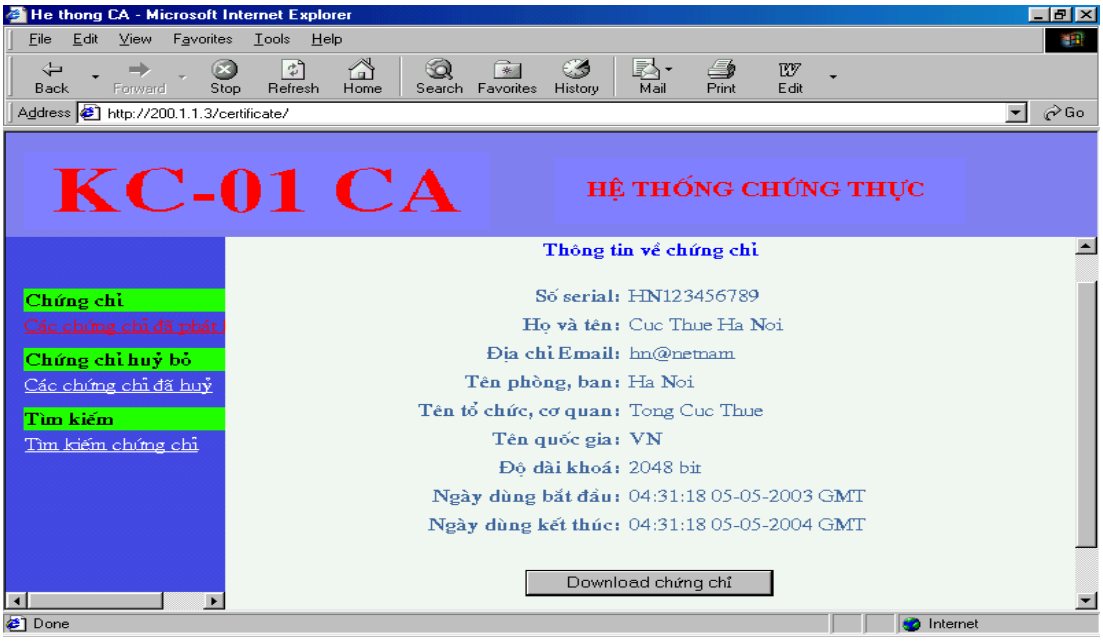


Hình 17: Xuất chứng chỉ ra LDAP

Sau khi chứng chỉ đã được đưa lên LDAPServer người dùng có thể xem, tìm kiếm ... các chứng chỉ bằng cách vào trang Web trên LDAPServer dành cho người dùng



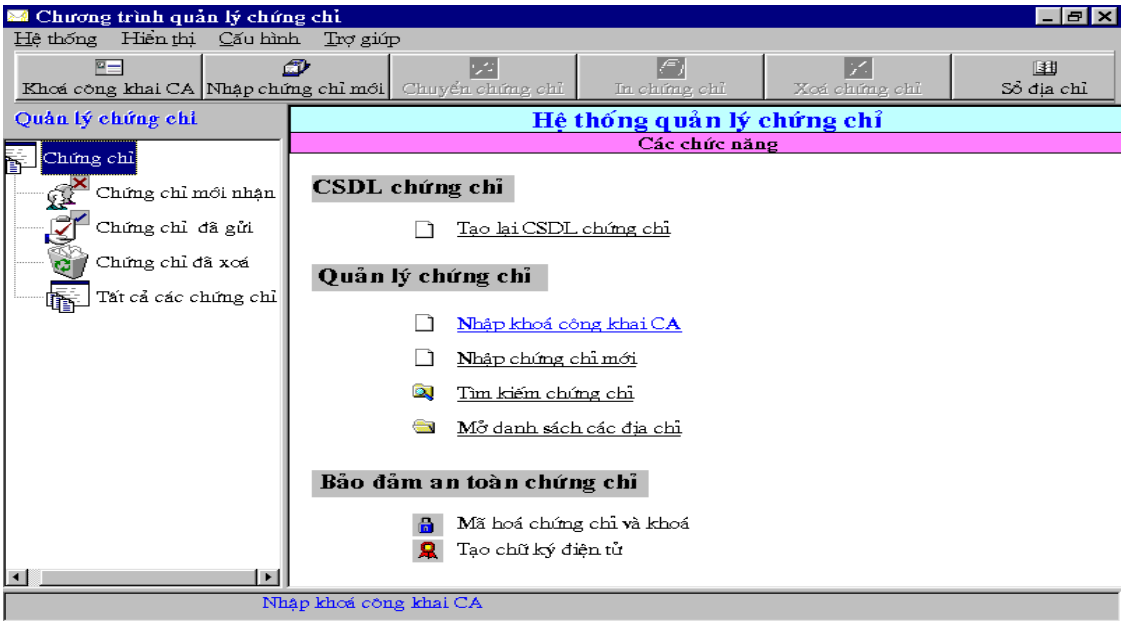
Hình 18: Trang Web dành cho người dùng truy cập LDAPServer



Hình 19: Xem và tải chứng chỉ từ LDAPServer

11. ĐƯA CHỨNG CHỈ VÀO RASERVER

RAServer quản lý tất cả các chứng chỉ đã được cấp phát bởi CA. Khởi động chương trình quản lý chứng chỉ trên RAServer bằng cách vào **Start-> Program -> KC01-05 RAServer-> Quản lý chứng chỉ** và đăng nhập với **user name** và mật khẩu mặc định là **"admin".**



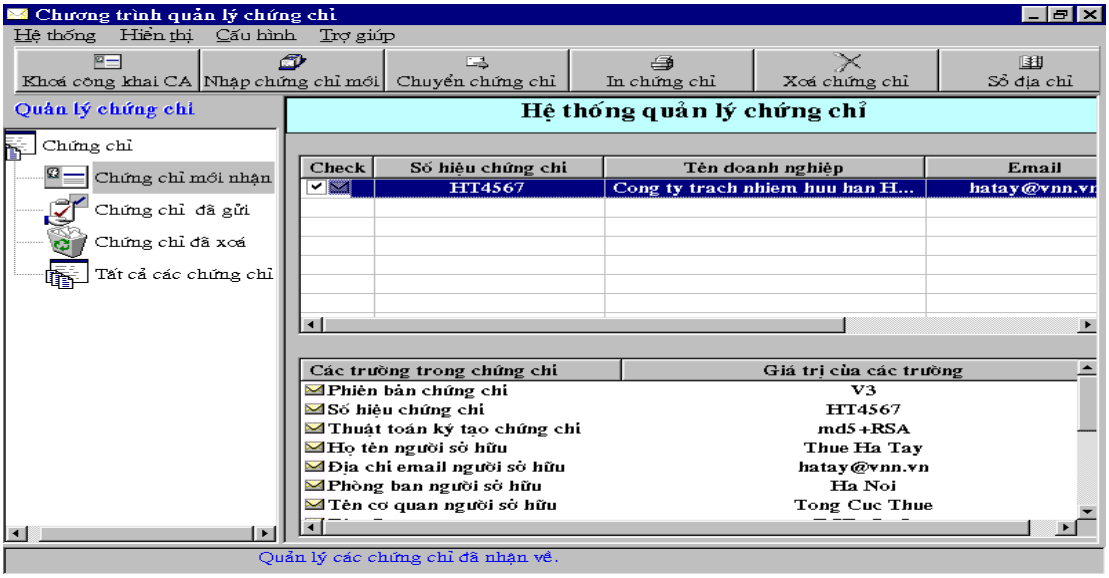
Hình 20- Màn hình chương trình quản lý chứng chỉ trên RAServer

Cho đĩa mềm chứa các chứng chỉ đã xuất ra từ CA vào ổ mềm, chọn chức năng **"Nhập chứng chỉ mới"** trên thanh công cụ.

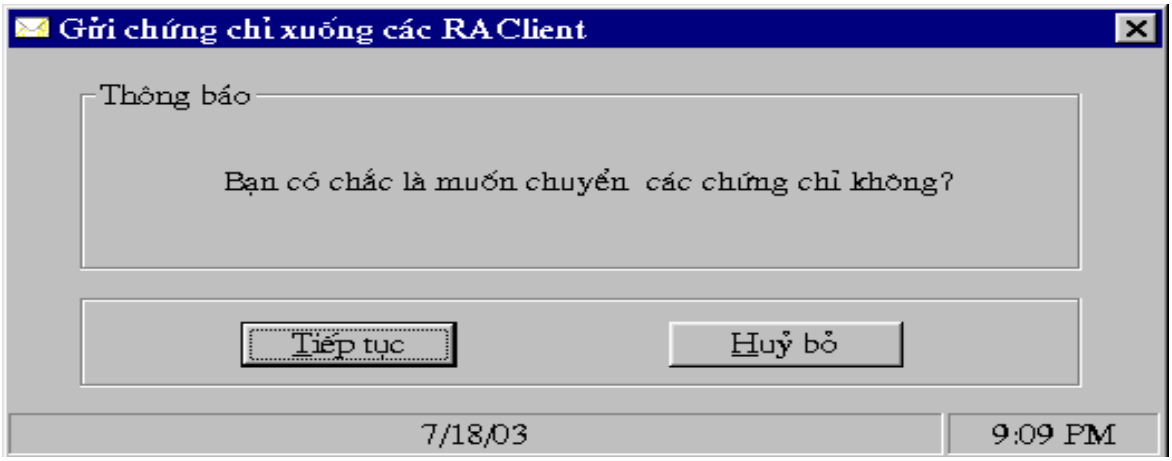
Chọn File chứng chỉ và File khoá riêng tương ứng trong ổ mềm rồi chọn **"Chấp nhận"**, chứng chỉ và khoá sẽ được đưa vào CSDL trên RAServer để quản lý

12. CHUYỂN CHỨNG CHỈ VÀO CÁC VÙNG CỦA CÁC RACLIENT

Sau khi chứng chỉ được đưa từ CA vào RAServer , người quản trị RAServer xem xét các chứng chỉ và chọn chức năng **"Chuyển chứng chỉ"** để chuyển các chứng chỉ vào các vùng tương ứng với các RAClient.



Hình 22- Xem và chuẩn bị chuyển các chứng chỉ



Hình 23- Xác nhận gửi chứng chỉ

13. NHẬN CHỨNG CHỈ VỀ

Các RAClient chủ động nhận các chứng chỉ đã đăng ký về bằng cách chạy chương trình quản lý chứng chỉ mức RAClient (vào **Start-> Program -> KC01-05 RAClient-> Quản lý chứng chỉ** và đăng nhập với **user name** và mật khẩu mặc định là **"admin"**)

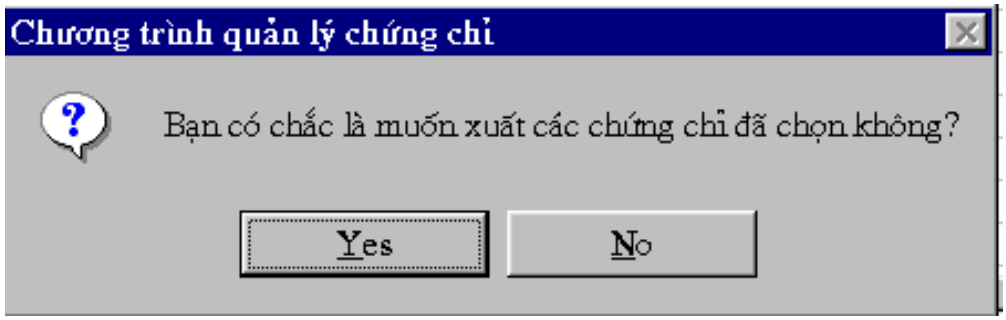
Chọn chức năng **"Nhận chứng chỉ"** trên thanh công cụ sau đó chọn **"Tiếp tục"** để nhận chứng chỉ về từ RAServer.

Hình 25 - Nhận chứng chỉ từ RASever

Khi nhận về, các chứng chỉ và khoá riêng của người dùng được lưu vào cơ sở dữ liệu ở dạng mã chỉ đến khi nào được xuất ra cho người dùng thì mới được giải mã.

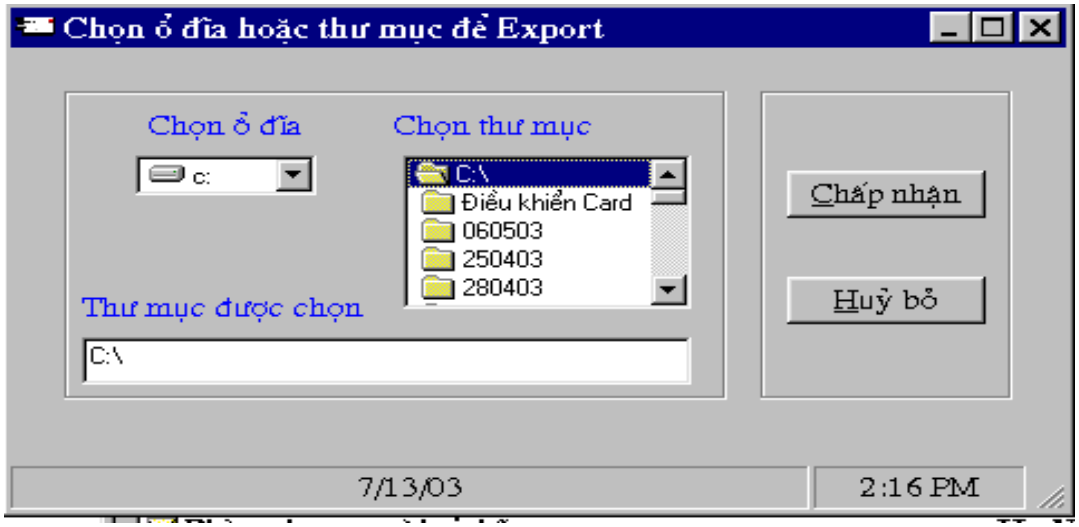
14. XUẤT CHỨNG CHỈ CHO NGƯỜI DÙNG

Người quản trị tại RAClient chọn chứng chỉ của người dùng sau đó chọn chức năng **"Export chứng chỉ"** trên thanh công cụ.



