

BAN CƠ YẾU CHÍNH PHỦ



**Tài liệu hướng dẫn sử dụng bộ công cụ ký số
GCA-01**

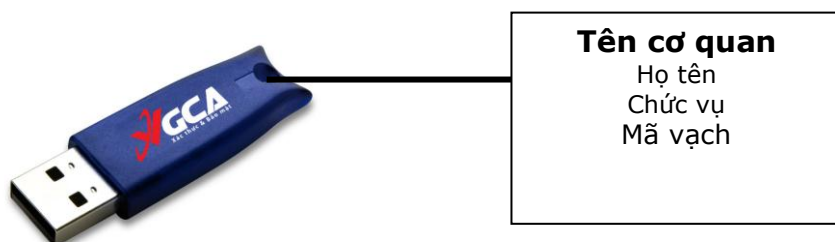
Hà Nội, 7/2011

Mục lục

Mục lục	2
1 Hướng dẫn cài đặt và sử dụng thiết bị USB Token.....	3
1.1 Giới thiệu chung	3
1.2 Hướng dẫn cài đặt.....	3
1.2.1 Yêu cầu phần cứng và hệ điều hành	3
1.2.2 Cài đặt trình điều khiển và thay đổi mật khẩu eToken	3
1.2.3 Cài đặt trình điều khiển và thay đổi mật khẩu thiết bị ST3	12
2 Hướng dẫn sử dụng bộ công cụ ký số GCA-01 để bảo mật và ký số tài liệu	
điện tử	17
2.1 Giới thiệu chung	17
2.1.1 Các đặc điểm của vSign	17
2.1.2 Các thành phần chính trong bộ phần mềm vSign	17
2.1.3 Các chuẩn đáp ứng	18
2.2 Cài đặt phần mềm vSign2.0.....	19
2.3 Cấu hình cho phần mềm vSign2.0.....	21
2.3.1 Cấu hình tự động gắn dấu thời gian	22
2.3.2 Cấu hình kiểm tra danh sách hủy bỏ chứng thư số	23
2.3.3 Cấu hình proxy	25
2.4 Hướng dẫn sử dụng phần mềm vSign2.0 để ký số và bảo mật tài liệu điện tử	25
2.4.1 Khởi động chương trình xác thực và bảo mật tệp	25
2.4.2 Quản lý chứng thư số theo nhóm	26
2.4.3 Quản lý danh sách chứng thư số.....	32
2.4.4 Các chức năng chính của xác thực và bảo mật tệp.....	39
2.5 Xác thực và bảo mật nội dung thư.....	61
2.5.1 Ký số nội dung thư.....	61
2.5.2 Ký số/bảo mật nội dung thư.....	63
2.5.3 Xác thực chữ ký/giải mã nội dung thư	67
2.6 Xác thực và bảo mật PDF.....	68
2.6.1 Ký số tài liệu PDF	68
2.6.2 Ký số/bảo mật tài liệu PDF	72
2.6.3 Kiểm tra chữ ký số và giải mã tài liệu PDF	78
2.7 Bảo mật ổ đĩa	84
2.7.1 Tạo ổ đĩa mật.....	85
2.7.2 Mở ổ đĩa mật	88
3 Kết luận	93

1 Hướng dẫn cài đặt và sử dụng thiết bị USB Token

1.1 Giới thiệu chung



Thiết bị USB Token là thiết bị lưu trữ chứng thư số và khóa an toàn, khi đăng ký chứng thư số, mỗi người sử dụng sẽ được cấp phát một thiết bị USB Token.

1.2 Hướng dẫn cài đặt

1.2.1 Yêu cầu phần cứng và hệ điều hành

Bộ nhớ Ram tối thiểu 64MB, có cổng USB, sử dụng hệ điều hành Windows 9x, Windows 2000, Windows 2003, Windows XP, Windows Vista 32bit, 64bit, Windows 7 32bit, 64bit.

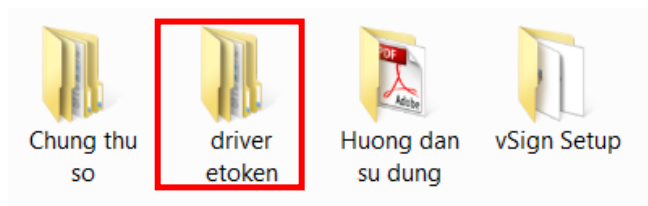
1.2.2 Cài đặt trình điều khiển và thay đổi mật khẩu eToken

1.2.2.1 Thiết bị eToken



1.2.2.2 Cài đặt trình điều khiển thiết bị eToken

Bước 1: Mở đĩa CD được cấp phát



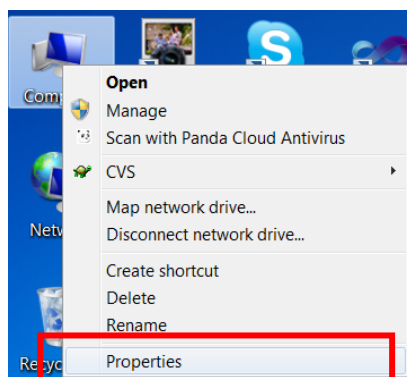
Chọn thư mục driver etoken → chọn Win_32bit hoặc Win_64bit tùy vào hệ điều hành windows đang sử dụng.



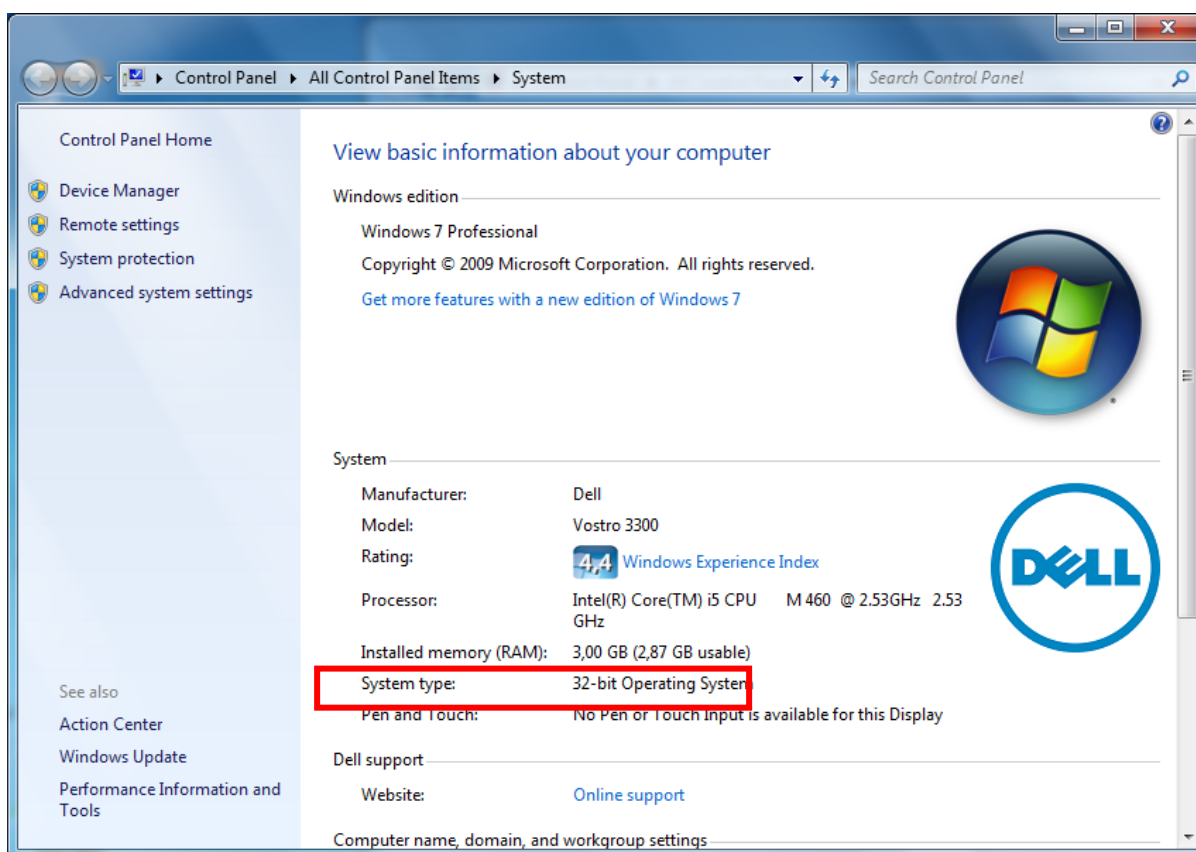
Nhấp đúp chuột để chạy chương trình cài đặt.

Chú ý:

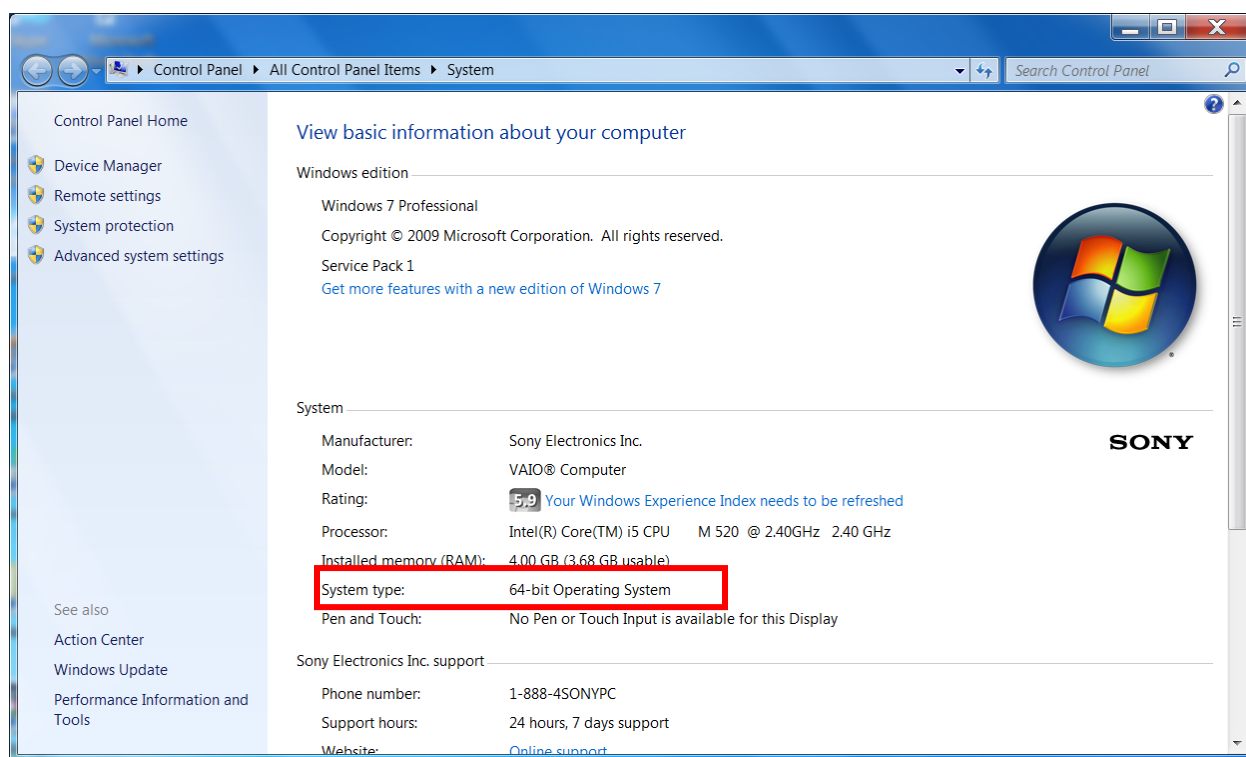
- **Để biết được hệ điều hành mình đang sử dụng là hệ điều hành 32bit hay 64bit, bấm chuột phải vào biểu tượng My Computer (trên màn hình) → Properties.**



○ **Hệ điều hành 32 bit (Windows 7):**



○ **Hệ điều hành 64 bit (Windows 7):**

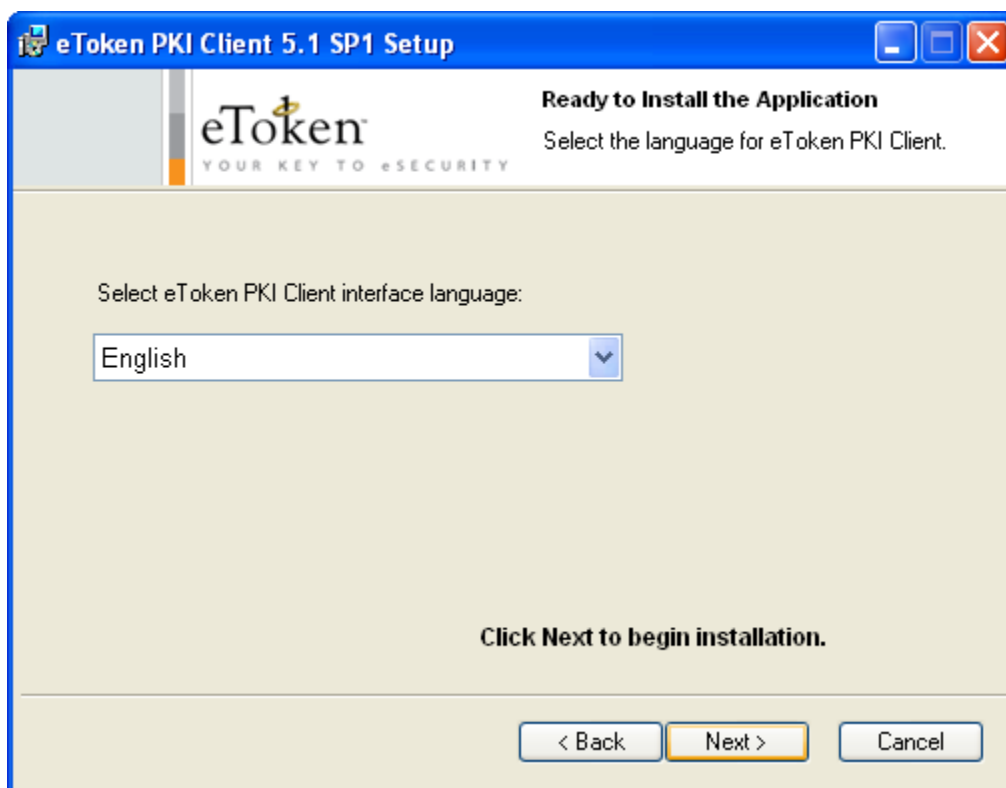


- **Đối với Windows XP chủ yếu là hệ điều hành 32bit, Windows Vista 32bit và 64bit giao diện kiểm tra có khác hơn một chút nhưng vẫn có thể kiểm tra được bằng phương pháp trên.**
- **Bộ công cụ ký số GCA-01 chủ yếu sử dụng hệ điều hành Windows 32bit, đối với hệ điều hành Windows 64bit, chức năng chuột phải của phần mềm không hiển thị còn các chức năng khác đều hoạt động tốt.**

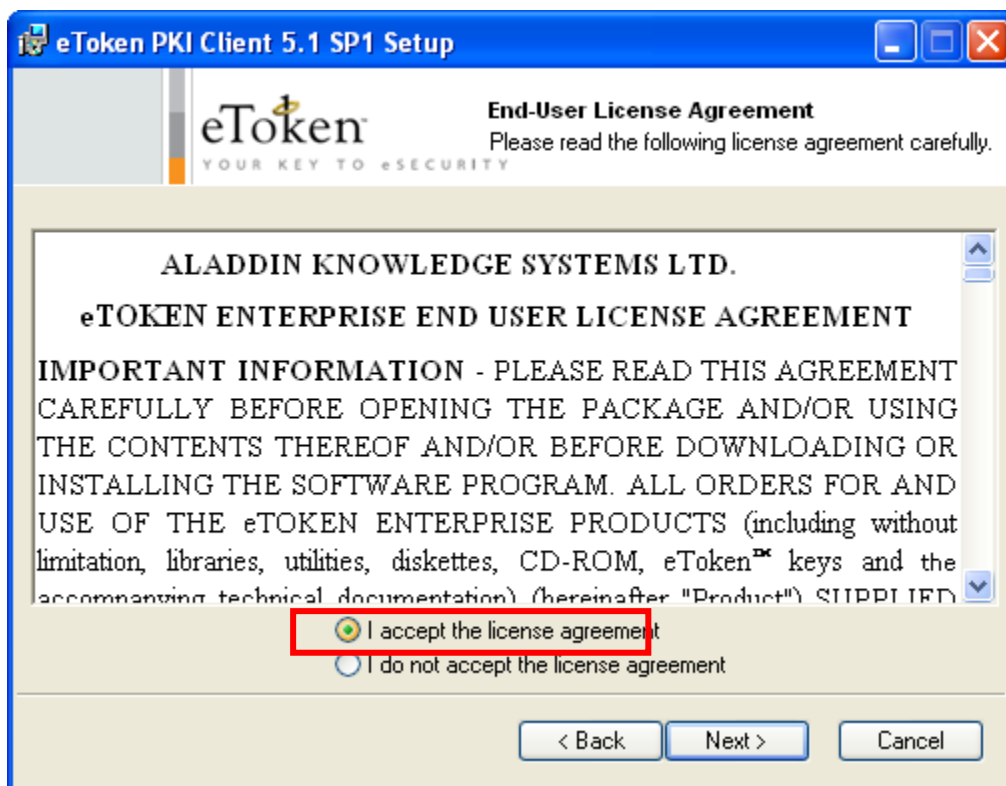
Bước 2: Cài đặt driver USB Token



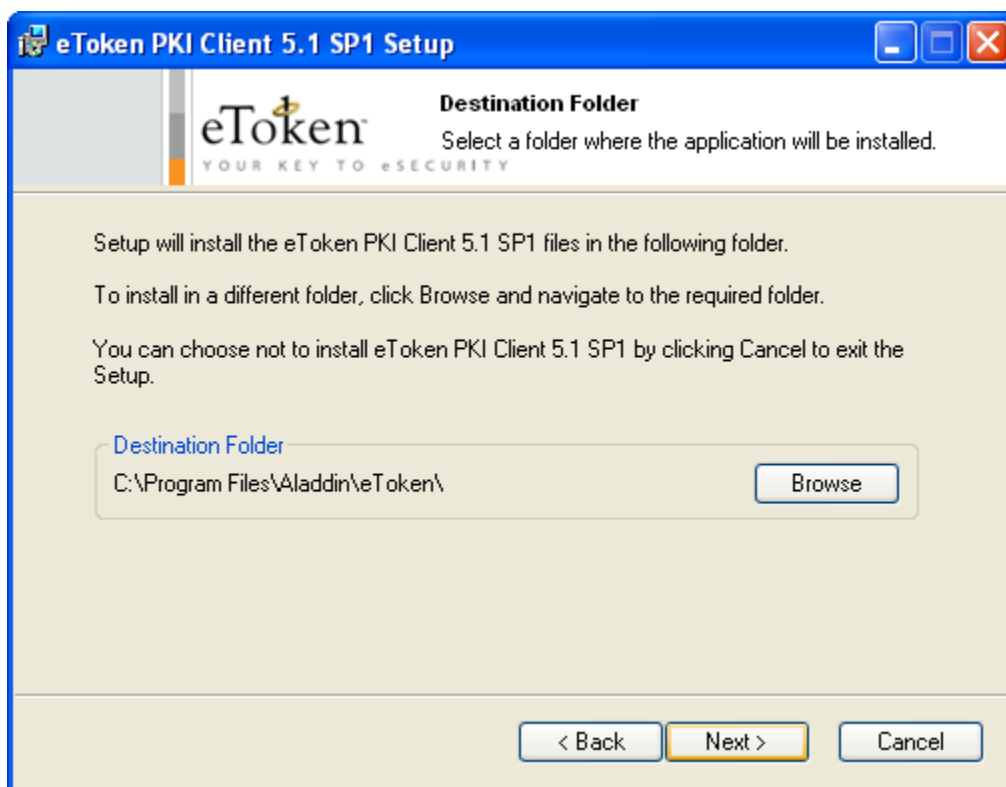
Chọn Next



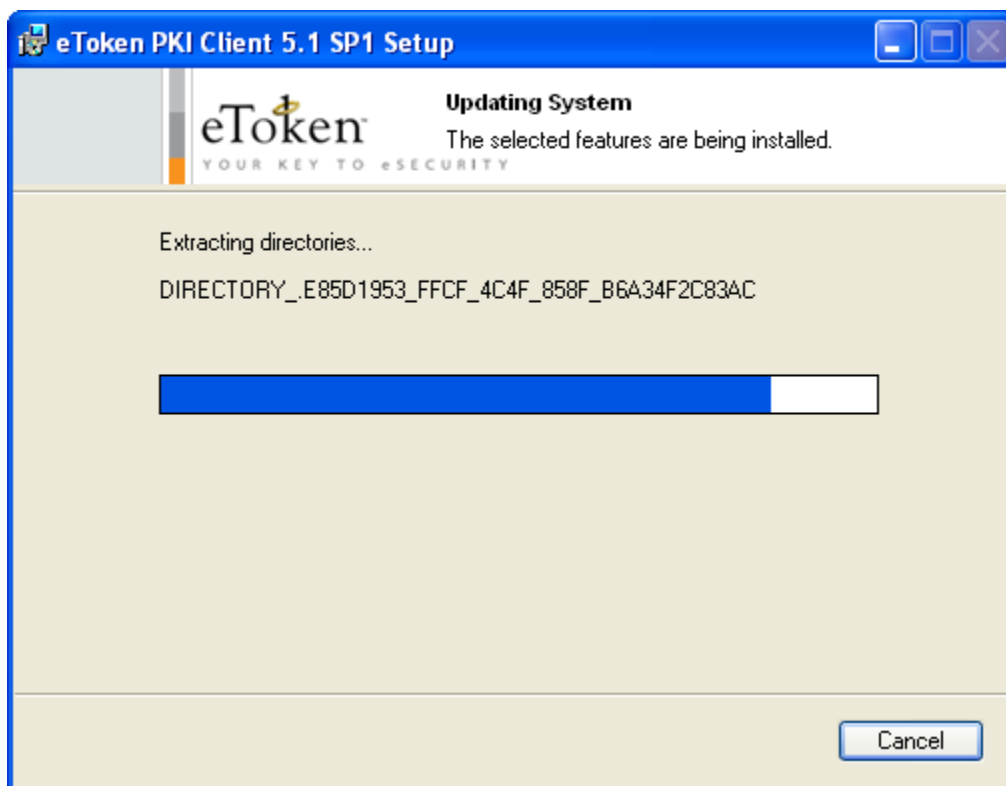
Chọn Next



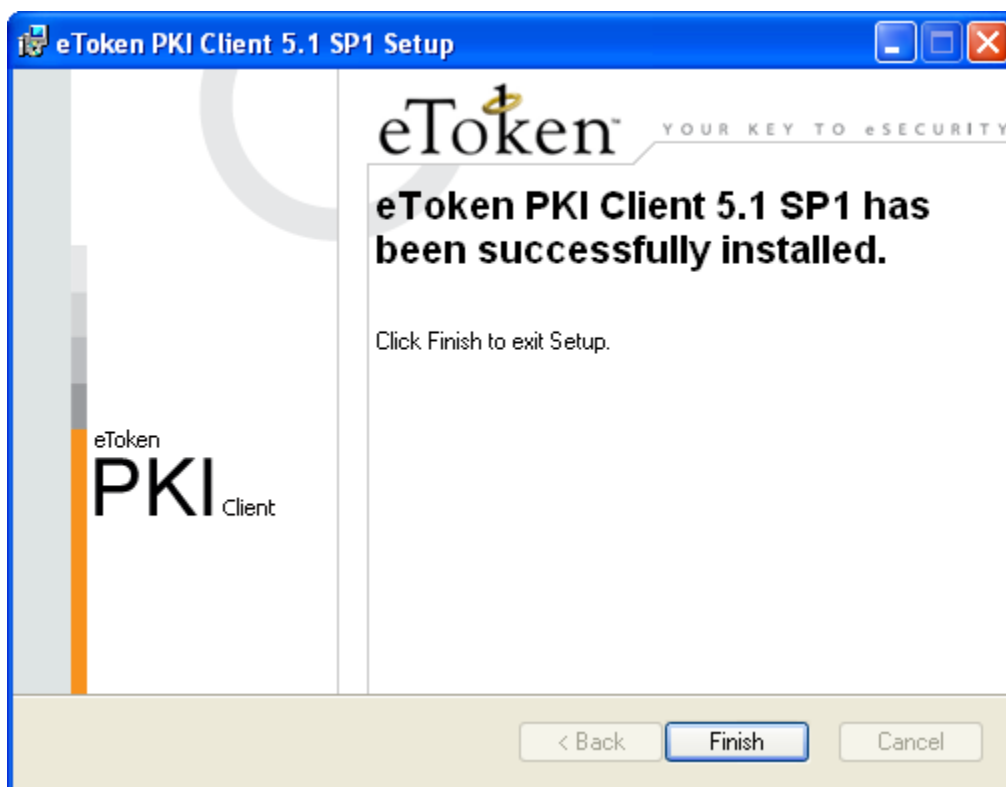
Chọn "I accept the license agreement", chọn Next



Chọn Next



Chọn Next



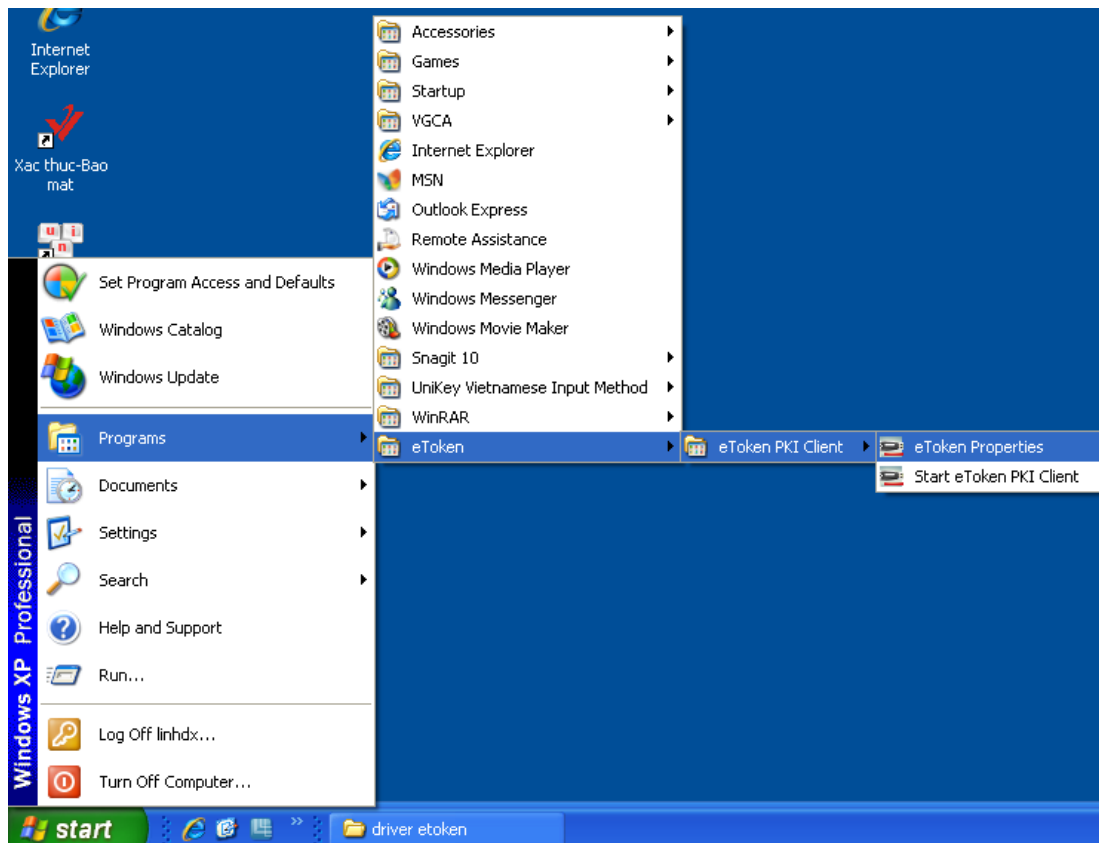
Chọn “Finish” để kết thúc quá trình cài đặt thiết bị USB Token.

Bước 3: Kiểm tra

Xem dưới góc phải màn hình có biểu tượng USB Token



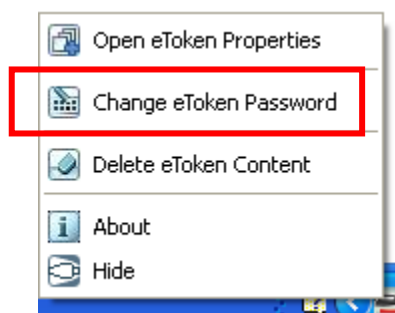
Hoặc vào menu start → eToken → eToken PKI Client



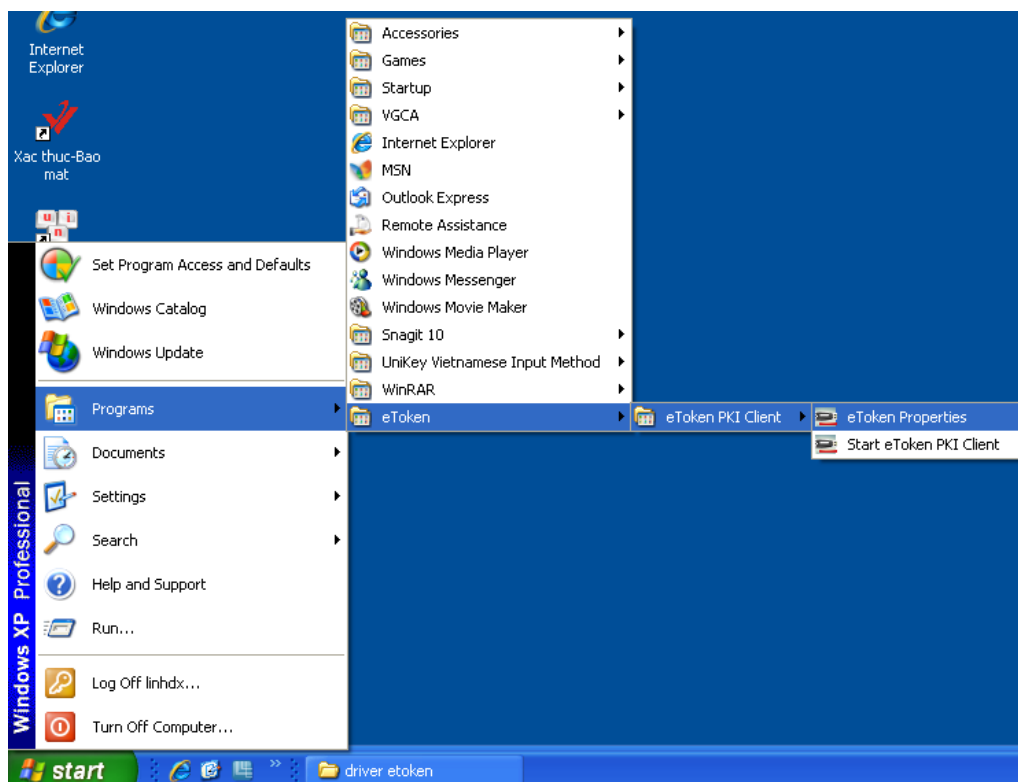
1.2.2.3 Đổi mật khẩu cho thiết bị eToken

Bước 1: Cắm thiết bị USB Token vào cổng USB của máy tính, thấy đèn đỏ nhấp nháy.

