

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM
CỤC CÔNG NGHỆ TIN HỌC

**Tài liệu hướng dẫn Gia hạn chứng thư số
lưu trên iKey 1032, eToken Pro
hoặc iKey 2032**

Hà Nội 04/2013



MỤC LỤC

I. Tổng quan.....	3
1. Mục đích.....	3
2. Phạm vi áp dụng.....	3
3. Các từ viết tắt	3
II. Cài đặt Entrust Entelligence Security Provider 9.1	3
1. Tải phần mềm EPS.....	3
2. Cài đặt phần mềm EPS.....	4
III. Gia hạn CTS và Update CTS về thiết bị lưu trữ.....	8
1. Các bước thực hiện trước khi Update CTS.....	8
2. Thực hiện Update CTS	18
3. Kiểm tra thông tin CTS sau khi Update.....	20
IV. Thông tin liên lạc hỗ trợ.....	27



I. Tổng quan

1. Mục đích

Tài liệu này hướng dẫn các tổ chức, cá nhân thực hiện Gia hạn chứng thư số và sử dụng phần mềm Entrust Entelligence Security Provider (ESP) để Update Chứng thư số vào thiết bị lưu trữ (iKey 1032, iKey 2032, eToken Pro...).

2. Phạm vi áp dụng

a. Đối tượng

Các tổ chức, cá nhân được Tổ chức cung cấp dịch vụ chứng thực chữ ký số NHNN (CA-NHNN) cấp chứng thư số, sau đây gọi là người sử dụng.

b. Điều kiện sử dụng

Người sử dụng có kết nối mạng NHNN qua NHNN chi nhánh tỉnh/thành phố hoặc qua Cục Công nghệ tin học.

3. Các từ viết tắt

Trong tài liệu này, những từ dưới đây được hiểu như sau:

- NHNN: Ngân hàng Nhà nước Việt Nam
- TCTD: Tổ chức tín dụng
- CTS: Chứng thư số
- ESP: Entelligence Security Provider
- CNTH: Công nghệ tin học

II. Cài đặt Entrust Entelligence Security Provider 9.1

1. Tải phần mềm EPS

Phần mềm **Entrust Entelligence Security Provider 9.1** dùng để kích hoạt CTS của người sử dụng vào thiết bị lưu trữ iKey. Phần mềm này có tại địa chỉ <http://www.sbv.gov.vn> chuyên mục: **Hệ thống chữ ký số và chứng**



thực số/Phần mềm kích hoạt chứng thư số Entrust Intelligence Security Provider.

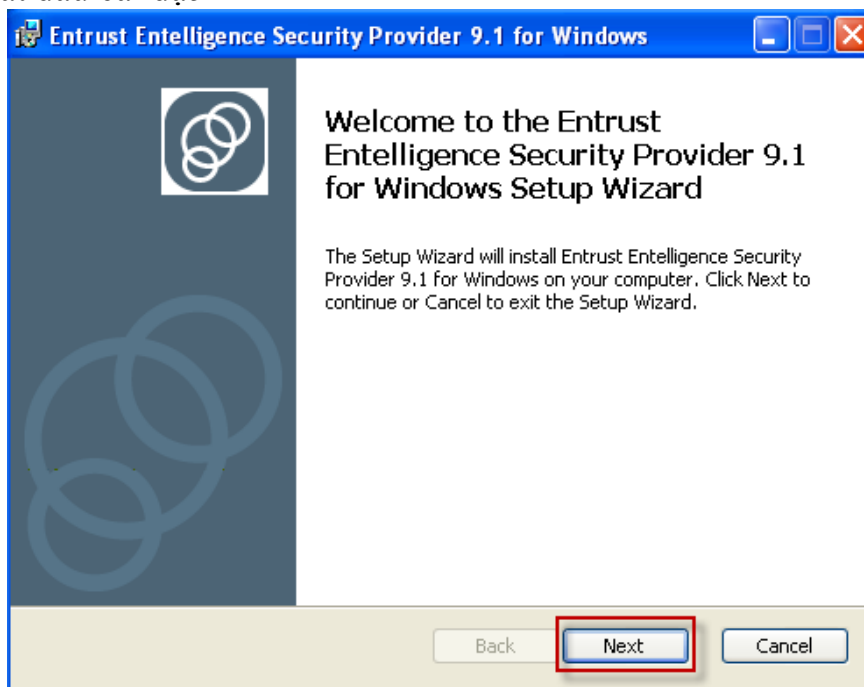
2. Cài đặt phần mềm EPS

Bước 1:

- Mở thư mục chứa bộ cài phần mềm **Entrust Intelligence Security Provider**.

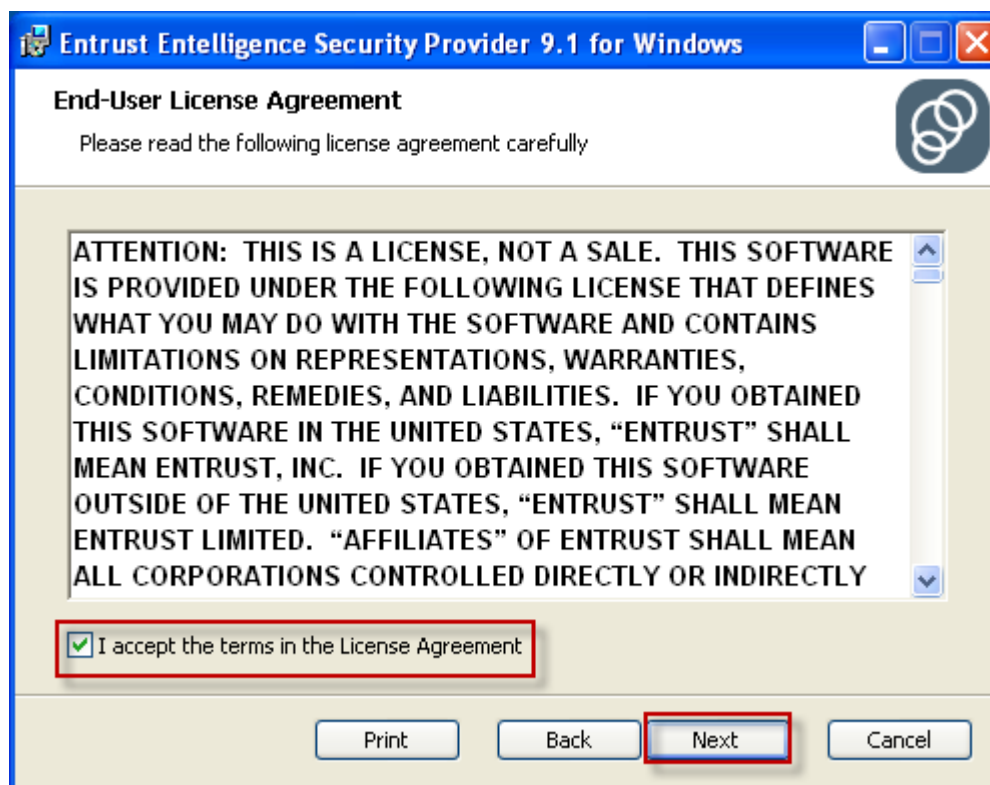
Name	Size	Type	Date Modified
AncillaryLicenses.txt	13 KB	Text Document	4/30/2009 8:14 AM
eecustwiz.exe	1,503 KB	Application	7/27/2010 5:07 PM
eespwin32.msi	8,640 KB	Windows Installer P...	2/12/2010 3:28 AM
eespwin32.mst	8 KB	MST File	2/22/2013 10:44 AM
entrust.ini	5 KB	Configuration Settings	2/21/2013 2:44 PM
entrustra.ini	1 KB	Configuration Settings	2/21/2013 2:44 PM
license.txt	22 KB	Text Document	11/16/2009 11:34 AM
setup.exe	62 KB	Application	2/12/2010 3:28 AM
setup.ini	1 KB	Configuration Settings	2/21/2013 3:41 PM

Nhấp chuột vào file **Setup.exe**, hộp thoại chào mừng hiện thị, nhấp chuột vào **Next** để bắt đầu cài đặt