Hình 26 - Xác nhận quá trình xuất chứng chỉ

Chọn thiết bị lưu trữ sẽ chứa chứng chỉ và khoá riêng của người dùng, khoá công khai của CA sau đó chọn **"Chấp nhận"**



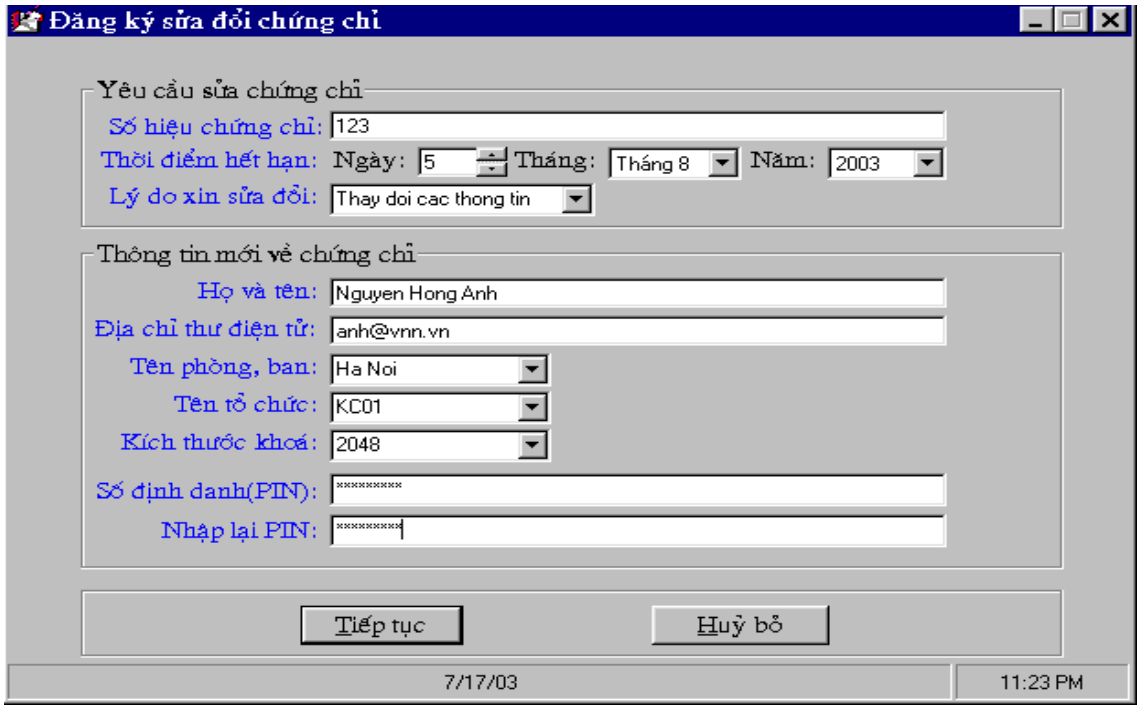
Hình 27 - Chọn nơi lưu trữ chứng chỉ và khoá sẽ xuất ra

Khi đó chứng chỉ và khoá riêng của người dùng trong cơ sở dữ liệu sẽ được giải mã và ghi ra thiết bị lưu trữ (thường là đĩa mềm) cùng với khoá công khai của CA (khoá này đã được Import vào CSDL ngay từ khi khởi tạo hệ thống) để chuyển cho người dùng. Khoá riêng của người dùng trong cơ sở dữ liệu của RAClient sẽ được xoá đi để đảm bảo chỉ có người dùng là người duy nhất giữ khoá riêng của họ.

SỬA ĐỔI CHỨNG CHỈ

Chứng chỉ cần sửa đổi khi người dùng thay đổi một số thông tin trong chứng chỉ như tên người dùng, địa chỉ ... hoặc người dùng cần thay đổi kích thước khoá. Trình tự đăng ký và sửa đổi chứng chỉ cho người dùng được thực hiện như sau:

Người dùng đến gặp người quản trị tại RAClient xin đăng kí sửa đổi chứng chỉ và điền các thông tin cần thiết vào mẫu đăng ký. Sau khi người dùng đăng ký sửa đổi chứng chỉ và điền các thông tin cần thiết, người quản trị tại RAClient xác minh lại các thông tin. Nếu thông tin nào chưa chính xác thì yêu cầu người dùng đăng ký lại, nếu các thông tin là chính xác thì vào chương trình quản lý các đăng ký tại RAClient, chọn mục **"Đăng kí sửa đổi chứng chỉ"** và điền các thông tin của người dùng vào Form đăng ký rồi chọn **"Tiếp tục"**



Hình 28 - Form đăng ký sửa chứng chỉ

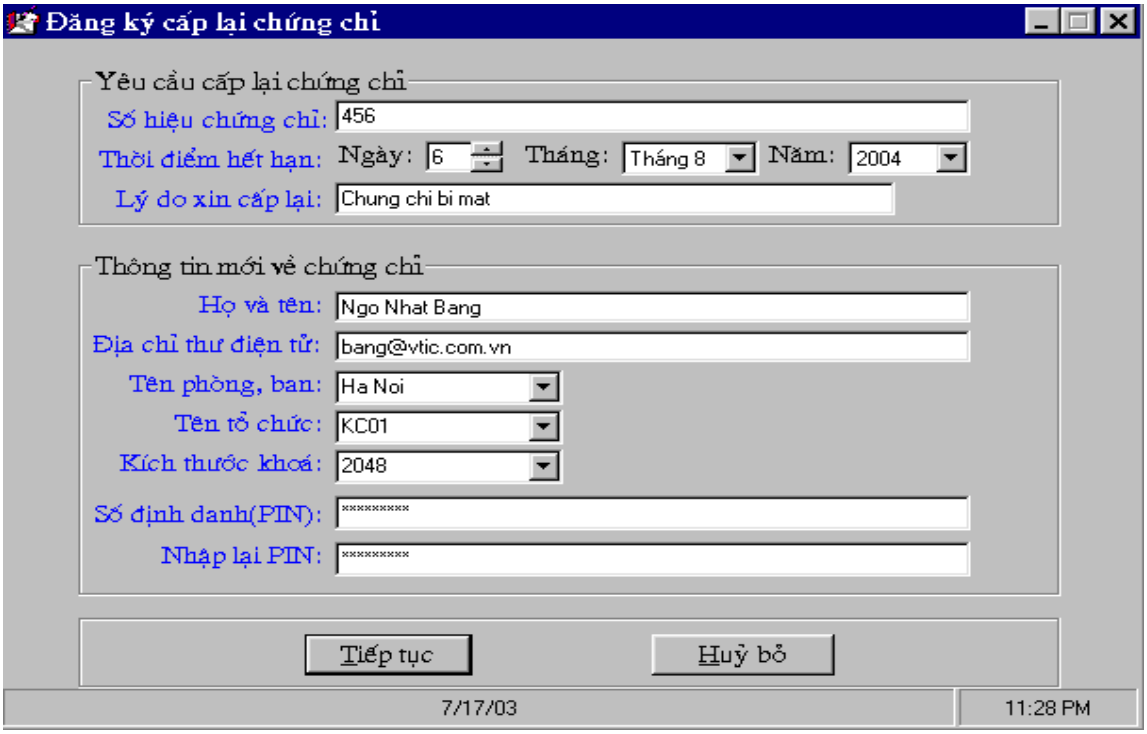
RAClient kiểm tra lại các thông tin đã nhập, nếu chưa đúng thì chọn **"Huỷ bỏ"** để về Form nhập dữ liệu ban đầu sửa đổi lại, nếu đúng thì chọn **"Chấp nhận"** để đưa yêu cầu vào CSDL chờ ký nhận và gửi đi.

Các bước tiếp theo như ký nhận, gửi lên RAServer, xuất sang CA ... được thực hiện hoàn toàn tương tự như quá trình đăng ký, cấp phát chứng chỉ mới.

QUI TRÌNH CẤP LẠI CHỨNG CHỈ

Chứng chỉ cần cấp lại khi người dùng bị mất hoặc chứng chỉ hết hạn. Trình tự đăng ký và cấp lại chứng chỉ cho người dùng được thực hiện như sau:

Người dùng đến gặp người quản trị tại RAClient xin đăng kí cấp lại chứng chỉ và điền các thông tin cần thiết vào mẫu đăng ký. Sau khi người dùng đăng ký cấp lại chứng chỉ và điền các thông tin cần thiết, người quản trị tại RAClient xác minh lại các thông tin. Nếu thông tin nào chưa chính xác thì yêu cầu người dùng đăng ký lại, nếu các thông tin là chính xác thì vào chương trình quản lý các đăng ký tại RAClient, chọn mục **"Đăng kí cấp lại chứng chỉ"** và điền các thông tin của người dùng vào Form đăng ký rồi chọn **"Tiếp tục"**



Hình 30 - Form đăng ký cấp lại chứng chỉ

RAClient kiểm tra lại các thông tin đã nhập, nếu chưa đúng thì chọn **"Huỷ bỏ"** để về Form nhập dữ liệu ban đầu sửa đổi lại, nếu đúng thì chọn **"Chấp nhận"** để đưa yêu cầu vào CSDL chờ ký nhận và gửi đi.

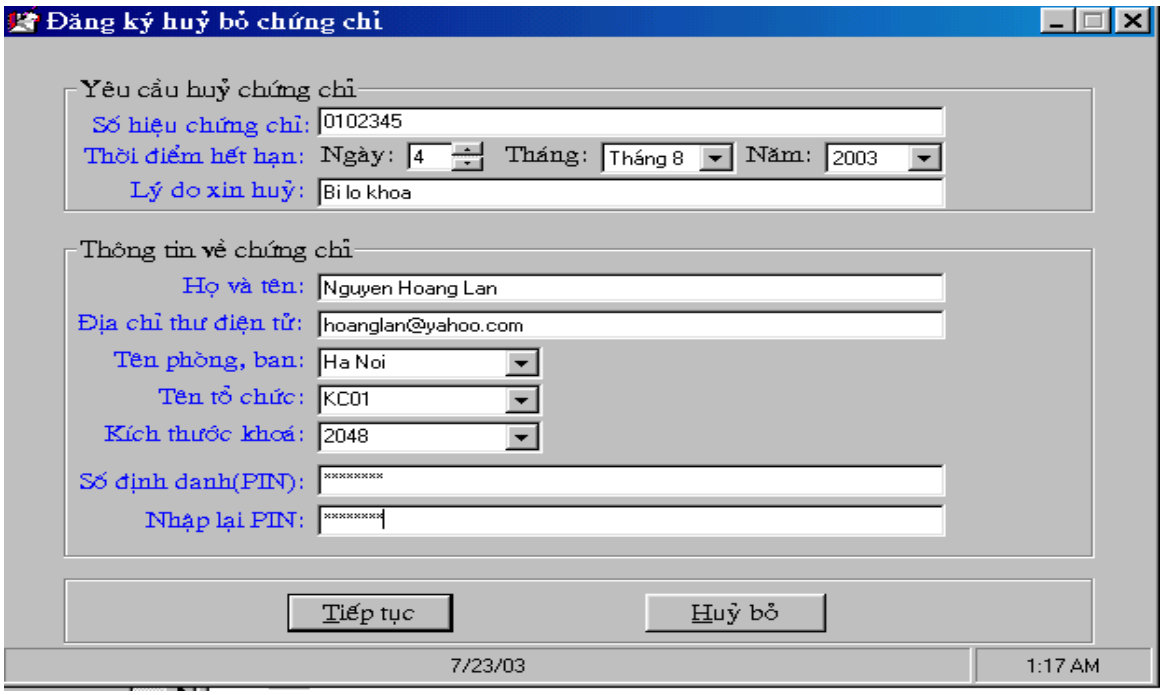
Các bước tiếp theo như ký nhận, gửi lên RAServer, xuất sang CA ... được thực hiện hoàn toàn tương tự như quá trình đăng ký, cấp phát chứng chỉ mới.