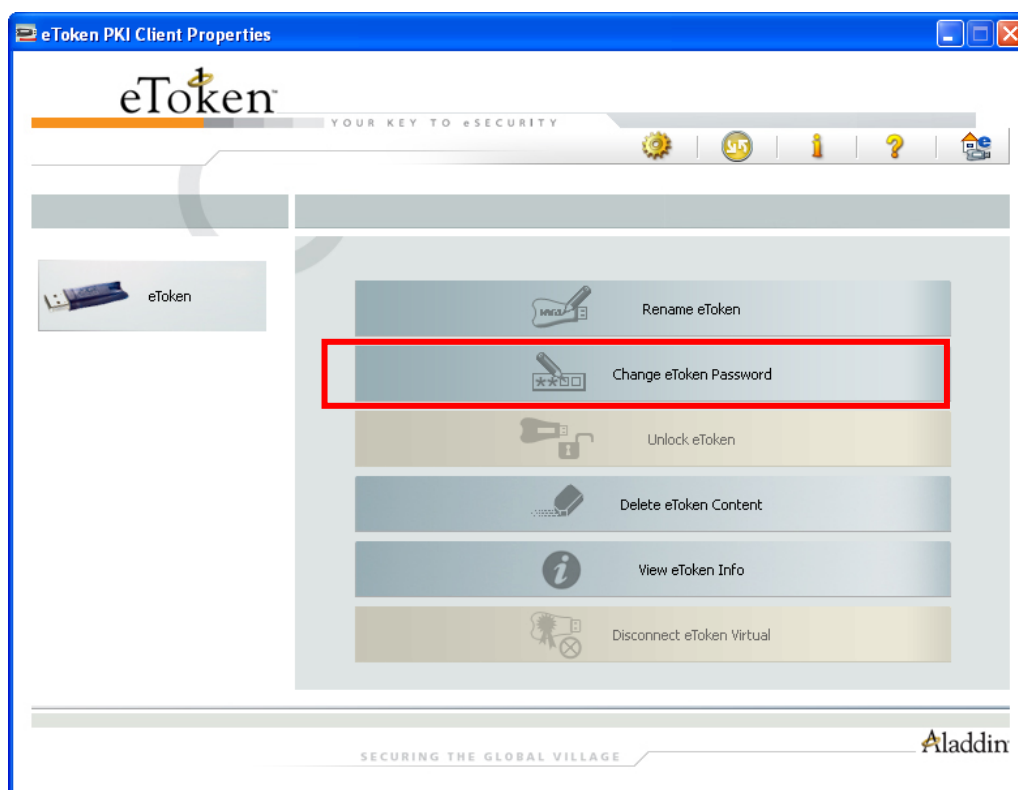
Bước 2: Nhấp chuột phải vào biểu tượng USB Token ở góc phải màn hình và chọn “Change eToken Password”.



Hoặc vào menu start → eToken → eToken PKI Client → eToken Properties.



Nhấp chuột trái



Bước 3: Thay đổi mật khẩu



Nhập mật khẩu cần thay vào ô “Current USB Token Password”. Nhập mật khẩu mới vào ô “New USB Token Password” và “Confirm New USB Token Password”. Sau khi nhập xong nhấn OK để xác nhận sự thay đổi trên.

Giao diện thông báo thay đổi mật khẩu thành công



Chú ý:

- **Mật khẩu mới phải có độ dài ít nhất 8 ký tự, phải chứa chữ hoa, chữ thường và số.**
- **Người sử dụng phải nhớ kỹ mật khẩu của mình.**
- **Theo mặc định của thiết bị USB Token, người dùng nhập sai mật khẩu liên tiếp quá 15 lần, thì USB Token sẽ tự động khóa và người dùng sẽ không tiếp tục sử dụng được USB Token!**
- **Để mở khóa thiết bị người sử dụng phải liên hệ và chuyển thiết bị về cho các cơ quan đăng ký để thực hiện mở khóa.**

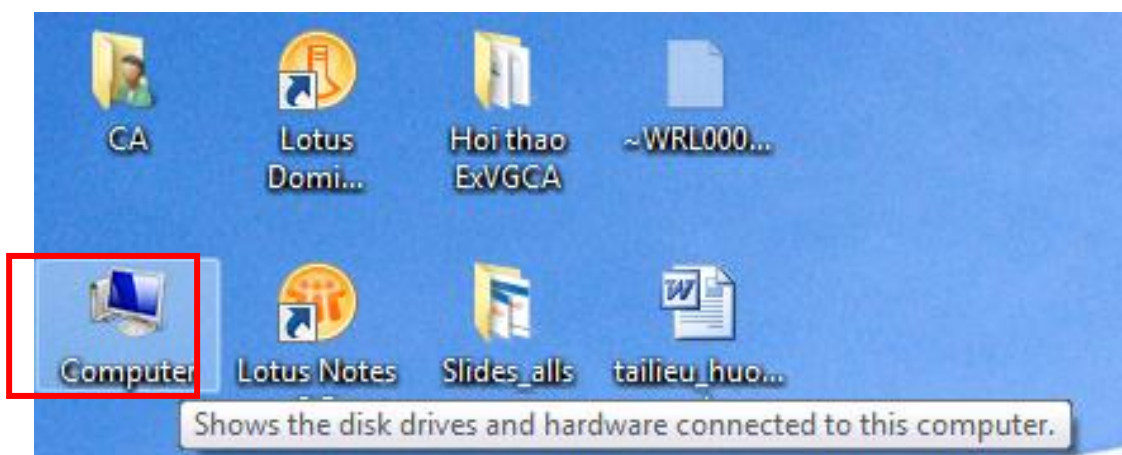
1.2.3 Cài đặt trình điều khiển và thay đổi mật khẩu thiết bị ST3

1.2.3.1 Thiết bị ST3

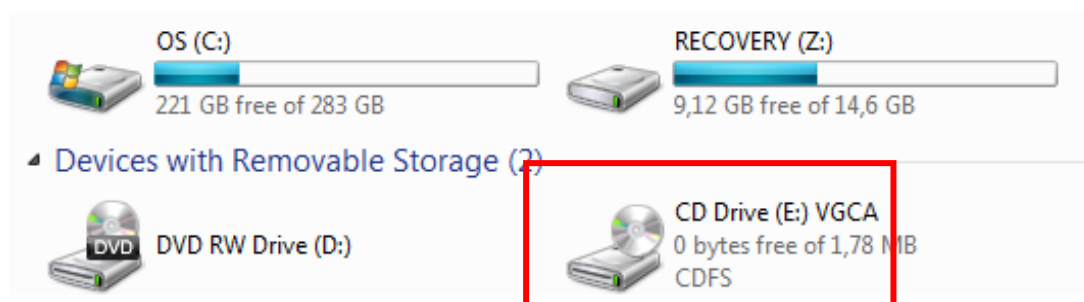


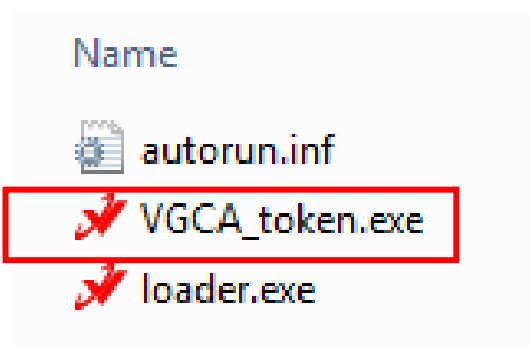
1.2.3.2 Cài đặt trình điều khiển thiết bị ST3

Bước 1: cắm thiết bị USB Token vào cổng USB của máy tính, mở chương trình “My computer” nằm trên màn hình



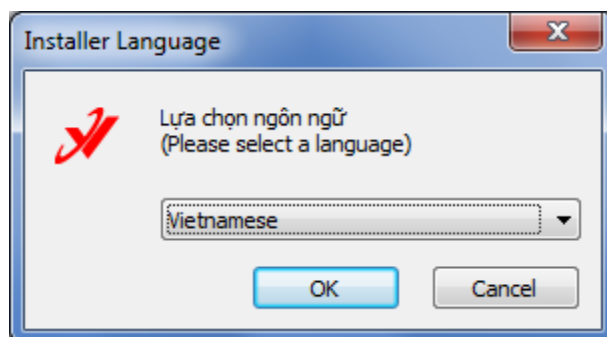
Mở ổ đĩa VGCA:



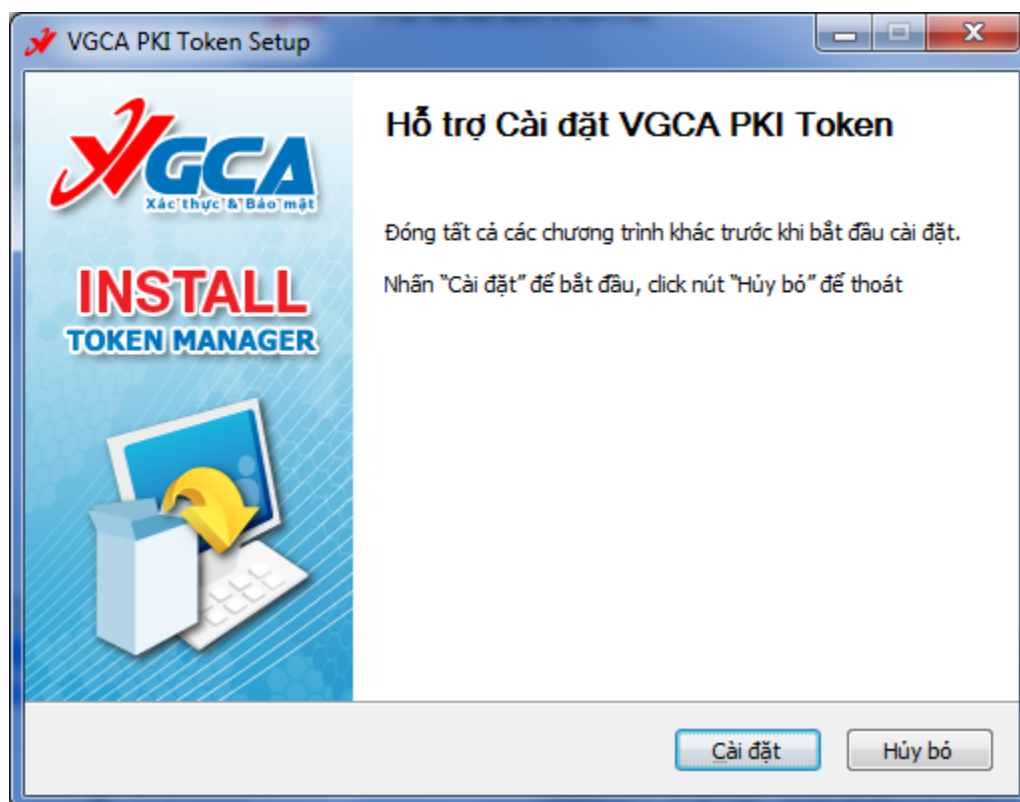


Kích đúp chuột vào tệp VGCA_token.exe để cài đặt.

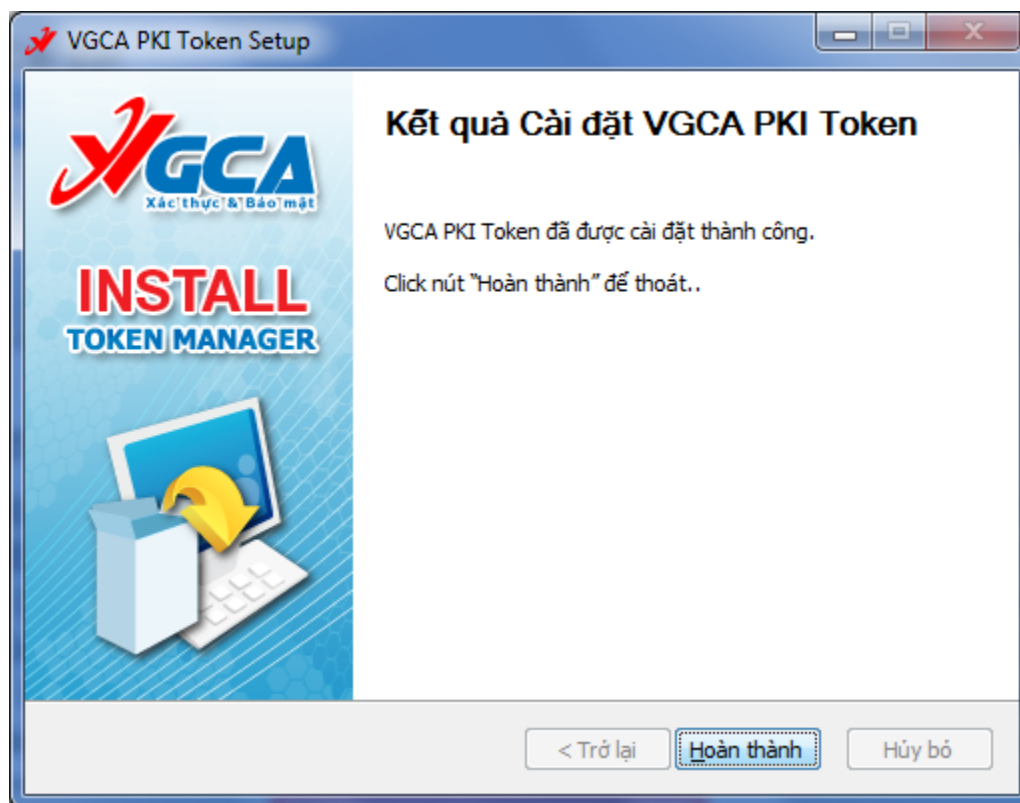
Bước 2: Cài đặt driver USB Token



Chọn OK



Chọn Cài đặt



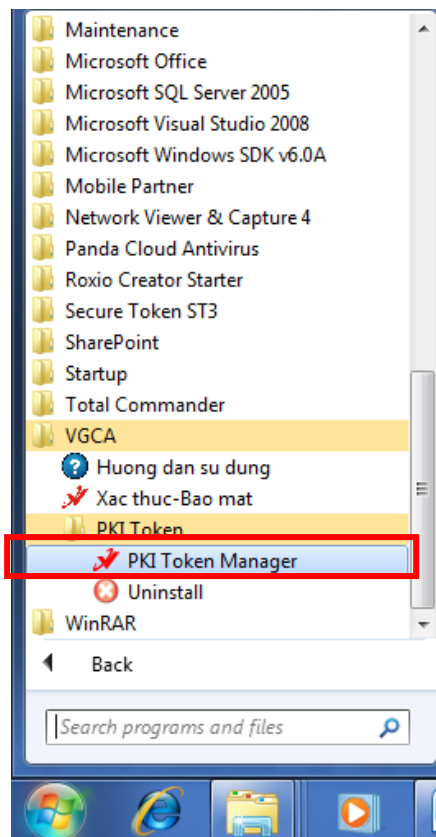
Chọn “Hoàn thành” để kết thúc quá trình cài đặt thiết bị USB Token.

Bước 3: Kiểm tra.

Xem dưới góc phải màn hình có biểu tượng USB Token.



Hoặc vào menu start → VGCA → PKI Token → PKI Token Manager.

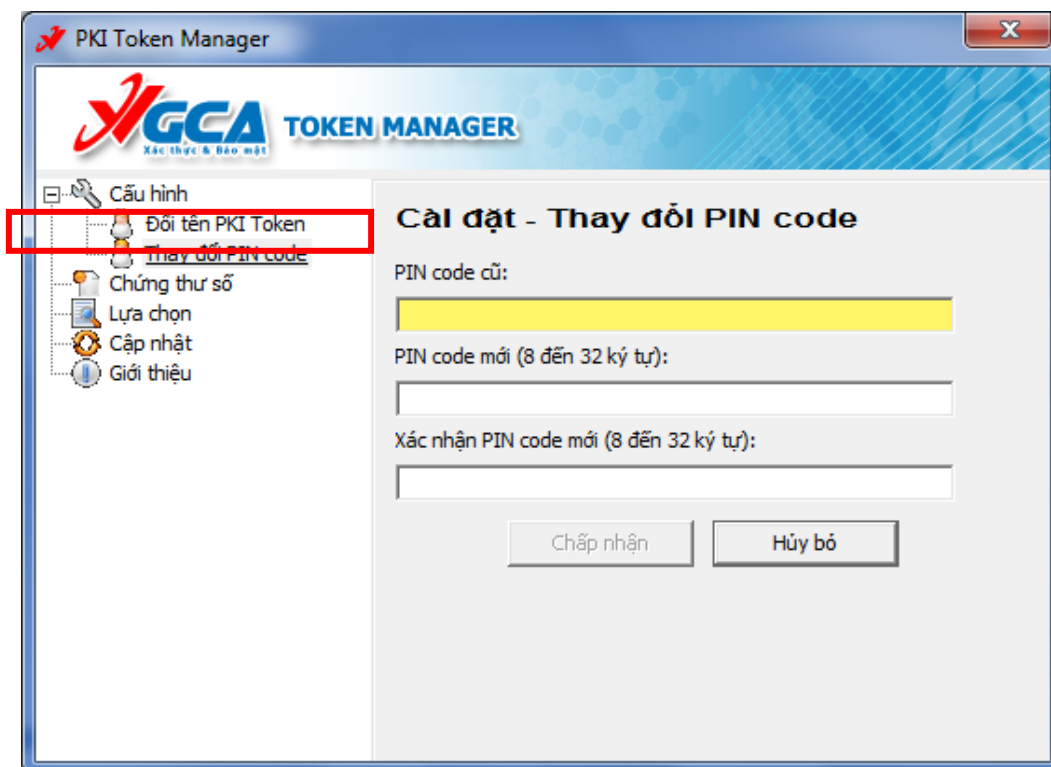


Giao diện PKI Token Manager:



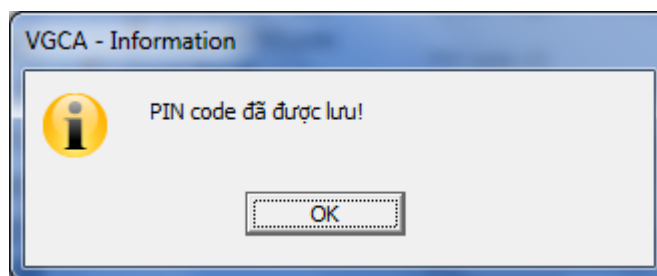
1.2.3.3 Đổi mật khẩu cho thiết bị USB Token ST3

Giao diện thay đổi mật khẩu



Nhập mật khẩu cần thay vào ô “PIN code cũ”. Nhập mật khẩu mới vào ô “PIN code mới” và “Xác nhận PIN code mới”. Sau khi nhập xong nhấn “Chấp nhận” để xác nhận sự thay đổi trên.

Giao diện thông báo thay đổi mật khẩu thành công.



Chú ý:

- **Mật khẩu mới phải có độ dài ít nhất 8 ký tự, phải chứa chữ hoa, chữ thường và số.**
- **Người sử dụng phải nhớ kỹ mật khẩu của mình.**
- **Theo mặc định của thiết bị USB Token, người dùng nhập sai mật khẩu liên tiếp quá 06 lần, thì USB Token sẽ tự động khóa và người dùng sẽ không tiếp tục sử dụng được USB Token!**
- **Để mở khóa thiết bị người sử dụng phải liên hệ và chuyển thiết bị về cho các cơ quan đăng ký để thực hiện mở khóa.**

2 Hướng dẫn sử dụng bộ công cụ ký số GCA-01 để bảo mật và ký số tài liệu điện tử

2.1 Giới thiệu chung

Bộ công cụ ký số CGA-01 là bộ sản phẩm cấp phát cho người dùng cuối. Các thành phần trong bộ công cụ ký số GCA-01 gồm:

- Thiết bị lưu khóa và chứng thư số USB Token.
- Đĩa CD chứa chứng thư số, driver thiết bị USB Token.
- Bộ phần mềm ký số vSign 2.0.
- Tài liệu giới thiệu sản phẩm.

Trong đó bộ phần mềm ký số vSign là bộ phần mềm cung cấp miễn phí cho người sử dụng để bảo mật và xác thực tài liệu điện tử trong môi trường giao dịch điện tử, bộ phần mềm vSign chỉ hoạt động trên các hệ điều hành Windows.

vSign sử dụng các dịch vụ chứng thực chữ ký số của hệ thống cơ sở hạ tầng khóa công khai PKI chuyên dùng Chính phủ để tạo chữ ký số an toàn trên các tài liệu điện tử và bảo mật các tài liệu đó bằng các thuật toán mật mã an toàn.

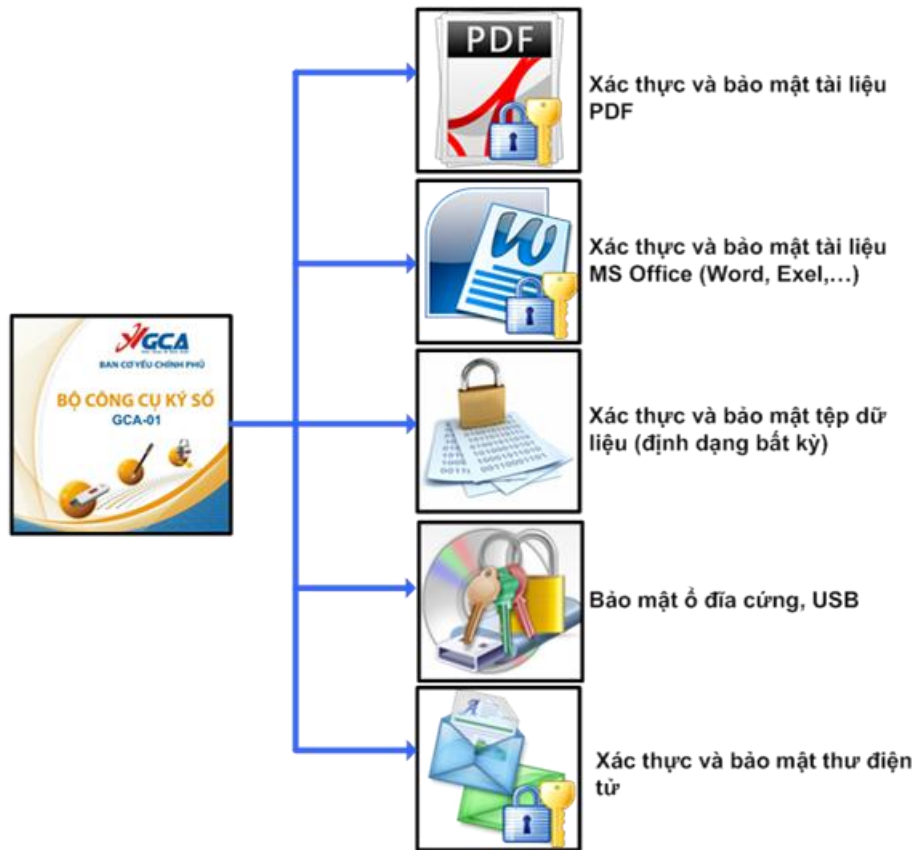
vSign đảm bảo toàn bộ các yêu cầu về xác thực và bảo mật tài liệu:

- Đảm bảo tính xác thực của người ký trên tài liệu ký.
- Đảm bảo tính toàn vẹn dữ liệu của tài liệu ký.
- Đảm bảo tính chống chối bỏ khi ký tài liệu.
- Đảm bảo tính bảo mật của dữ liệu.

2.1.1 Các đặc điểm của vSign

- Giao diện thân thiện dễ dàng sử dụng.
- Sử dụng các chuẩn PKI của thế giới về chữ ký số và mã hóa dữ liệu: chuẩn khuôn dạng chữ ký số XaDES, chuẩn mã hóa dữ liệu PKC#7, XML-Encryption,...
- Các thuật toán mật mã và ký số trong vSign đáp ứng danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số của bộ Thông tin và Truyền thông.
- Sử dụng các dịch vụ chứng thực trực tuyến trên mạng truyền số liệu chuyên dùng Chính phủ: gắn dấu thời gian, kiểm tra chứng thư số trực tuyến,...
- Tích hợp dấu thời gian vào chữ ký điện tử.
- Kiểm tra trạng thái chứng thư số trực tuyến khi ký số và bảo mật tài liệu.
- vSign được triển khai cho các cơ quan thuộc hệ thống chính trị.

2.1.2 Các thành phần chính trong bộ phần mềm vSign



- vSign - PDF ký số và bảo mật tài liệu PDF, cung cấp cho người dùng thông tin xác thực về chủ thể của tài liệu, đảm bảo tính tin cậy và toàn vẹn nội dung và an toàn của tài liệu PDF trong giao dịch điện tử.
- vSign - F có thể ký số và bảo mật tất cả các định dạng tệp dữ liệu trên môi trường Windows.
- vSign-Disk có thể tạo các ổ đĩa logic có bảo mật với dung lượng lớn.
- vSign - Mail có thể xác thực và bảo mật nội dung các văn bản được soạn thảo trên các trình soạn thảo văn bản thông qua bộ nhớ đệm clipboard của hệ điều hành Windows.

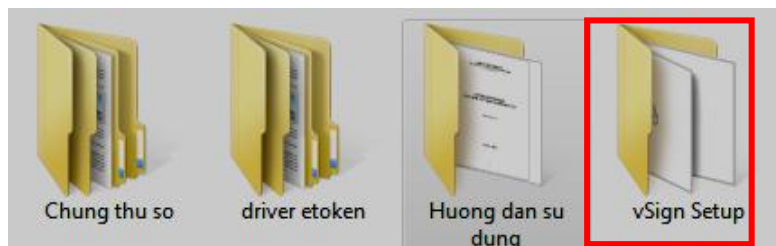
2.1.3 Các chuẩn đáp ứng

- Chuẩn khuôn dạng chứng thư số X509 v3, phần mềm vSign có thể sử dụng cho các chứng thư số của các nhà cung cấp dịch vụ khác có định dạng chuẩn X509 v3.
- Chuẩn khuôn dạng CRL và chứng thư số theo RFC3280 Certificate and Certificate Revocation List (CRL) Profile.
- Hàm băm bảo mật (FIPS PUB 180-2) SHA-1, SHA-512.
- Chuẩn khuôn dạng chữ ký số XAdES (XML Advanced Electronic Signatures) v1.3.2.
- Chuẩn khuôn dạng mã dữ liệu XML-Encryption.
- Bảo mật cho khối an ninh phần cứng HSM (FIPS PUB 140-2) level 3.
- Chuẩn gắn dấu thời gian theo giao thức TSP RFC3161 Time-Stamp Protocol (TSP).

- Chuẩn ký số và bảo mật tài liệu PDF theo ISO 32000-12.

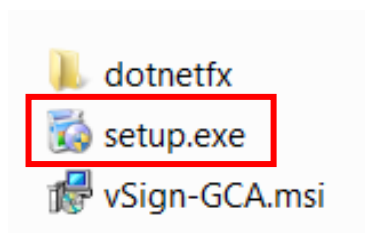
2.2 Cài đặt phần mềm vSign2.0

Bước 1: Mở đĩa CD được cấp phát theo chứng thư số.



Bước 2: Cài đặt chương trình vSign Setup

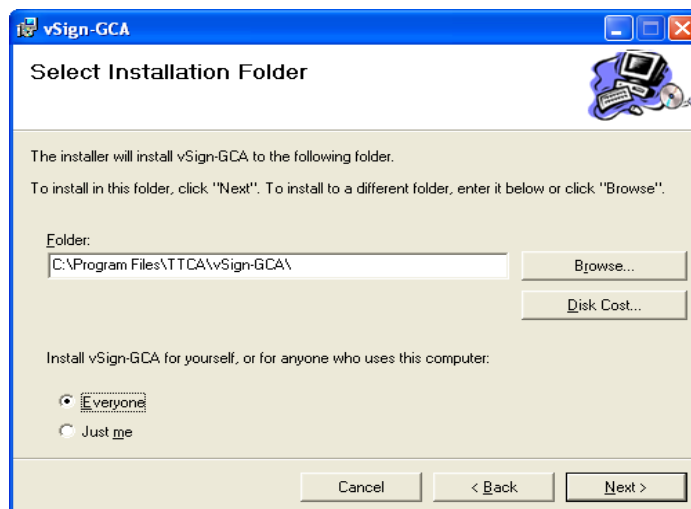
- Mở thư mục vSign Setup, chọn setup.exe.



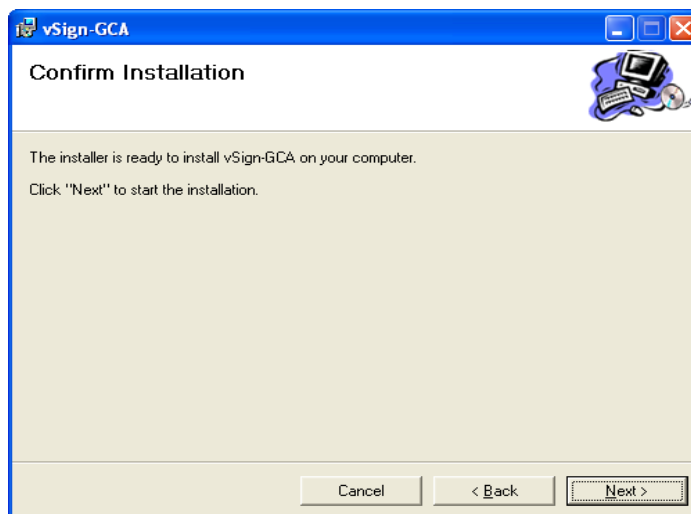
- Giao diện cài đặt



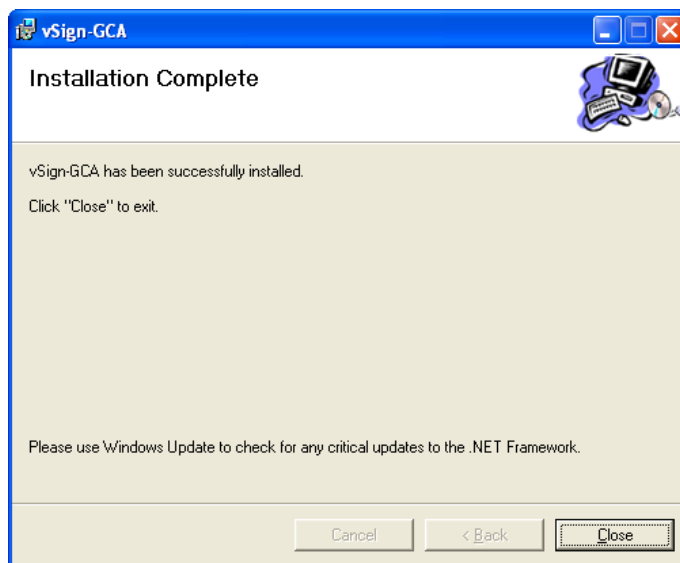
- Chọn Next



- Chọn **Next**



- Chọn **Next**



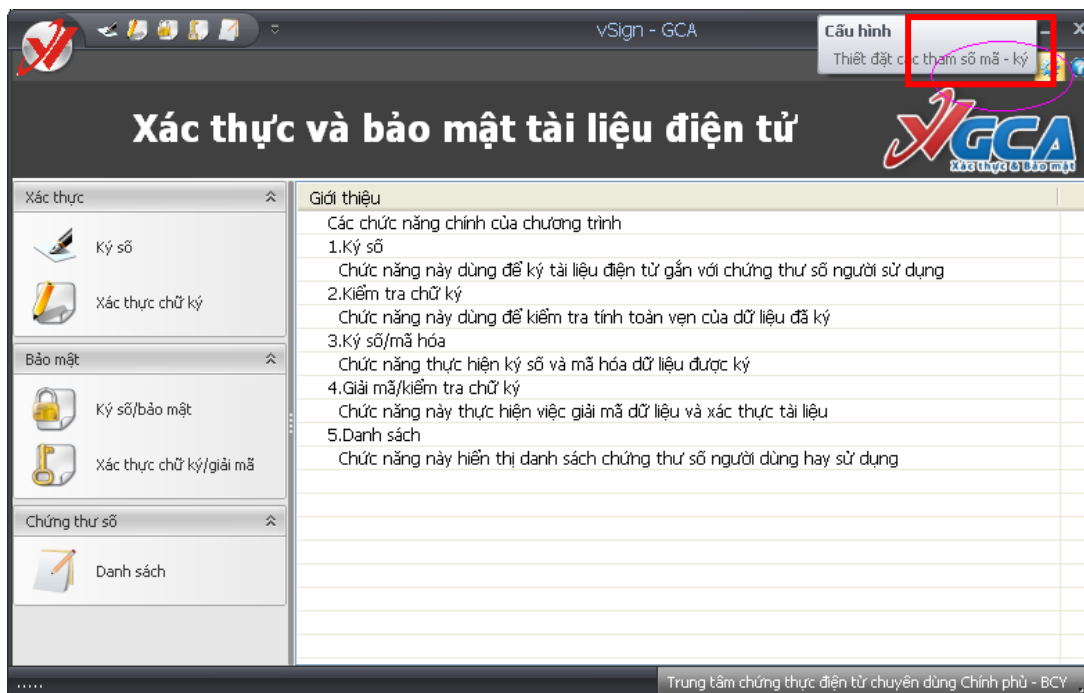
Chọn **Close** để kết thúc quá trình cài đặt.