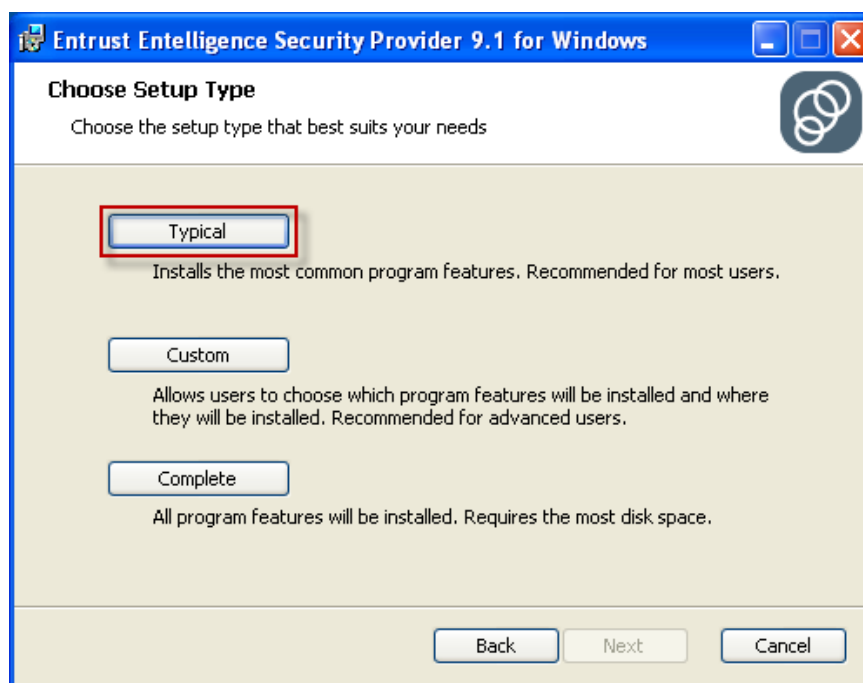


**Bước 2:**

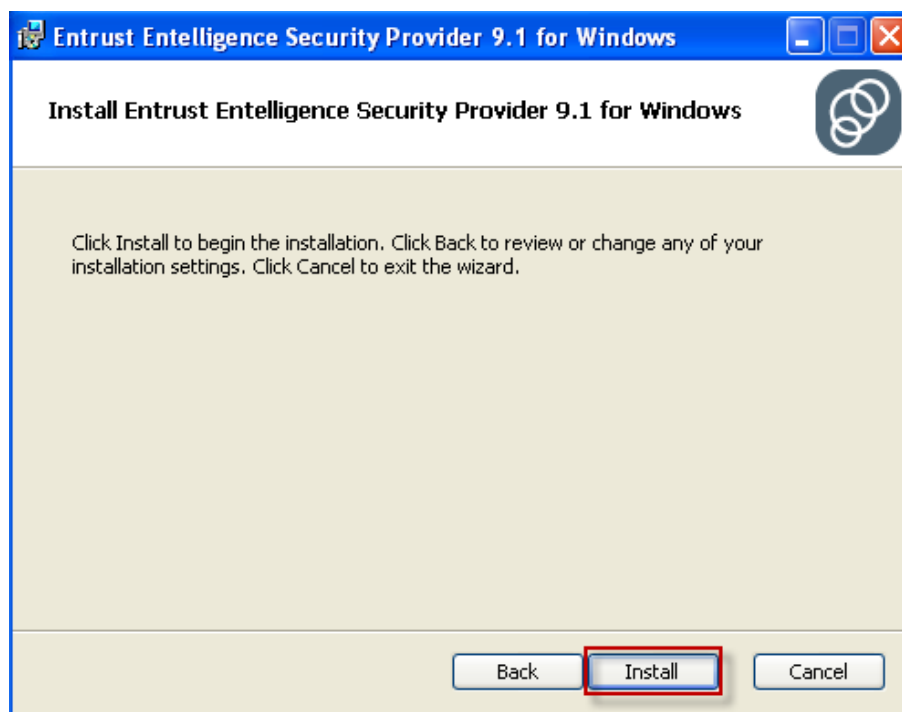
Tích vào ô **I accept the terms in the license agreement** và nhấp chuột vào **Next**

**Bước 3:**

Chọn loại cài đặt, chọn **Typical** rồi nhấn **Next**.

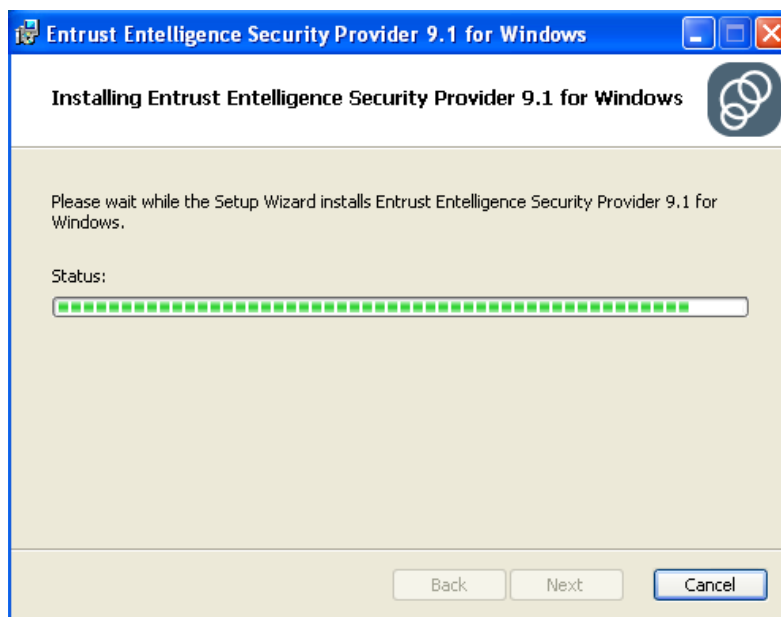
**Bước 4:**

Sẵn sàng cài đặt, nhấp chuột vào Next bắt đầu cài đặt chương trình

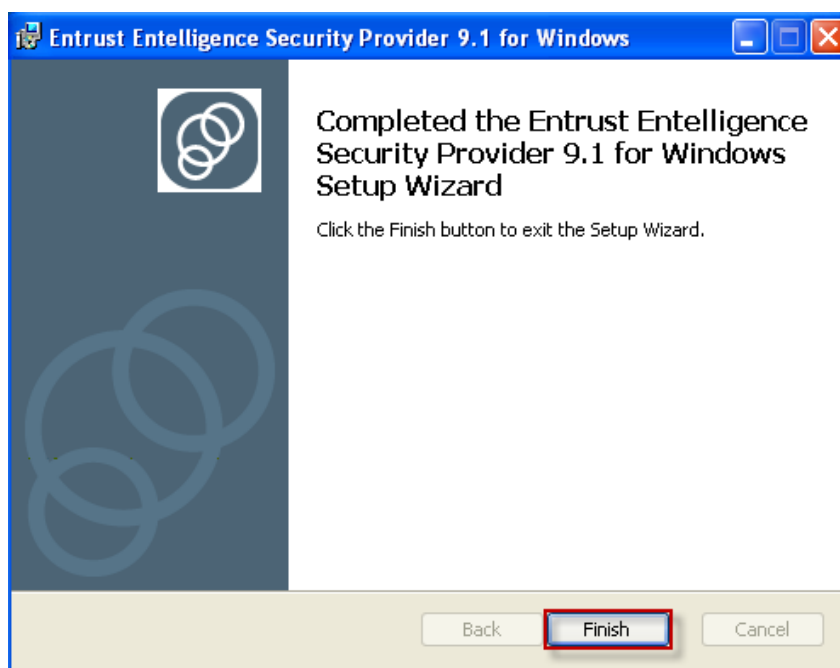


Bước 5:

Chờ vài phút để hệ thống cài đặt

**Bước 6:**

Nhấp chuột vào **Finish** để kết thúc quá trình cài đặt.





Sau khi cài đặt thành công sẽ có biểu tượng  ở System Tray.

III. Gia hạn CTS và Update CTS về thiết bị lưu trữ

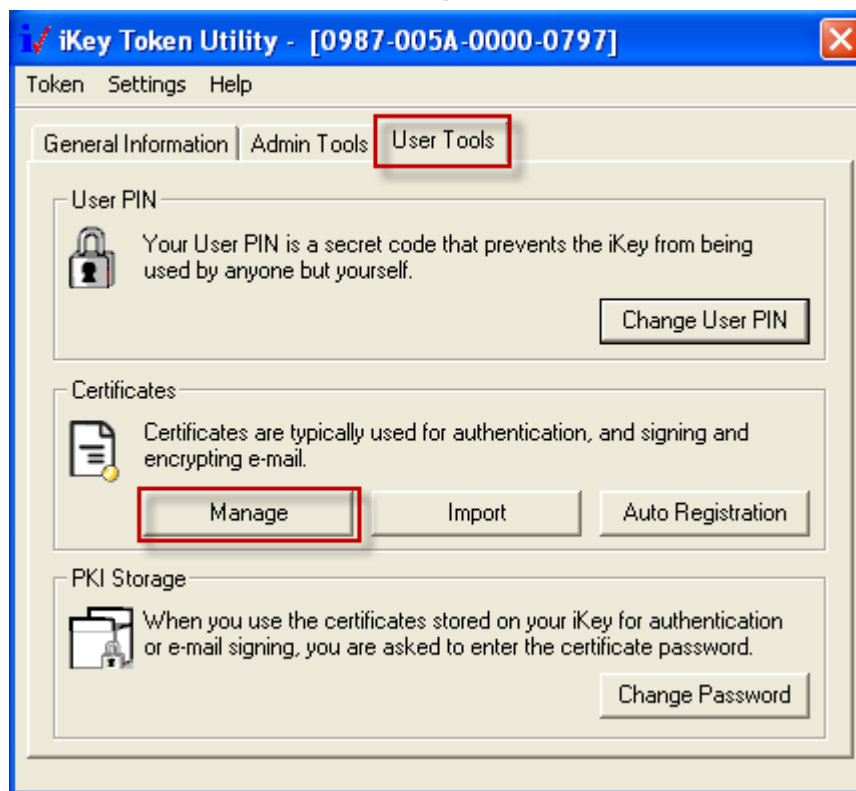
Để Gia hạn và Update CTS người sử dụng phải thực hiện tuần tự theo đúng các bước sau:

1. Các bước thực hiện trước khi Update CTS

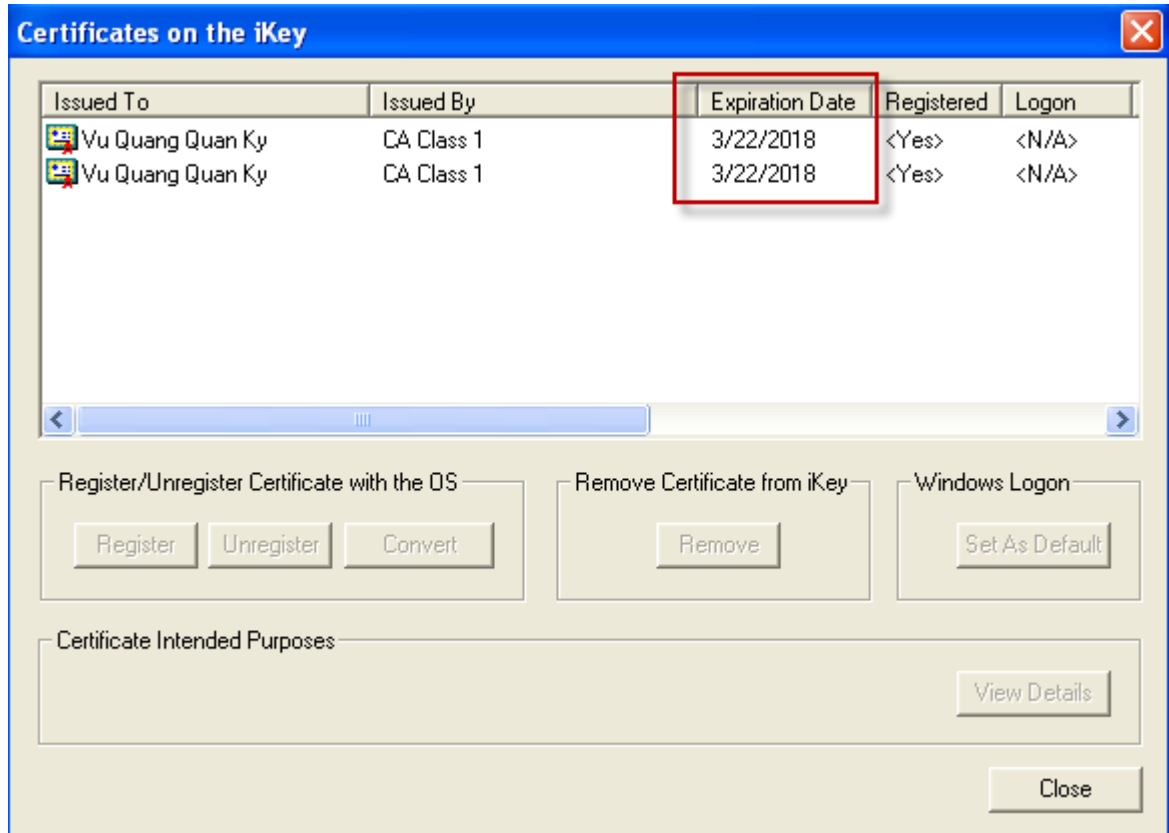
Bước 1:

a. Kiểm tra thời hạn sử dụng của CTS

- Mở **iKey Token Utility** bằng cách click đúp vào biểu tượng .
- Chọn tab **User Tools**, nhấn nút **Manage**.



- Thông tin CTS sẽ hiện ra:



- Tại Tab **Expiration Date** cho biết thời gian hết hiệu lực của CTS (như hình trên CTS có thời hạn hết hiệu lực là 22/03/2018).

b. Làm thủ tục gia hạn CTS

- Trước khi CTS hết hạn ít nhất 30 ngày, người sử dụng phải làm thủ tục gia hạn CTS (Mẫu số 02- Giấy đề nghị gia hạn chứng thư số tại Thông tư 12/2011/TT-NHNN ngày 17/05/2011) và gửi về Phòng CA- Cục CNTH-NHNN.

Bước 2:

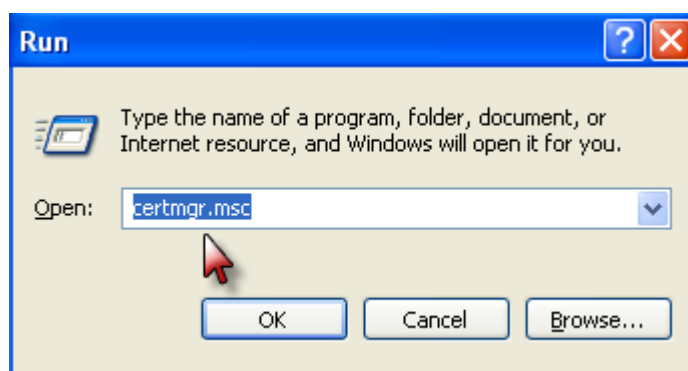
a. Cài đặt phần mềm Entrust Entelligence Security Provider 9.1

b. Cài đặt phần mềm quản lý iKey

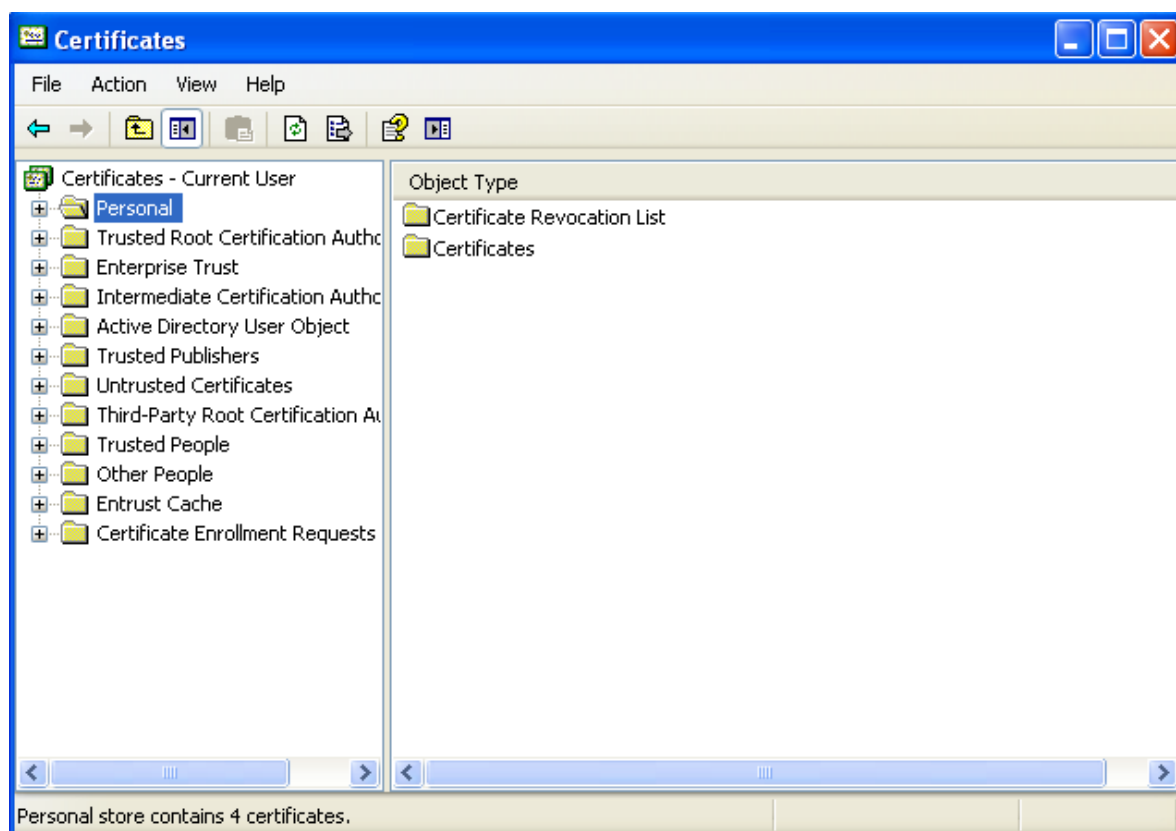
Bước 3:

Xóa các CTS cũ lưu trên máy của người sử dụng:

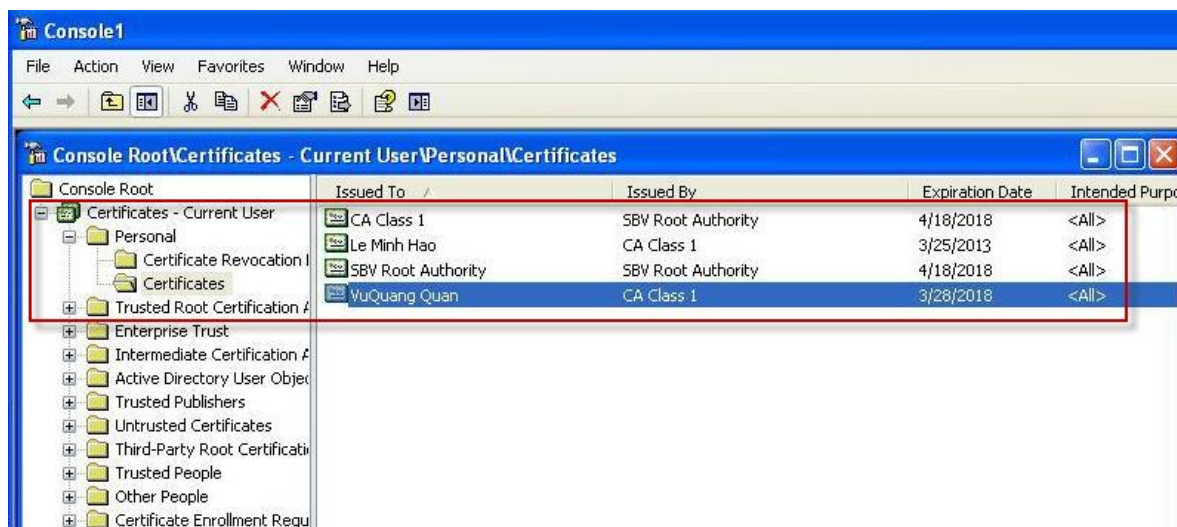
Chọn **Start/ run**, gõ **certmgr.msc** trong hộp thoại **Open**:



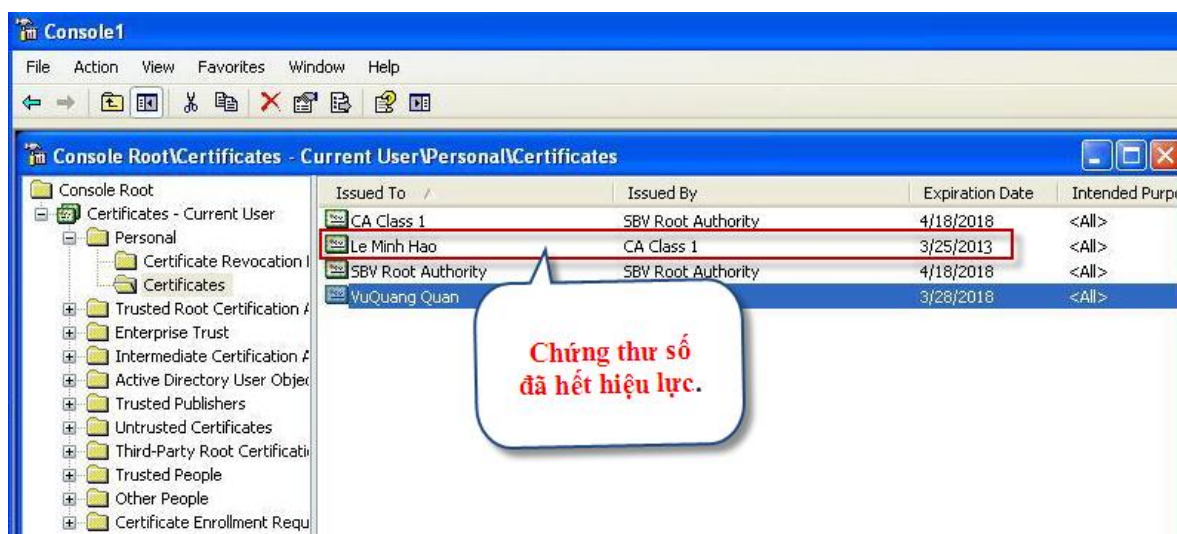
Màn hình **Certificates** hiện ra:

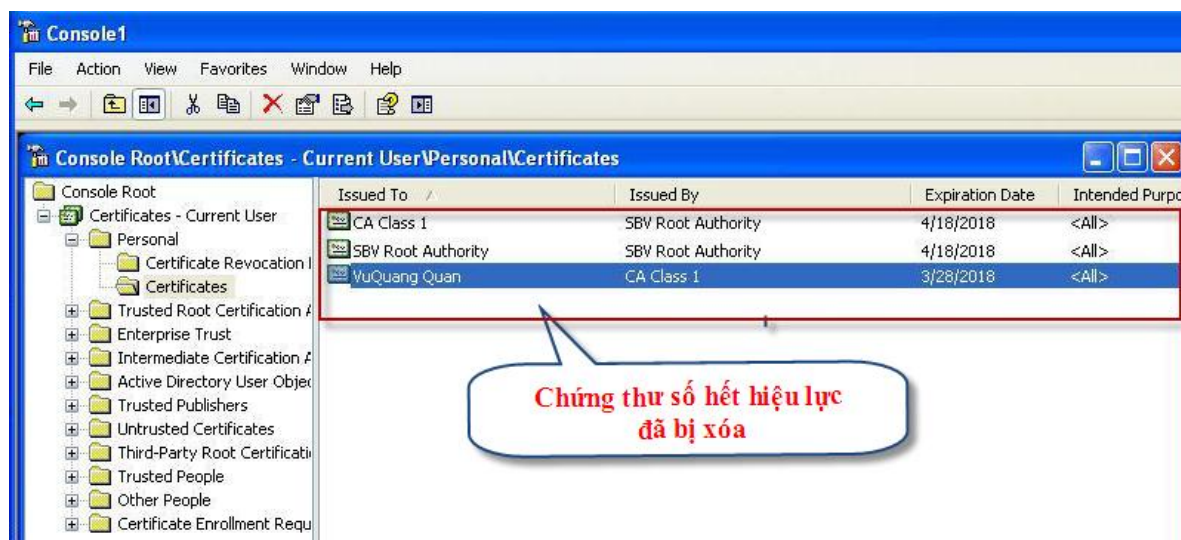
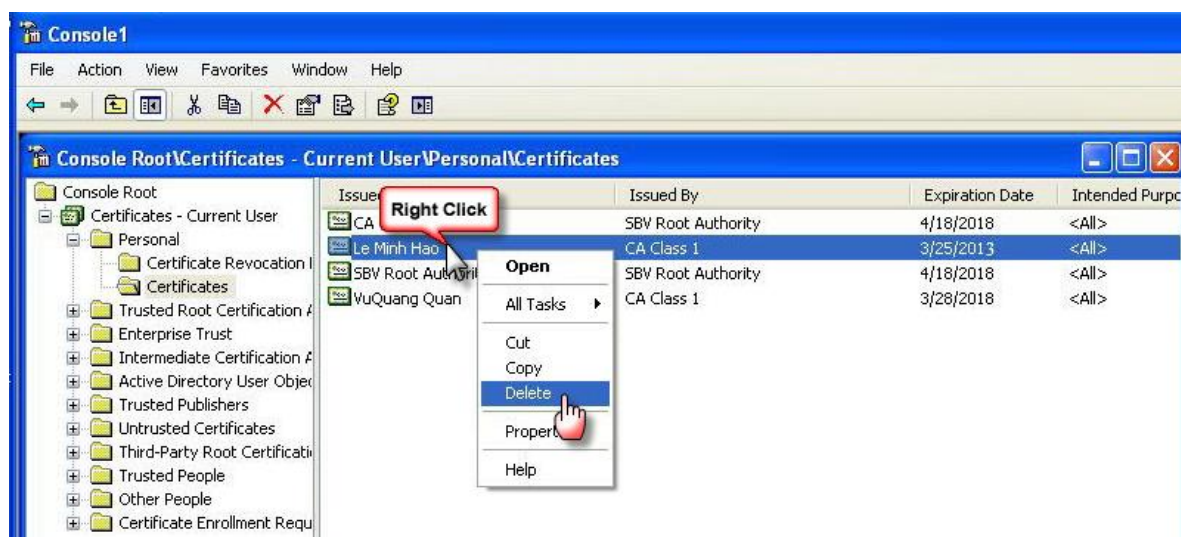


Tại màn hình **Certificates**, chọn mục **Certificates – Current User -> Personal -> Certificates**. Thông tin các CTS cũ được lưu tại đây.



Chọn các CTS cũ hết hiệu lực (so sánh thời gian tương ứng của dòng CTS tại cột **Expiration Date** với thời gian hiện tại), nhấp chuột phải vào dòng CTS cũ đó và nhấn **Delete** (Ví dụ ở đây là dòng CTS khoanh đỏ như hình dưới).





Bước 4:

4.1. Tạo kết nối mạng thành công tới NHNN:

Lưu ý: Chỉ những người sử dụng không thuộc NHNN mới phải thực hiện Bước 4.1 này.

Người sử dụng tạo kết nối mạng NHNN bằng một trong các cách sau:

a. Kết nối VPN- NHNN

Các TCTD thực hiện triển khai kết nối VPN tới NHNN (sử dụng các đường truyền: Megawan, Metronet...) truy cập vào địa chỉ <http://sbv.gov.vn> chuyên

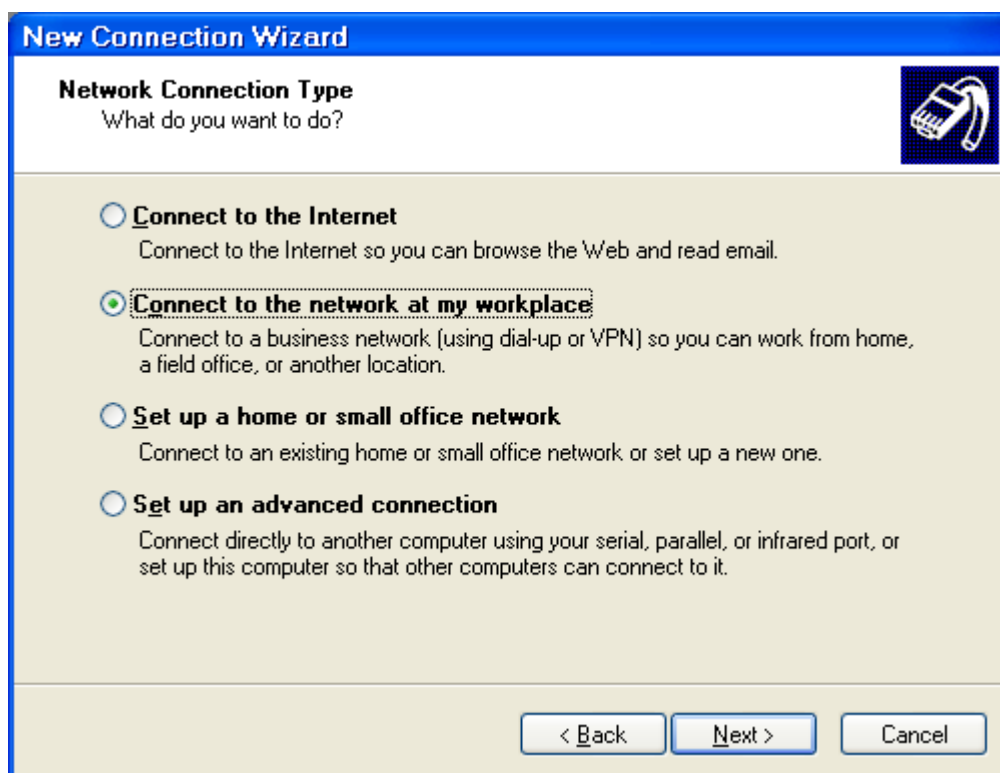
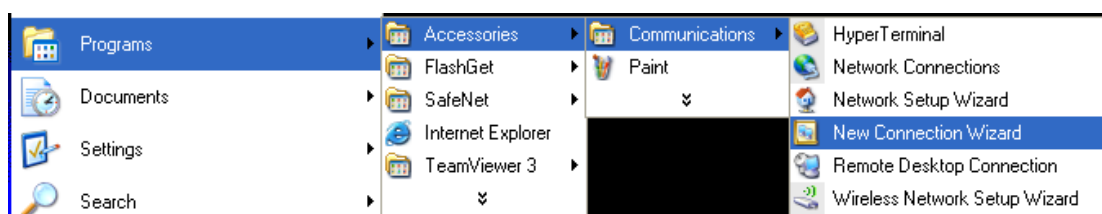
mục: *Các hoạt động khác của NHTW* → *Công nghệ thông tin-Truyền thông* → *Hỗ trợ kỹ thuật* tải phần mềm, tài liệu và thực hiện theo hướng dẫn kết nối VPN tới NHNN.