QUI TRÌNH HUỶ BỎ CHỨNG CHỈ

1. ĐĂNG KÝ HUỶ CHỨNG CHỈ

Chứng chỉ cần huỷ bỏ khi người dùng bị lộ khoá hoặc chứng chỉ hết hạn. Trình tự đăng ký và huỷ bỏ chứng chỉ cho người dùng được thực hiện như sau:

Người dùng đến gặp người quản trị tại RAClient xin đăng kí huỷ bỏ chứng chỉ và điền các thông tin cần thiết vào mẫu đăng ký. Sau khi người dùng đăng ký huỷ bỏ chứng chỉ và điền các thông tin cần thiết, người quản trị tại RAClient xác minh lại các thông tin. Nếu thông tin nào chưa chính xác thì yêu cầu người dùng đăng ký lại, nếu các thông tin là chính xác thì vào chương trình quản lý các đăng ký tại RAClient, chọn mục **"Đăng kí huỷ chứng chỉ"** và điền các thông tin của người dùng vào Form đăng ký rồi chọn **"Tiếp tục"**



Hình 32 - Form đăng ký huỷ chứng chỉ

RAClient kiểm tra lại các thông tin đã nhập, nếu chưa đúng thì chọn **"Huỷ bỏ"** để về Form nhập dữ liệu ban đầu sửa đổi lại, nếu đúng thì chọn **"Chấp nhận"** để đưa yêu cầu vào CSDL chờ ký nhận và gửi đi.

Hình 33 - Xác nhận lại các thông tin đăng ký

Các bước tiếp theo gồm ký nhận, gửi lên RAServer, xuất sang CA, nhập các yêu cầu vào CA được thực hiện hoàn toàn tương tự như quá trình đăng ký, cấp phát chứng chỉ mới.

2. HUỶ CHỨNG CHỈ

Người quản trị tại CA xem các yêu cầu huỷ chứng chỉ chờ ký đã nhập vào CA bằng cách chọn mục **"Các yêu cầu chờ ký"** trong phần **"Yêu cầu huỷ chứng chỉ"**, nháy chuột vào số hiệu của yêu cầu để xem các thông tin trên yêu cầu. Nếu các thông tin là chính xác, người quản trị CA chọn nút **"Huỷ chứng chỉ"** để huỷ chứng chỉ có số hiệu đã đăng ký. Nếu thông tin đăng ký không chính xác, người quản trị CA có thể chọn nút **"Xoá yêu cầu"** để xoá bỏ yêu cầu huỷ chứng chỉ trên CA.

3. TẠO DANH SÁCH CHỨNG CHỈ HUỶ BỎ (CRL)

Danh sách chứng chỉ hủy bỏ (CRL: Certificate Revocation List) là một danh sách chứa các chứng chỉ đã bị huỷ bỏ cùng với ngày giờ đã huỷ bỏ chúng và chữ ký của CA. Người quản trị CA tạo và xuất danh sách chứng chỉ huỷ bỏ bằng cách đưa đĩa mềm vào ổ sau đó chọn mục **"Xuất danh sách"** trong phần **"Chứng chỉ huỷ bỏ"**. Khi đó danh sách chứng chỉ huỷ bỏ sẽ được tạo và xuất ra thư mục CRL trên đĩa mềm.

4. NHẬP DANH SÁCH CHỨNG CHỈ HUỶ BỎ VÀO LDAPSERVER

Chuyển đĩa mềm có chứa danh sách chứng chỉ huỷ bỏ vừa tạo trên CA vào LDAPServer, vào trang Web dành cho người quản trị LDAPServer, chọn chức năng **"Nhập danh sách"** trong mục **"Chứng chỉ huỷ bỏ"**

5. XUẤT DANH SÁCH CHỨNG CHỈ HUỶ BỎ

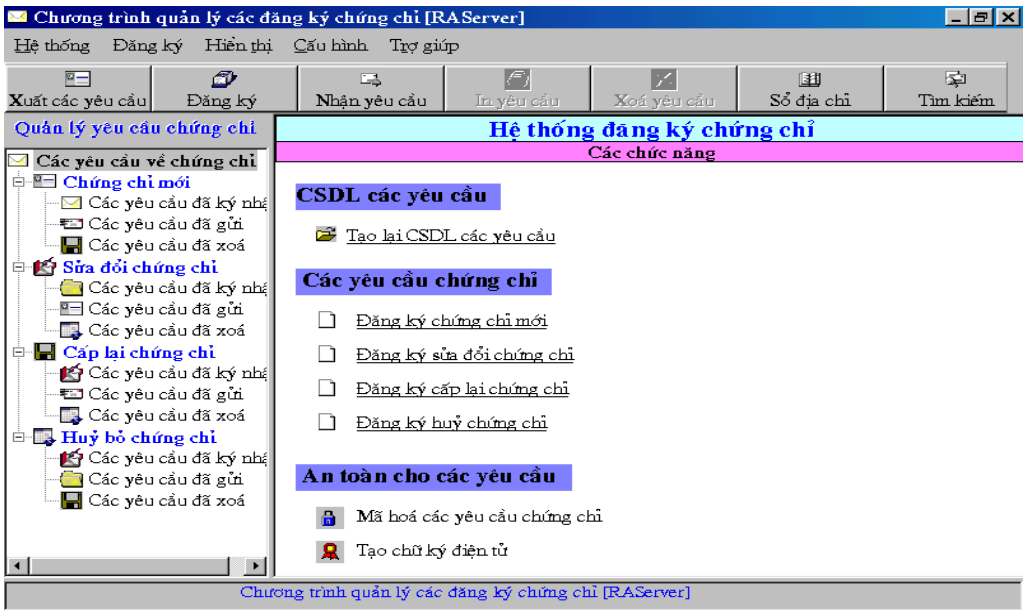
Để mọi người dùng có nhu cầu sử dụng chứng chỉ đều biết chứng chỉ của những người dùng nào đã bị hủy bỏ thì danh sách chứng chỉ huỷ phải được công khai trên trang Web của LDAPServer. Người quản trị LDAPServer thực hiện việc này bằng cách chọn mục **"Xuất danh sách ra LDAP"** trong phần **"Chứng chỉ huỷ bỏ"** trên trang Web dành cho người quản trị LDAPServer.

B. TỔ CHỨC CẤP PHÁT CHỨNG CHỈ TẠI TỔNG CỤC THUẾ

QUY TRÌNH CẤP PHÁT CHỨNG CHỈ

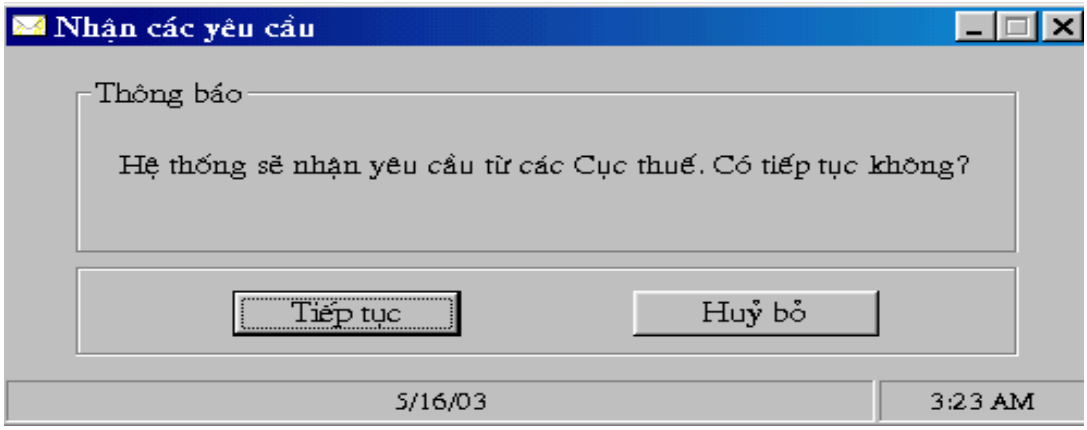
1. NHẬN YÊU CẦU CHỨNG CHỈ

Trên Tổng cục thuế , người quản trị chạy chương trình quản lý các đăng ký như sau: **Start-> Program -> RAServer Tong Cuc Thue-> Quản lý đăng ký chứng chỉ** và đăng nhập với tên người dùng và mật khẩu mặc định là **"admin".**



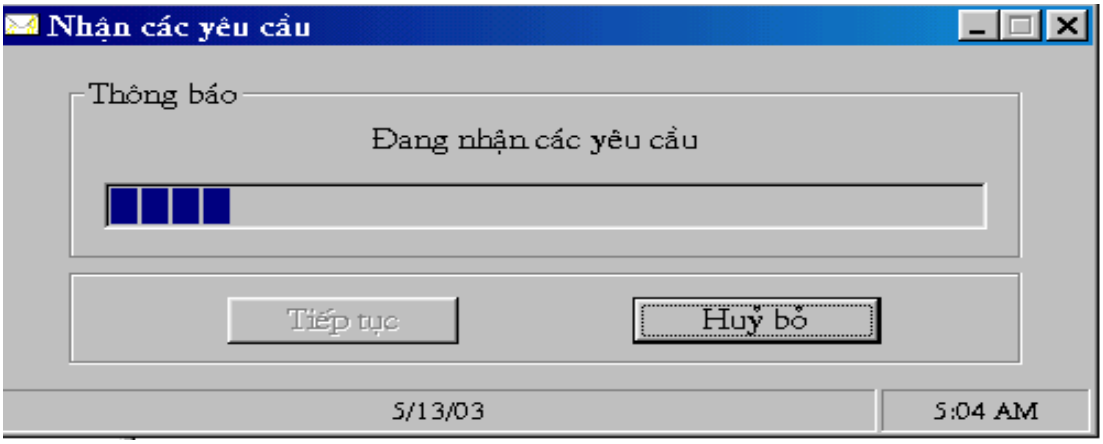
Hình 1. Chương trình quản lý đăng ký trên Tổng cục thuế

Để nhận các yêu cầu từ Cục thuế, người quản trị chọn chức năng **"Nhận yêu cầu"** trên thanh công cụ.



Hình 2. Xác nhận việc nhận các yêu cầu xin cấp chứng chỉ

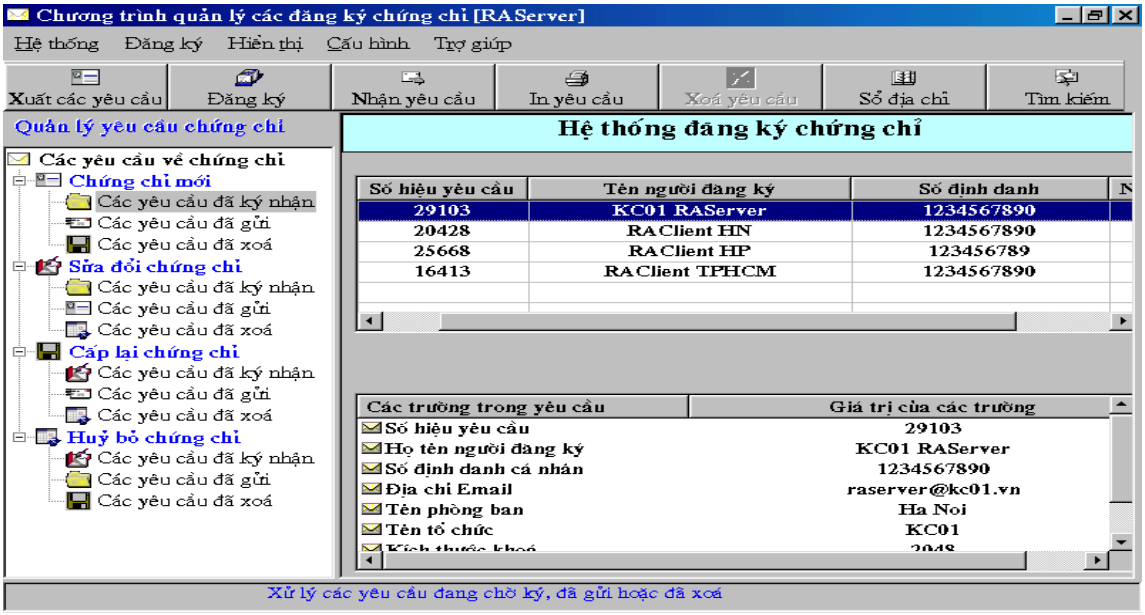
Sau khi nhận được các yêu cầu xin cấp chứng chỉ, chúng được phân tích, giải mã và cập nhật vào cơ sở dữ liệu trên Tổng cục.



Hình 3. Nhận và phân tích các yêu cầu trên Tổng cục

2. XUẤT YÊU CẦU VÀ TẠO CHỨNG CHỈ

Sau khi nhận được các đăng ký xin cấp chứng chỉ, người quản trị trên Tổng cục xem lại các đăng ký bằng cách chọn mục **"Các yêu cầu đã ký nhận"** trong phần **"Chứng chỉ mới"**, chọn các đăng ký, sau đó chọn chức năng **"Xuất các yêu cầu"** trên thanh công cụ và chọn thiết bị lưu trữ, chẳng hạn là đĩa mềm.



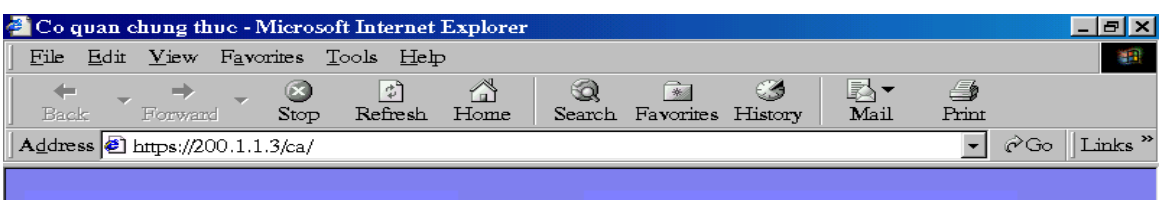
Hình 4 Xem và xuất các yêu cầu sang CA

Các đăng ký xin cấp chứng chỉ sẽ được chuyển vào thư mục **requests** trên đĩa mềm.