2.3 Cấu hình cho phần mềm vSign2.0

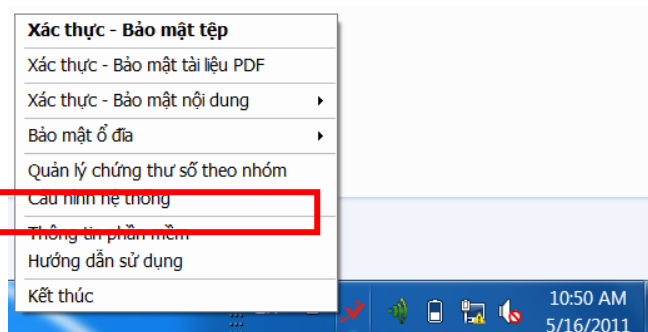
Chức năng cấu hình hệ thống giúp người sử dụng có thể sử dụng chương trình offline, không sử dụng các dịch vụ chứng thực chữ ký số khi xác thực và bảo mật dữ liệu.

Có hai cách để khởi động giao diện cấu hình cho phần mềm:

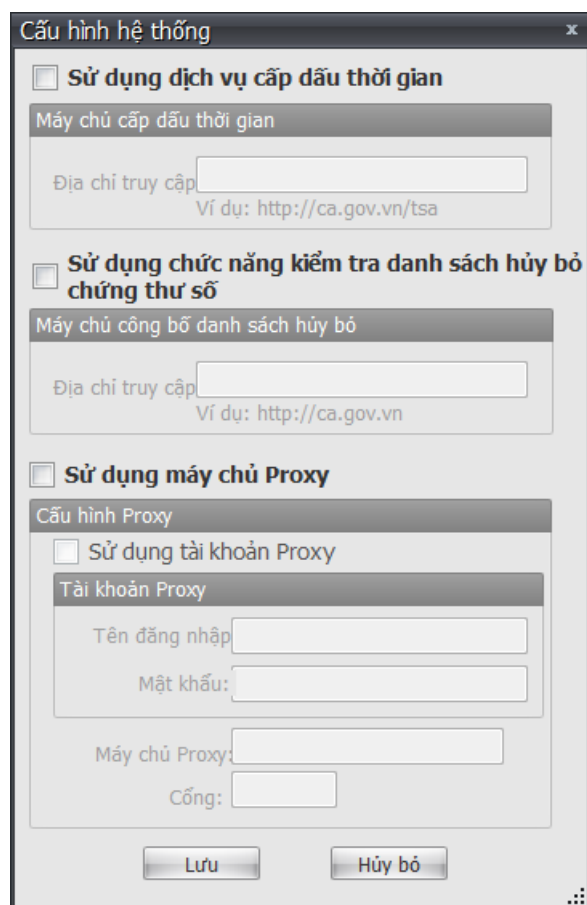
Cách 1: Từ giao diện chính click vào chức năng cấu hình.



Cách 2: Chuột phải vào TrayIcon trên khay hệ thống và chọn chức năng “Cấu hình”.



Thực hiện một trong hai cách trên giao diện cài đặt sẽ như sau:



2.3.1 Cấu hình tự động gắn dấu thời gian

Đánh dấu vào mục “Sử dụng dịch vụ tem thời gian” để cấu hình cho phép hệ thống tự động gắn dấu thời gian vào văn bản ký số, bảo mật.

Cấu hình hệ thống

☒ **Sử dụng dịch vụ cấp dấu thời gian**

Máy chủ cấp dấu thời gian

Địa chỉ truy cập:
Ví dụ:

☐ **Sử dụng chức năng kiểm tra danh sách hủy bỏ chứng thư số**

Máy chủ công bố danh sách hủy bỏ

Địa chỉ truy cập:
Ví dụ:

☐ **Sử dụng máy chủ Proxy**

Cấu hình Proxy

☐ Sử dụng tài khoản Proxy

Tài khoản Proxy

Tên đăng nhập:

Mật khẩu:

Máy chủ Proxy:

Cổng:

Gõ vào tên máy chủ cung cấp dịch vụ cấp dấu thời gian, máy chủ dấu thời gian của hệ thống PKI chuyên dùng Chính phủ <http://ca.gov.vn/tsa>, nhấp nút “Lưu” để lưu cấu hình.

2.3.2 Cấu hình kiểm tra danh sách hủy bỏ chứng thư số

Đánh dấu vào mục “Sử dụng kiểm tra danh sách hủy bỏ chứng thư số” để cấu hình cho phép hệ thống tự động truy cập danh sách hủy bỏ chứng thư số xác định tình trạng chứng thư số.

Cấu hình hệ thống

☒ **Sử dụng dịch vụ cấp dấu thời gian**

Máy chủ cấp dấu thời gian

Địa chỉ truy cập:
Ví dụ: http://ca.gov.vn/tsa

☒ **Sử dụng chức năng kiểm tra danh sách hủy bỏ chứng thư số**

Máy chủ công bố danh sách hủy bỏ

Địa chỉ truy cập:
Ví dụ: http://ca.gov.vn

☐ **Sử dụng máy chủ Proxy**

Cấu hình Proxy

☐ Sử dụng tài khoản Proxy

Tài khoản Proxy

Tên đăng nhập:

Mật khẩu:

Máy chủ Proxy:

Cổng:

Thông thường, địa chỉ máy chủ truy cập máy chủ CRL để trống, chương trình sẽ tự động tìm kiếm CRL, khi có máy chủ CRL khác với địa chỉ lưu trong chứng thư số thì mới phải nhập địa chỉ máy chủ CRL, nhấp nút “Lưu” để lưu cấu hình.

2.3.3 Cấu hình proxy

The screenshot shows the 'Cấu hình hệ thống' (System Configuration) window. The 'Sử dụng máy chủ Proxy' (Use Proxy Server) checkbox is checked and highlighted with a red rectangle. Below it, the 'Cấu hình Proxy' (Proxy Configuration) section is visible, containing the following fields:

- ☒ Sử dụng tài khoản Proxy
- Tài khoản: user01
- Mật khẩu: *****
- Máy chủ Proxy: ProxyServer
- Cổng: 8080

Other sections in the window include:

- ☒ Sử dụng dịch vụ cấp dấu thời gian (Use Time Stamping Service)
- Máy chủ cấp thời gian (Time Stamping Server): Địa chỉ máy chủ truy cập: http://ca.gov.vn/tsa
- ☒ Sử dụng chức năng kiểm tra danh sách hủy bỏ chứng thư số trực tuyến (Use Online Certificate Revocation List Checking)
- Máy chủ CRL (CRL Server): Địa chỉ máy chủ truy cập: http://ca.gov.vn

Buttons at the bottom: Lưu (Save), Hủy bỏ (Cancel).

Khi hệ thống có ProxyServer thì phải cấu hình sử dụng máy chủ Proxy cho chương trình, nhập tên máy chủ Proxy hoặc địa chỉ IP, nhập cổng (thường là 8080). Nếu có thiết lập tài khoản để đăng nhập Proxy thì nhập tài khoản và mật khẩu cho tài khoản.

Chú ý: với Proxy ISA người quản trị hệ thống cần cài đặt thêm một số phương thức xác thực kiểu Basic để chương trình hoạt động đúng.

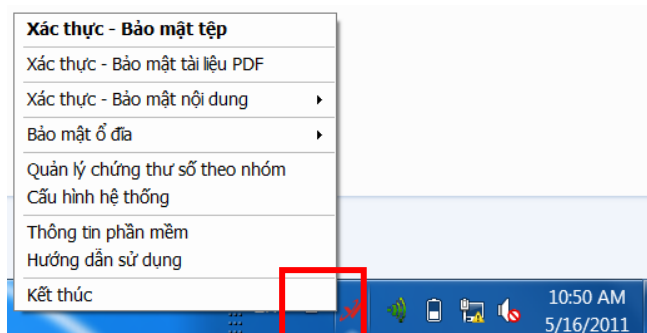
2.4 Hướng dẫn sử phần mềm vSign2.0 để ký số và bảo mật tài liệu điện tử

2.4.1 Khởi động chương trình xác thực và bảo mật tệp

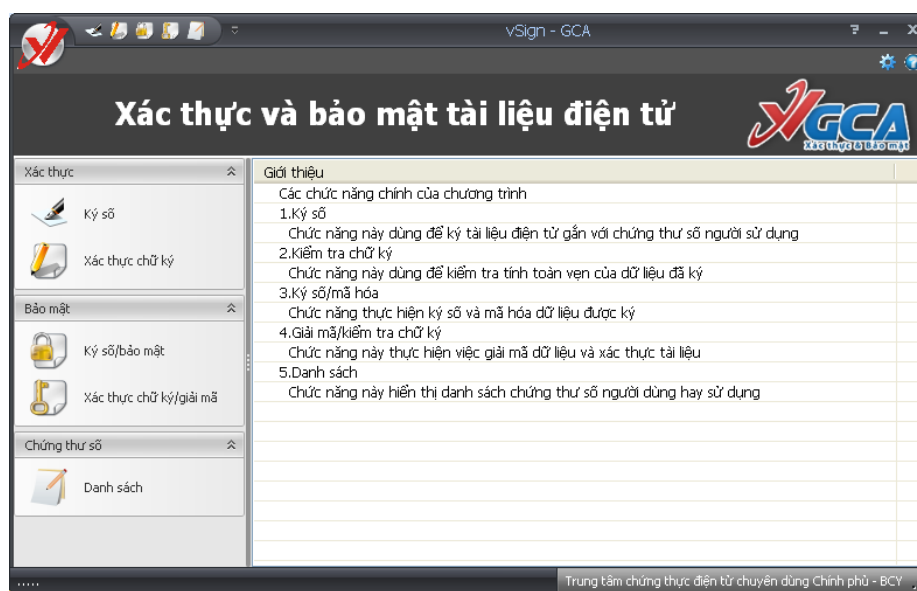
Để khởi động phần mềm kích đúp vào biểu tượng chữ “V” màu đỏ trên màn hình, hoặc chọn Start → Programs → VGCA → Xac Thuc - Bao Mat.exe.



Chương trình sau khi được khởi động sẽ thường trú trong bộ nhớ, biểu tượng của chương trình nằm dưới khay hệ thống.

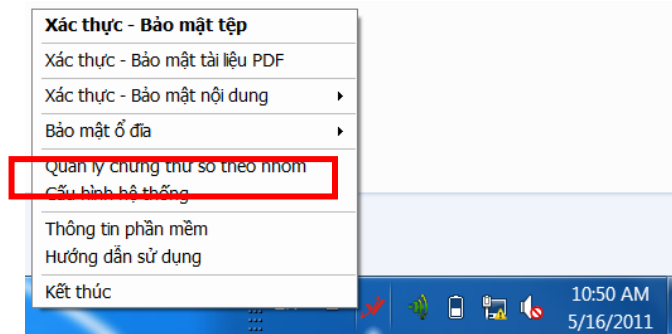


Giao diện chính của chương trình.

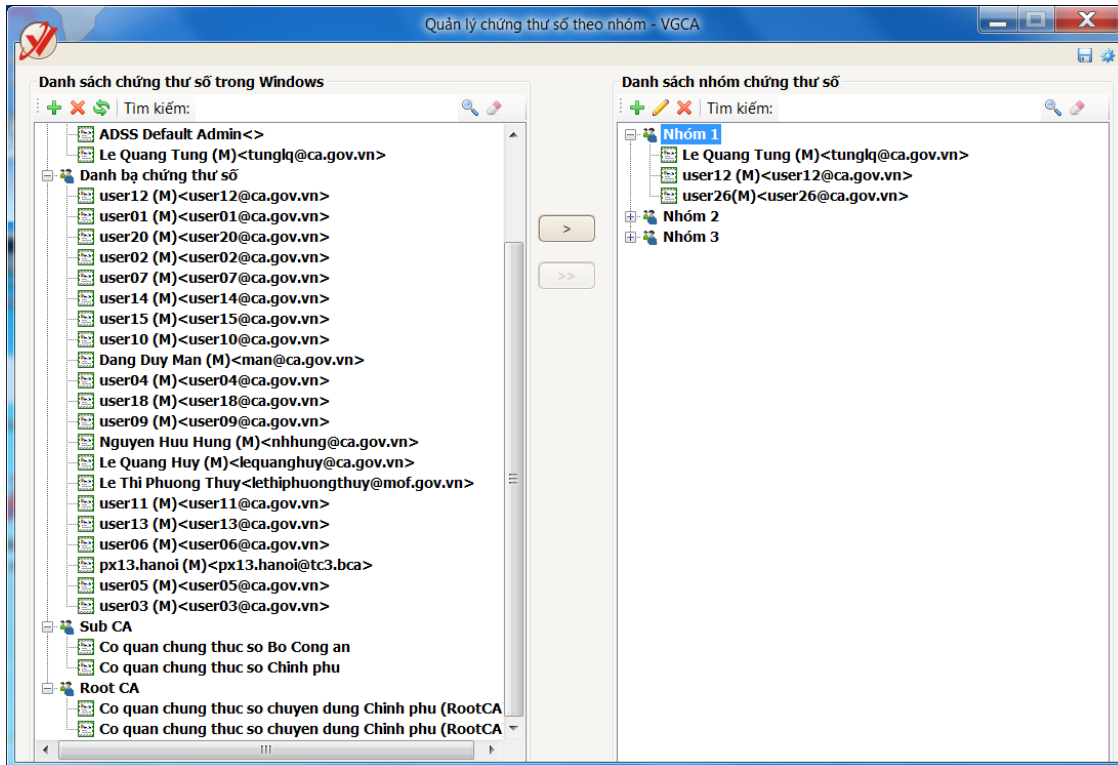


2.4.2 Quản lý chứng thư số theo nhóm

Chức năng quản lý chứng thư số theo nhóm giúp người sử dụng dễ dàng quản lý danh sách chứng thư số trong trường hợp danh sách chứng thư số lớn, để khởi động chức năng quản lý chứng thư số theo nhóm, bấm chuột phải vào biểu tượng chữ “V” màu đỏ ở góc phải màn hình.



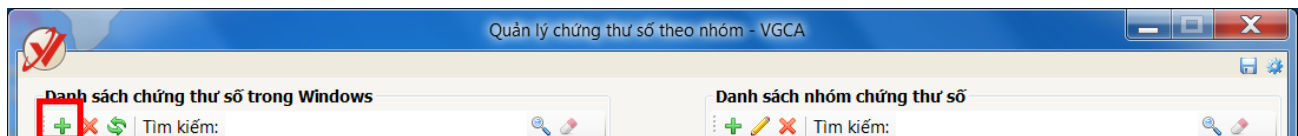
Giao diện chính của chức năng quản lý chứng thư số theo nhóm:



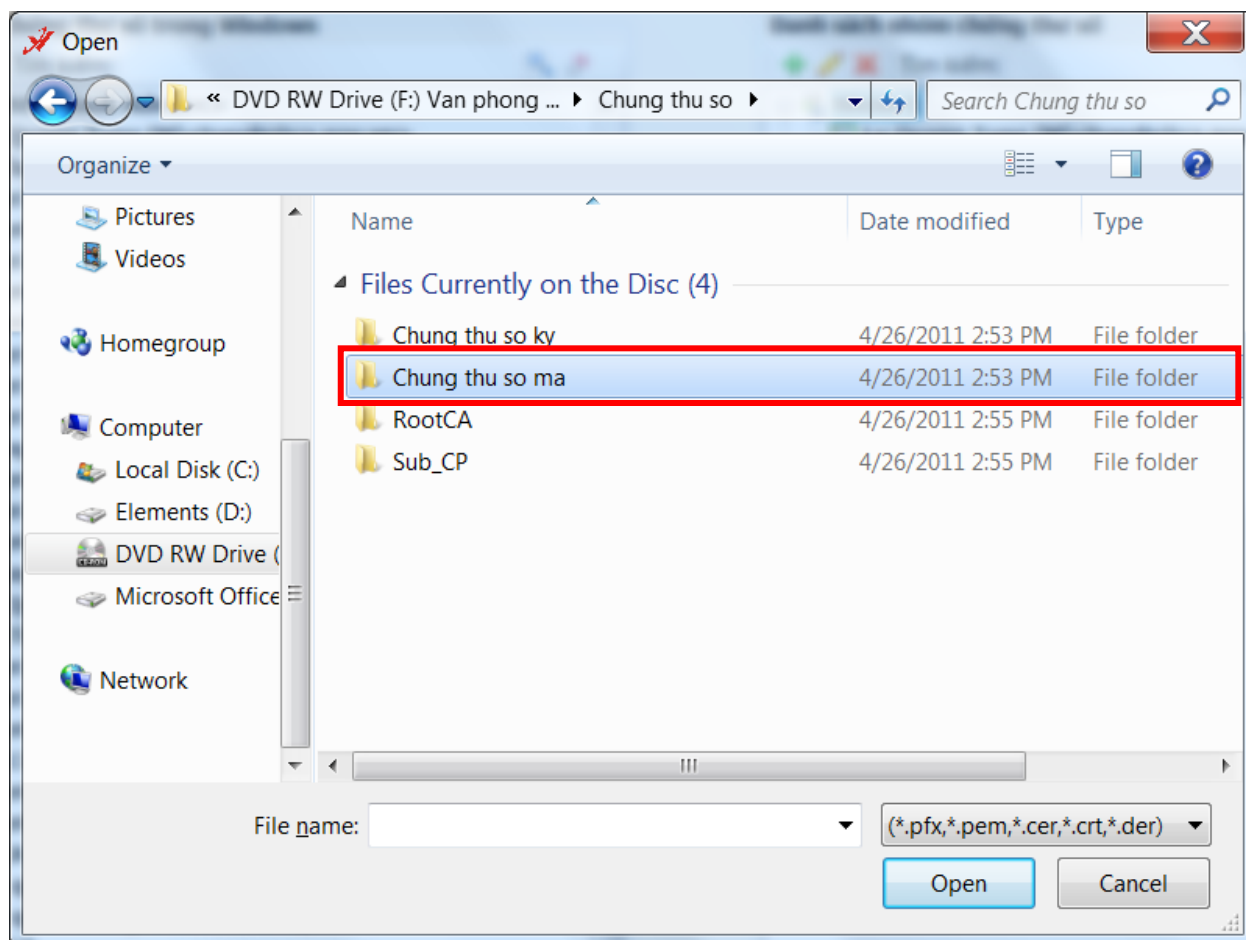
Giao diện có 02 cột, cột thứ nhất chứa các chứng thư số trong kho lưu trữ của hệ điều hành windows, cột thứ 2 thể hiện các nhóm chứng thư số.

Trong cột thứ nhất, người sử dụng có thể cài đặt thêm các chứng thư số (có thể cài đặt nhiều chứng thư số cùng một lúc) hoặc xóa chứng thư số (có thể xóa nhiều chứng thư số).

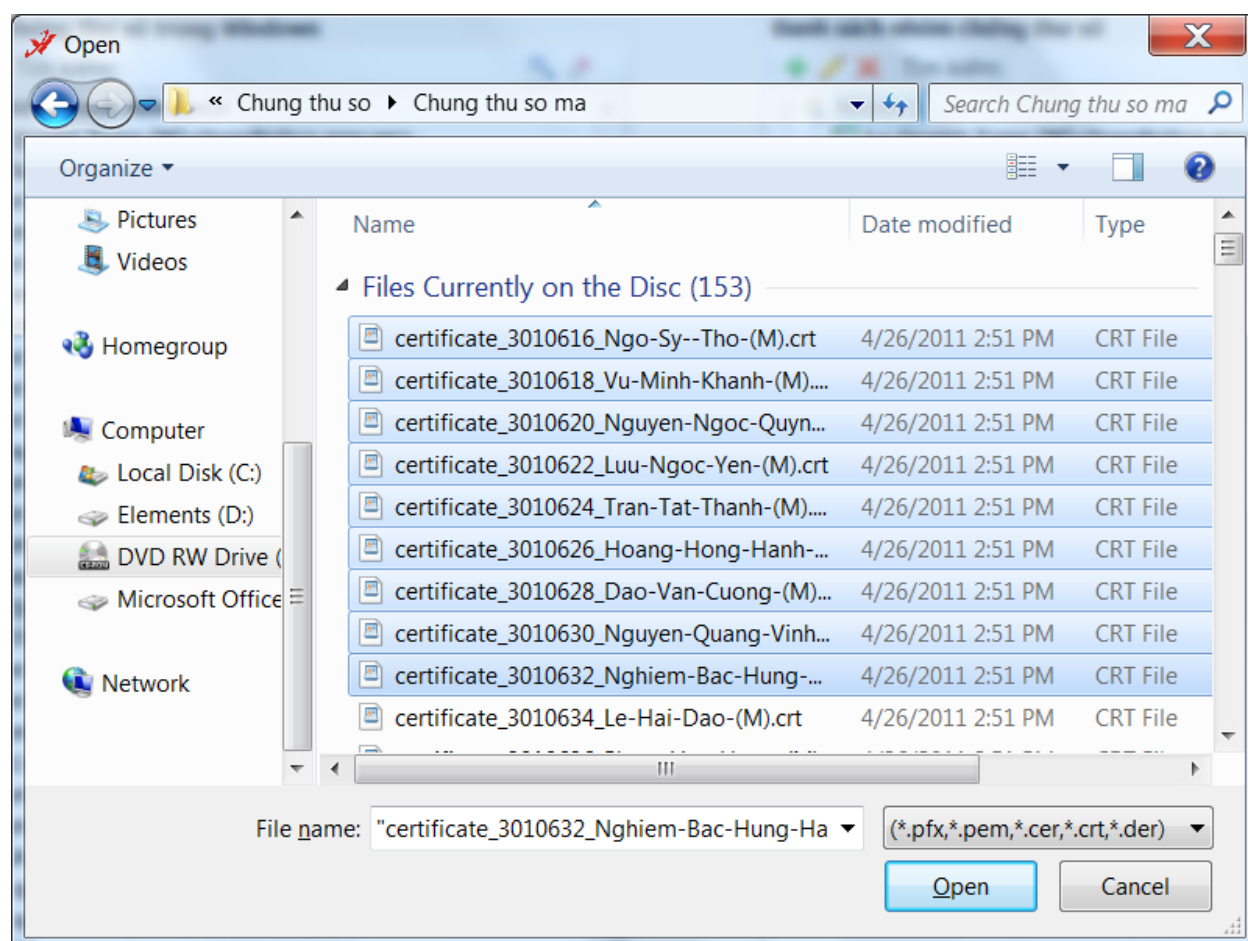
Để thêm chứng thư số vào cột 1, chọn biểu tượng dấu cộng màu xanh bên góc trái:



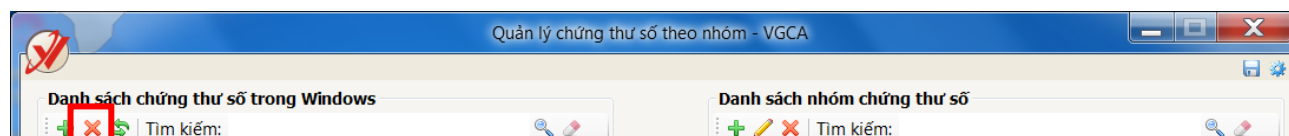
Có thể thêm nhiều chứng thư số, để thêm chứng thư số, đưa đĩa CD được cấp phát theo bộ GCA-01 vào:



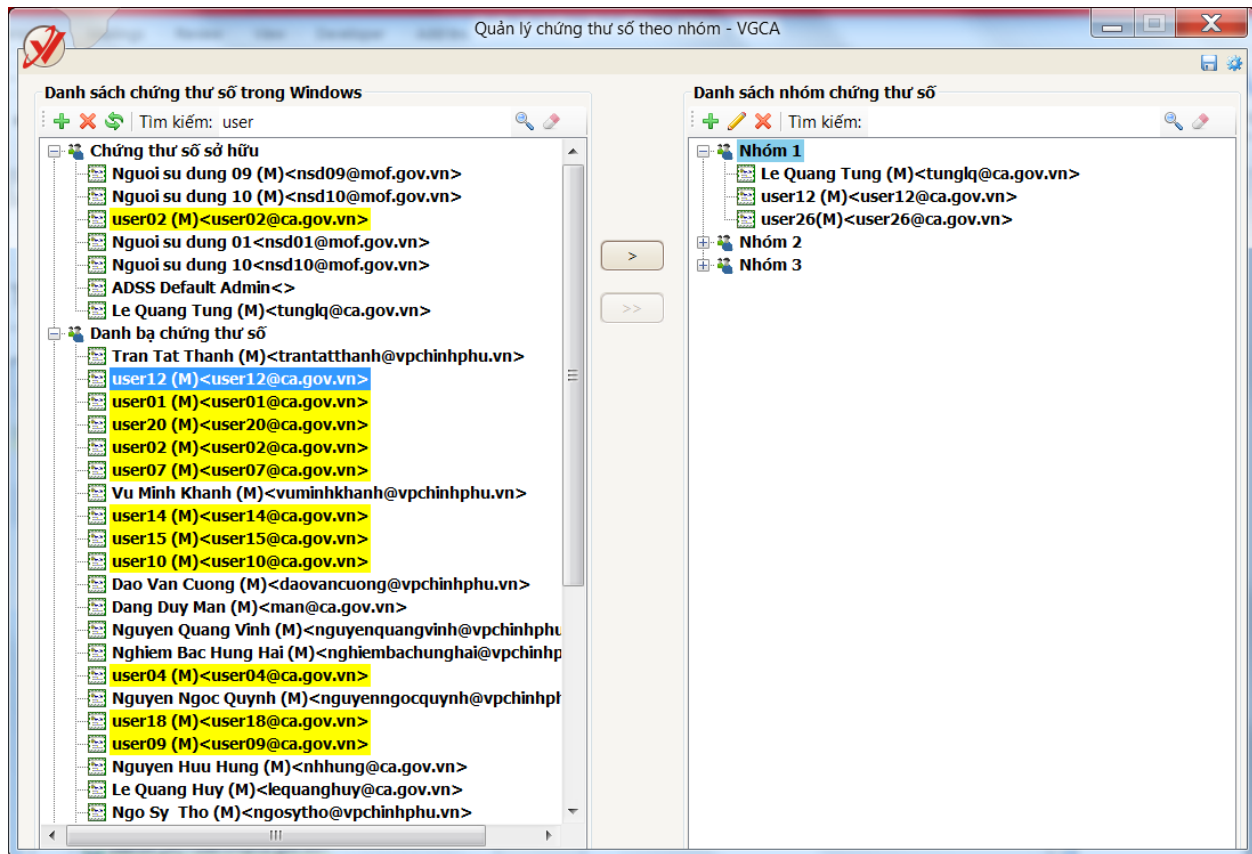
Chọn thư mục chứng thư số mã, lưu ý người sử dụng chỉ sử dụng chứng thư số mã:



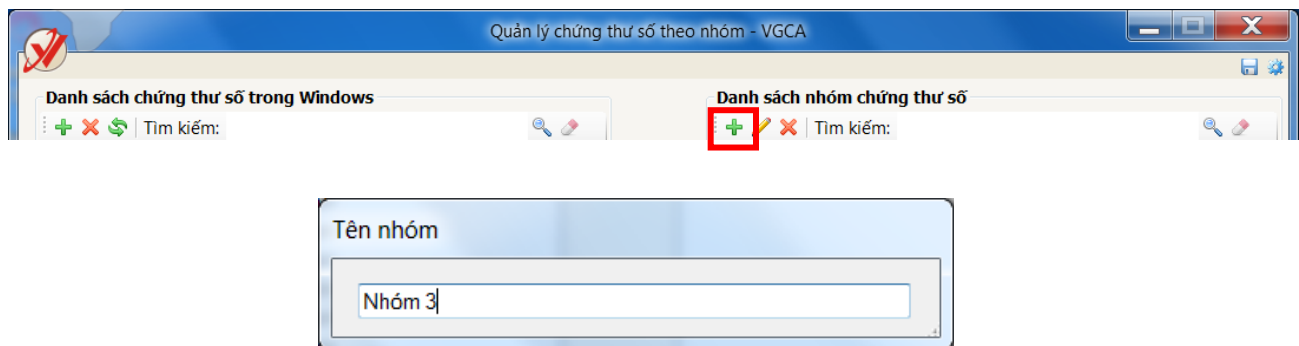
Để xóa chứng thư số trong cột một, chọn chứng thư số cần xóa (có thể chọn nhiều chứng thư số để xóa) sau đó chọn biểu tượng “x” bên góc trái để xóa các chứng thư số.