b. Kết nối Leased line

Các TCTD có kết nối Leased line với NHNN thì thực hiện ngay Bước 4.2. **Kiểm tra kết nối mạng với NHNN.**

c. Kết nối Dialup (**khuyến nghị hạn chế sử dụng**)

Các bước thực hiện kết nối quay số (dial-up) như sau:





New Connection Wizard

Network Connection
How do you want to connect to the network at your workplace?

Create the following connection:

☒ **Dial-up connection**
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

☐ **Virtual Private Network connection**
Connect to the network using a virtual private network (VPN) connection over the Internet.

< Back Next > Cancel

New Connection Wizard

Connection Name
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

SBV CA

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back Next > Cancel



New Connection Wizard

Phone Number to Dial
What is the phone number you will use to make this connection?

Type the phone number below.

Phone number:

You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.

< Back Next > Cancel

New Connection Wizard

 **Completing the New Connection Wizard**

You have successfully completed the steps needed to create the following connection:

SBV CA

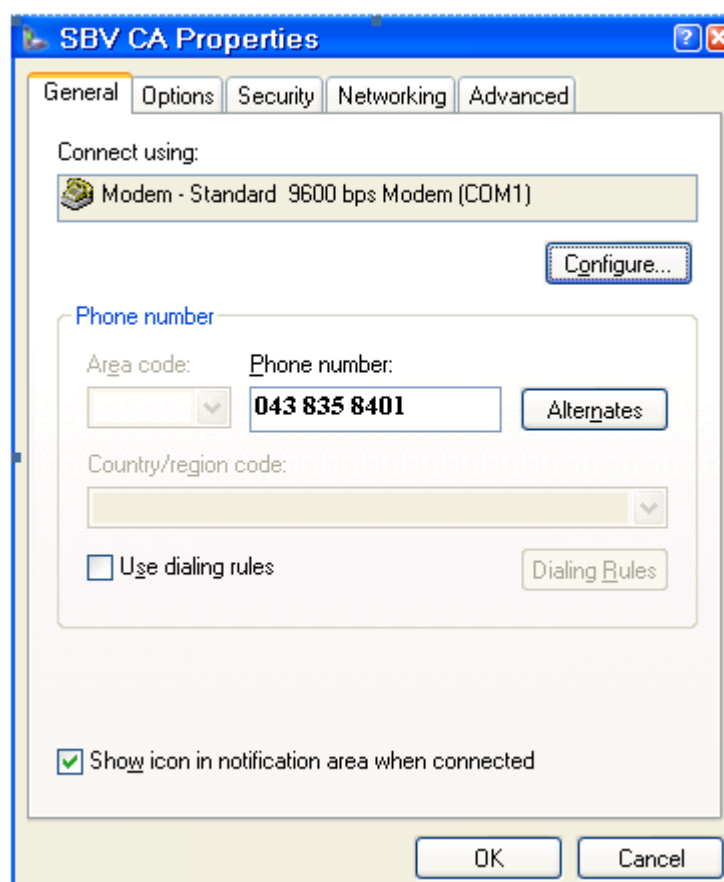
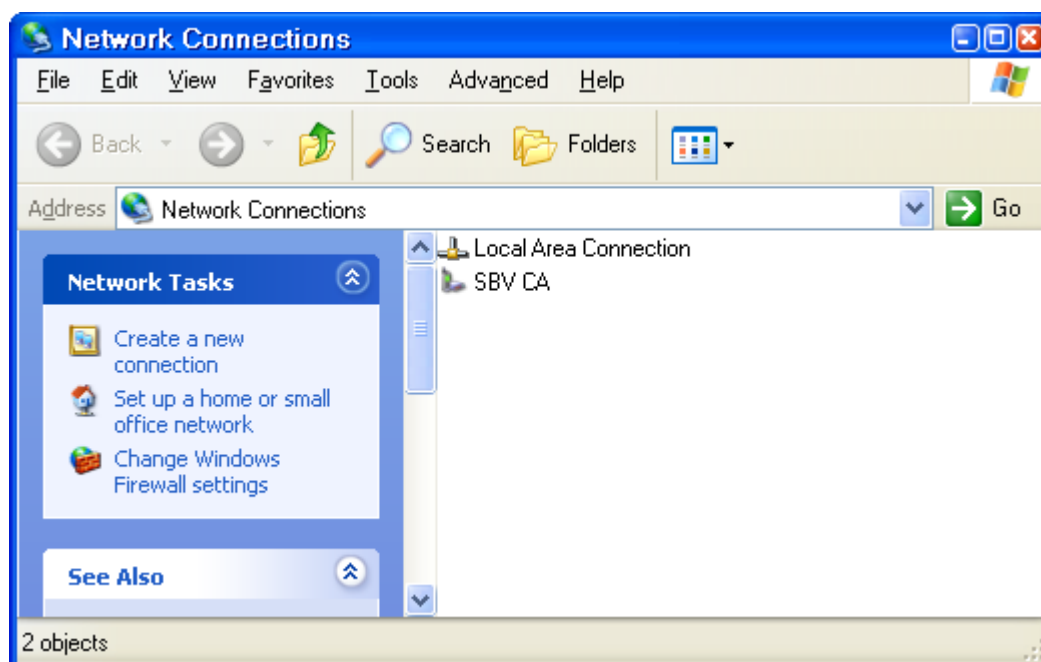
- Share with all users of this computer

The connection will be saved in the Network Connections folder.

☒ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

< Back Finish Cancel



**Thông tin kết nối:**

- + Số điện thoại: **043 835 8401; 043 8354502**
- + User Name/ Password Dialup: Sử dụng username, password như đã thông báo tại Thông báo mật cấp chứng thư số cho người sử dụng trước đây.

4.2.Kiểm tra kết nối mạng với NHNN

Thực hiện kết nối mạng tới NHNN bằng một trong các cách kết nối nêu trên. Sau khi kết nối thành công thực hiện kiểm tra tình trạng mạng như sau:

Vào cửa sổ CMD thực hiện lệnh ping và telnet như sau:

ping 192.168.12.18

telnet 192.168.12.18 829

ping 192.168.12.38

telnet 192.168.12.38 389

Nếu **ping** hoặc **telnet không thành công** (như hình dưới) sẽ không Update được CTS về thiết bị iKey.

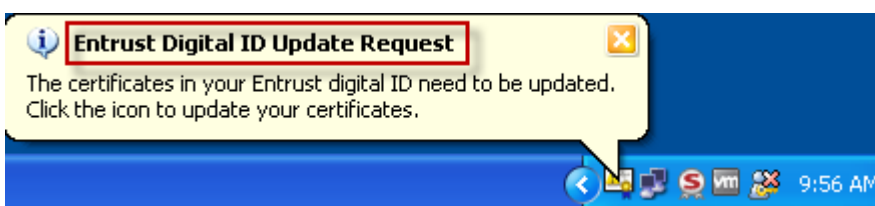
```
C:\WINDOWS\system32\cmd.exe
G:\>telnet 192.168.12.18 829
Connecting To 192.168.12.18...Could not open connection to the host, on port 829
: Connect failed
G:\>_
```

2. Thực hiện Update CTS

Người sử dụng sau khi làm đầy đủ thủ tục gia hạn chứng thư số và gửi về Phòng CA- Cục CNTH - NHNN, trong thời gian 10 ngày kể từ ngày gửi hồ sơ hợp lệ người sử dụng tiến hành:

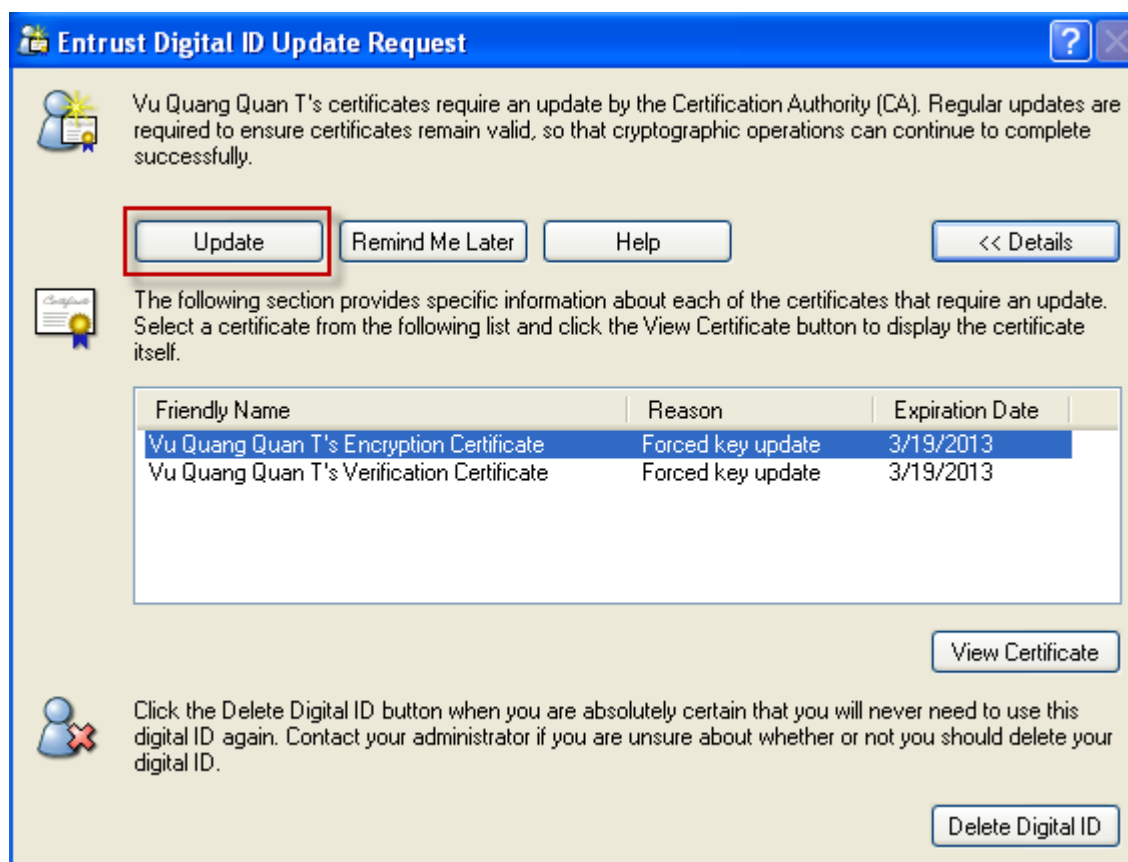
- Cắm thiết bị iKey của người sử dụng cần thực hiện Update chứng thư số vào cổng USB trên máy tính (**chú ý chỉ cắm 01 thiết bị iKey của người sử dụng tại thời điểm thực hiện Update trên máy tính**) .

Trong khoảng thời gian từ 01 đến 03 phút kể từ khi cắm thiết bị iKey người sử dụng sẽ thấy xuất hiện thông báo như sau ở thanh Taskbar:

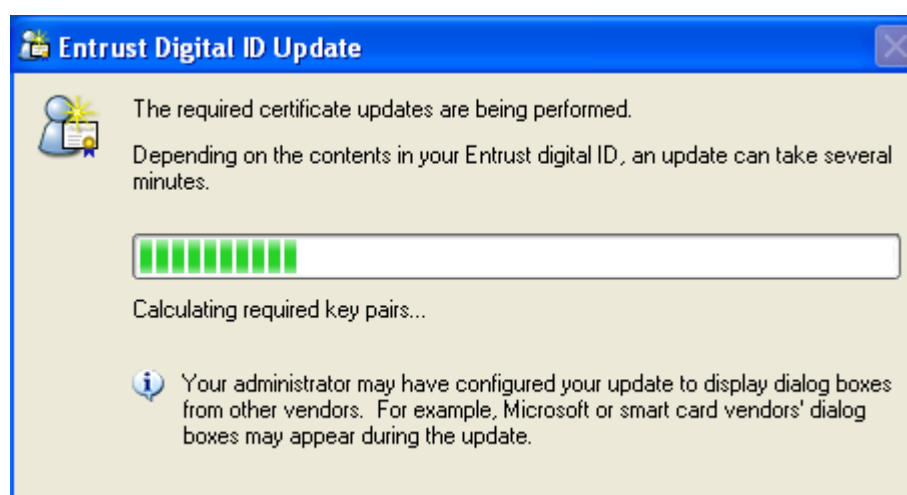


Click vào thông báo để xem chi tiết, nhấn **Details**:





Nhấn nút **Update** để thực hiện cập nhật CTS mới về iKey.



Màn hình thông báo xác thực truy xuất CTS trong iKey xuất hiện:



Tiến hành nhập mật khẩu truy xuất chứng thư số lưu trong iKey (mật khẩu ký duyệt) và nhấn **OK**. Quá trình cập nhật CTS thành công:



Chú ý: Để đảm bảo an toàn giao dịch điện tử, người sử dụng đặt mật khẩu chứng thư số đủ mạnh theo quy tắc như sau:

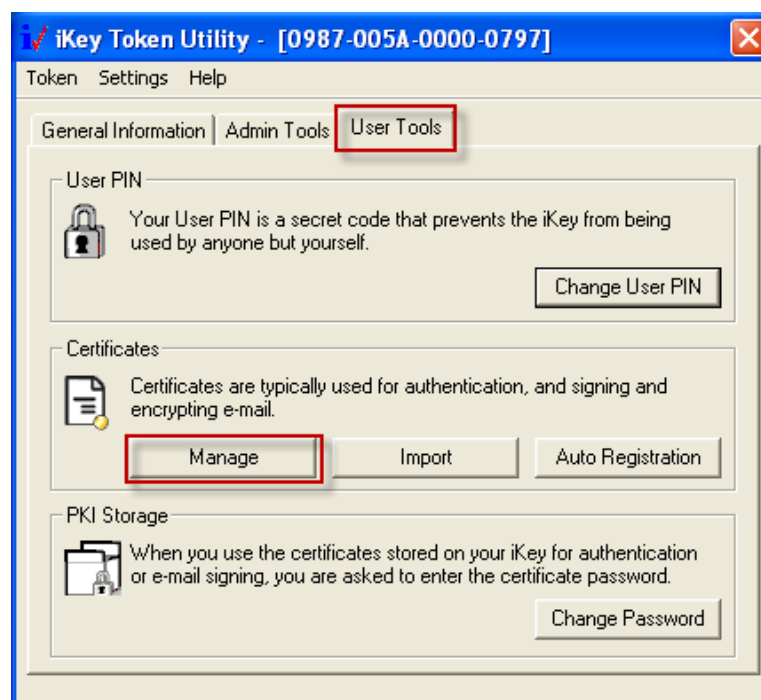
+ Độ dài mật khẩu tối thiểu 8 kí tự bao gồm cả số, chữ thường và chữ hoa.

+ Thay đổi mật khẩu 3 tháng 1 lần hoặc ngay khi bị lộ. Thay đổi mật khẩu bằng cách vào **iKey Token Utility** - > Chọn tab **User Tools** -> Nhấn nút **Change Password**.

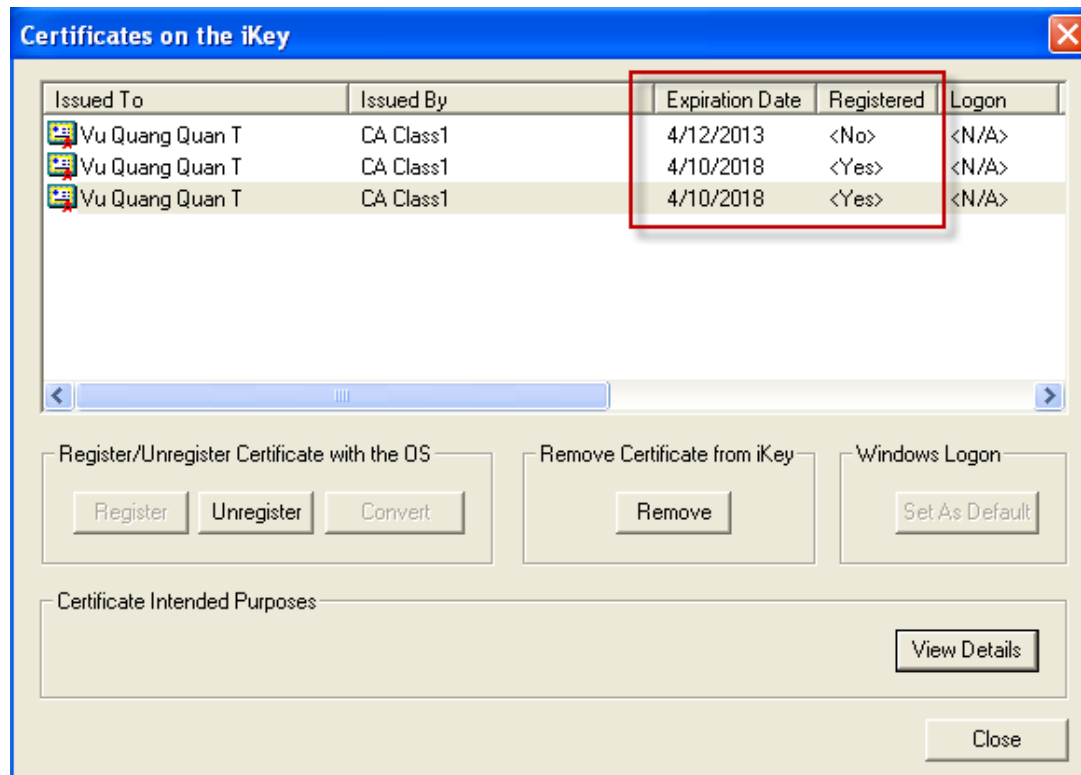
3. Kiểm tra thông tin CTS sau khi Update

3.1. Kiểm tra CTS

- Mở **iKey Token Utility** bằng cách click đúp vào biểu tượng .
- Chọn tab **User Tools**, nhấn nút **Manage**.