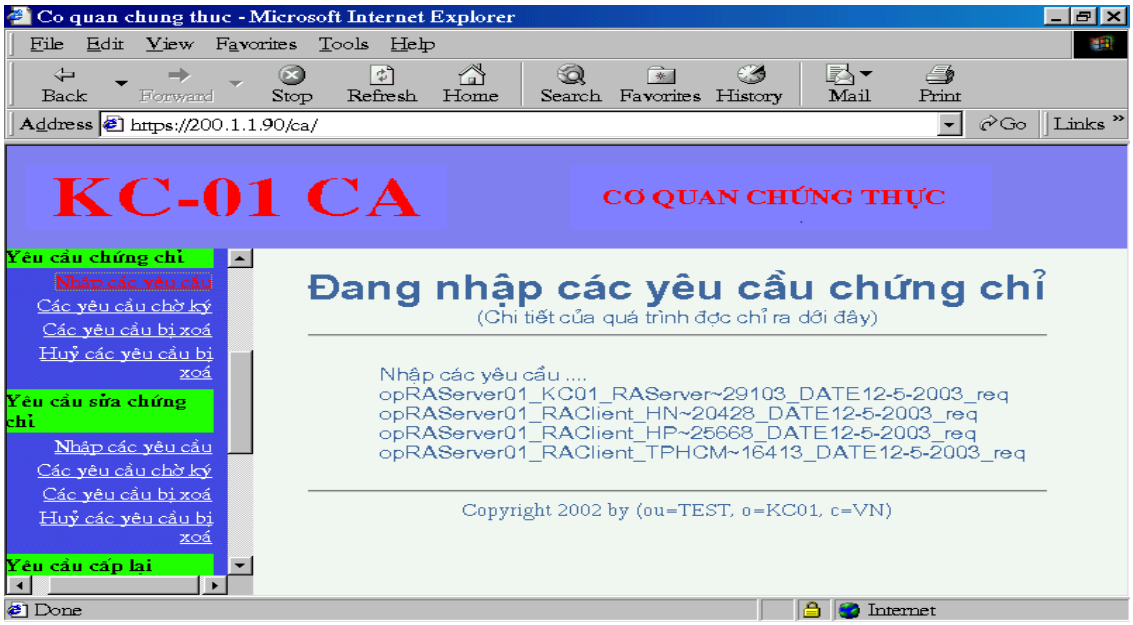
3. NHẬP CÁC YÊU CẦU ĐĂNG KÝ CHỨNG CHỈ VÀO CA

Vào trang Web của CA bằng cách khởi động **Netscape**, nhập địa chỉ Web có dạng: **https://tên_máy (hoặc địa chỉ IP)/tên trang Web CA/** . Ví dụ: **https://linux/ca/** hoặc https://10.64.0.251/ca/

Màn hình CA có dạng:



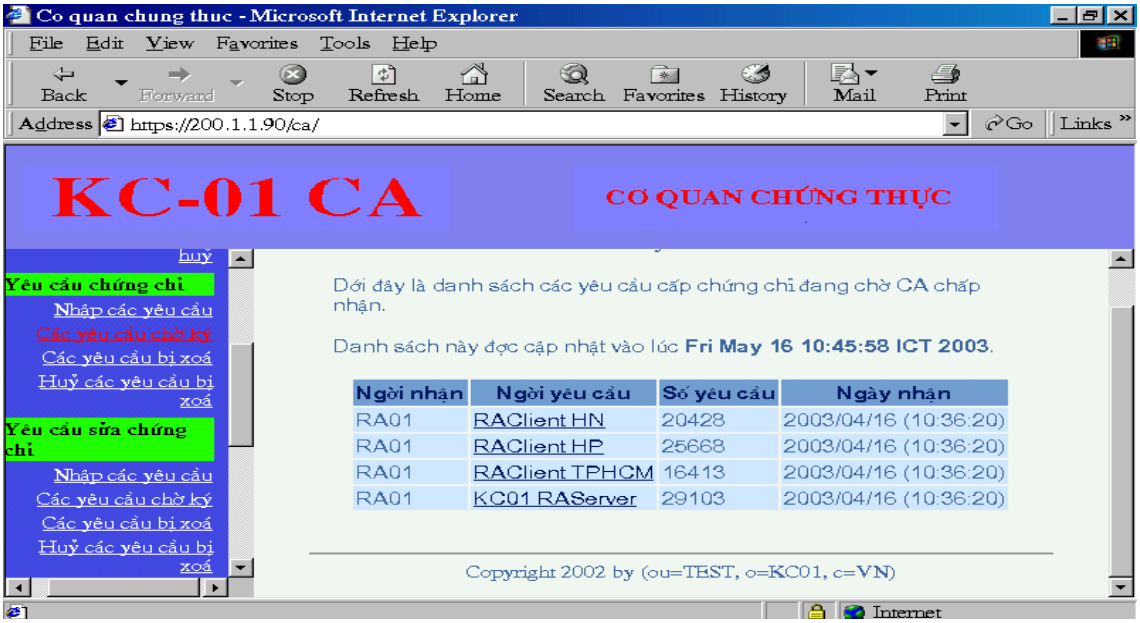
Cho đĩa mềm vào ổ A, trên trang Web của CA chọn mục **"Nhập các yêu cầu"** trong phần **"Yêu cầu chứng chỉ".**



Hình 5. Nhập các yêu cầu vào CA

4. XEM CÁC YÊU CẦU XIN CẤP CHỨNG CHỈ ĐÃ NHẬP

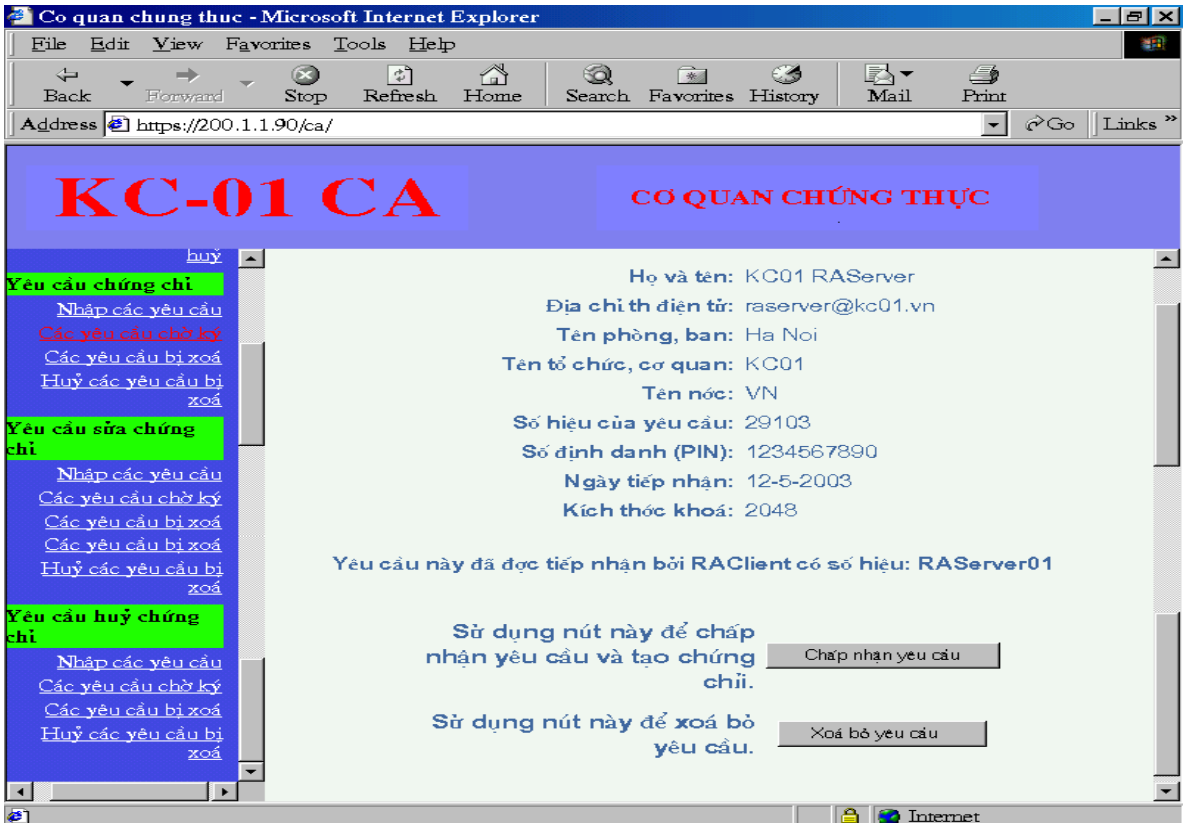
Chọn mục **"Các yêu cầu chờ ký"** trong phần **"Yêu cầu chứng chỉ",** chương trình cho phép xem danh sách các yêu cầu xin cấp chứng chỉ đang chờ CA phê chuẩn.



Hình 6. Các yêu cầu xin cấp chứng chỉ đang chờ CA phê chuẩn

5. TẠO CHỨNG CHỈ

Chọn yêu cầu cần tạo chứng chỉ trong danh sách các yêu cầu chờ ký, kiểm tra thông tin đăng ký. Nếu thông tin chưa chính xác, CA có thể xoá bỏ yêu cầu. Nếu thông tin chính xác, CA chấp nhận yêu cầu để sinh cặp khoá và chứng chỉ cho doanh nghiệp.



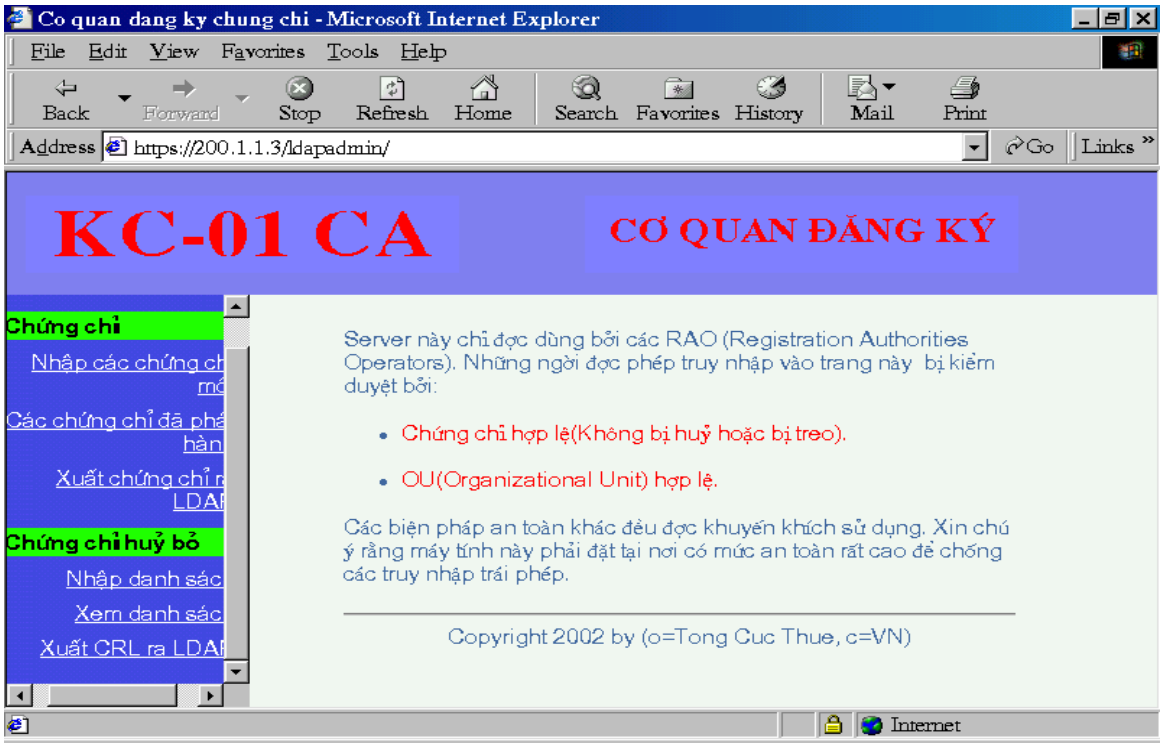
Hình 7. Xem thông tin đăng ký trước khi tạo chứng chỉ

7. XUẤT CHỨNG CHỈ

Sau khi được CA tạo ra, các chứng chỉ phải được xuất ra thiết bị lưu trữ để chuyển cho RAServer và LDAPServer trên Tổng cục. Việc xuất các chứng chỉ được tiến hành như sau: cho đĩa vào ổ mềm, chọn mục **"Xuất các chứng chỉ"** trên màn màn hình CA, các chứng chỉ sẽ được đưa vào thư mục **certificates**, khoá riêng tương ứng với khoá công khai có trong chứng chỉ được đưa vào thư mục **keys** trên đĩa mềm.