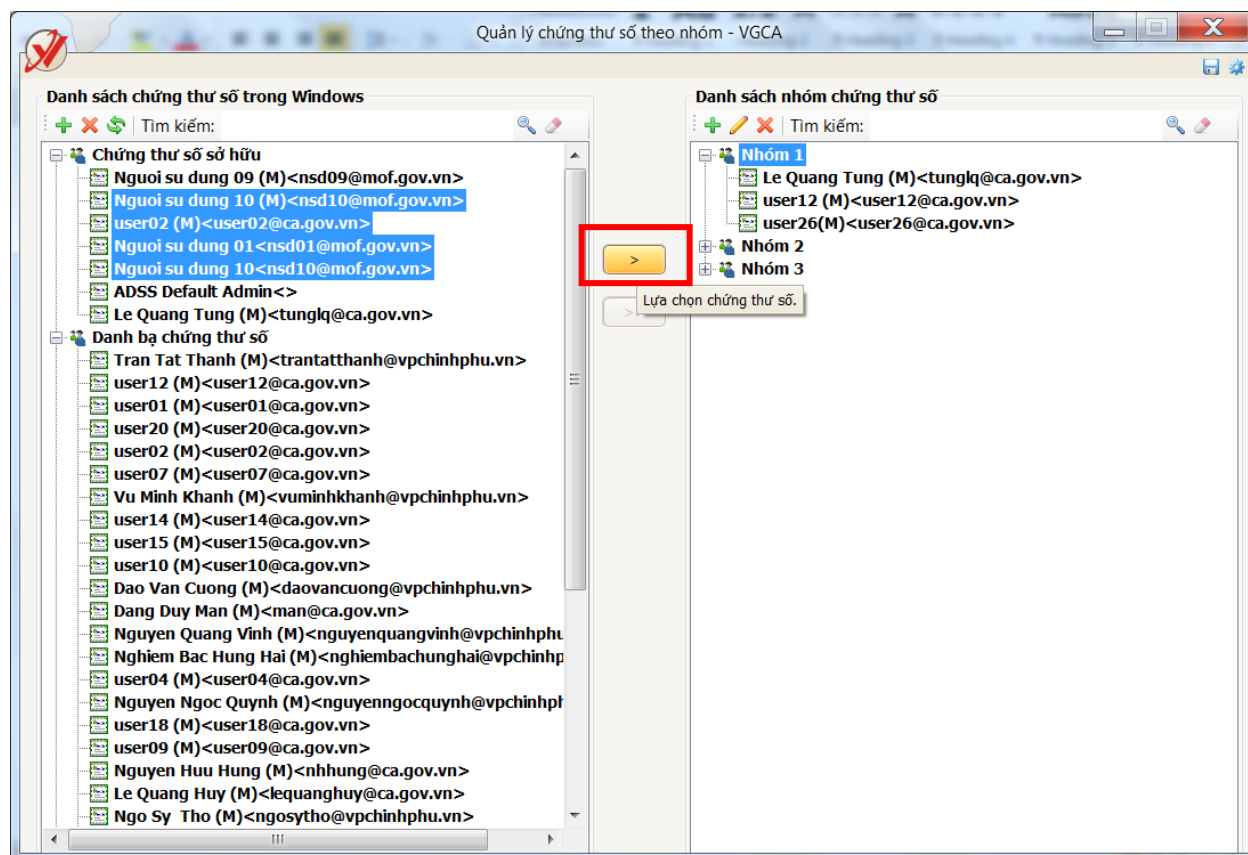
Để tìm kiếm các chứng thư số bên cột 1 có thể sử dụng chức năng tìm kiếm đặt góc dưới cột 1, gõ tên chứng thư số cần tìm vào ô tìm kiếm, các chứng thư số có chứa dãy ký tự tìm kiếm sẽ được đánh dấu màu vàng.



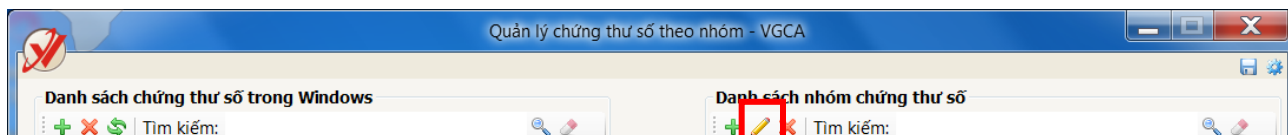
Trong cột thứ 2, người sử dụng có thể tạo nhóm của mình để dễ dàng quản lý chứng thư phục vụ cho quá trình mã hóa được dễ dàng hơn, để tạo một nhóm bấm nút dấu cộng màu xanh bên phải:



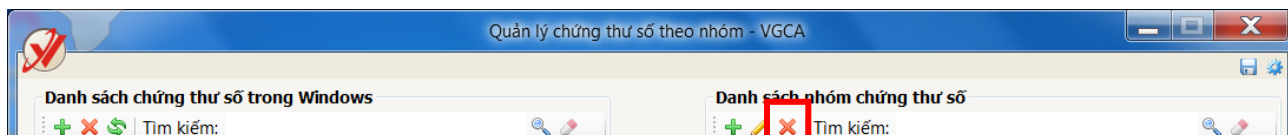
Nhập tên nhóm và bấm Enter để kết thúc thêm nhóm, để thêm chứng thư số vào nhóm, chọn nhóm cần thêm chứng thư số ở cột thứ 2, sau đó chọn các chứng thư số cần thêm ở cột thứ nhất, có thể thêm nhiều chứng thư số, chọn dấu mũi tên ở giữa 2 cột để thêm chứng thư số vào nhóm, hoặc có thể sử dụng chuột để kéo thả các chứng thư số từ cột 1 sang cột 2.



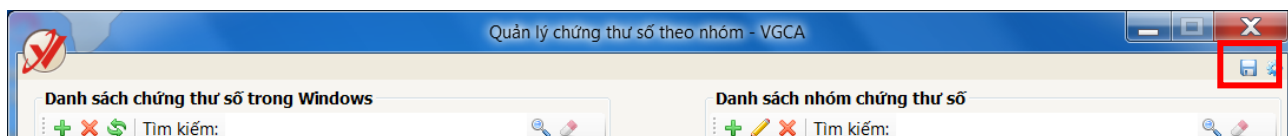
Để sửa nhóm: chọn nhóm cần sửa sau đó chọn chức năng sửa nhóm (hình cây bút trên góc phải), sau đó nhập tên mới của nhóm và bấm Enter để kết thúc quá trình sửa.



Để xóa nhóm: chọn nhóm cần xóa và bấm biểu tượng "x" ở bên góc phải để xóa nhóm.



Để lưu quá trình tạo nhóm chứng thư số, bấm vào biểu tượng hình đĩa mềm bên góc phải để lưu.



Để tìm kiếm chứng thư số trong cột 2, tương tự chức năng tìm kiếm trong cột 1, chức năng tìm kiếm chứng thư số trong cột 2 nằm phía dưới cột 2, nhập chuỗi ký tự tìm

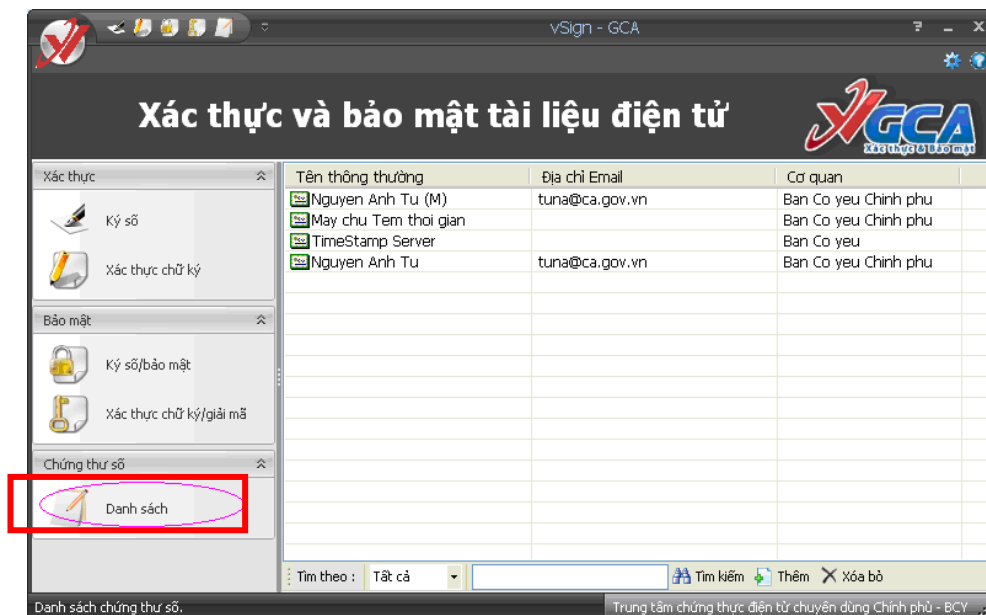
kiểm để tìm kiếm các chứng thư số, các chứng thư số có chứa chuỗi tìm kiếm sẽ được đánh dấu màu vàng.

2.4.3 Quản lý danh sách chứng thư số

Danh sách chứng thư số liệt kê các chứng thư số của các thuê bao cần giao dịch. Danh sách này được lưu trong registry của hệ thống của Windows.

Bước 1: Xem danh sách chứng thư số.

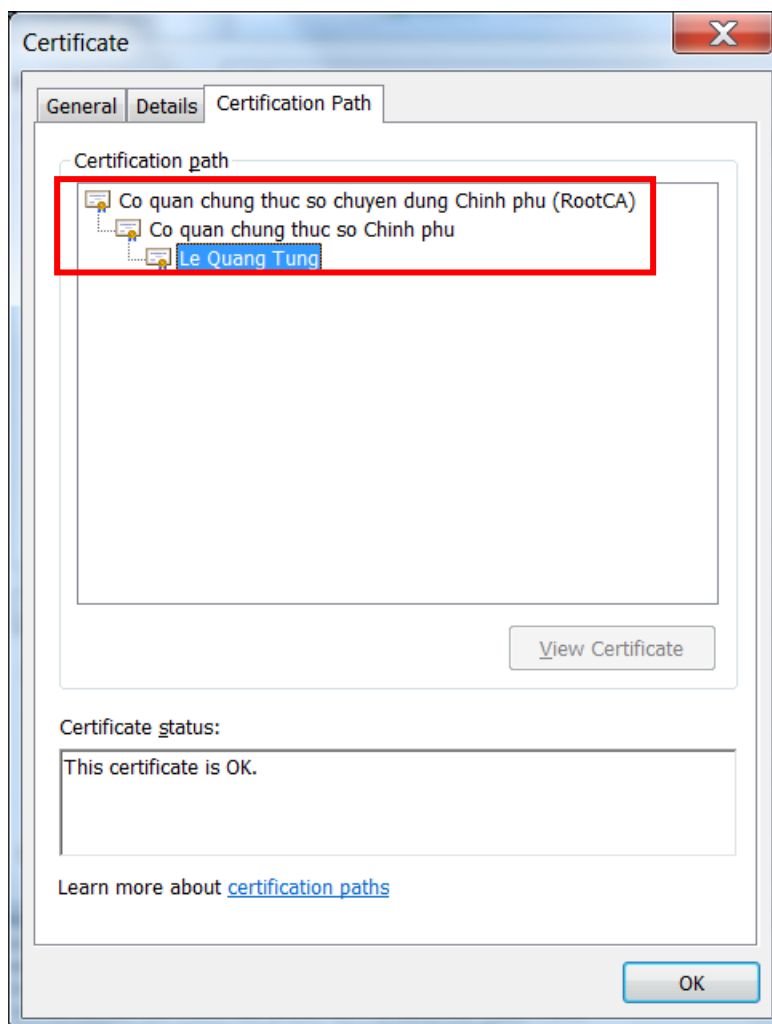
Từ giao diện chính của chương trình nhấp vào “Danh sách” để hiển thị danh sách chứng thư số.



Ở giao diện này người sử dụng có thể “Tìm kiếm” chứng thư số trong danh sách chứng thư số.

Bước 2: Thêm chứng thư số RootCA và SubCA

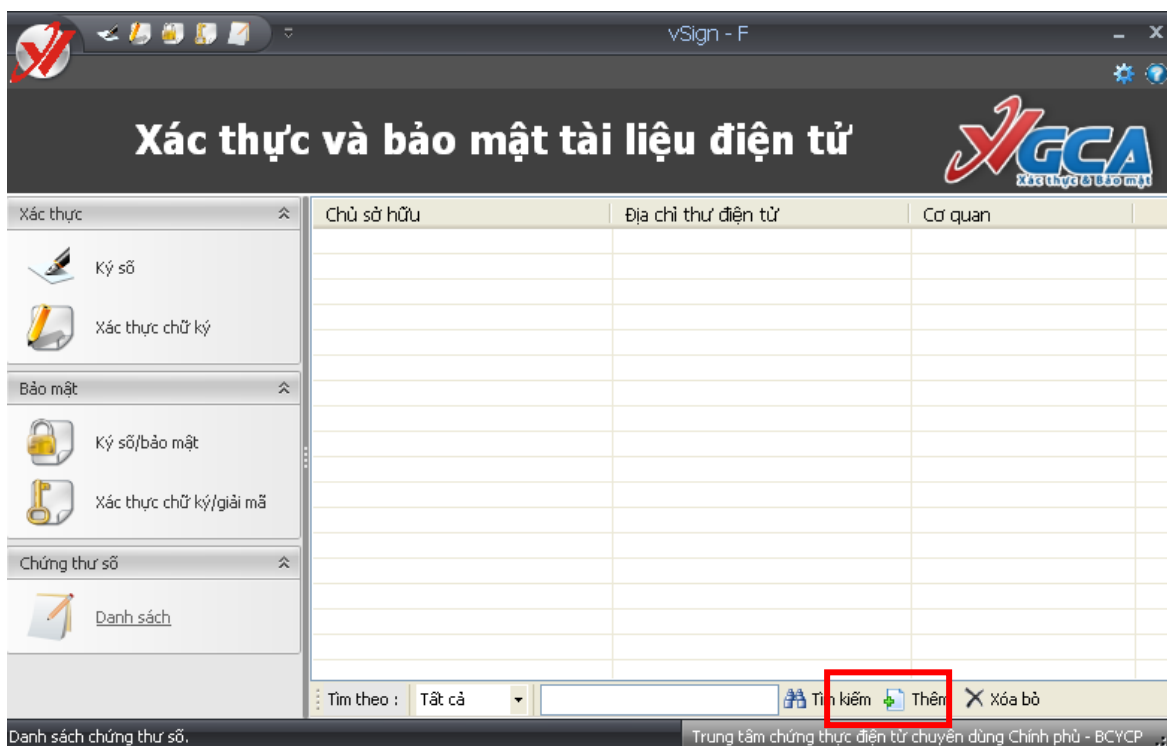
Chứng thư số của RootCA và của SubCA phải được cài đặt để tạo ra đường dẫn chứng thực đúng của chứng thư số.



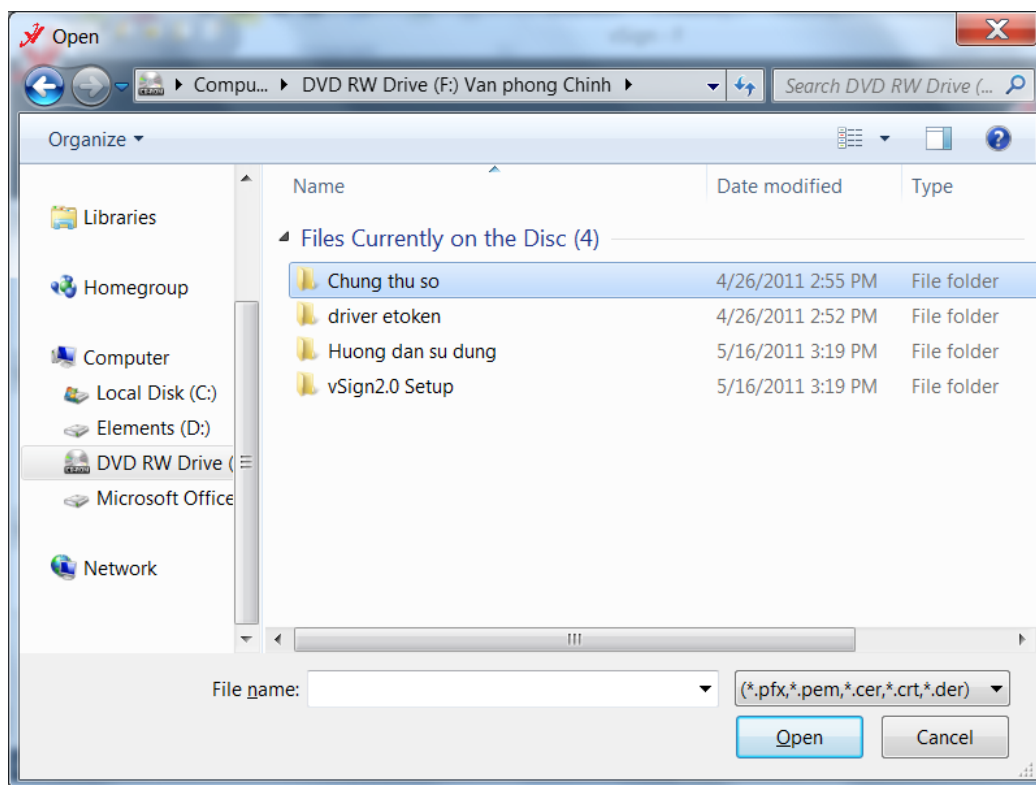
Việc cài đặt chứng thư số của RootCA và SubCA chỉ thực hiện 1 lần duy nhất trên một máy tính (khi dỡ bỏ phần mềm, chứng thư số của RootCA và SubCA cũng không bị dỡ bỏ)

Để cài đặt chứng thư số của RootCA, SubCA:

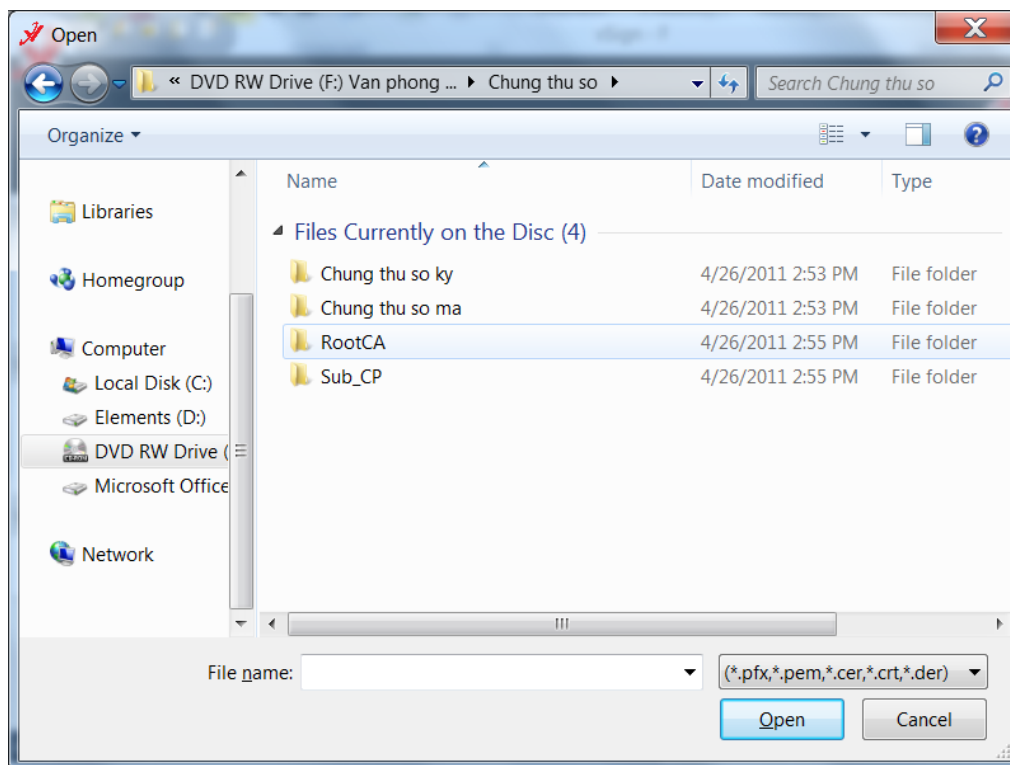
- Cho đĩa CD được cấp phát vào ổ đĩa CD-ROM
- Chọn nút “Thêm” trên giao diện chương trình vSign



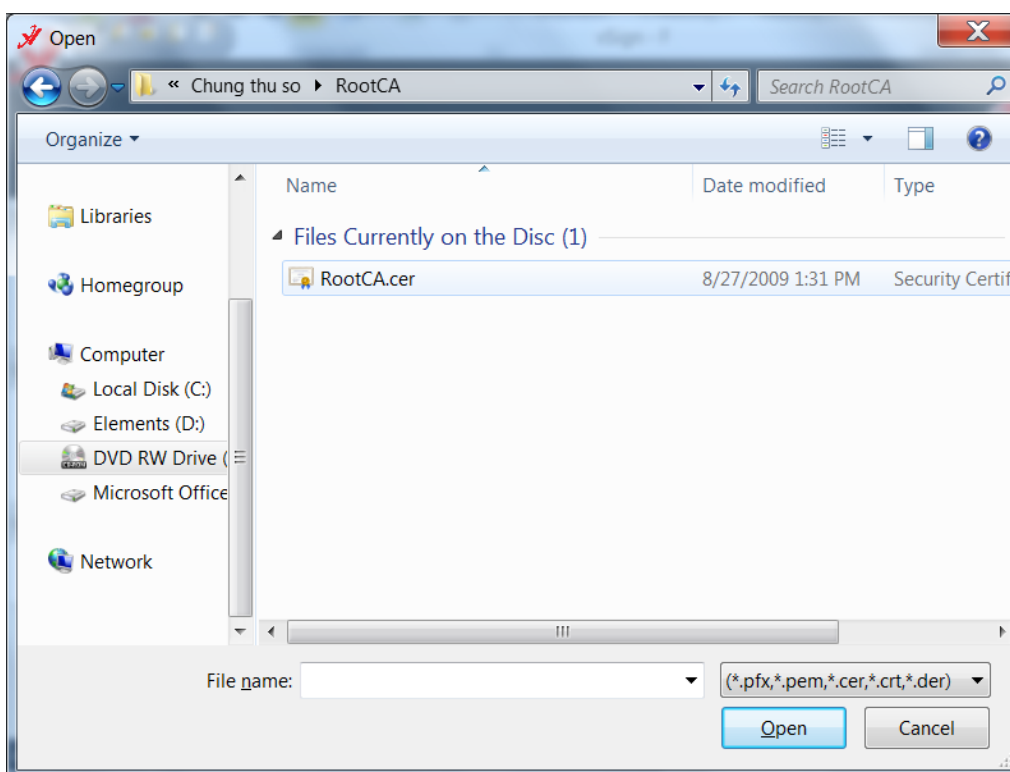
- Chọn thư mục lưu chứng thư số trên đĩa CD



- Chọn thư mục “Chung thu so”



- Chọn thư mục RootCA



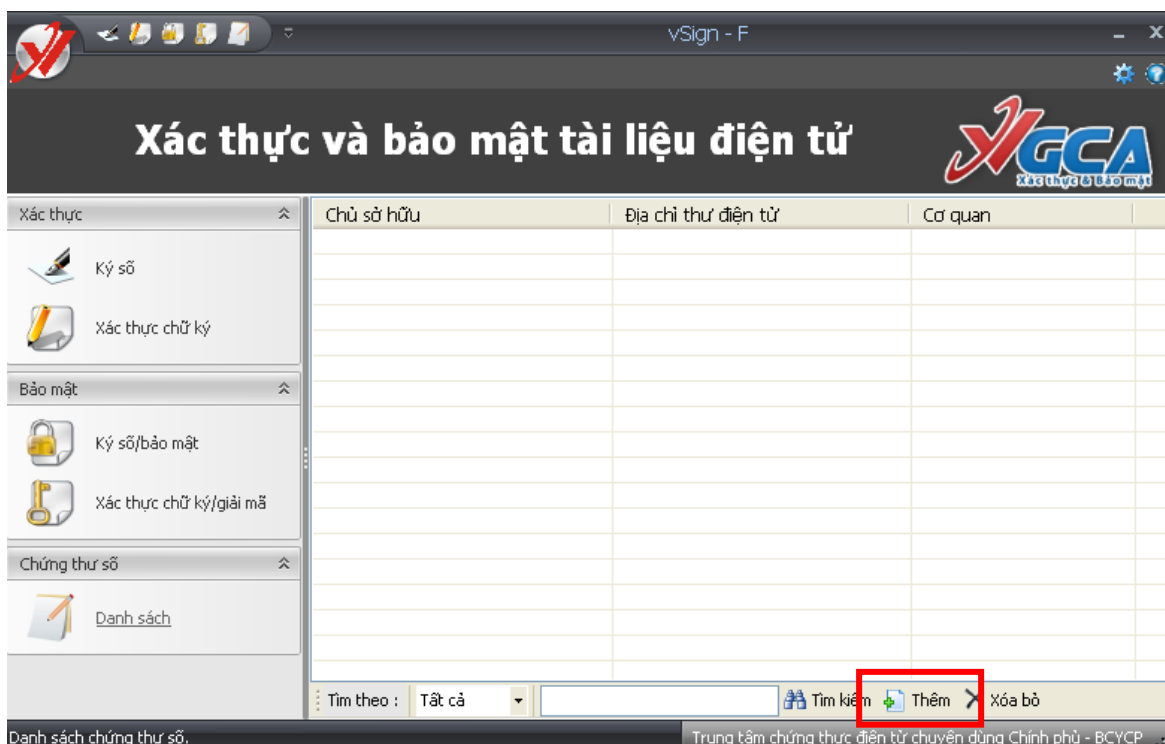
- Chọn chứng thư số RootCA.cer để cài đặt

- Để cài đặt chứng thư số của SubCA làm tương tự như cài đặt chứng thư số của RootCA

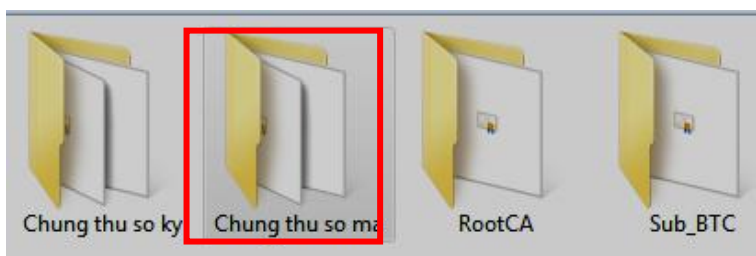
Bước 3: Thêm chứng thư số

Mục đích của thêm chứng thư số là để bảo mật tài liệu gửi cho những người sở hữu chứng thư số được thêm vào danh sách, chỉ cần nhập các chứng thư số mã (có ký hiệu “M”). Khi muốn gửi tài liệu có bảo mật cho một ai đó người sử dụng phải có được chứng thư số của người đó. Để có được chứng thư số của đối tác cần gửi, người sử dụng có thể lên kho chứng thư số công cộng để lấy về hoặc lấy trong đĩa CD được cấp phát kèm theo. Để thêm chứng thư số làm như sau;

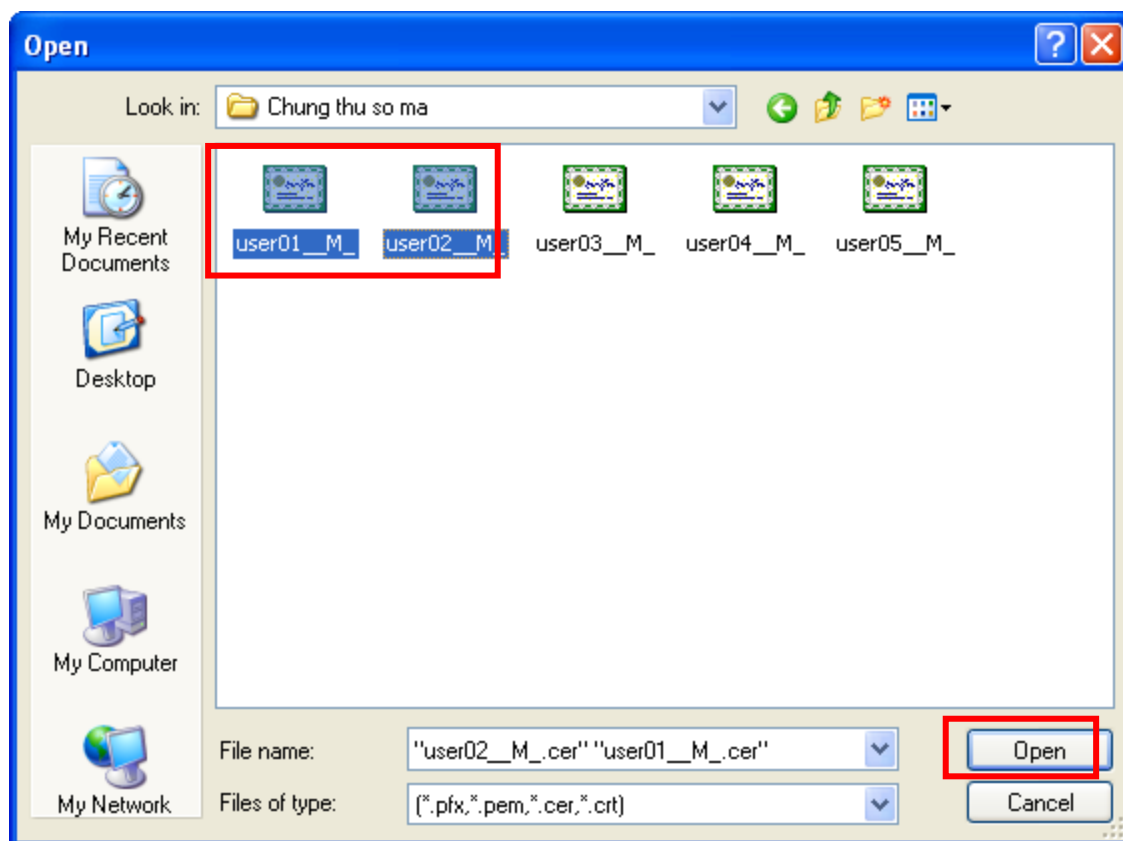
- Cho đĩa CD được cấp phát vào ổ đĩa CD-ROM.
- Chọn nút “Thêm” trên giao diện chương trình vSign.