- Thông tin CTS sẽ hiện ra:

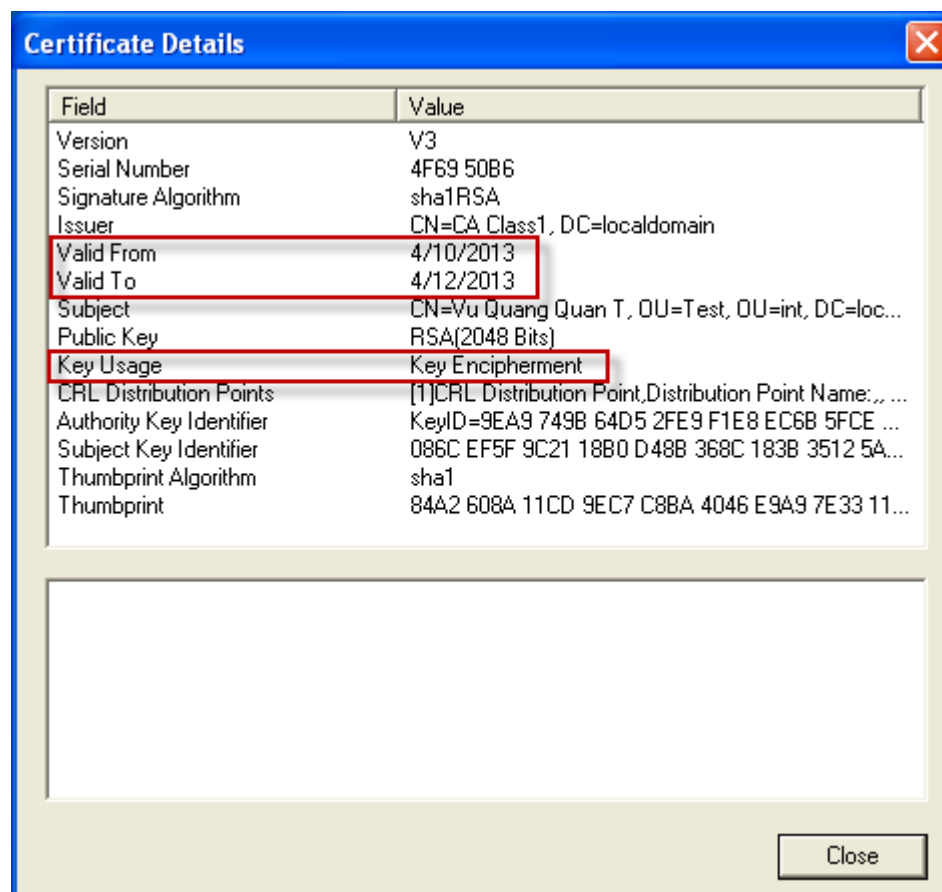




(CTS cũ hết hạn ngày 12/04/2013 và được gia hạn 05 năm tức có hiệu lực đến năm 10/04/2018)

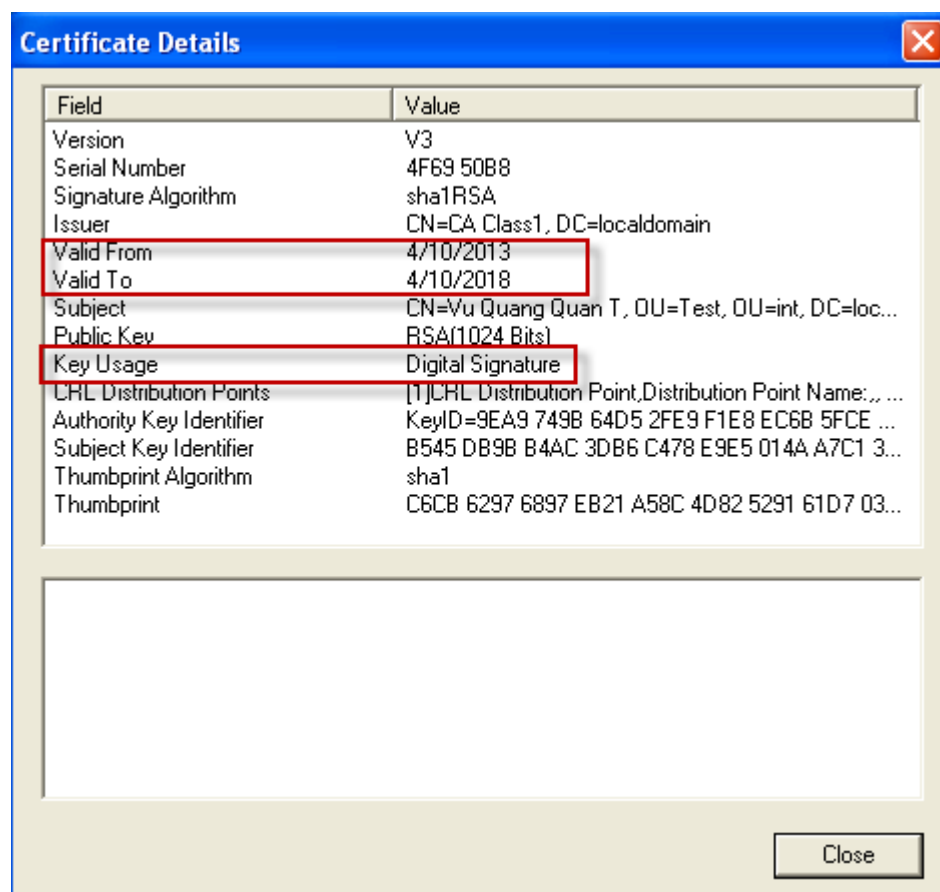
- CTS sau khi Update sẽ có **03** dòng:

➤ Dòng đầu tiên là **dòng khóa mã hóa cũ** (tự động Unregister). Để xem chi tiết thông tin nhấn **Detail**.



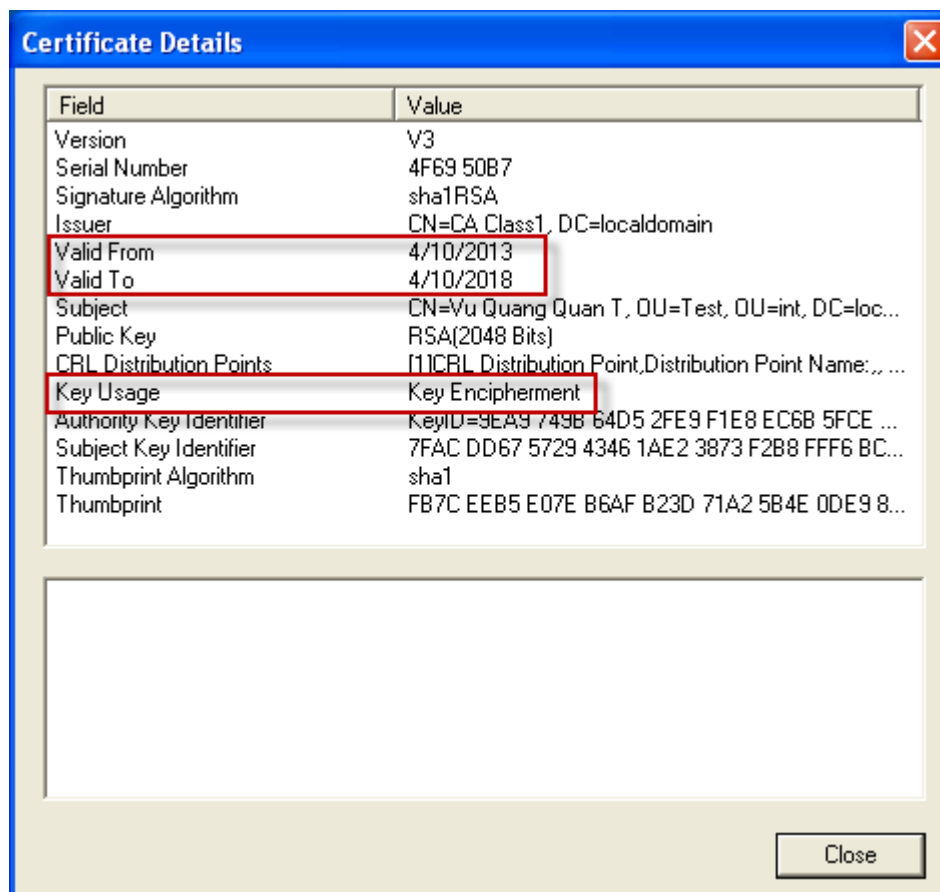
Khóa mã hóa có thuộc tính Key Usage là Key Encipherment

➤ Dòng thứ 2 là dòng **khóa ký** mới vừa được Update. Để xem chi tiết thông tin nhấn **Detail**.



Khóa ký có thuộc tính Key Usage là Digital Signature

➤ Dòng thứ 3 là dòng khóa mã hóa mới vừa được Update. Để xem chi tiết thông tin nhấn **Detail**.