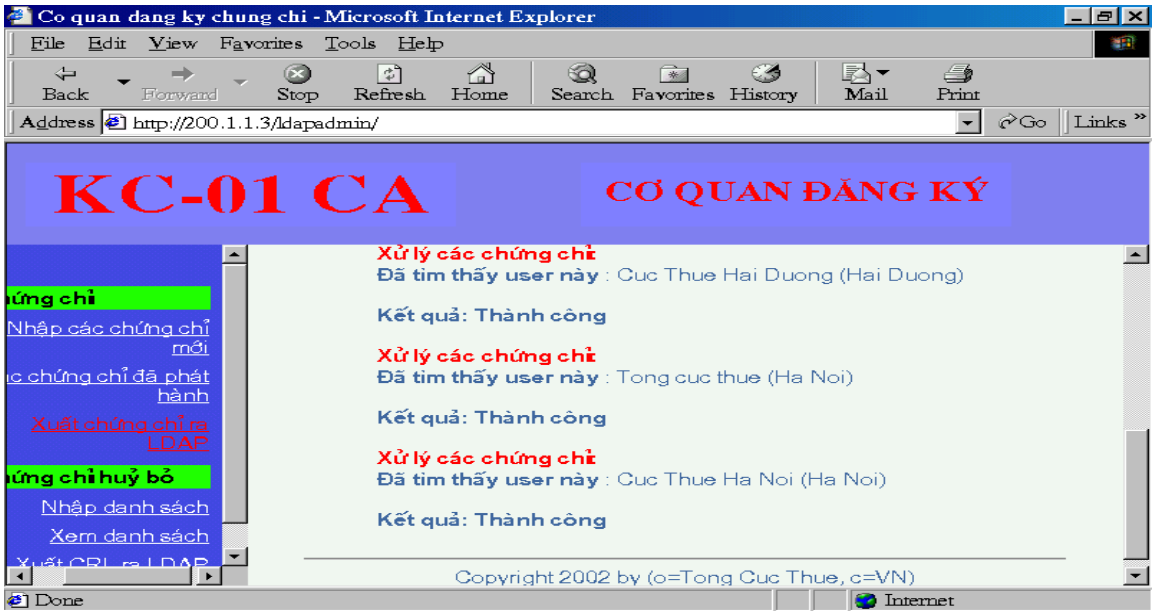
8. ĐƯA CHỨNG CHỈ VÀO LDAPSERVER

Vào trang Web quản trị LDAPServer bằng cách khởi động **Netscape**, nhập địa chỉ Web có dạng: **http://tên_máy (hoặc địa chỉ IP)/tên trang Web quản trị LDAP/**. Ví dụ: **http://hanoi/ldapadmin/** hoặc **http://10.64.0.252/ldapadmin/**



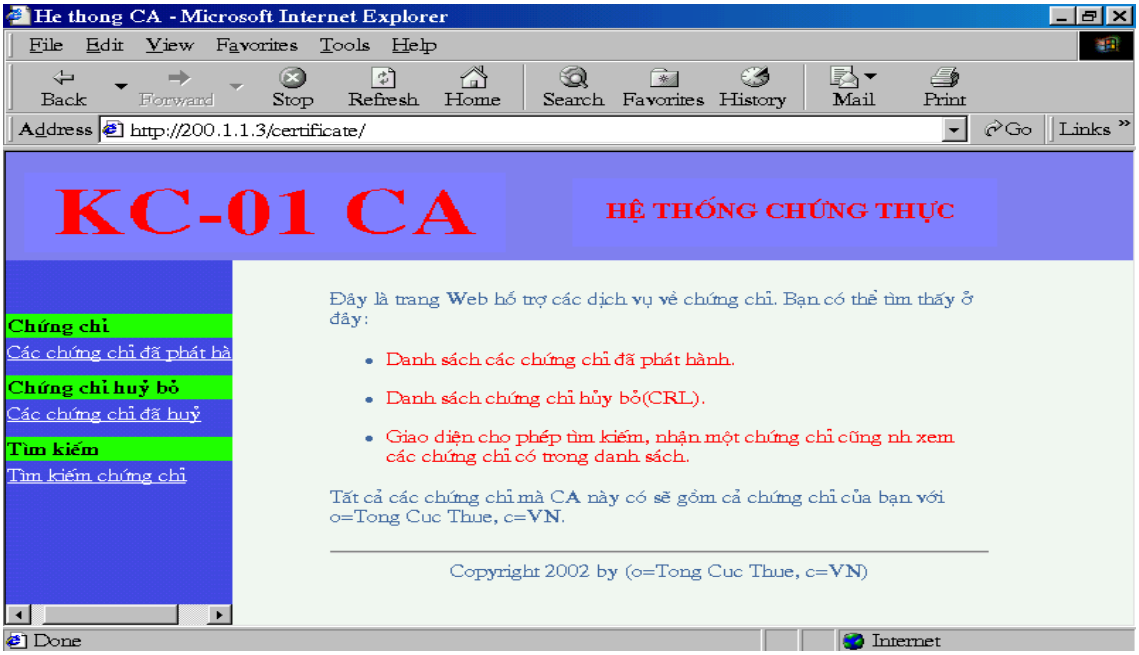
Hình 8 - Trang Web quản trị LDAPServer

Đưa đĩa mềm có lưu các chứng chỉ mà CA vừa xuất ra vào ổ mềm của LDAPserver, chọn chức năng **"Nhập các chứng chỉ mới"**, sau khi các chứng chỉ đã được nhập xong chọn tiếp chức năng **"Xuất chứng chỉ ra LDAP"**, khi đó các chứng chỉ sẽ được đưa vào LDAP Server để mọi người có thể tìm kiếm và tải về.

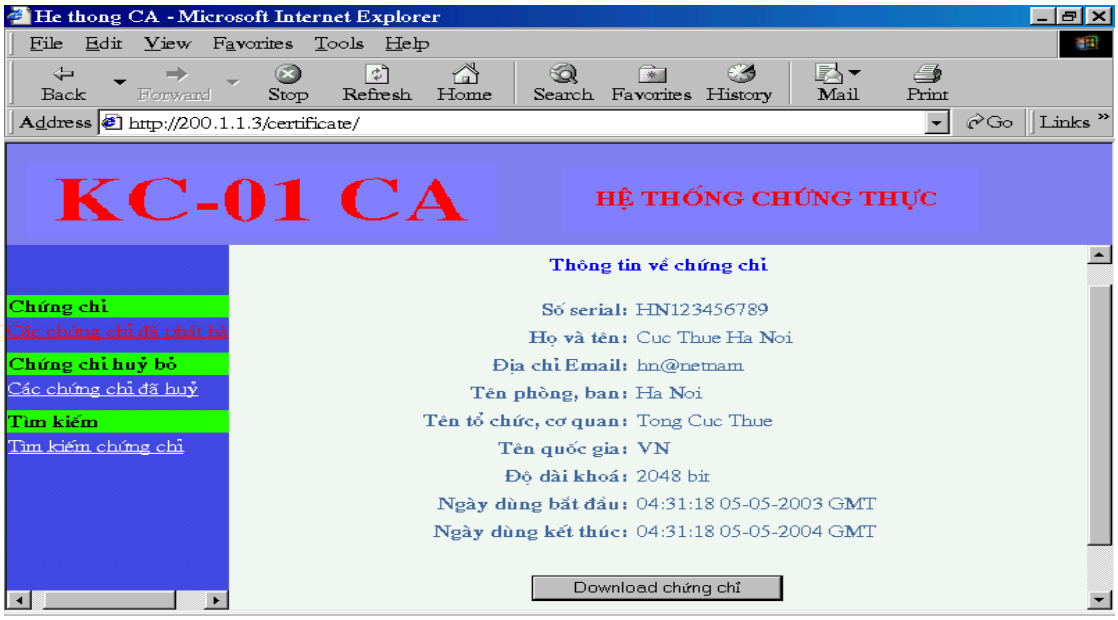


Hình 9- Kết quả xuất chứng chỉ ra LDAPServer

Khi các chứng chỉ đã được đưa vào LDAPServer mọi người dùng có thể xem và Download chứng chỉ về bằng cách vào trang Web trên LDAPServer dành cho người dùng theo địa chỉ có dạng: **http://tên_máy (hoặc địa chỉ IP)/tên trang Web phục vụ chứng chỉ** /. Ví dụ: **http://hanoi/certificate/** hoặc **http://10.64.0.252/certificate/**



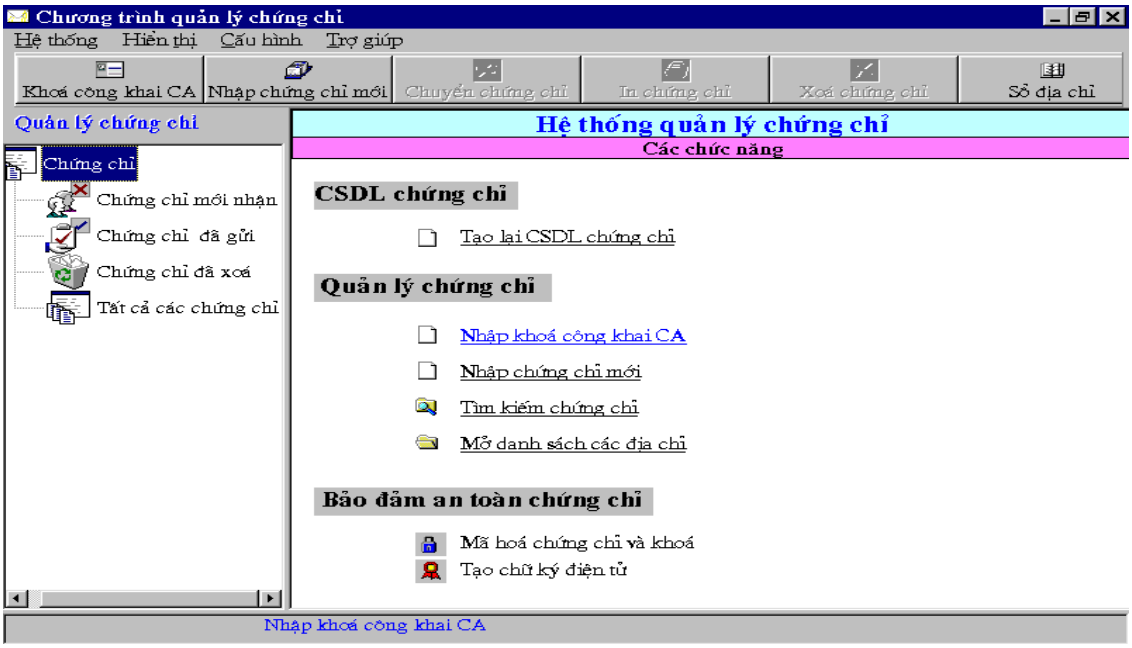
Hình 10- Trang Web phục vụ chứng chỉ cho người dùng



Hình 11 - Xem và download chứng chỉ

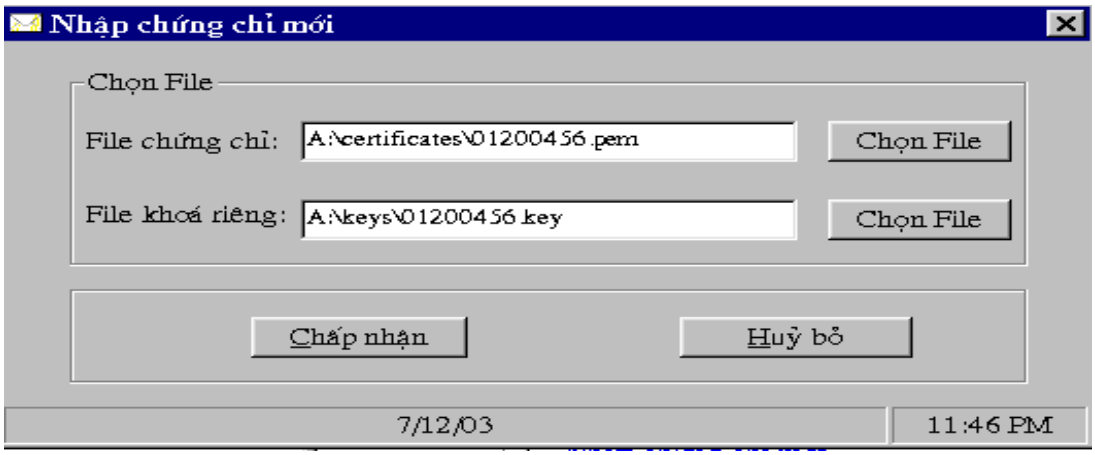
11. ĐƯA CHỨNG CHỈ VÀO RASERVER TỔNG CỤC

RAServer Tổng cục quản lý tất cả các chứng chỉ do CA cấp phát. Chạy chương trình quản lý chứng chỉ trên RAServer Tổng cục như sau: **Start-> Program -> RAServer Tong Cuc Thue-> Quản lý chứng chỉ** và đăng nhập với tên người dùng và mật khẩu mặc định là **"admin"**.



Hình 12. Chương trình quản lý chứng chỉ mức Tổng cục

Đưa đĩa mềm có lưu các chứng chỉ mà CA đã xuất ra vào ổ mềm, chọn chức năng **"Nhập chứng chỉ mới"** trên thanh công cụ.