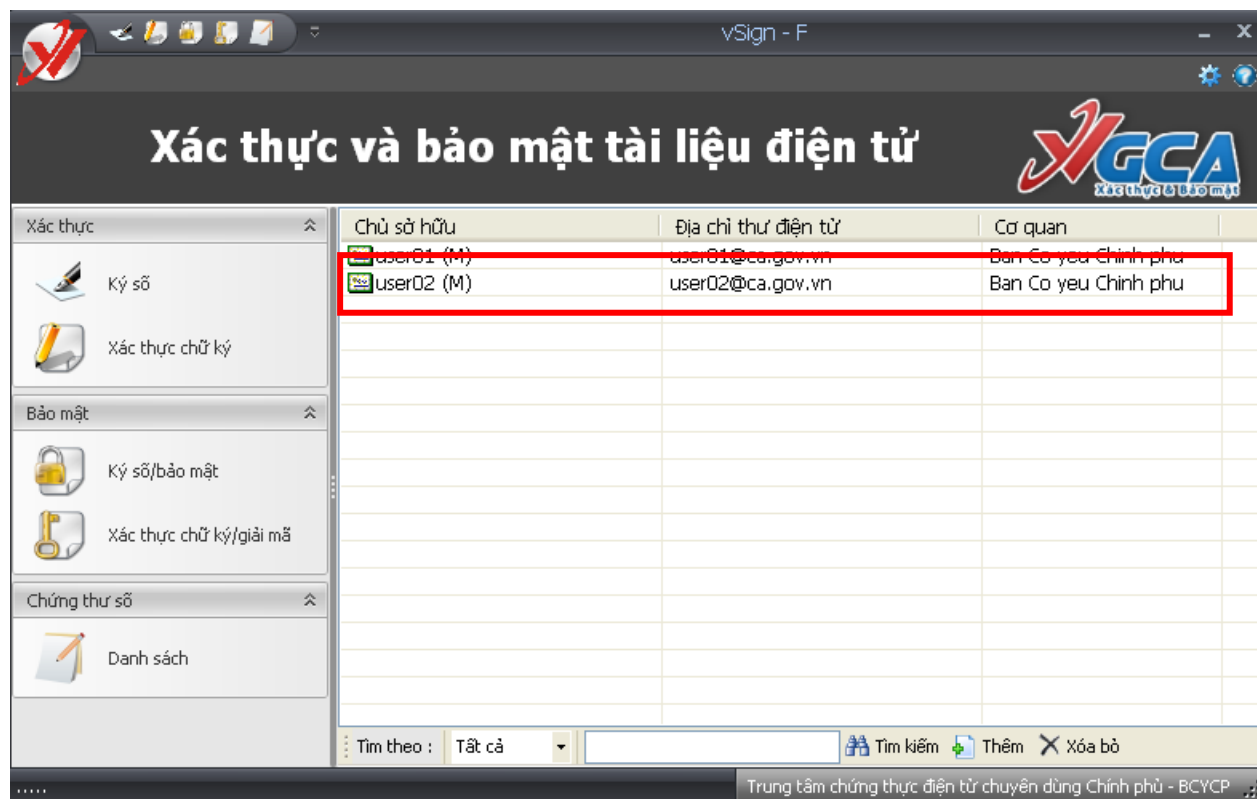
- Chọn thư mục “chung thu so”.
- Chọn thư mục “chung thu so ma” trên đĩa CD.



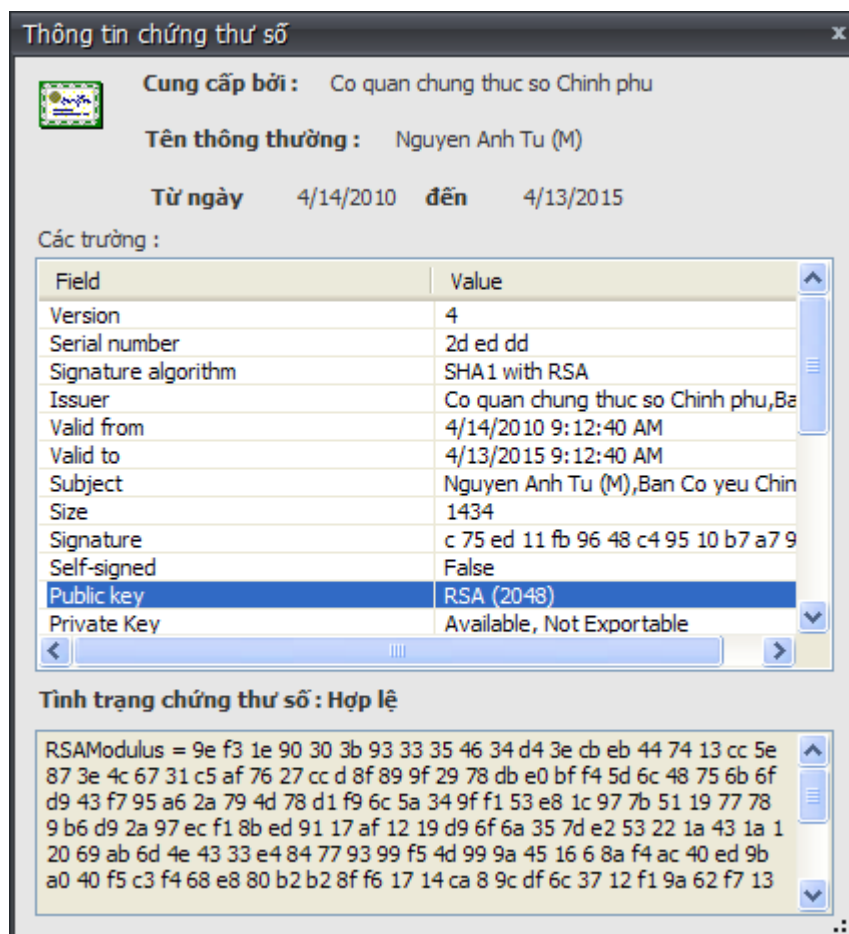
- Chọn các chứng thư số cần cài đặt, có thể chọn cài nhiều chứng thư số cùng một lúc.
- Lưu ý chỉ cần cài đặt chứng thư số mã có ký tự (M).



- Các chứng thư số đã được thêm vào danh sách.



- Click đúp vào tên thông thường để xem thông tin chi tiết chứng thư số.



Khi xem một chứng thư số, chương trình sẽ tự động kiểm tra tình trạng chứng thư số.

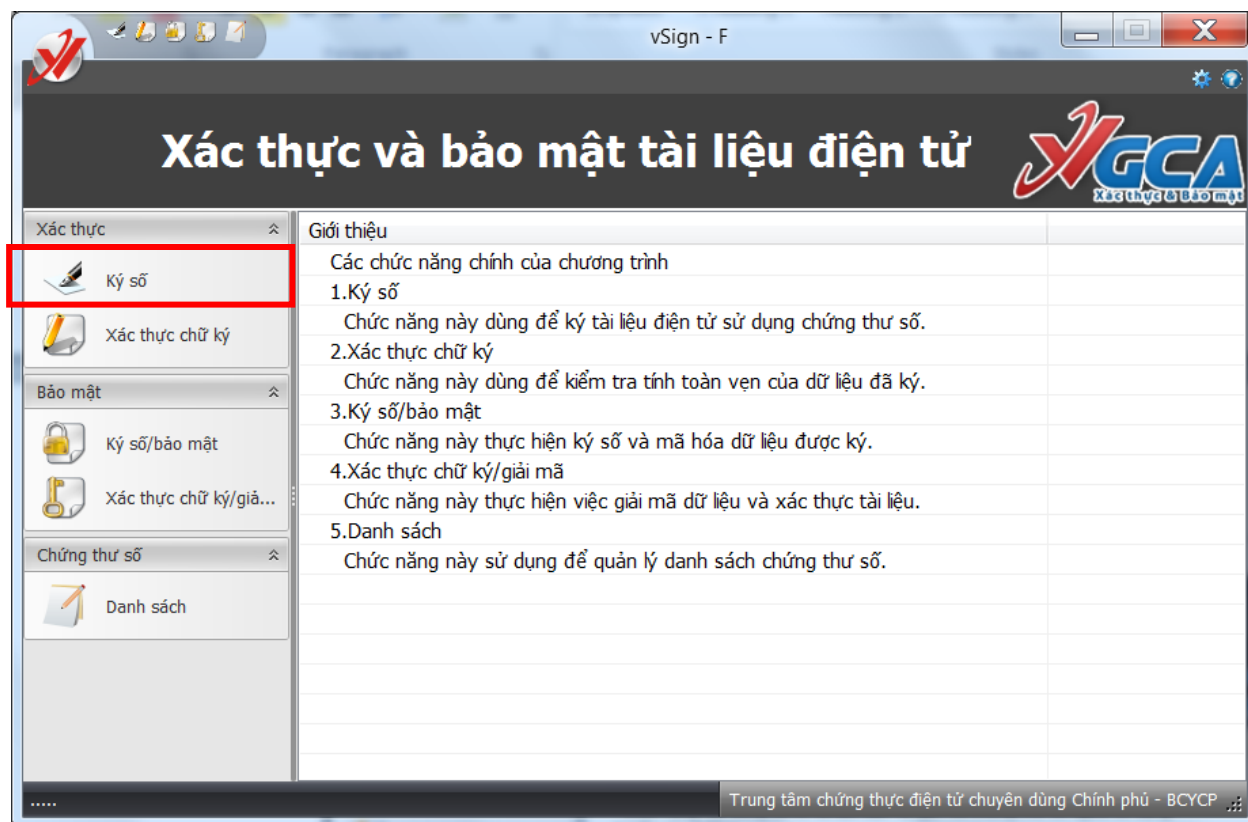
2.4.4 Các chức năng chính của xác thực và bảo mật tệp

Ký số tệp dữ liệu

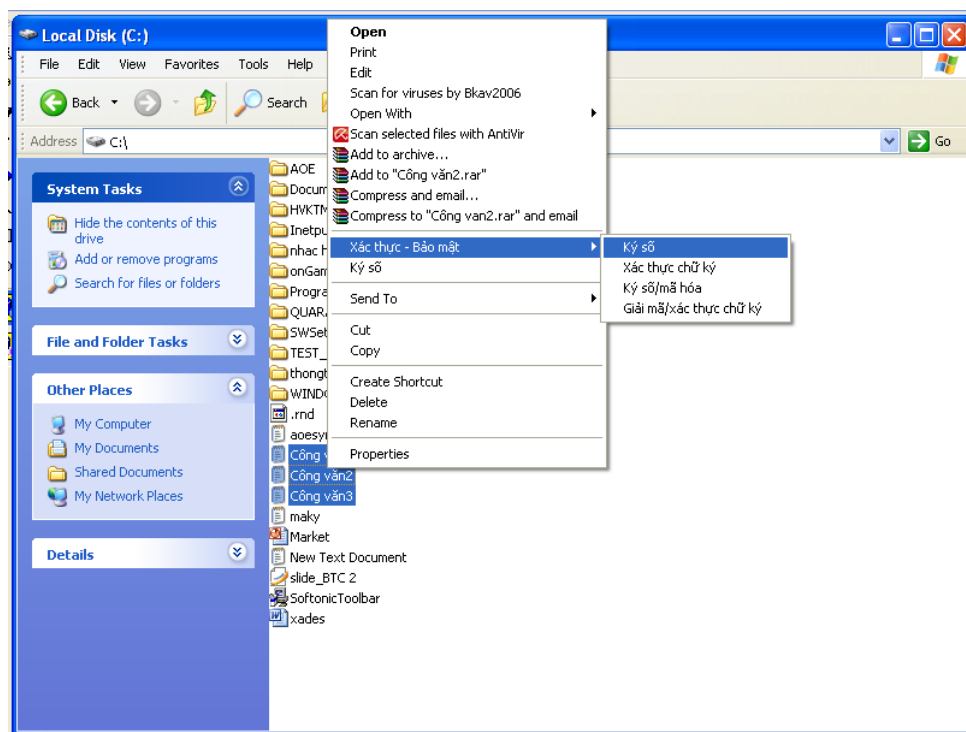
Có 2 cách để ký số tệp dữ liệu bao gồm: sử dụng chức năng “Ký số” trong giao diện chính của chương trình, hoặc từ thực đơn ngữ cảnh của Windows nhấp chuột phải vào tệp chuẩn bị ký số sau đó chọn “Xác thực – Bảo mật” -> “Ký số”.

Bước 1: chọn cách ký số tệp dữ liệu.

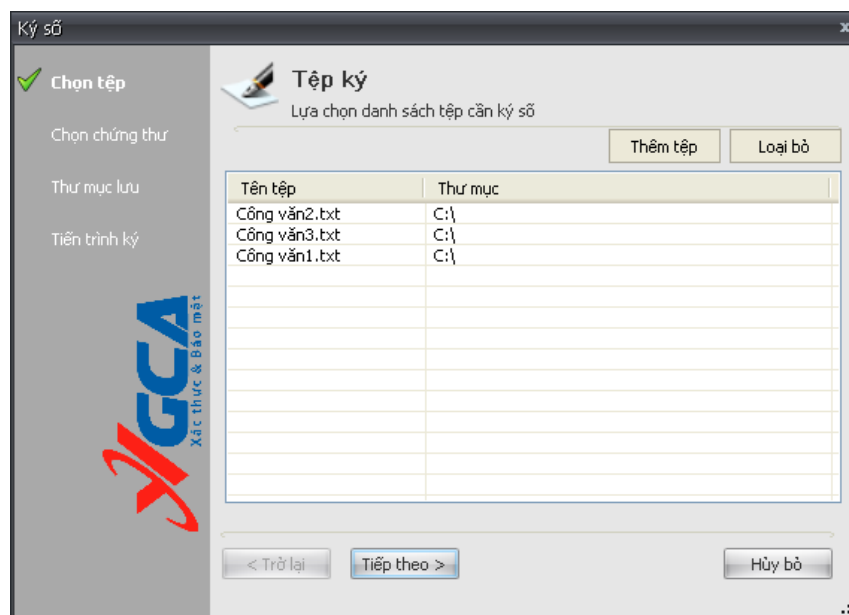
Cách 1 : ký số trong giao diện chính của chương trình.



Cách 2 : Ký từ thực đơn chuột phải.



Giao diện ký hiển thị như sau :

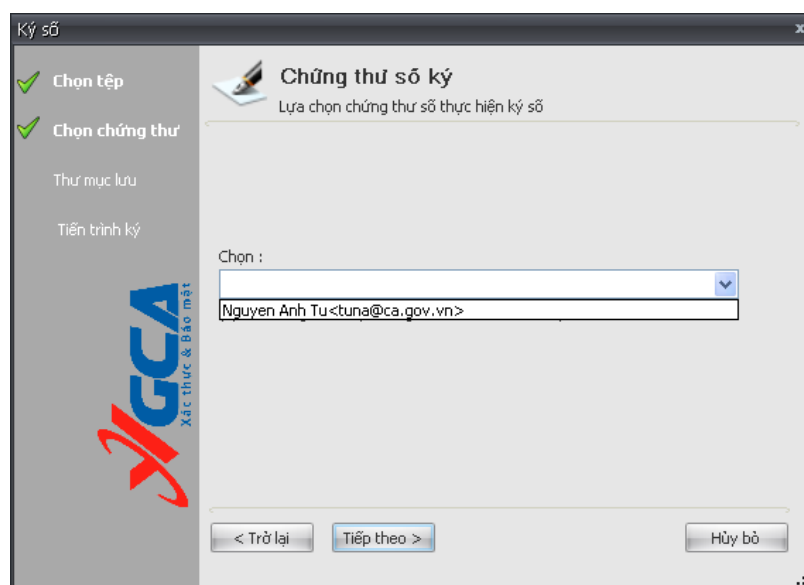


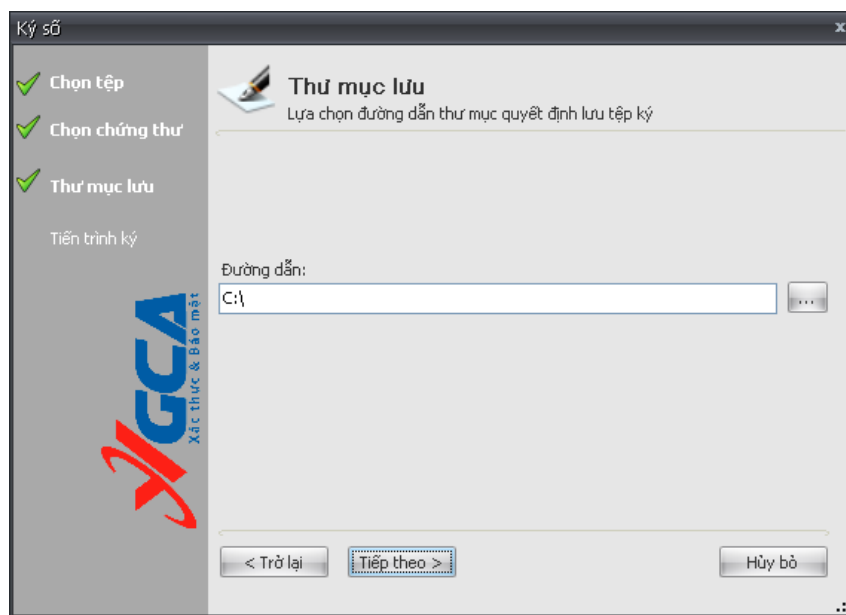
Bước 2: Thêm tệp, xóa tệp vào danh sách.

Bằng cách nhấp vào nút “Thêm tệp” hoặc loại bỏ tệp ra khỏi danh sách bằng cách nhấp vào nút “Loại bỏ”.

Nhấp “Tiếp theo” để tiến trình ký số được tiếp tục.

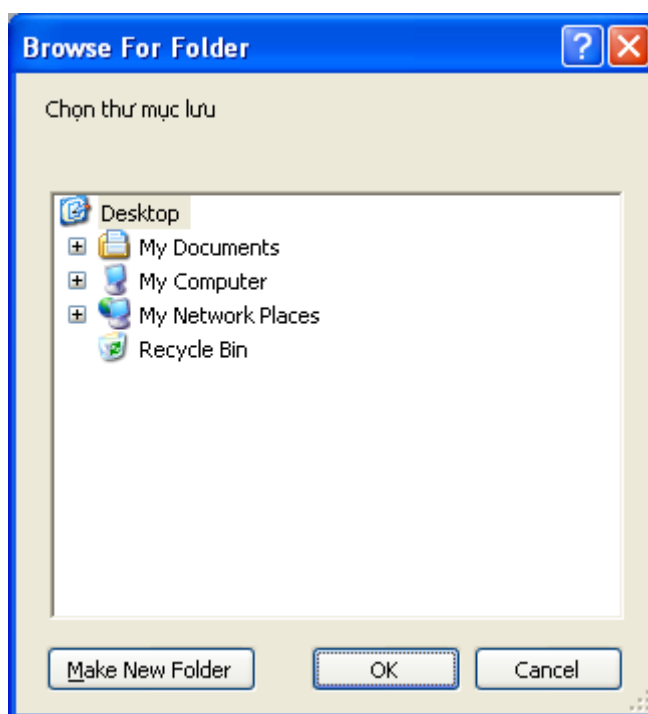
Bước 3: Chọn chứng thư số sử dụng để ký số dữ liệu.





Nhấp “Tiếp theo” để tiến trình ký số được tiếp tục.

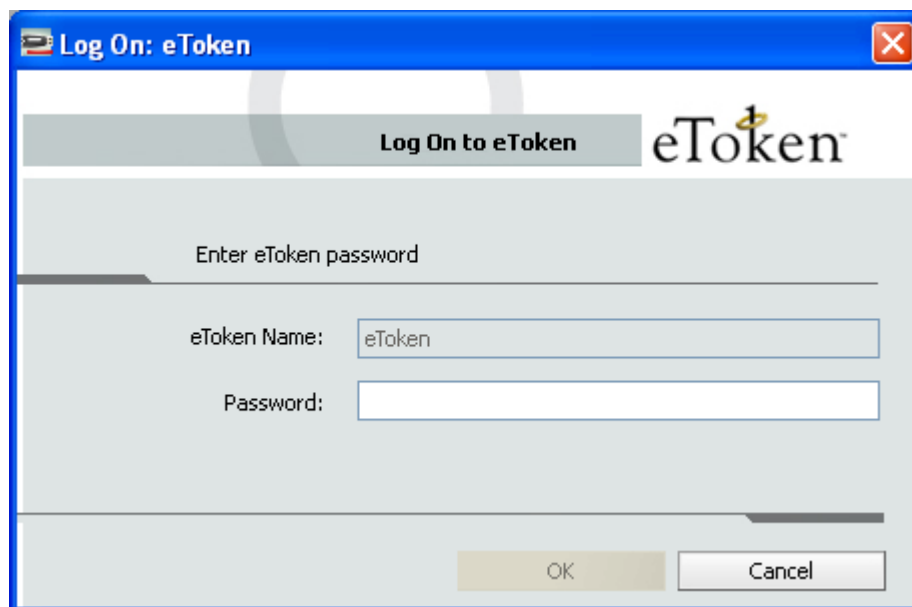
Bước 4: Chọn đường dẫn lưu tệp ký số.



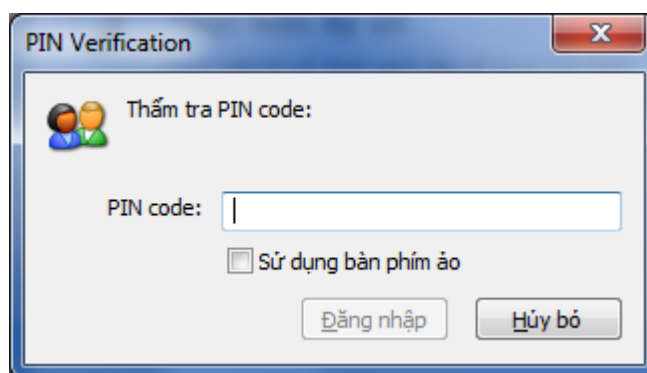
Chương trình sẽ dựa vào tên các tệp đầu vào để tự động lựa chọn tên tệp lưu giá trị chữ ký.

Bước 5: Nhập mật khẩu đăng nhập thiết bị USB Token:

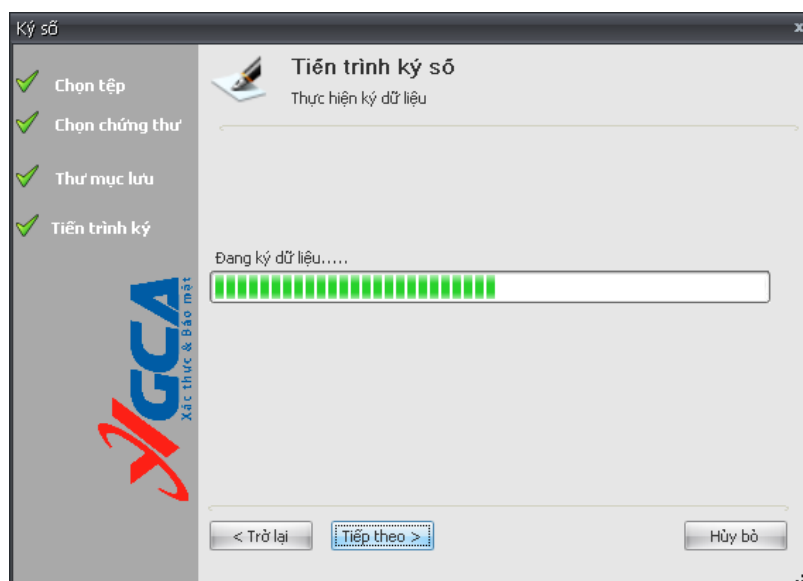
- eToken:



- ST3:

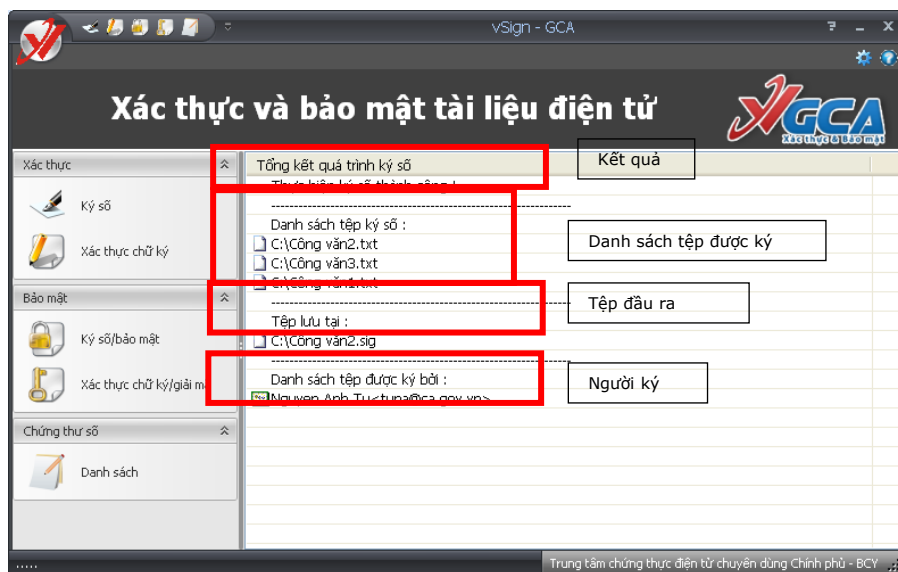


Nhập mật khẩu truy cập USB Token.



Thực hiện tác vụ ký số. Chờ trong giây lát và xem bảng tổng kết quá trình ký số tệp dữ liệu.

Bước 6: Kiểm tra quá trình ký số.



Chú ý: Chương trình có thể ký nhiều tệp cùng một lúc, các tệp được gộp lại và ký, lấy tên là tệp đầu tiên trong danh sách các tệp được ký. Như ví dụ trên, tệp đầu ra là “Công văn 2” là tệp được ký gộp của 3 tệp “Công văn 1.txt”, “Công văn 2.txt”, “Công văn 3.txt”.



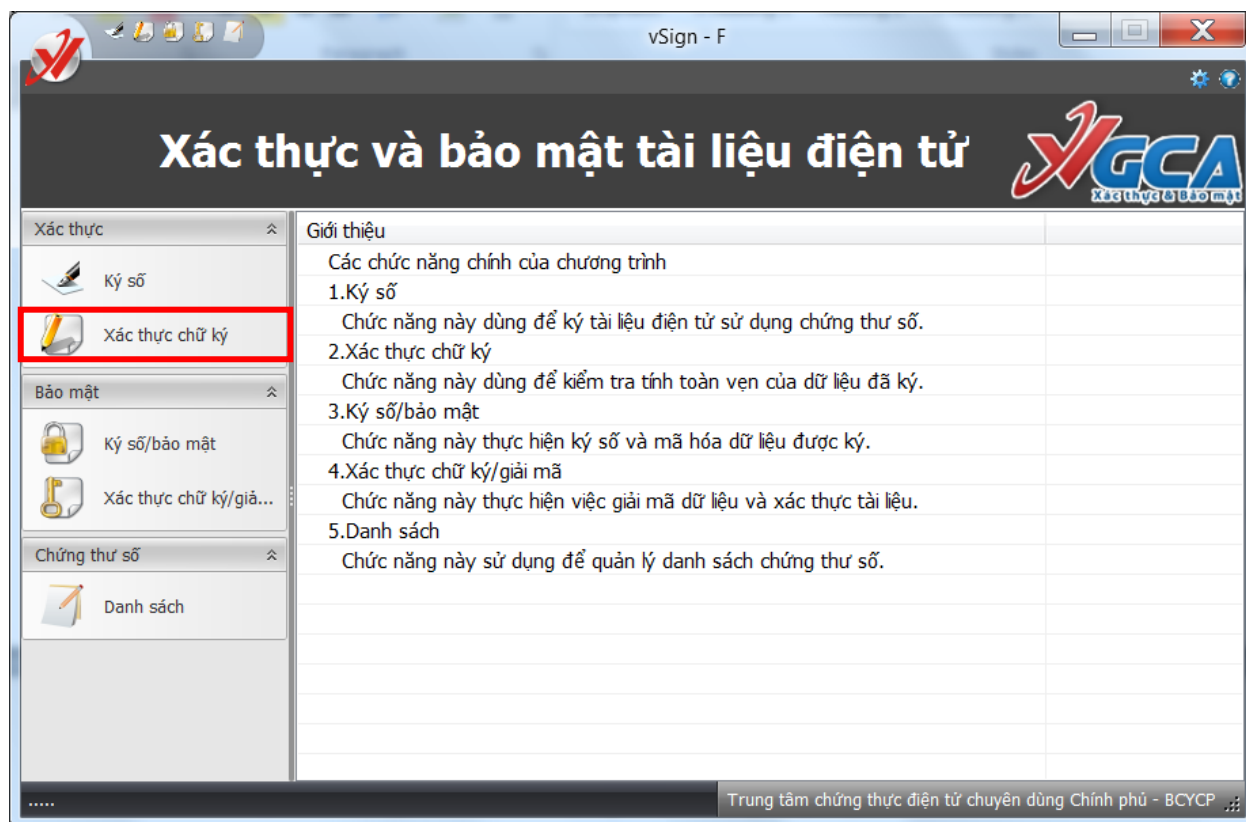
Tệp ký đầu ra có đuôi là “.sig” và có biểu tượng chữ “V” màu đỏ.

Xác thực chữ ký

Có 3 cách để xác thực chữ ký như sau: Từ giao diện chính của chương trình chọn chức năng “Xác thực chữ ký” và lựa chọn tệp cần xác thực, từ thực đơn chuột phải của windows chọn “Xác thực – Bảo mật” -> “Xác thực chữ ký”, kích đúp vào tệp cần xác thực(tệp có phần mở rộng là sig).

Bước 1: chọn cách xác thực chữ ký.

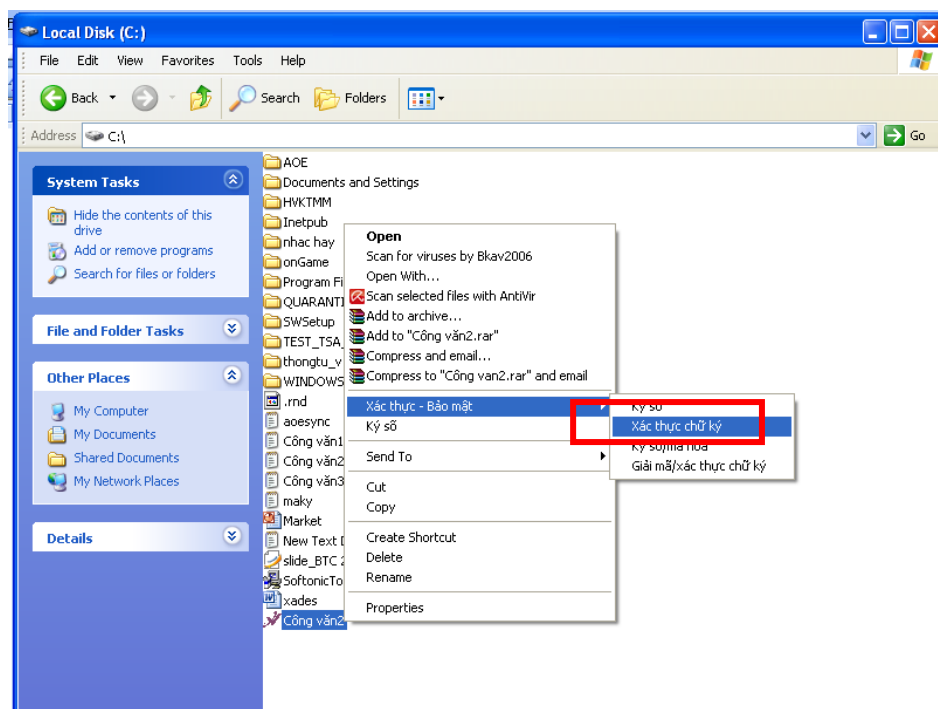
Cách 1: từ giao diện chính của chương trình.



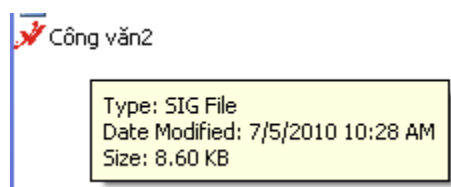
Chọn tệp cần xác thực chữ ký.

Cách 2 : sử dụng thực đơn chuột phải.

Chọn tệp cần xác thực chữ ký và nhấp chuột phải lên tệp đó để chọn chức năng xác thực chữ ký.