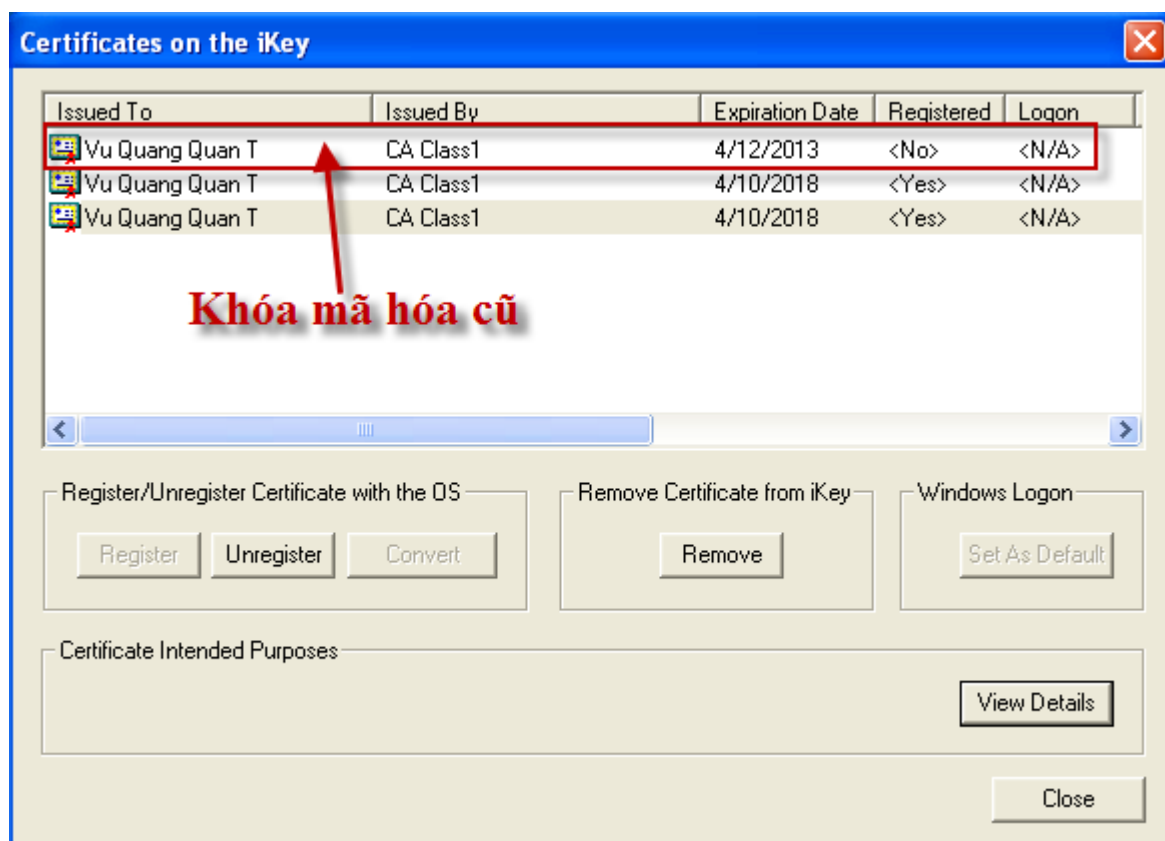


Khóa mã hóa có thuộc tính Key Usage là Key Encipherment

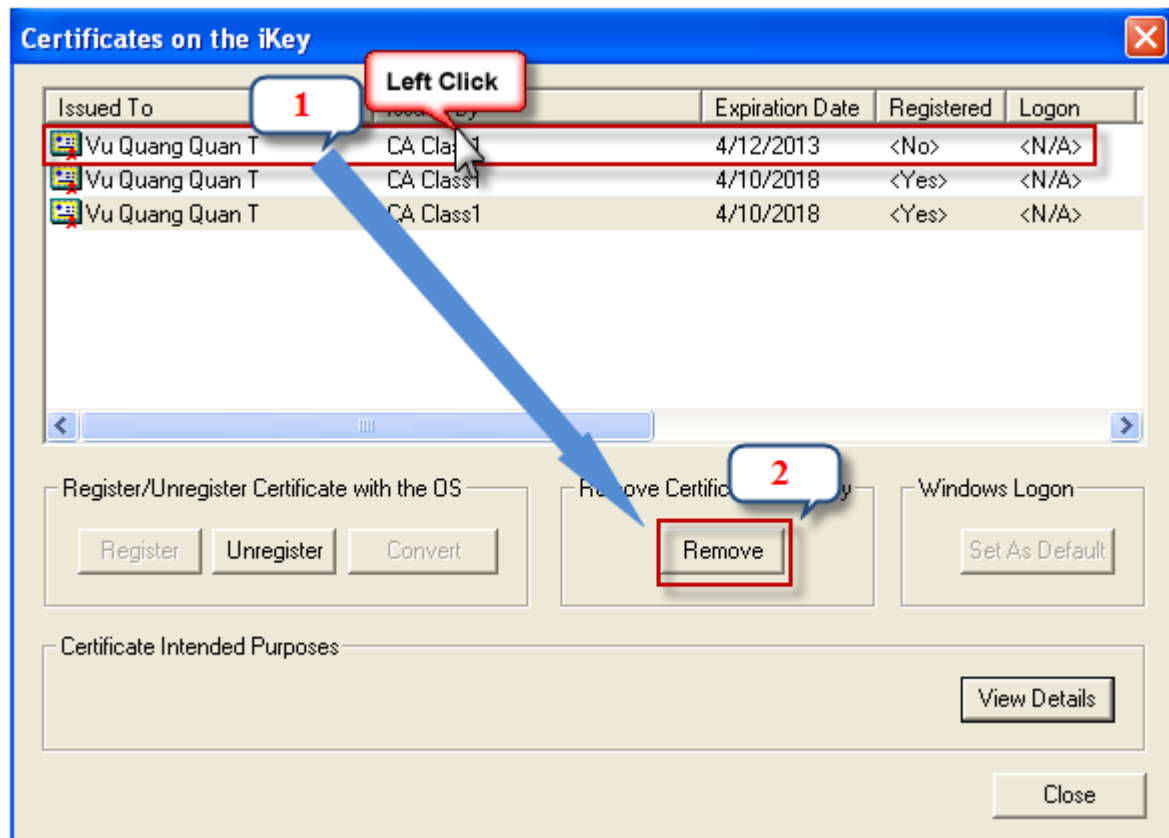
3.2. Xóa thông tin CTS cũ trong iKey

Sau khi Update và kiểm tra CTS đã Update thành công. Người sử dụng tiến hành xóa dòng **khóa mã hóa cũ** trong iKey như sau:

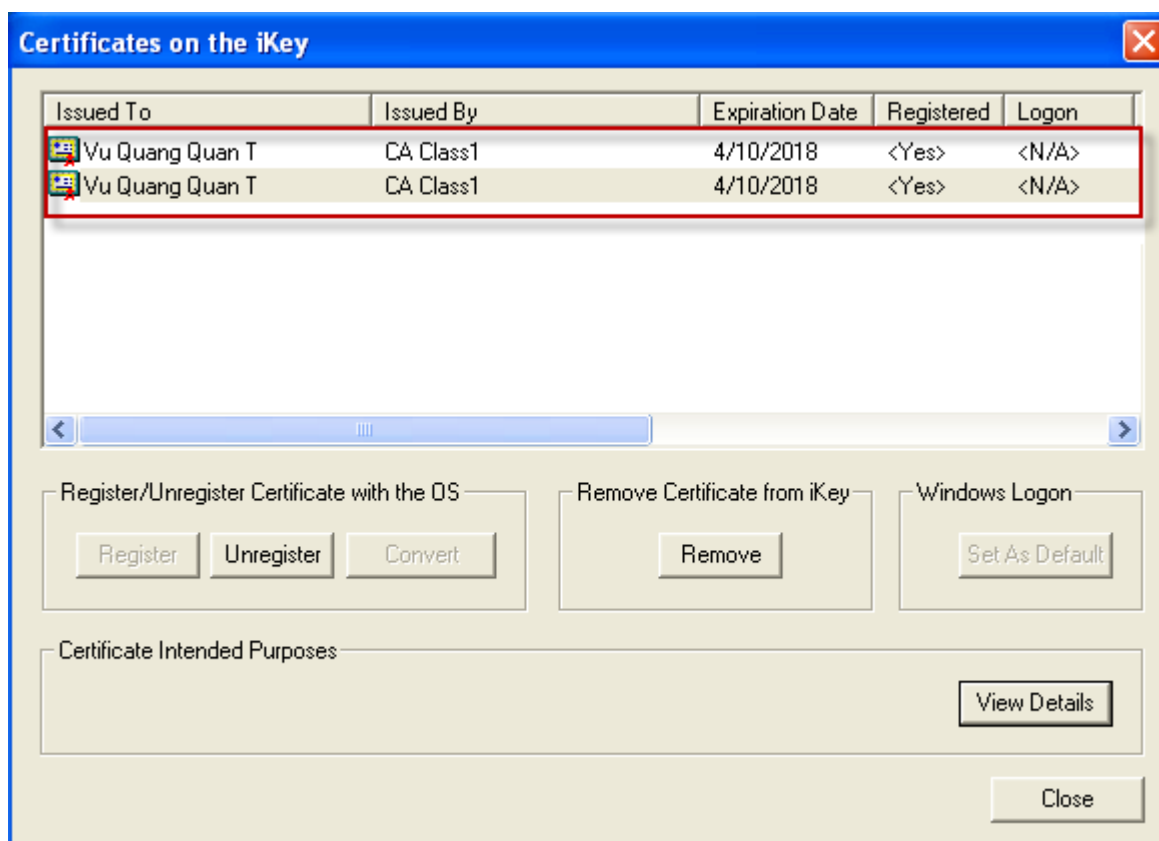
Trước khi xóa dòng khóa mã hóa cũ:



Nhấp trái chuột tại dòng **khóa mã hóa cũ** -> Nhấn nút **Remove**.



Sau khi xóa dòng khóa mã hóa cũ, trong iKey còn lại 2 dòng khóa mới: Khóa mã hóa mới và Khóa ký mới.



IV. Thông tin liên lạc hỗ trợ

Phòng CA – Cục Công nghệ tin học – Ngân hàng Nhà nước

Địa chỉ; 64 Nguyễn Chí Thanh – Đống Đa – Hà Nội

Điện thoại: 04.38354775

Fax: 04.38358135