Hình 13. Chọn file lưu chứng chỉ và file lưu khoá riêng

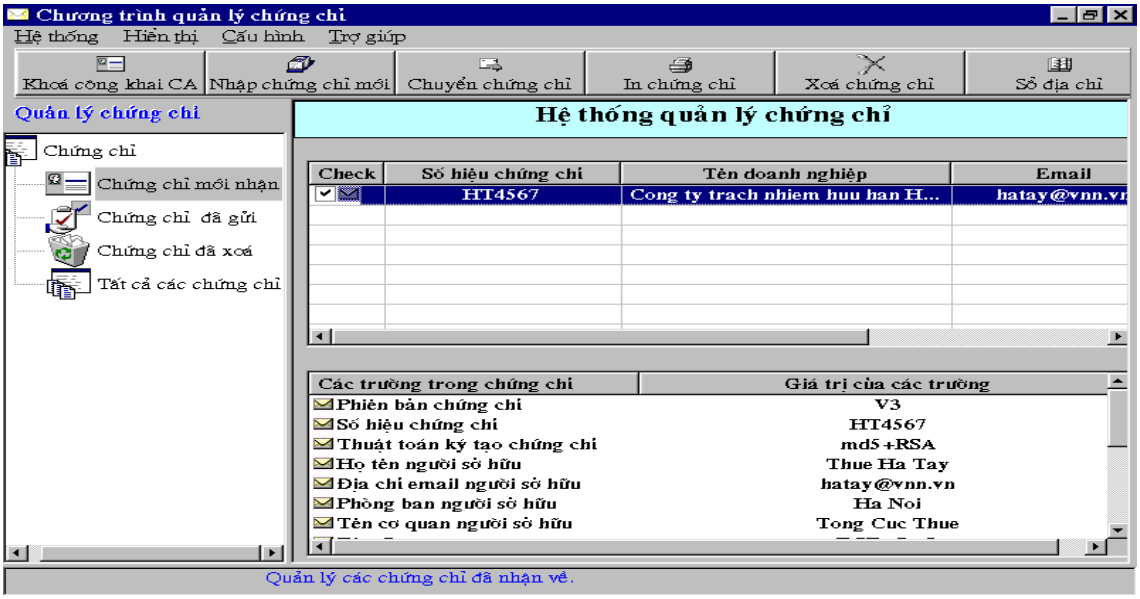
Chọn file lưu chứng chỉ và file lưu khoá riêng tương ứng trong ổ mềm rồi chọn **"Chấp nhận"**, chứng chỉ và khoá sẽ được đưa vào cơ sở dữ liệu trên Tổng cục.

12. CHUYỂN CHỨNG CHỈ VÀO VÙNG CỦA CÁC CỤC THUẾ

Sau khi chứng chỉ được đưa từ CA vào RAServer Tổng cục, người quản trị RAServer xem xét các chứng chỉ và chọn chức năng **"Chuyển chứng chỉ"** để chuyển các chứng chỉ vào các vùng tương ứng với các Cục thuế.

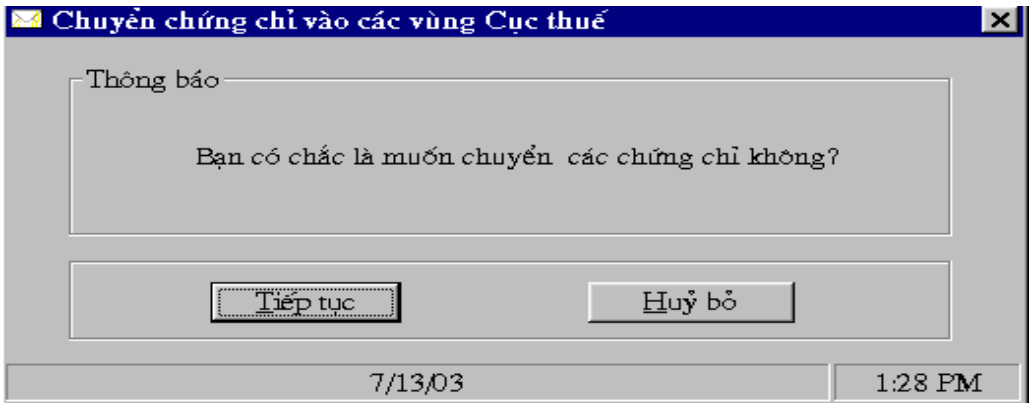
Bản gốc báo cáo không có trang 42

(Thông tin vẫn đầy đủ)



Hình 14. Xem và chuẩn bị chuyển các chứng chỉ

Chọn **"Tiếp tục"** để chuyển các chứng chỉ.



Hình 15. Chuyển chứng chỉ

IV. QUY TRÌNH SỬA ĐỔI CHỨNG CHỈ

Khi doanh nghiệp muốn sửa đổi một số thông tin trong chứng chỉ, chẳng hạn như tên doanh nghiệp, địa chỉ, kích thước khoá v.v, doanh nghiệp cần đăng ký tại Cục thuế.. Trình tự đăng ký và sửa đổi chứng chỉ cho doanh nghiệp được thực hiện như sau:

Doanh nghiệp đến gặp người quản trị tại Cục thuế xin đăng ký sửa đổi chứng chỉ và điền các thông tin cần thiết vào mẫu đăng ký. Sau đó, người quản trị tại Cục thuế xác minh lại các thông tin. Nếu thông tin nào chưa chính xác thì người quản trị yêu cầu doanh nghiệp điền lại, nếu các thông tin chính xác thì người quản trị chạy chương trình quản lý các đăng ký tại Cục thuế, ký xác nhận các đăng ký và gửi lên RAServer Tổng cục.

Tại Tổng cục các bước nhận yêu cầu, xuất yêu cầu sang CA, sửa chứng chỉ và chuyển vào vùng các Cục thuế v.v. được thực hiện tương tự như quá trình đăng ký, cấp phát chứng chỉ mới.

V. QUY TRÌNH CẤP LẠI CHỨNG CHỈ

Doanh nghiệp cần cấp lại chứng chỉ trong trường hợp chứng chỉ của doanh nghiệp bị mất hoặc đã hết hạn. Trình tự đăng ký và cấp lại chứng chỉ cho doanh nghiệp được thực hiện như sau:

Doanh nghiệp đến gặp người quản trị tại Cục thuế xin đăng ký cấp lại chứng chỉ và điền các thông tin cần thiết vào mẫu đăng ký. Sau đó, người quản trị tại Cục thuế xác minh lại các thông tin. Nếu thông tin nào chưa chính xác thì người quản trị yêu cầu doanh nghiệp điền lại, nếu các thông tin chính xác thì người quản trị chạy chương trình quản lý các đăng ký tại Cục thuế, ký xác nhận các đăng ký và gửi lên RAServer Tổng cục.

Tại Tổng cục, các bước tiếp nhận, xuất các yêu cầu sang CA, cấp lại chứng chỉ và chuyển vào vùng các Cục thuế v.v. được thực hiện tương tự như quá trình đăng ký, cấp phát chứng chỉ mới.

VI. QUY TRÌNH HUỶ BỎ CHỨNG CHỈ

1. NHẬN ĐĂNG KÝ HUỶ BỎ CHỨNG CHỈ

Khi doanh nghiệp muốn huỷ bỏ chứng chỉ vì lý do nào đó, chẳng hạn như lộ khoá. Trình tự đăng ký và huỷ bỏ chứng chỉ được thực hiện như sau:

Doanh nghiệp đến gặp người quản trị tại Cục thuế xin đăng ký huỷ bỏ chứng chỉ và điền các thông tin cần thiết vào mẫu đăng ký. Sau đó, người quản trị tại Cục thuế xác minh lại các thông tin. Nếu thông tin nào chưa chính xác thì yêu cầu doanh nghiệp điền ký lại, nếu các thông tin chính xác thì người quản trị chạy chương trình quản lý các đăng ký tại Cục thuế, ký nhận các đăng ký và gửi lên RAServer Tổng cục.

Tại Tổng cục quá trình nhận các đăng ký huỷ chứng chỉ, xuất các yêu cầu huỷ sang CA được thực hiện như nhận các đăng ký chứng chỉ mới.

2. HUỶ BỎ CHỨNG CHỈ

Người quản trị tại CA xem xét các yêu cầu huỷ bỏ chứng chỉ chờ ký đã được nhập vào CA bằng cách chọn mục **"Các yêu cầu chờ ký"** trong phần **"Yêu cầu huỷ chứng chỉ"**, nháy chuột vào số hiệu của yêu cầu để xem các thông tin trên yêu cầu. Nếu các thông tin là chính xác, người quản trị CA chọn nút **"Huỷ chứng chỉ"** để huỷ chứng chỉ có số hiệu đã đăng ký. Nếu thông tin đăng ký không chính xác, người quản trị CA có thể chọn nút **"Xoá yêu cầu"** để xoá bỏ yêu cầu huỷ chứng chỉ.

3. TẠO DANH SÁCH CHỨNG CHỈ HUỶ BỎ (CRL)

CRL là một danh sách chứa các chứng chỉ đã bị huỷ bỏ cùng với ngày giờ đã huỷ bỏ chúng và chữ ký của CA. Người quản trị CA tạo và xuất danh sách chứng chỉ huỷ bỏ bằng cách đưa đĩa mềm vào ổ sau đó chọn mục **"Xuất danh sách"** trong phần **"Chứng chỉ huỷ bỏ"**. Khi đó danh sách chứng chỉ bị huỷ bỏ sẽ được tạo và xuất ra thư mục CRL trên đĩa mềm.

4. NHẬP DANH SÁCH CHỨNG CHỈ HUỶ BỎ VÀO LDAPSERVER

Chuyển đĩa mềm có chứa danh sách chứng chỉ bị huỷ bỏ vừa tạo ra vào LDAPServer. Vào trang Web dành cho người quản trị LDAPServer, chọn chức năng **"Nhập danh sách"** trong mục **"Chứng chỉ huỷ bỏ"**.

5. XUẤT DANH SÁCH CHỨNG CHỈ HUỶ BỎ

Để mọi doanh nghiệp có nhu cầu sử dụng chứng chỉ đều biết chứng chỉ của những doanh nghiệp nào đã bị hủy bỏ thì danh sách chứng chỉ huỷ phải được công khai trên trang Web của LDAPServer. Người quản trị LDAPServer thực hiện việc này bằng cách chọn mục **"Xuất danh sách ra LDAP"** trong phần **"Chứng chỉ huỷ bỏ"** trên trang Web dành cho người quản trị LDAPServer.

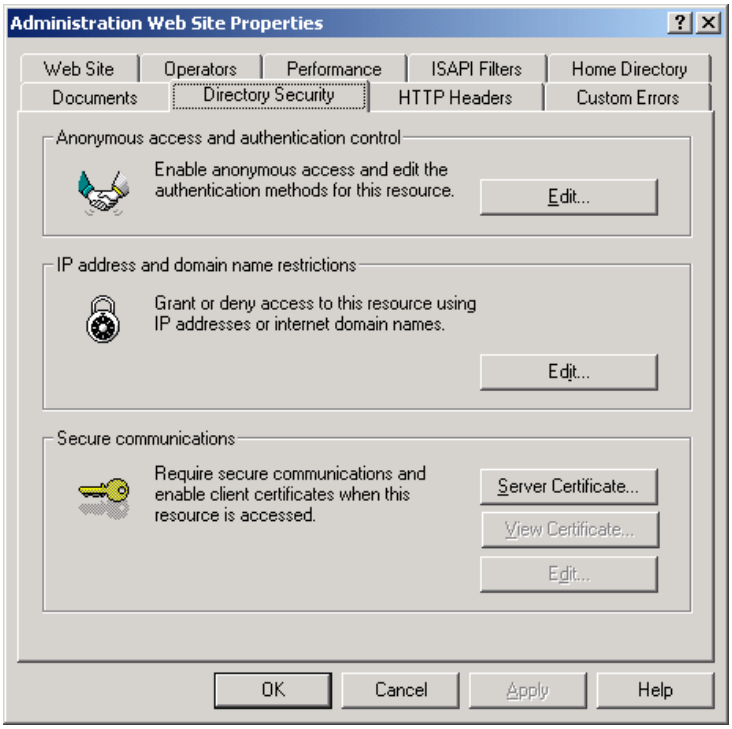
HƯỚNG DẪN CÀI ĐẶT MỘT CHỨNG CHỈ CHO MỘT TRANG WEB

Phần này sẽ hướng dẫn cách tích hợp một chứng chỉ được tạo ra bởi hệ thống CA để bảo vệ một trang Web.