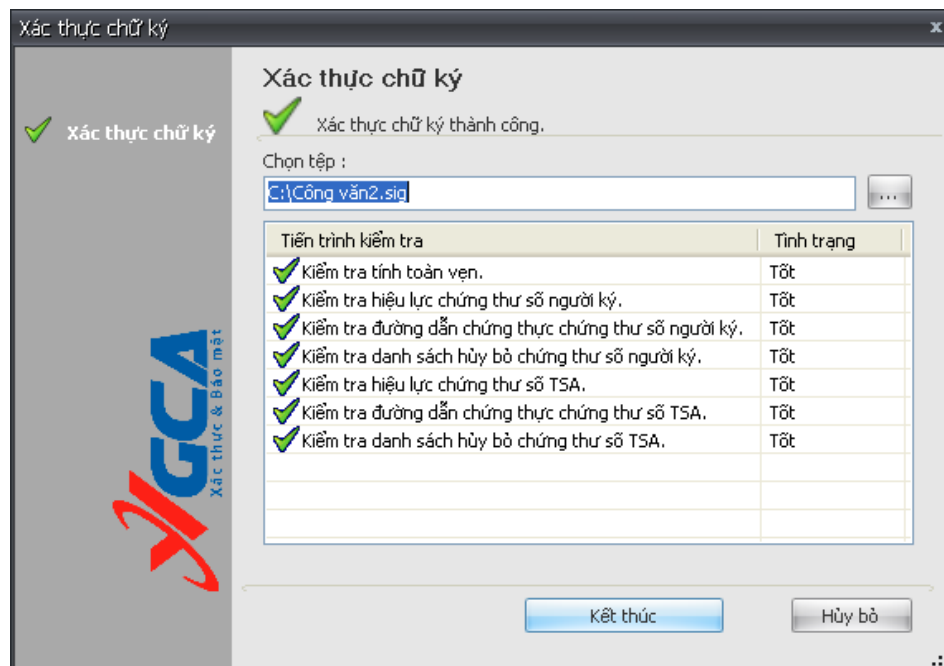


Cách 3: kích đúp vào tệp cần cần xác thực chữ ký.

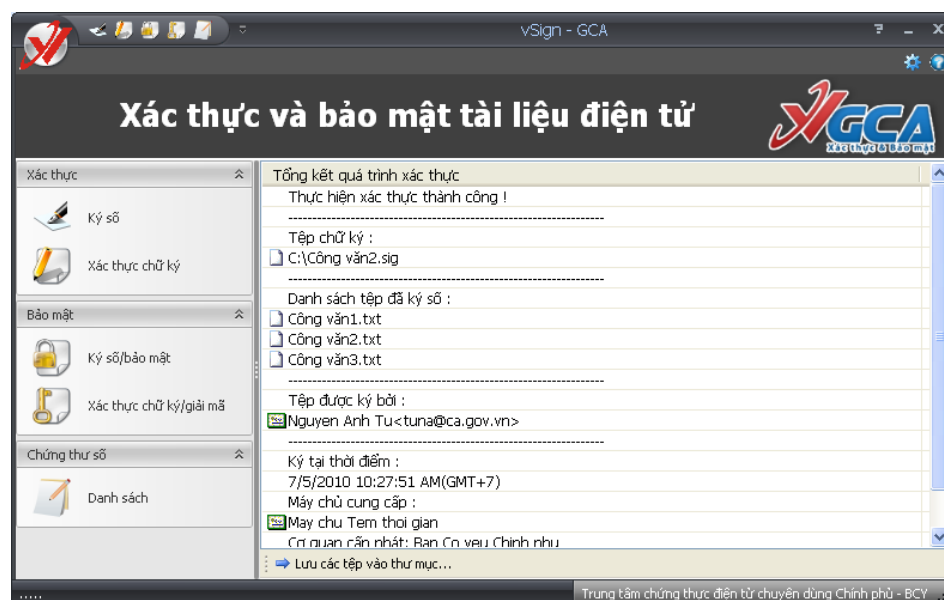


Bước 2: Xác thực chữ ký.

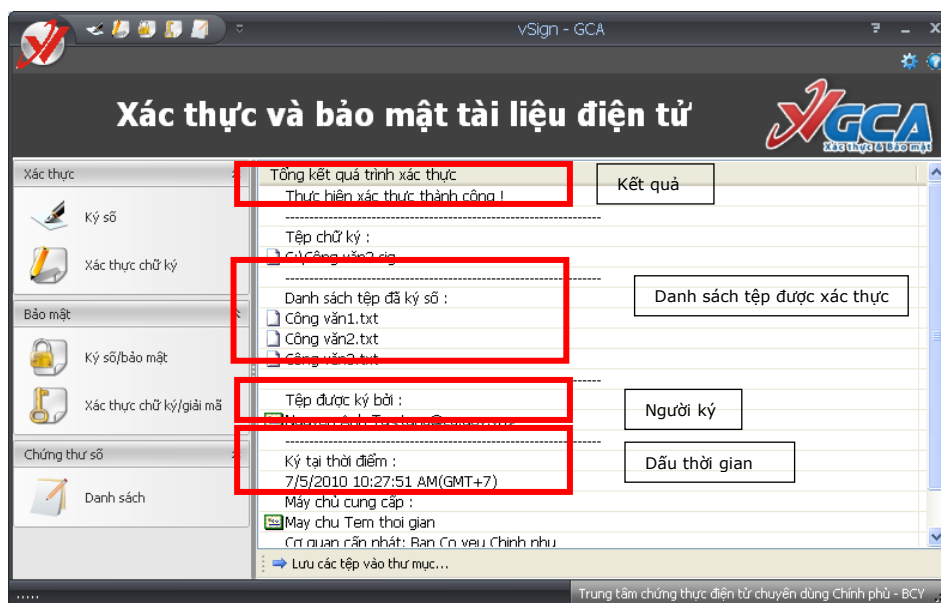
Sau khi thực hiện một trong 3 cách chương trình sẽ tự động xác thực chữ ký giao diện hiện lên như sau:



Nhấp “Kết thúc” để xem tổng kết quá trình xác thực.

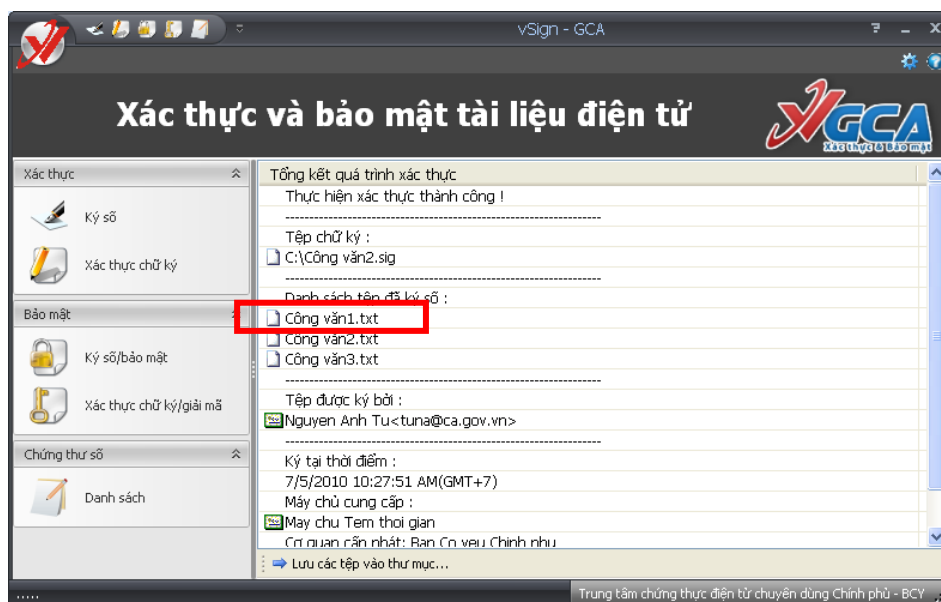


Bước 3: Kiểm tra thông tin về chữ ký trên giao diện tổng kết.

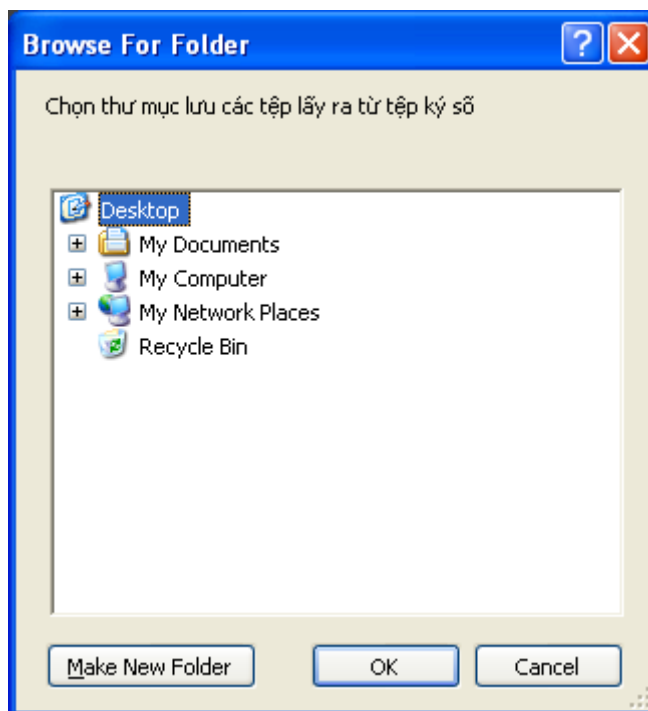


Bước 4: Xem và lưu tệp đã xác thực.

- Để xem các tệp có thể nhấp đúp chuột vào tệp cần xem.



Hoặc lưu tệp lại để xem, nhấp “Lưu các tệp vào thư mục...” để thực hiện việc lấy danh sách các tệp ký số ra khỏi tệp chữ ký.

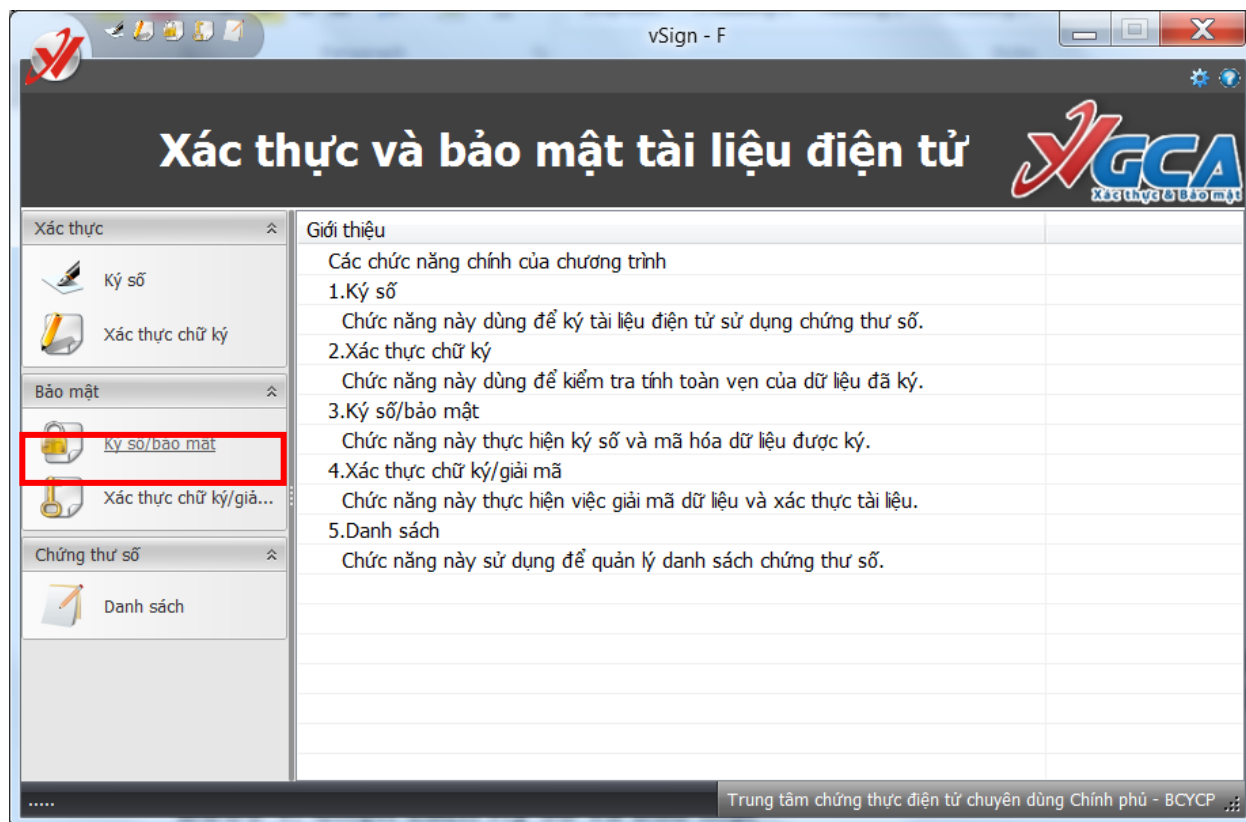


Ký số/bảo mật

Có 2 cách để thực hiện tác vụ Ký số/bảo mật như sau: từ giao diện chính của chương trình chọn chức năng “Ký số/bảo mật” , từ thực đơn chuột phải chọn “Xác thực – Bảo mật” -> “Ký số/bảo mật”.

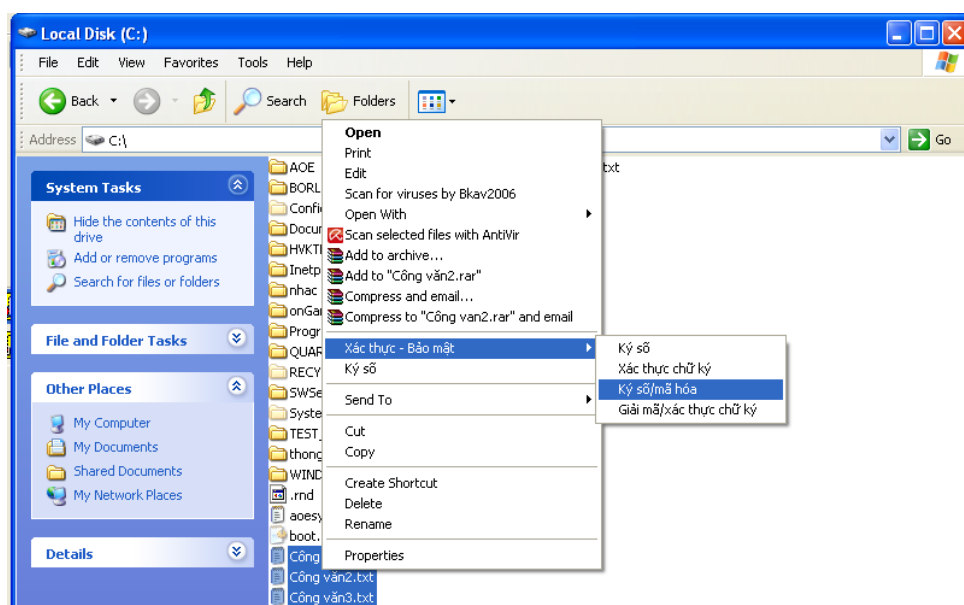
Bước 1: Chọn cách Ký số và bảo mật.

Cách 1: từ giao diện chính của chương trình.

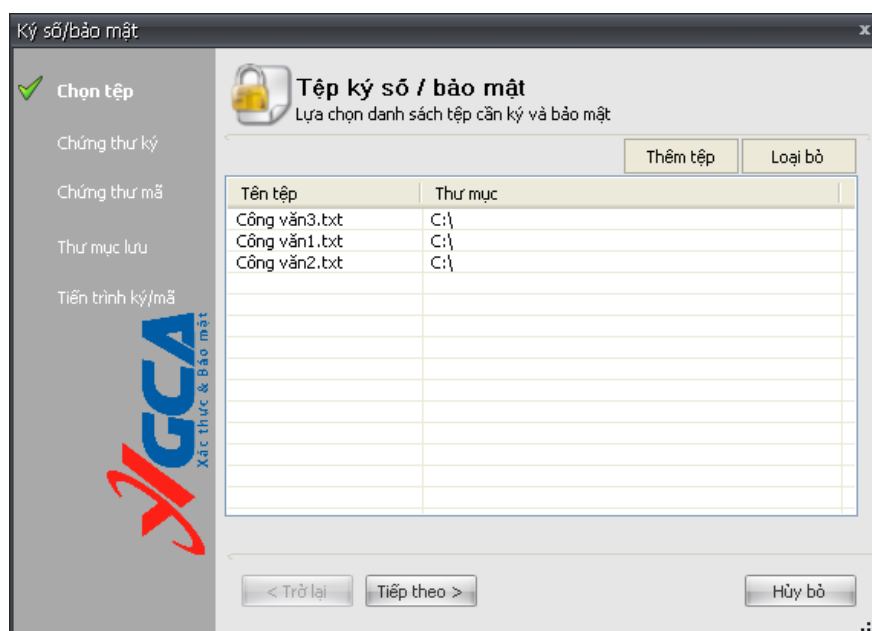


Sau đó chọn các tệp cần ký số và bảo mật.

Cách 2: từ thực đơn chuột phải, nhấp chuột phải vào tệp cần ký số và bảo mật.



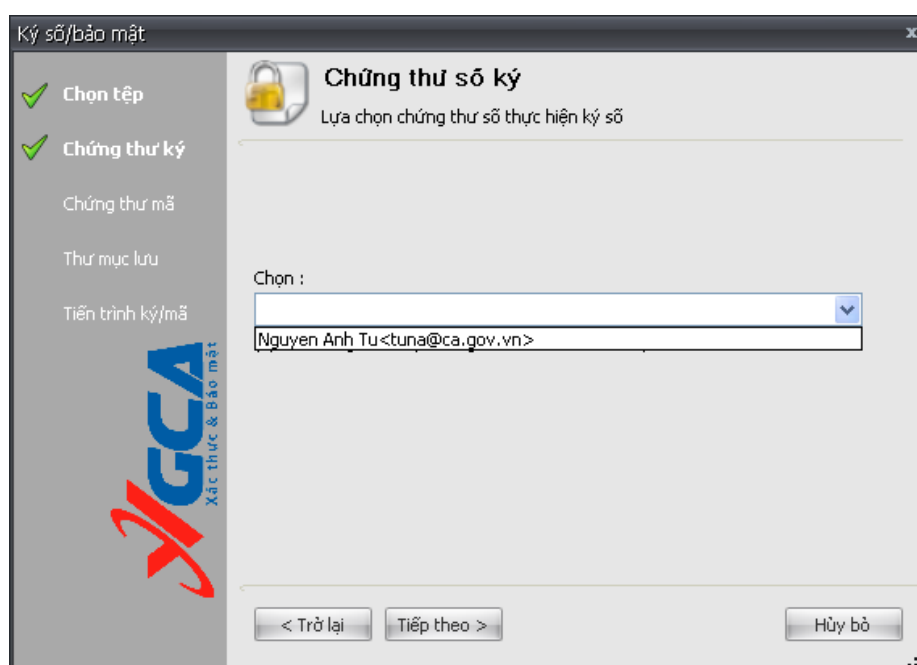
Sau khi chọn một trong hai cách trên chương trình sẽ hiển thị giao diện Ký số/bảo mật:



Có thể thêm tệp và loại bỏ tệp trong danh sách tệp ký số/bảo mật sử dụng nút “Thêm tệp” hoặc “loại bỏ”.

Nhấp nút “Tiếp theo” để tiếp tục quá trình ký số/bảo mật.

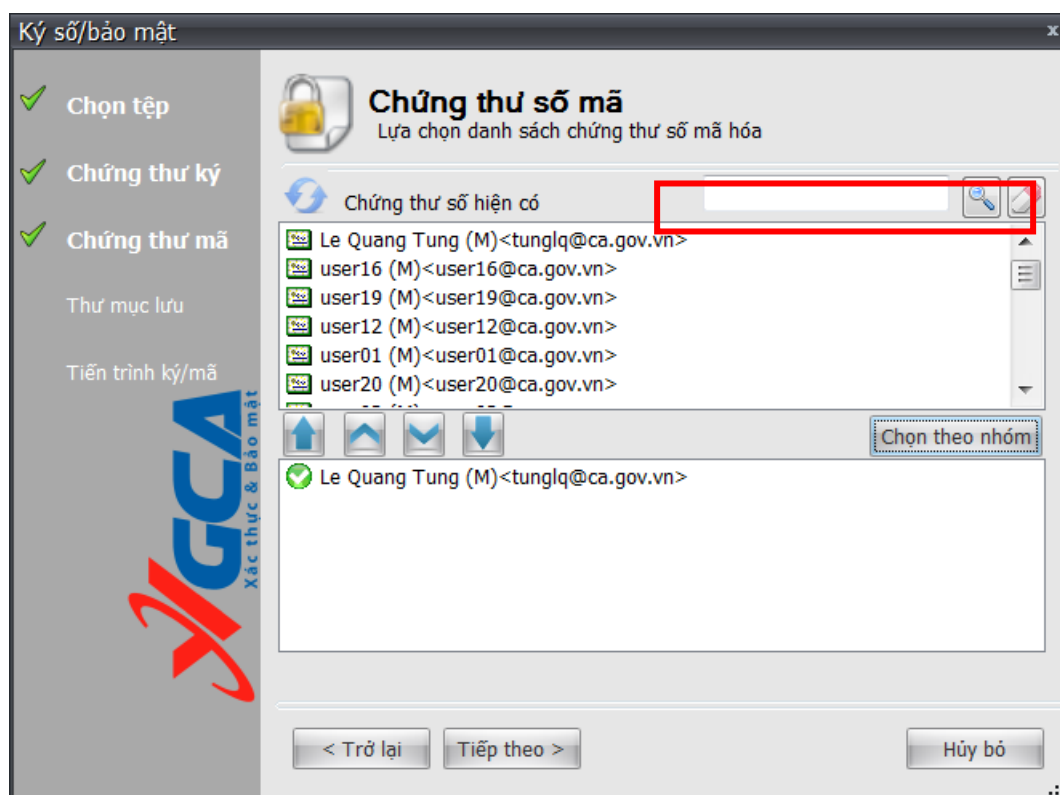
Bước 2: chọn chứng thư số để ký



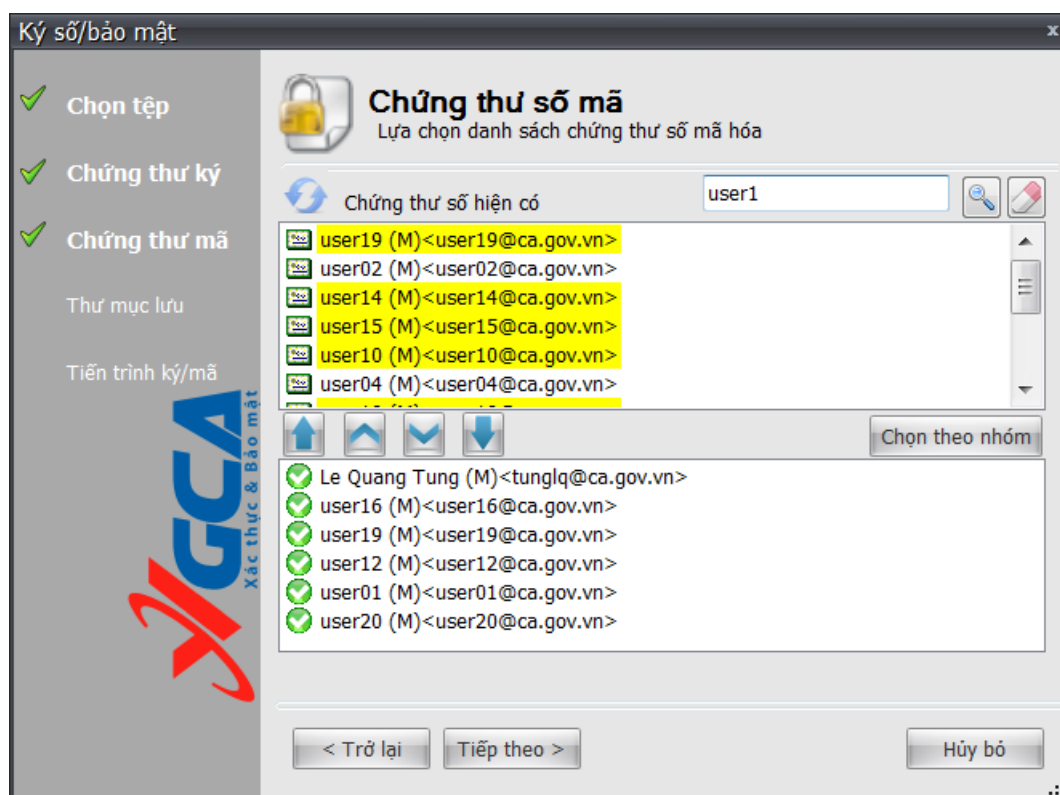
Chọn chứng thư số sử dụng để ký số. Nhấp nút “Tiếp theo” để quá trình tiếp tục.

Bước 3: Chọn các chứng thư số mã

Đây là bước chọn các chứng thư số của người nhận để mã tệp dữ liệu.

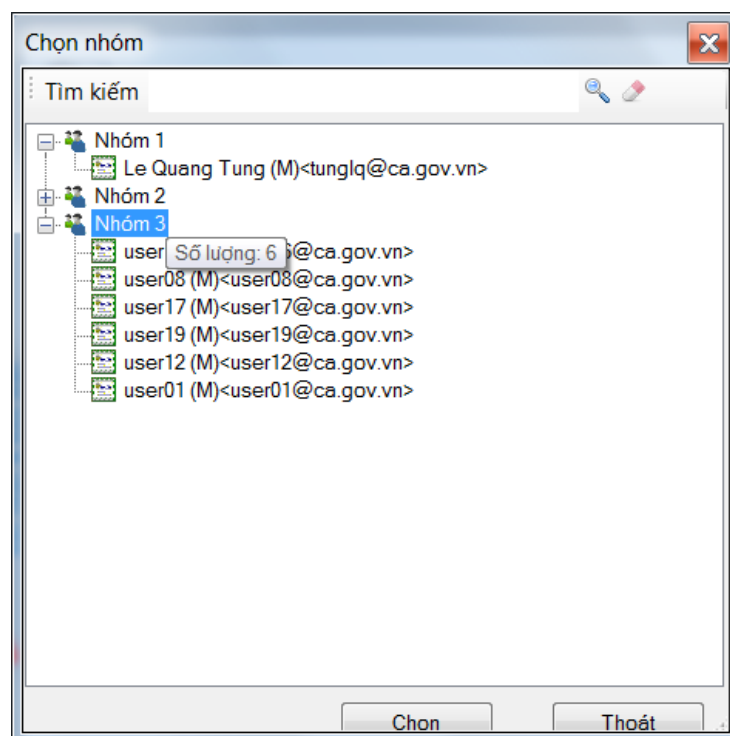


Nếu danh sách chứng thư số quá dài, có thể sử dụng chức năng tìm kiếm để tìm các chứng thư số cần sử dụng, để sử dụng chức năng tìm kiếm người sử dụng gõ tên cần tìm kiếm để tìm kiếm chứng thư số mong muốn, các chứng thư số phù hợp với tên tìm kiếm sẽ được đánh dấu màu vàng:

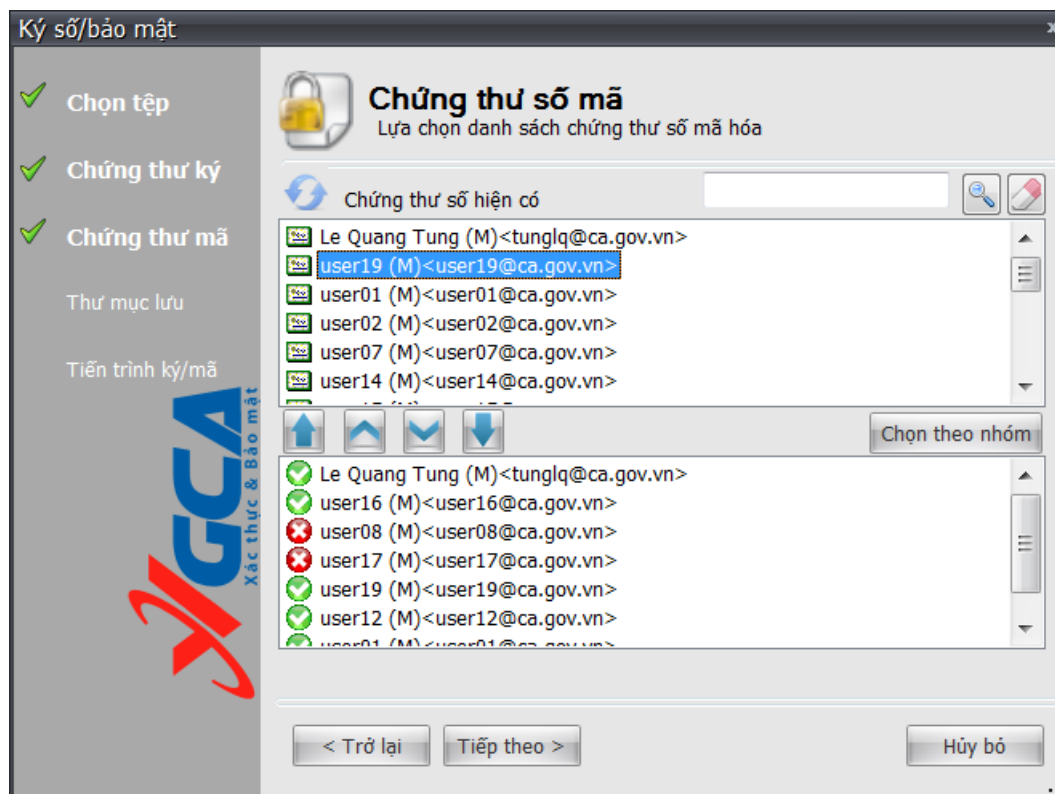


Chọn chứng thư số thích hợp để đưa xuống danh sách bên dưới.