I/ Cài đặt chứng chỉ cho IIS

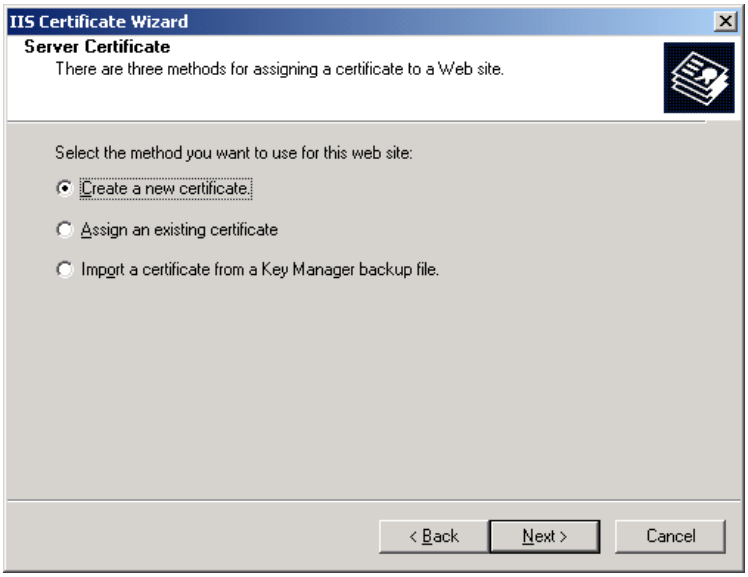
Để cài đặt 1 chứng chỉ cho 1 trang web trên IIS 5.0 trên Windows2000 Server:

- Khởi động chương trình Internet Service Management
- Chọn trang web cần cài đặt chứng chỉ, nhấn phím phải chuột, chọn Properties
- Chọn Directory Security, nhấn vào nút Server Certificate



- Winzard để cài đặt chứng chỉ sẽ hiện ra

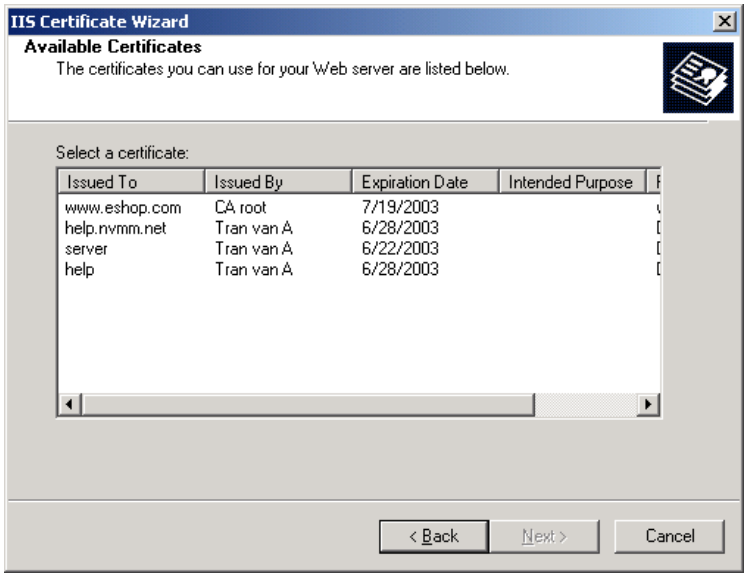
- Bấm vào nút Next để tiếp tục



- Ở đây có 3 tùy chọn:
  - Tạo 1 certificate mới: Khi chọn chức năng này, IIS sẽ thực sinh ra 1 cặp khóa công khai, cất giữ khóa vào cơ sở dữ liệu của hệ thống và sau đó sinh 1 yêu cầu cấp chứng chỉ để người quản trị gửi đi ký bởi 1 CA nào đó
  - Chọn 1 chứng chỉ có sẵn trong hệ thống và gán cho trang web.
  - Nhập chứng chỉ và khóa riêng được cất giữ trong 1 tệp được tạo ra bởi chương trình Key Manager vốn có sẵn trên Windows NT 4.0. Chức năng này được sử dụng trong trường hợp máy chủ được nâng cấp từ Windows NT lên Windows 2000 và người quản trị muốn sử dụng lại các chứng chỉ đã có sẵn từ trước.

Trong trường hợp hệ thống hiện có, toàn bộ khóa và chứng chỉ được nhập vào từ bên ngoài nên ta sẽ chỉ quan tâm đến chức năng thứ hai: Lựa chọn 1 chứng chỉ có sẵn trong hệ thống. Chứng chỉ sẽ được đưa vào hệ thống nhờ chương trình ***mmc*** của Micrsoft

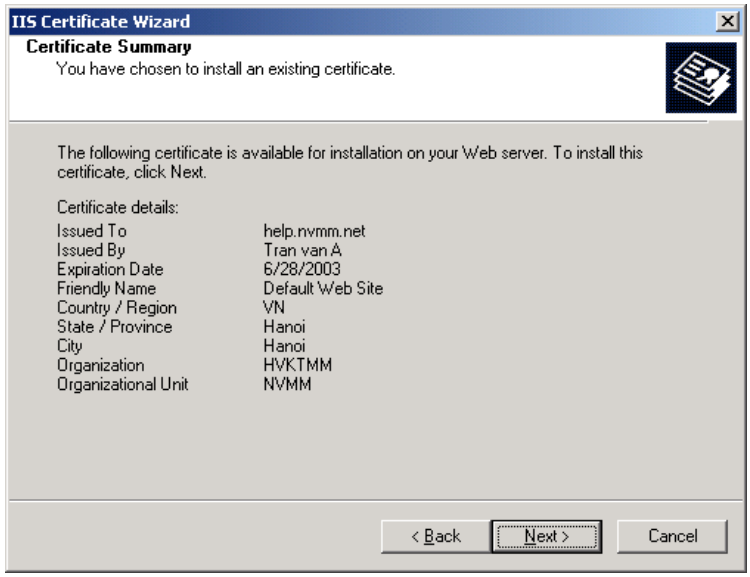
Để sử dụng chức năng này, chọn "Assign an existing certificate" rồi bấm nút Next. Một danh sách các chứng chỉ có thể dùng để gán cho trang web sẽ hiện ra. Những chứng chỉ này là những chứng chỉ được coi là của cá nhân (chỉ của riêng máy này), không được là chứng chỉ của 1 CA (người cấp chứng chỉ) và chưa được gán cho trang web khác trên cùng máy chủ.



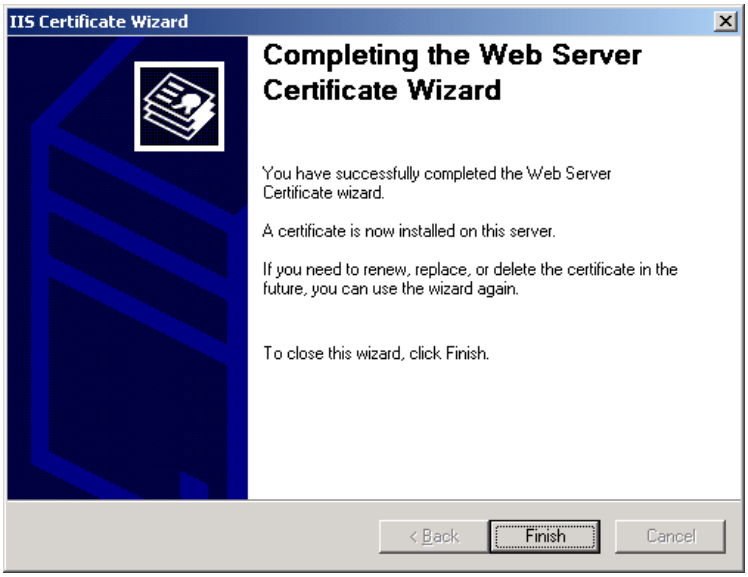
Ta chỉ việc chọn 1 chứng chỉ thích hợp rồi nhấn vào nút Next. Một chứng chỉ thích hợp là 1 chứng chỉ:

- Còn thời hạn sử dụng.
- Được cấp cho đúng trang web này (giá trị trường **cn** bằng đúng tên trang web, ví dụ: ecommerce.com.vn)
- Được ký bởi 1 CA mà người dùng (khách hàng truy cập trang web từ trình duyệt web) tin tưởng.

Sau khi 1 chứng chỉ đã được lựa chọn, thông tin về chứng chỉ sẽ được liệt kê ra.



Để quyết định việc sử dụng chứng chỉ này, ta nhấn nút Next.



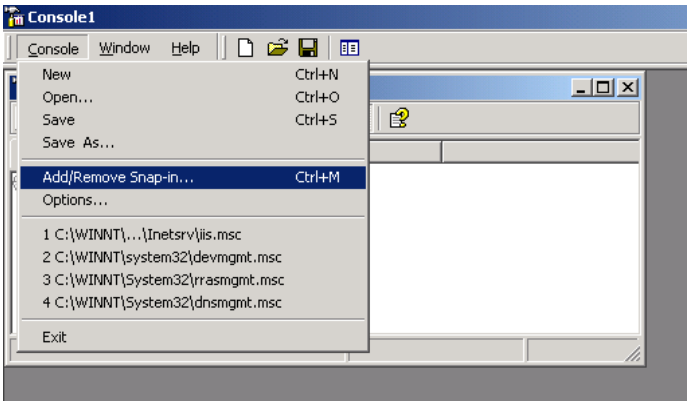
Nhấn nút Finish để kết thúc.

II/ Sử dụng mmc để cài đặt một chứng chỉ vào hệ thống

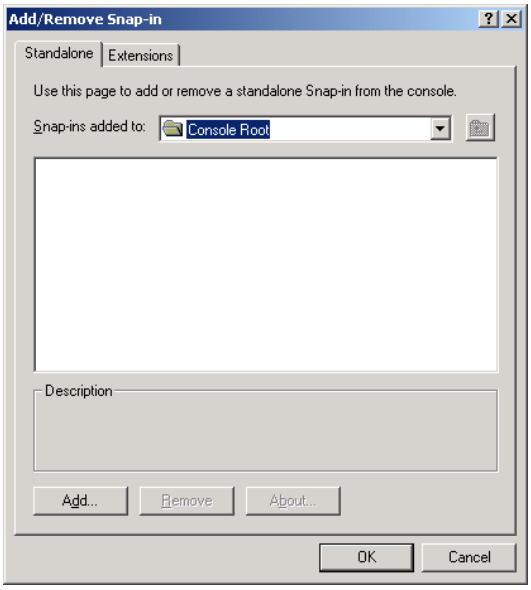
MMC (Microsoft Management Console) là 1 tiện ích thông qua nó ta có thể sử dụng các chức năng của hệ điều hành để quản lý phần cứng, phần mềm, và các thành phần mạng trong Windows 2000. Sử dụng MMC, ta có thể tạo ra những biểu tượng riêng biệt cho những chức năng khác nhau hoặc có thể gộp chung nhiều chức năng lại trong một cửa sổ.

Để tạo riêng 1 biểu tượng cho việc quản lý chứng chỉ trên máy chủ ta cần thực hiện những bước sau:

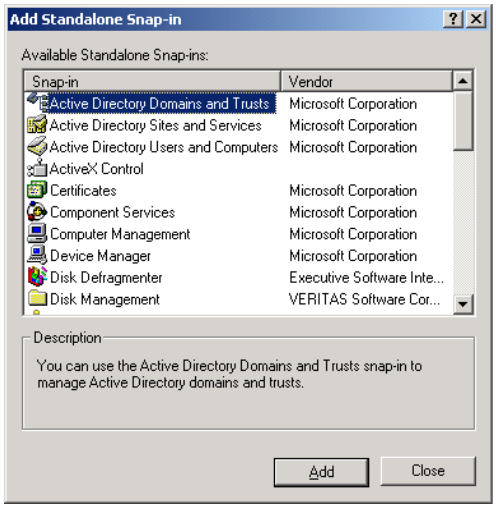
1. Chọn Run từ menu Start
2. Gõ vào MMC và nhấn vào nút OK
3. Trong cửa sổ của MMC, chọn menu Console, sau đó chọn tiếp "Add/Remove Snap-in"



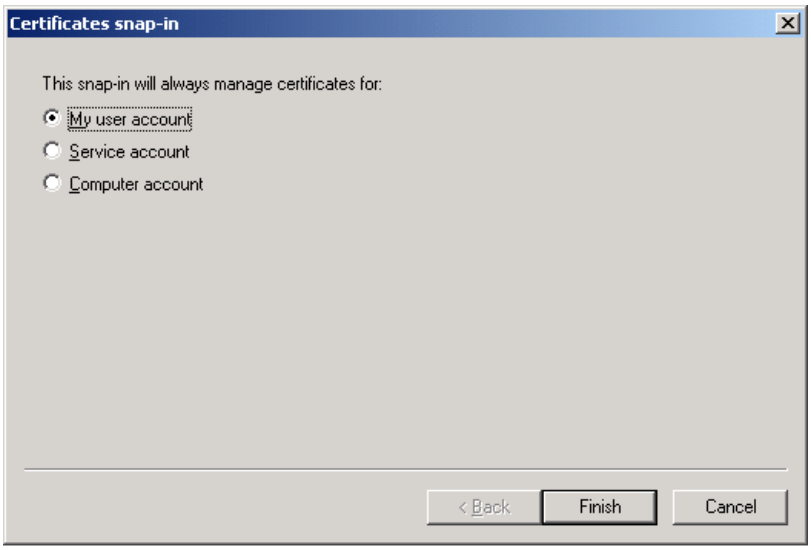
4. Nhấn vào nút Add trong hộp hội thoại



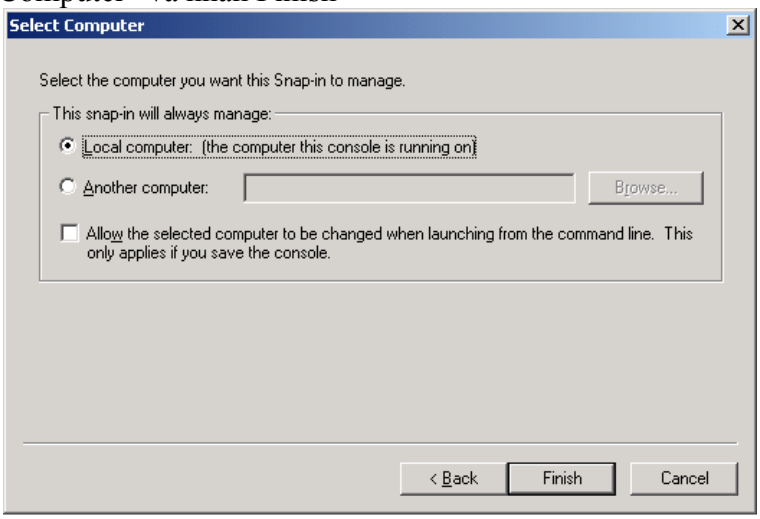
5. Chọn Certificate và nhấn vào nút Add



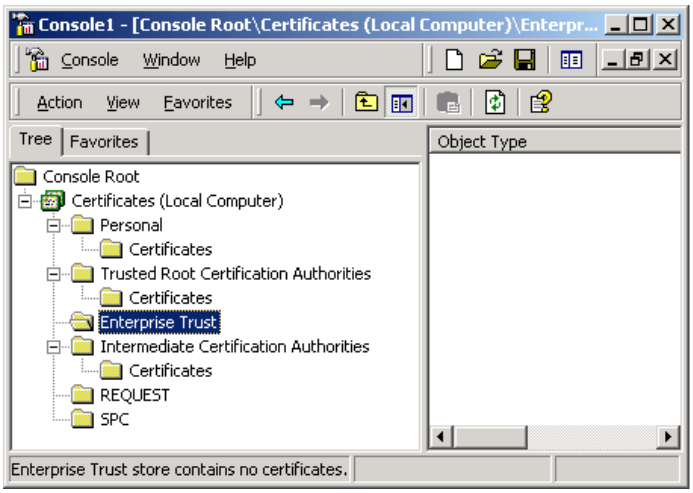
Chọn tiếp “Computer account” và nhấn vào nút Finish.