Có thể chọn chứng thư số theo nhóm để có thể quản lý chứng thư số một cách dễ dàng hơn. Để chọn chứng thư số theo nhóm, chọn nút “chọn theo nhóm”:

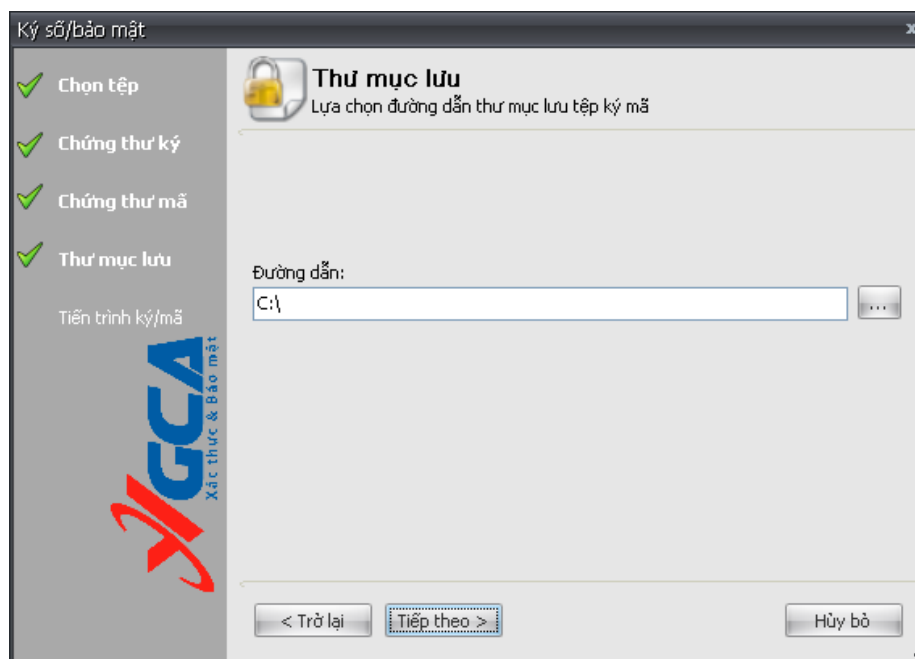


Chọn nhóm chứng thư số cần chọn, bấm chọn để kết thúc quá trình chọn nhóm, toàn bộ chứng thư số trong nhóm sẽ được lựa chọn để mã tệp dữ liệu:



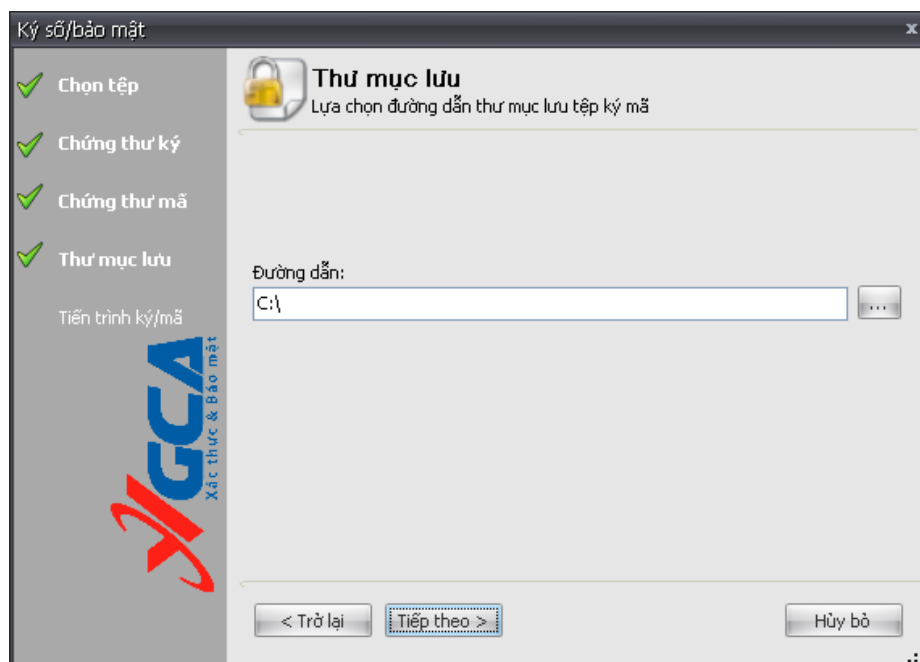
Những chứng thư số có biểu tượng dấu “x” đỏ là các chứng thư số bị hủy bỏ hoặc lỗi cần loại bỏ, kích đúp chuột vào chứng thư số này để loại bỏ.

Chọn chứng thư số sử dụng để mã hóa dữ liệu. Nhấp “Tiếp theo” để quá trình tiếp tục.



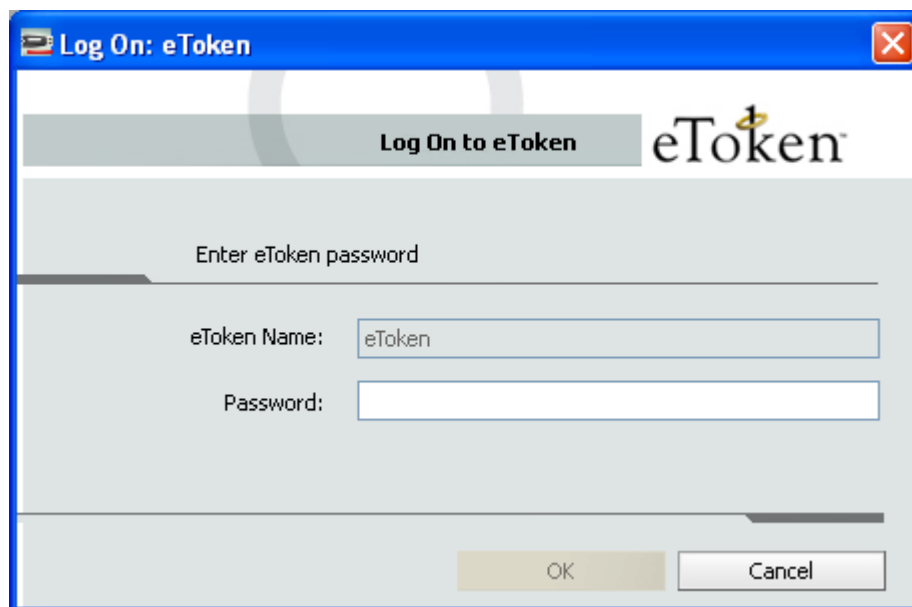
Bước 4: Lưu tệp .

Chọn đường dẫn để lưu tệp ký số/bảo mật . Nhấp “Tiếp theo” để quá trình tiếp tục.

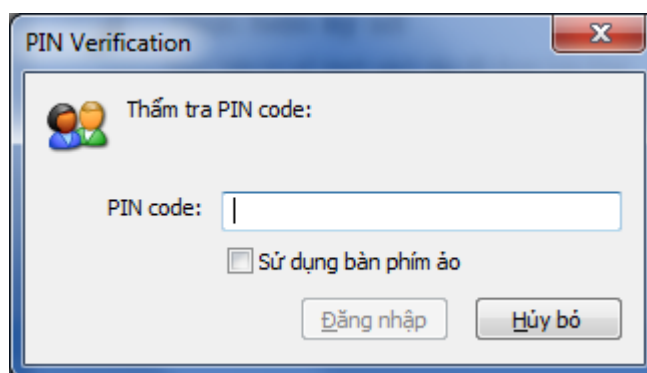


Bước 5: Nhập mật khẩu truy cập USB eToken.

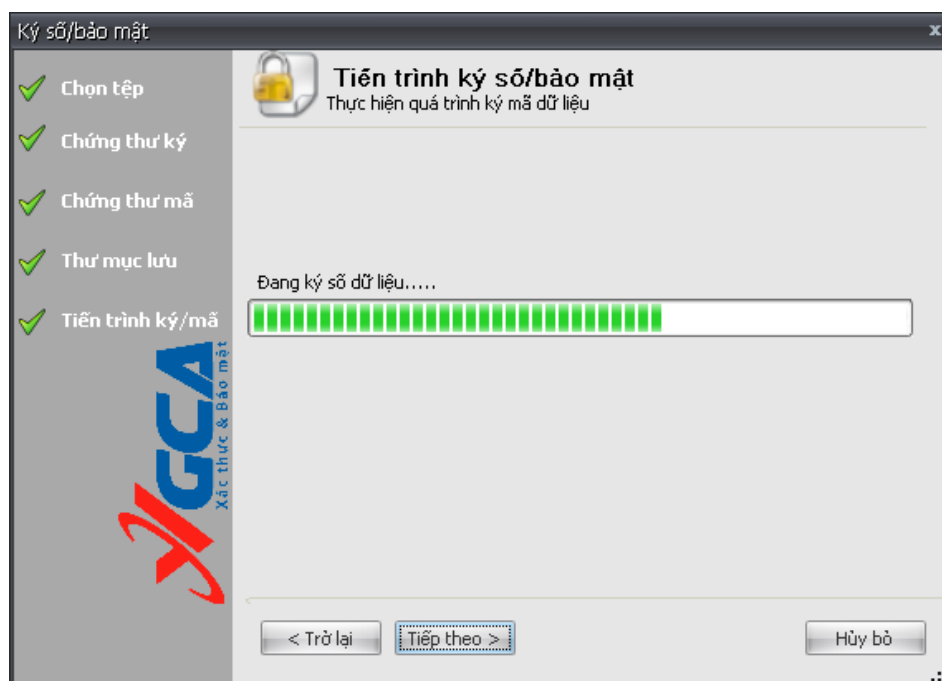
- eToken:



- ST3:

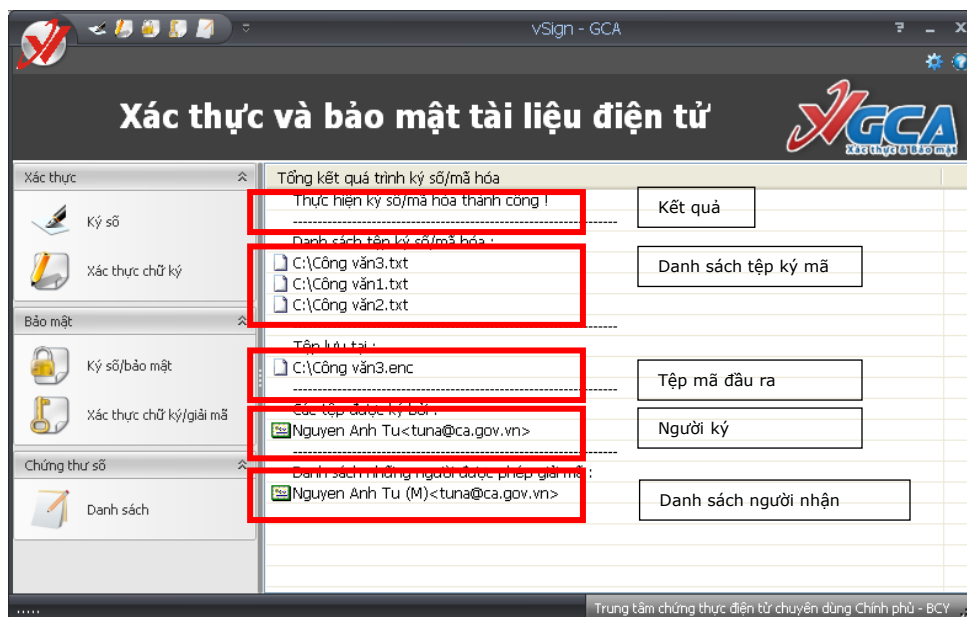


Tiến trình thực hiện ký số/bảo mật.



Bước 6: Kiểm tra quá trình thực hiện.

Khi quá trình kết thúc sẽ hiển thị thông tin tổng kết quá trình ký số/bảo mật.



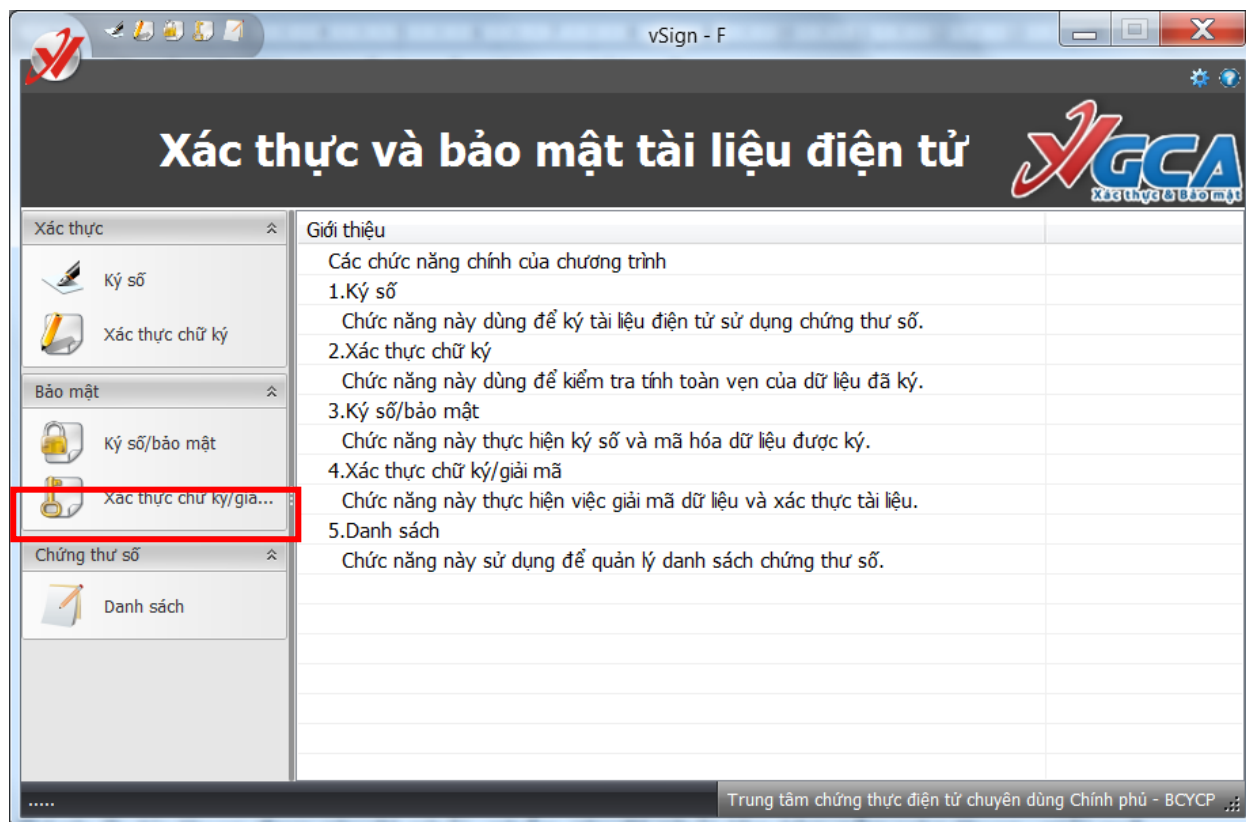
Chú ý: Chương trình có thể ký số, bảo mật nhiều tệp cùng một lúc, các tệp được gộp lại và ký số, bảo mật, lấy tên là tệp đầu tiên trong danh sách các tệp được ký. Như ví dụ trên, tệp đầu ra là “Công văn 3” là tệp được ký gộp của 3 tệp “Công văn 1.txt”, “Công văn 2.txt”, “Công văn 3.txt”. Tệp đầu ra có đuôi là “.enc” và có biểu tượng chữ “V” màu đỏ.

Xác thực chữ ký/giải mã

Có 3 cách để thực hiện tác vụ xác thực chữ ký/giải mã như sau: từ giao diện chính của chương trình chọn chức năng “Xác thực chữ ký/giải mã” và lựa chọn tệp cần xác thực chữ ký/giải mã, từ thực đơn chuột phải của windows chọn “Xác thực – Bảo mật” -> “Xác thực chữ ký/giải mã”, kích đúp vào tệp cần xác thực(tệp có phần mở rộng là enc).

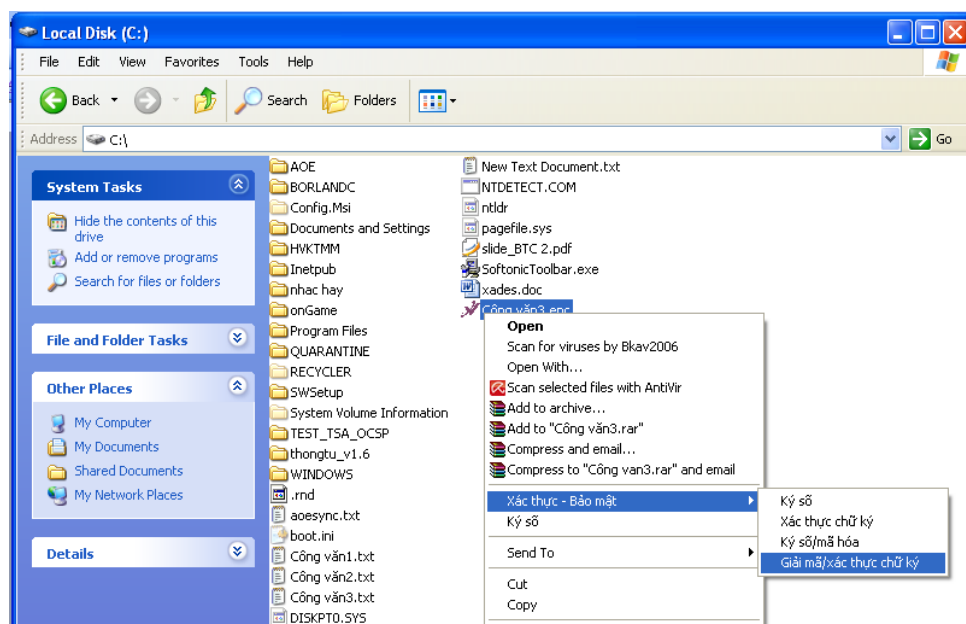
Bước 1: Chọn cách xác thực/giải mã.

Cách 1: từ giao diện chính của chương trình.

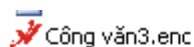


Chọn tệp cần xác thực, giải mã.

Cách 2: từ thực đơn chuột phải, nhấp chuột phải lên tệp cần xác thực, giải mã.



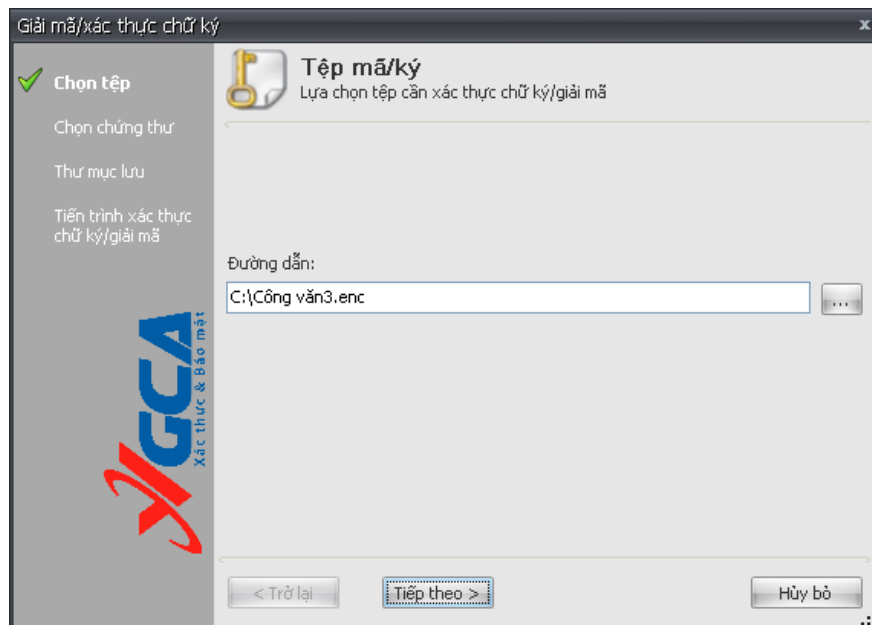
Cách 3 : nhấp đúp chuột lên tệp cần xác thực giải mã.



Type: ENC File
Date Modified: 7/6/2010 1:51 PM
Size: 9.04 KB

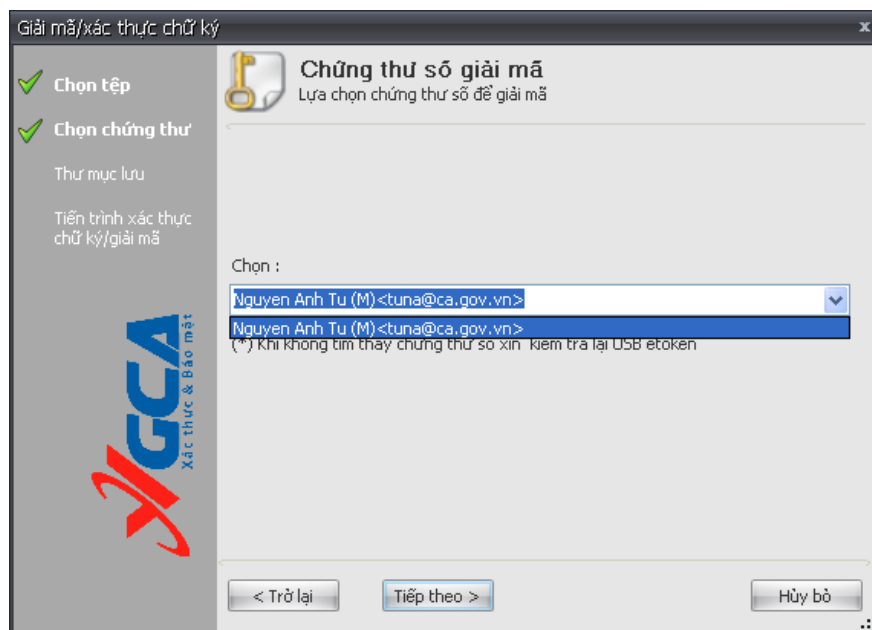
Bước 2: xác thực giải mã.

Sau khi chọn một trong 3 cách trên chương trình sẽ hiển thị giao diện xác thực chữ ký/giải mã như sau :



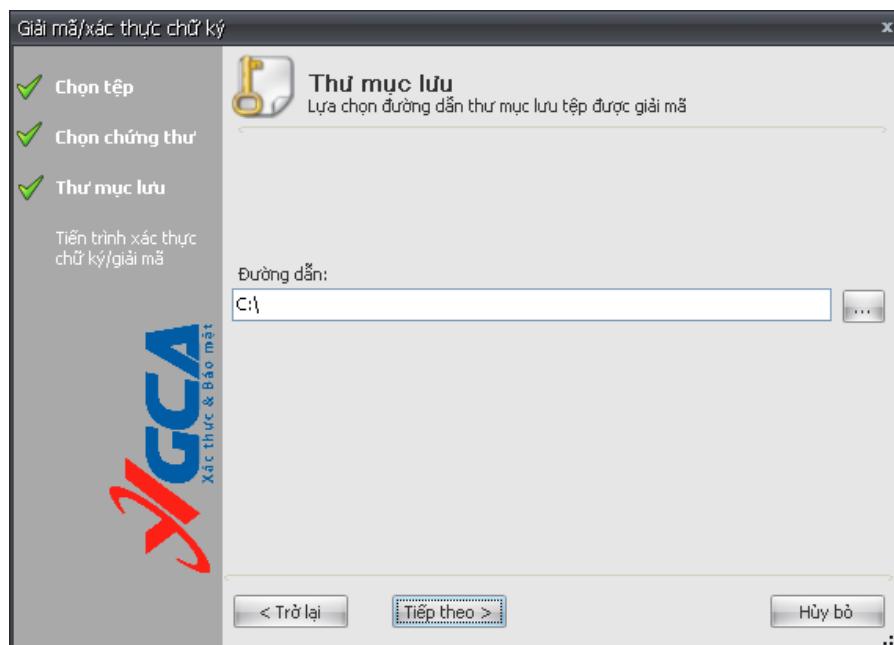
Chọn tệp cần xác thực chữ ký/giải mã, nhấp “Tiếp theo” để quá trình tiếp tục.

Bước 3: Chọn chứng thư số giải mã.



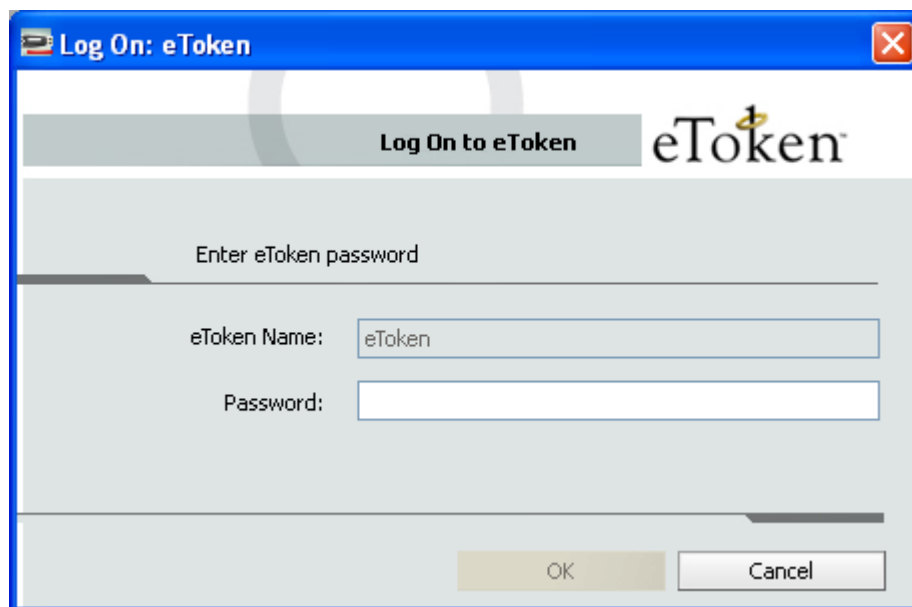
Chọn chứng thư số sử dụng để giải mã dữ liệu. Nhấp “Tiếp theo” để quá trình tiếp tục.

Bước 4: Chọn thư mục lưu các tệp được giải mã.

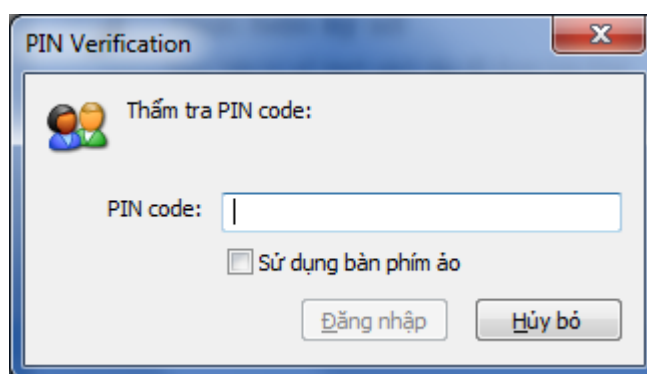


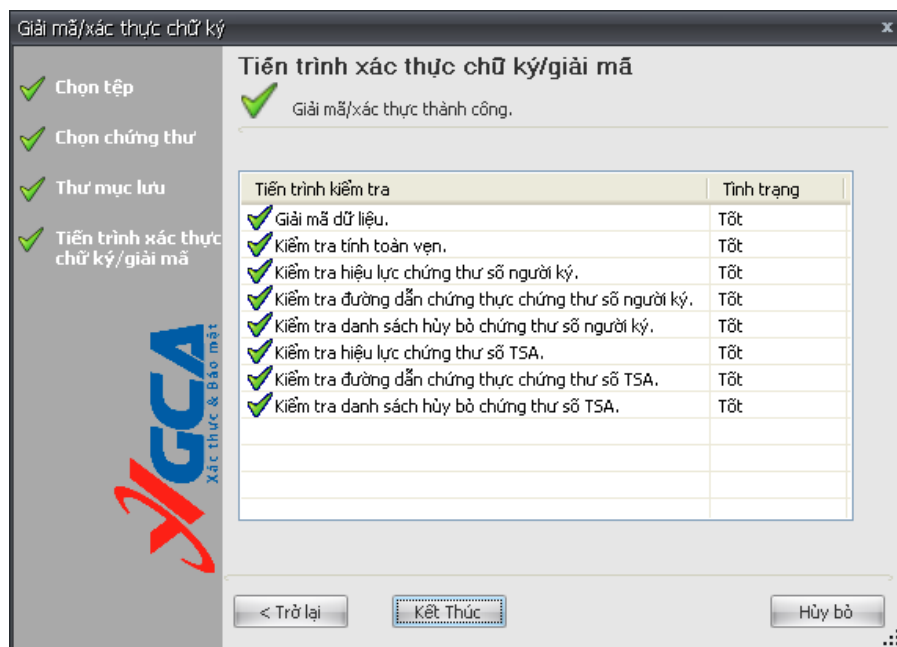
Bước 5: Nhập mật khẩu USB eToken để thực hiện giải mã dữ liệu.

- eToken



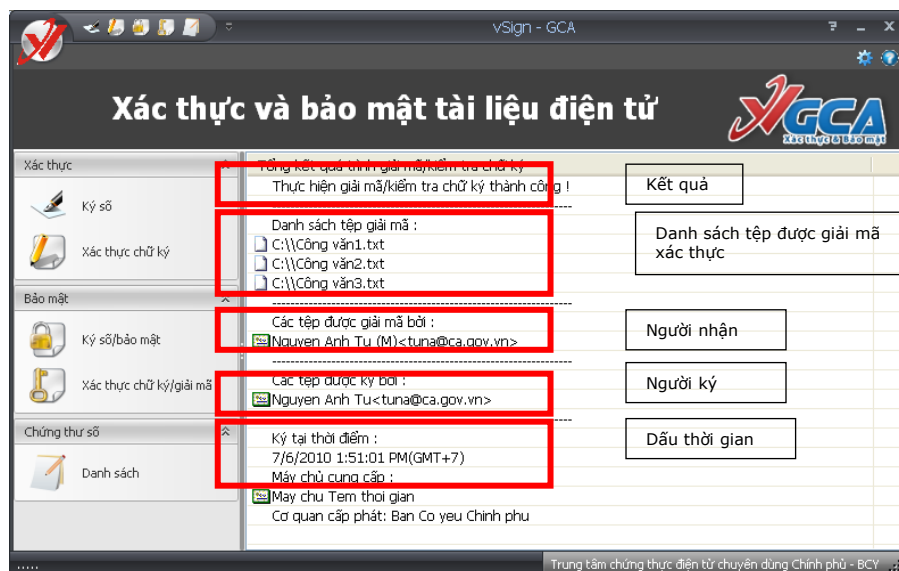
- ST3:





Bước 6: Kiểm tra quá trình xác thực, giải mã.

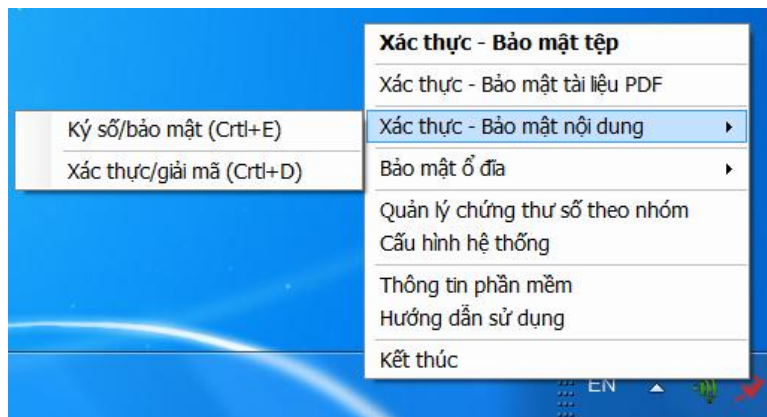
Tình trạng xác thực chữ ký/giải mã. Nhấp “Kết thúc” để hiển thị bảng tổng kết quá trình xác thực chữ ký/giải mã.