7. Chọn tiếp “Local Computer” và nhấn Finish



6. Trong cửa sổ của MMC sẽ xuất hiện mục quản lý chứng chỉ cho máy chủ chư sau



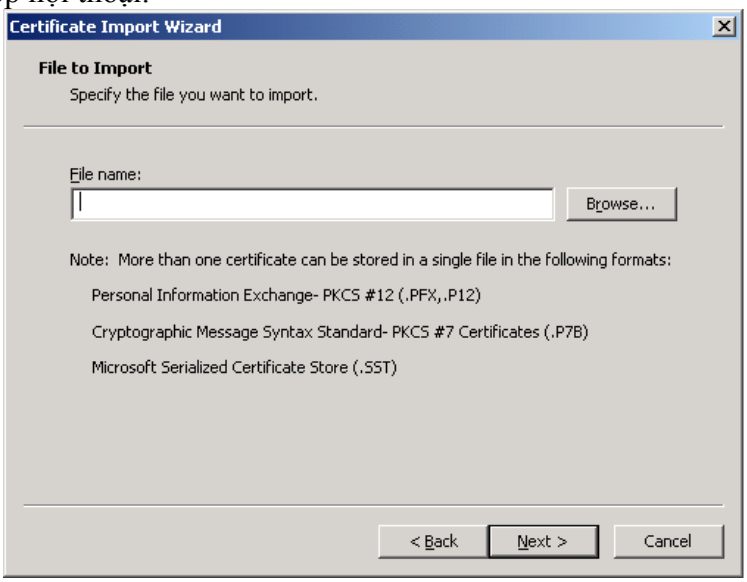
Các chứng chỉ trên máy chủ được chia làm 4 loại:

- Personal Certificate
- Trusted Root Cerfiticate
- Enterprise Trust
- Intermediate Certificate

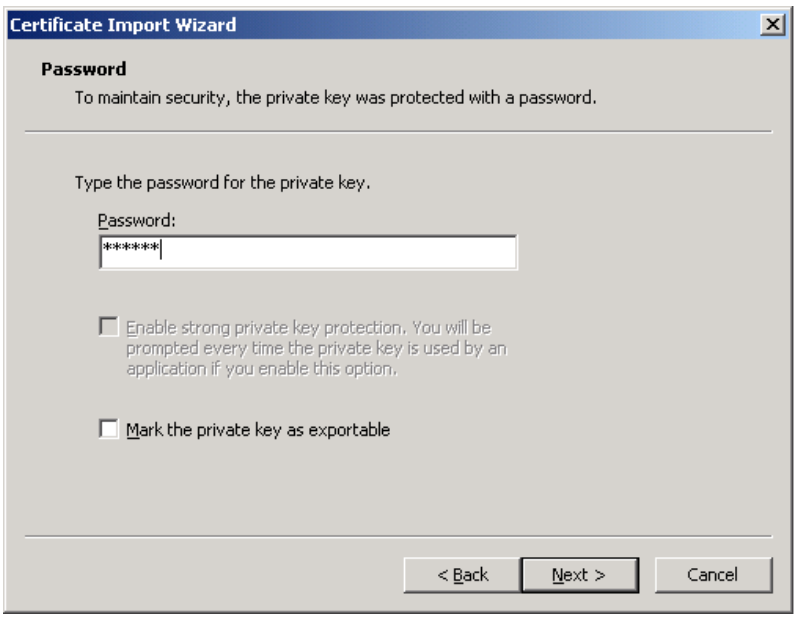
Để chứng chỉ có thể sử dụng cho 1 trang web, nó cần được cài đặt vào phần Personal Certificate. Thủ tục cài đặt như sau:

1. Chọn “Personal Certificate”, nhấn phím phải chuột và chọn “All task”, “Import”

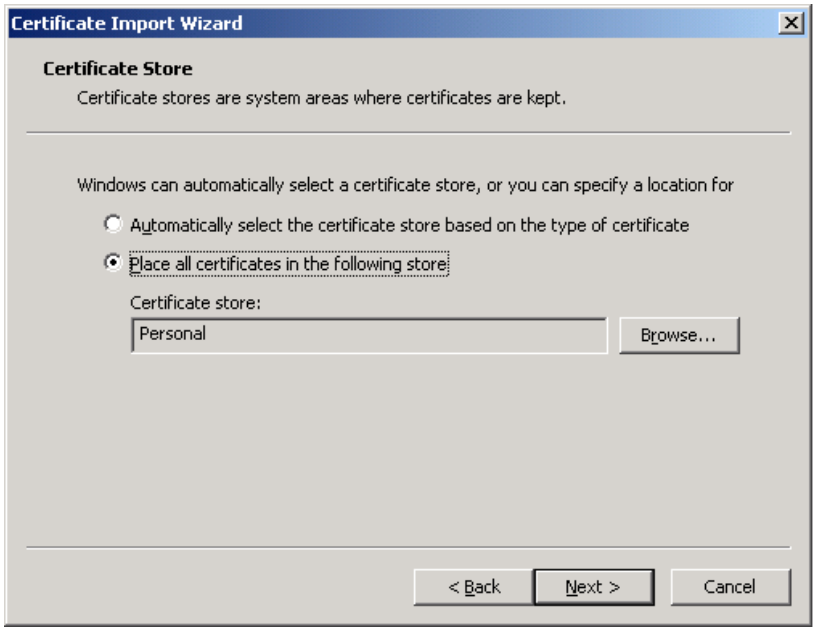
2. Sau khi nhấn nút Next, ta gõ vào tên tệp chứa chứng chỉ và khóa (ta cũng có thể nhấn vào nút Browse để chọn tệp). Tệp được chọn phải có khuôn dạng thuộc 1 trong 3 loại đã được liệt kê trên hộp hội thoại.



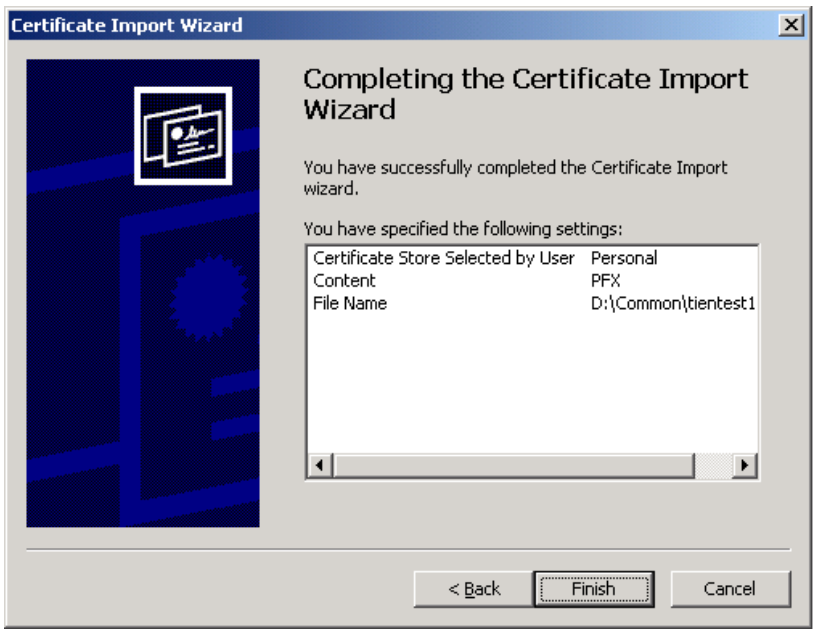
2. Tiếp theo cần gõ vào password nếu như tệp được bảo vệ bằng password.



3. Chọn mục để cất giữ chứng chỉ. Ở đây ta cần chọn Personal.



5. Nhấn nút Finish để kết thúc.



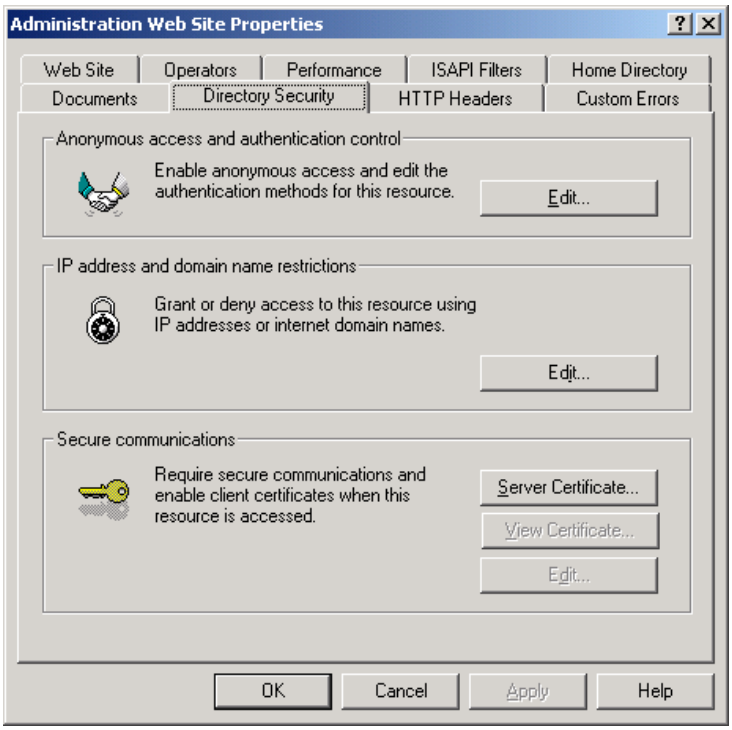
III/ Cài đặt chức năng yêu cầu xác thực người sử dụng qua chứng chỉ

Yêu cầu về hệ thống chứng chỉ:

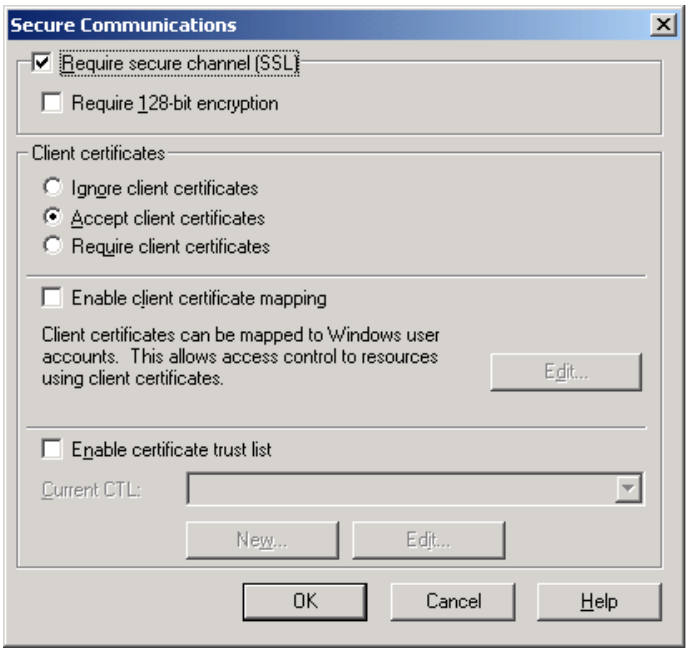
Cả web server và web browser đều cùng tin tưởng vào 1 nhà cung cấp chứng chỉ (CA). Chính nhà cung cấp chứng chỉ này sẽ ký các chứng chỉ cho người sử dụng.

Cài đặt web server:

- Khởi động chương trình Internet Service Management
- Chọn trang web cần cài đặt chứng chỉ, nhấn phím phải chuột, chọn Properties
- Chọn Directory Security, nhấn vào nút Edit



- Check vào ô “Require secure channel (SSL)” và chọn “Require client certificates”



- Nhấn nút OK để kết thúc.

Cài đặt web browser

1. Cài đặt Internet Explorer

Trên thanh menu chọn Tools\Internet Options…, sau đó chọn tiếp Content