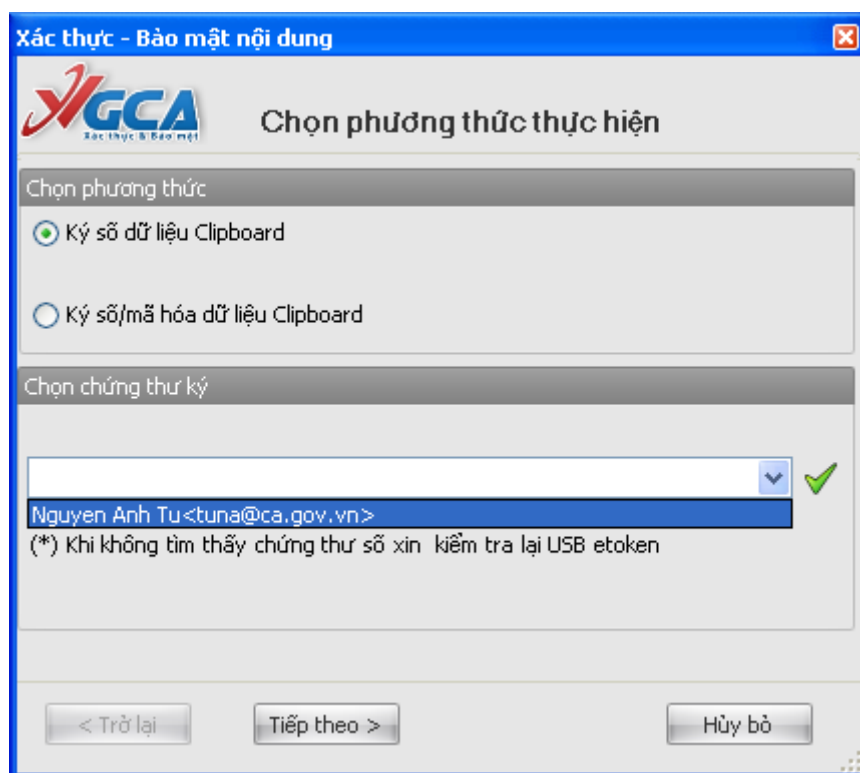
2.5 Xác thực và bảo mật nội dung thư

2.5.1 Ký số nội dung thư

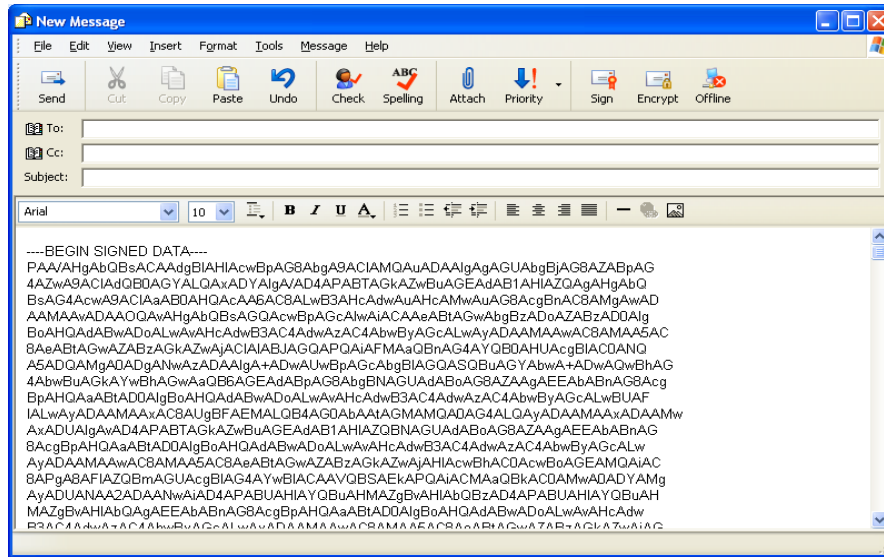
Có 2 cách để ký số nội dung thư như sau: từ trình soạn thảo thư sử dụng phím tắt Ctrl + E và chọn phương thức “Ký số dữ liệu Clipboard”, từ TrayIcon của hệ thống chọn “Xác thực – Bảo mật nội dung” -> “Ký số/bảo mật”.



Sau khi thực hiện xong tác vụ hiển thị giao diện như sau:



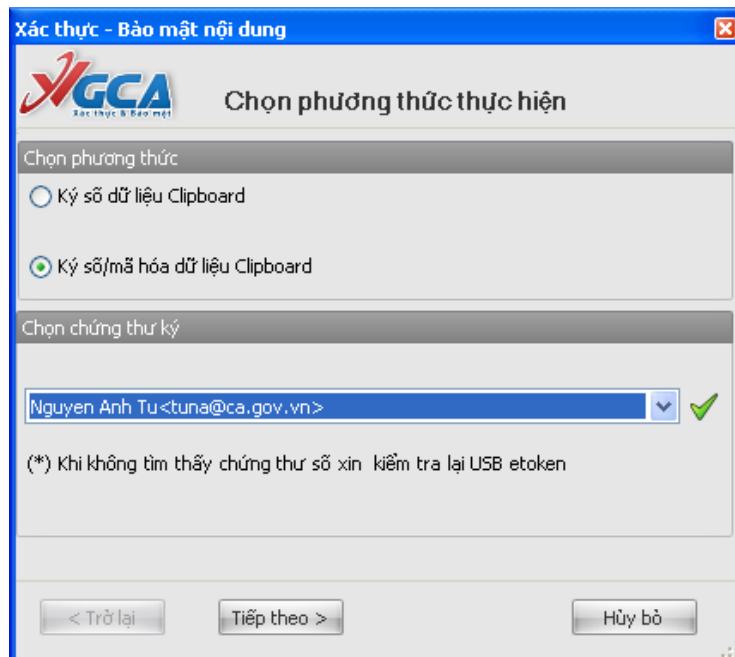
Chọn chứng thư số cần ký, nhấp "Tiếp theo" để quá trình tiếp tục.



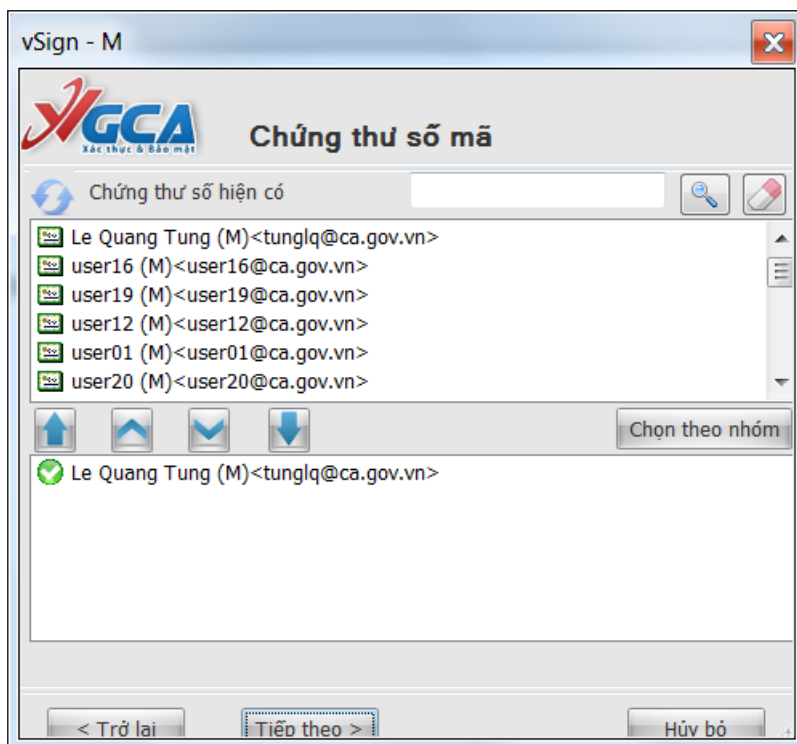
Kết quả hiện ký số Clipboard khi thực hiện trong trình soạn thư của OutlookExpress.

2.5.2 Ký số/bảo mật nội dung thư

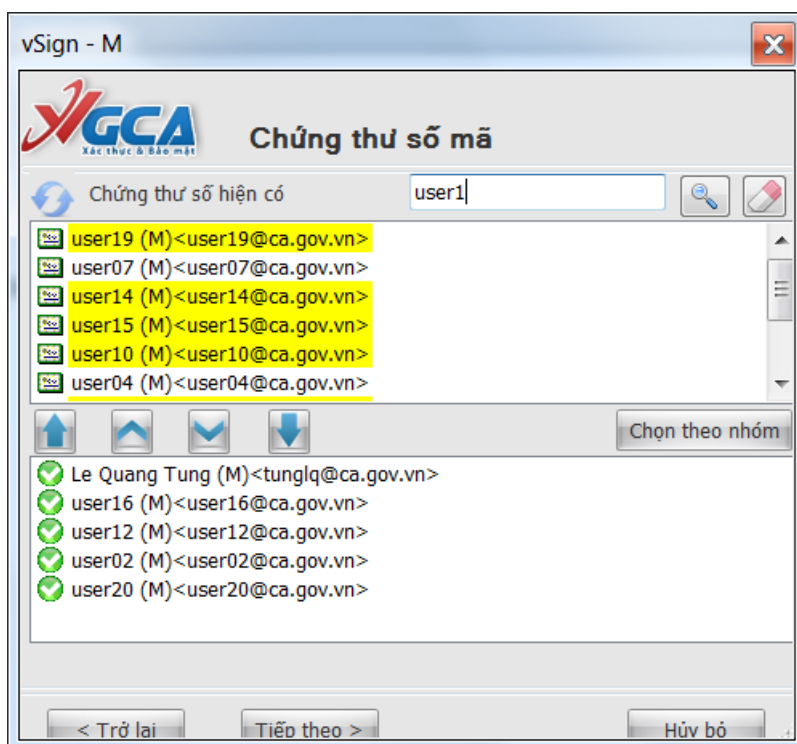
Có 2 cách để ký số nội dung thư như sau: từ trình soạn thảo thư sử dụng phím tắt Ctrl + E và chọn phương thức “Ký số/mã hóa dữ liệu Clipboard”, từ biểu tượng của chương trình trên khay hệ thống, chọn “Xác thực – Bảo mật nội dung” → “Ký số/mã bảo mật” và chọn phương thức “Ký số/mã hóa dữ liệu Clipboard”.



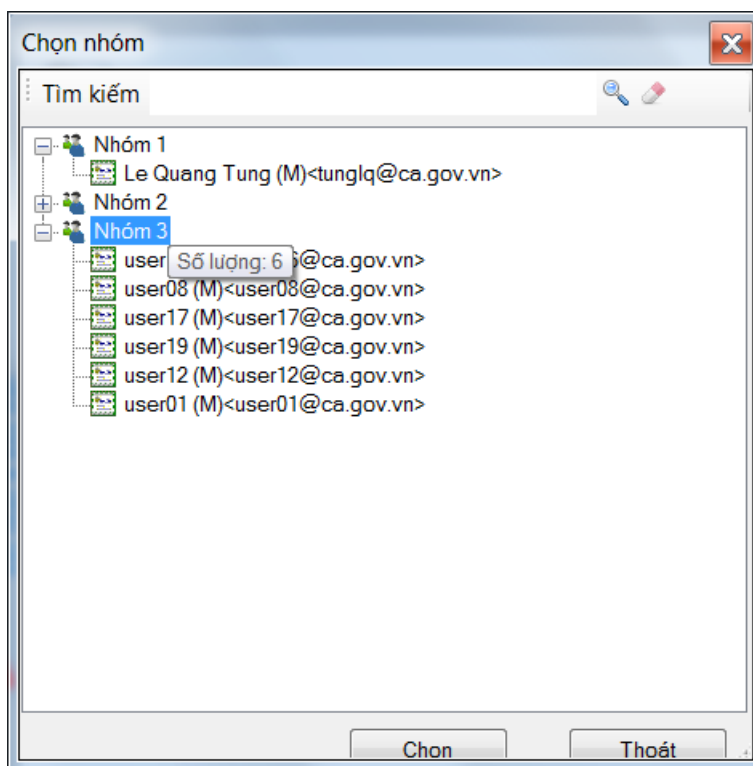
Chọn chứng thư số sử dụng để ký số dữ liệu. Nhấp “Tiếp theo” để quá trình tiếp tục.



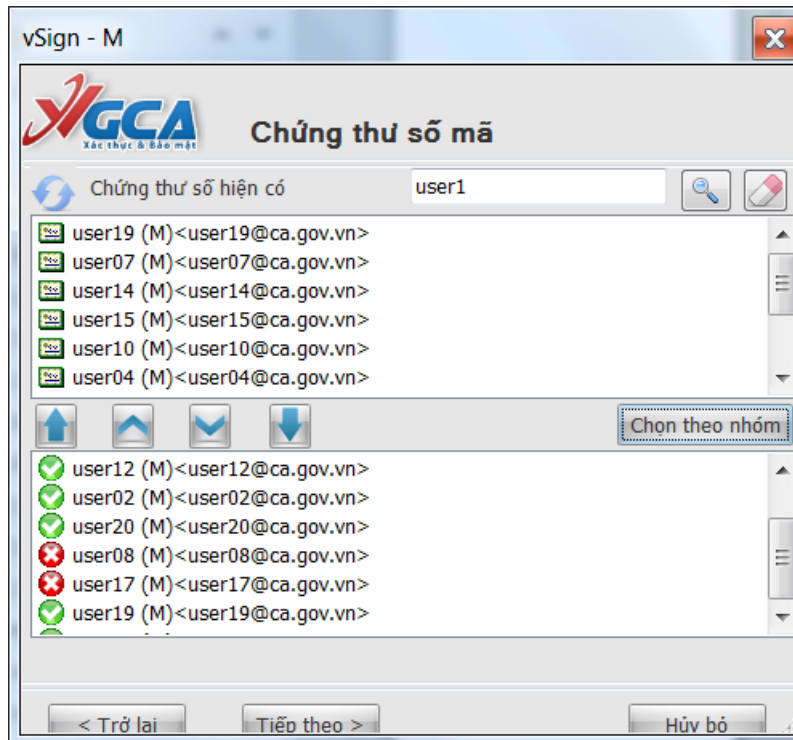
Nếu danh sách chứng thư số quá dài, có thể sử dụng chức năng tìm kiếm để tìm các chứng thư số cần sử dụng, để sử dụng chức năng tìm kiếm người sử dụng gõ tên cần tìm kiếm để tìm kiếm chứng thư số mong muốn, các chứng thư số phù hợp với tên tìm kiếm sẽ được đánh dấu màu vàng:



Chọn chứng thư số thích hợp để đưa xuống danh sách bên dưới.
Có thể chọn chứng thư số theo nhóm để có thể quản lý chứng thư số một cách dễ dàng hơn. Để chọn chứng thư số theo nhóm, chọn nút “chọn theo nhóm”:

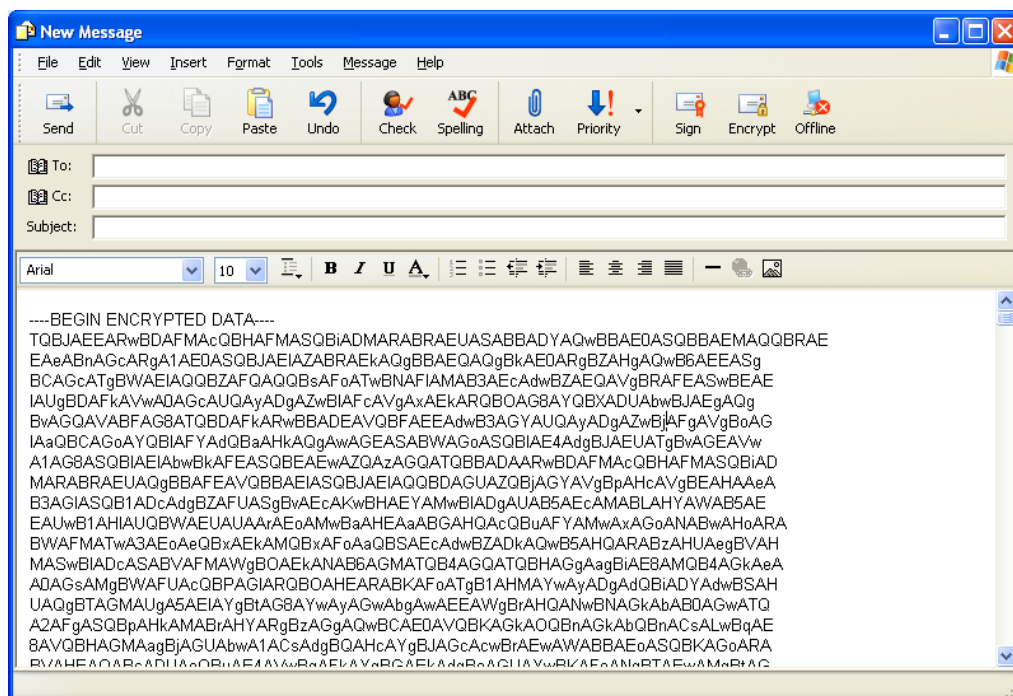


Chọn nhóm chứng thư số cần chọn, bấm chọn để kết thúc quá trình chọn nhóm, toàn bộ chứng thư số trong nhóm sẽ được lựa chọn để mã tệp dữ liệu:



Những chứng thư số có biểu tượng dấu “x” đỏ là các chứng thư số bị hủy bỏ hoặc lỗi cần loại bỏ, kích đúp chuột vào chứng thư số này để loại bỏ.

Chọn chứng thư số để mã hóa dữ liệu. Nhấp “Tiếp theo” để thực hiện tác vụ ký số/ bảo mật.

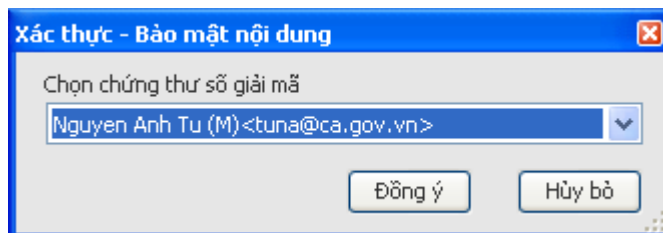


Kết quả hiện ký số Clipboard khi thực hiện trong trình soạn thư của OutlookExpress.

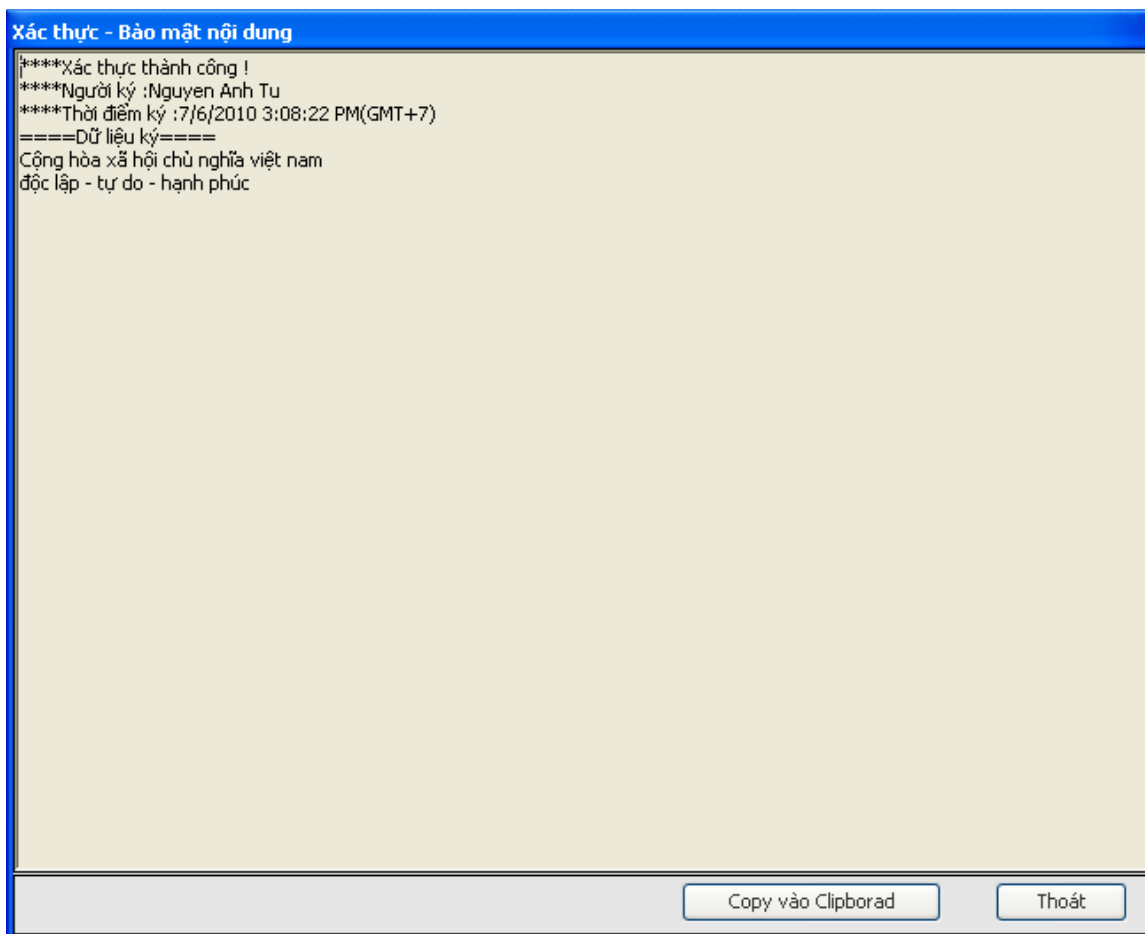
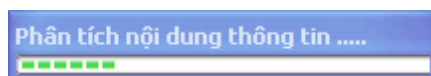
2.5.3 Xác thực chữ ký/giải mã nội dung thư

Khi nhận được thư đã ký số/mã hóa (ví dụ trên OutlookExpress) ta có 2 cách để tiến hành quá trình xác thực/giải mã là : từ giao diện có nội dung thư nhấp Ctrl +D , từ biểu tượng của chương trình trên khay hệ thống chọn “Xác thực – Bảo mật nội dung” -> “Xác thực/giải mã”.

Khi chọn một trong 2 tác vụ trên chương trình sẽ tự động phân tích nội dung thông tin và đưa ra kết quả.



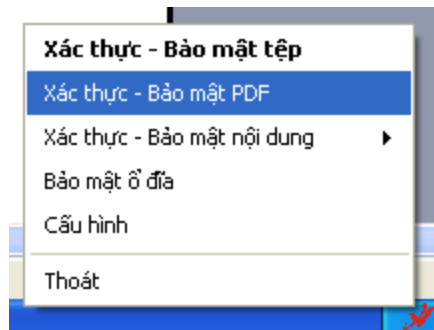
Giao diện chọn chứng thư số dùng để giải mã dữ liệu.



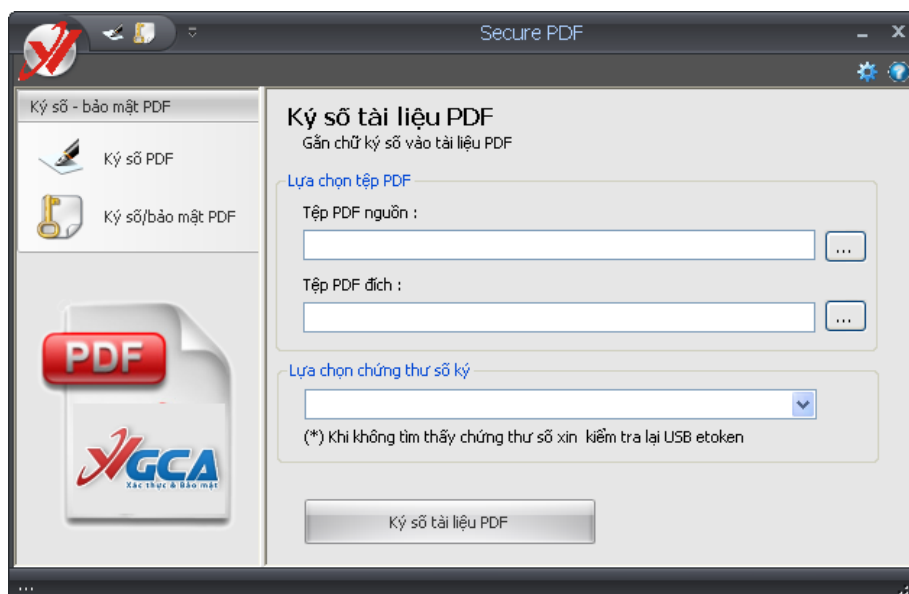
Giao diện hiển thị kết quả quá trình phân tích nội dung thông tin.

2.6 Xác thực và bảo mật PDF

Để khởi động chương trình xác thực và bảo mật PDF, từ thực đơn trên khay hệ thống chọn “Xác thực – Bảo mật PDF”.



Giao diện chính của chương trình như sau:



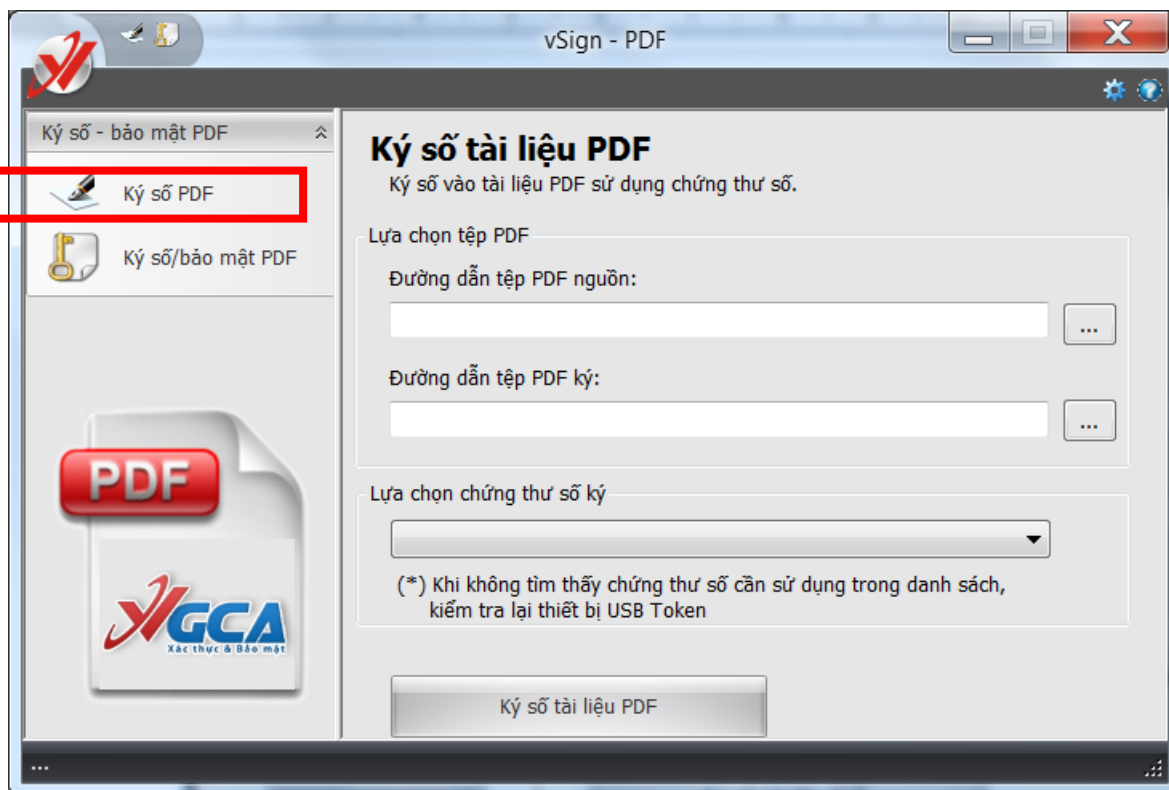
Chú ý:

- **Phần mềm vSign2.0 không thiết kế chức năng giải mã và xác thực chữ ký cho tài liệu PDF, người dùng sẽ sử dụng phần mềm Adobe Reader để giải mã xác thực tài liệu PDF.**
- **Sử dụng phần mềm Adobe Reader phiên bản 8.0 trở lên để tạo tệp PDF và kiểm tra xác thực chữ ký.**
- **Cần phải cấu hình phần mềm Adobe Reader trước khi xác thực chữ ký (việc cấu hình này chỉ làm một lần sau khi cài đặt phần mềm Adobe Reader).**

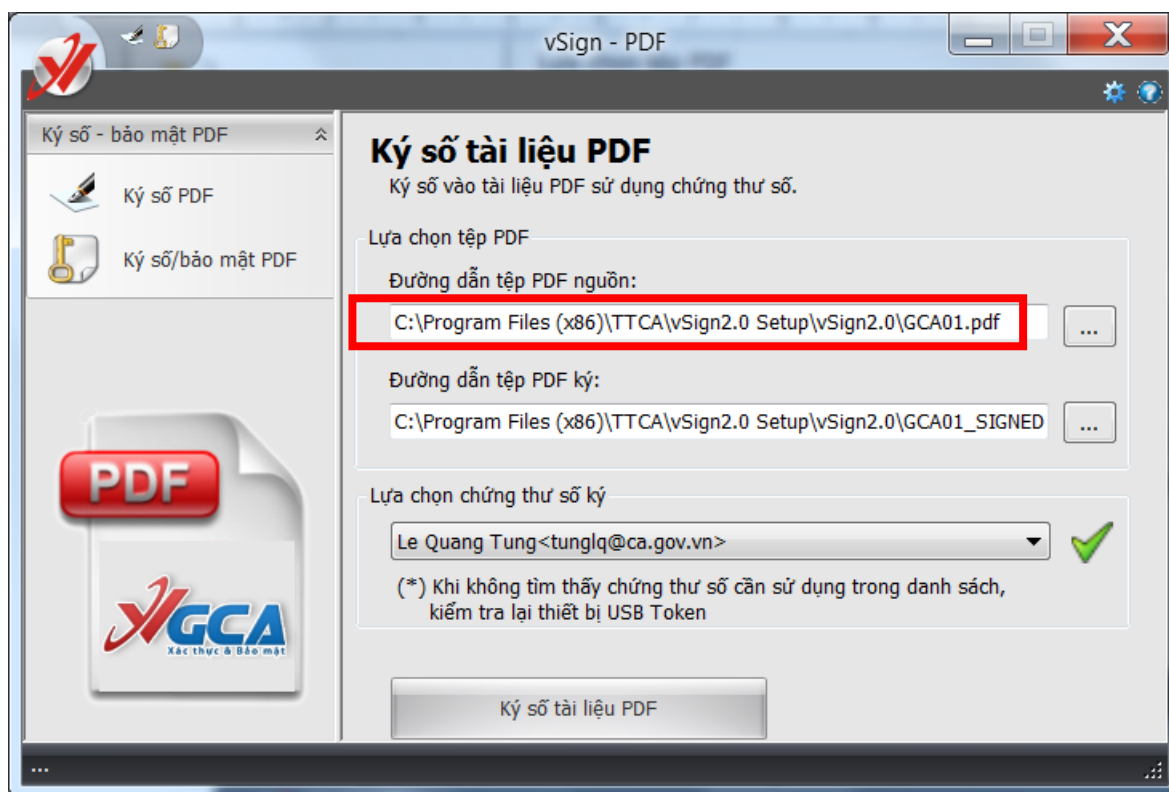
2.6.1 Ký số tài liệu PDF

Ký số tài liệu PDF giúp người sử dụng tự động gắn chữ ký số (dựa trên chứng thư số của người sử dụng) vào tệp tin dạng PDF. Quy trình thực hiện ký số như sau:

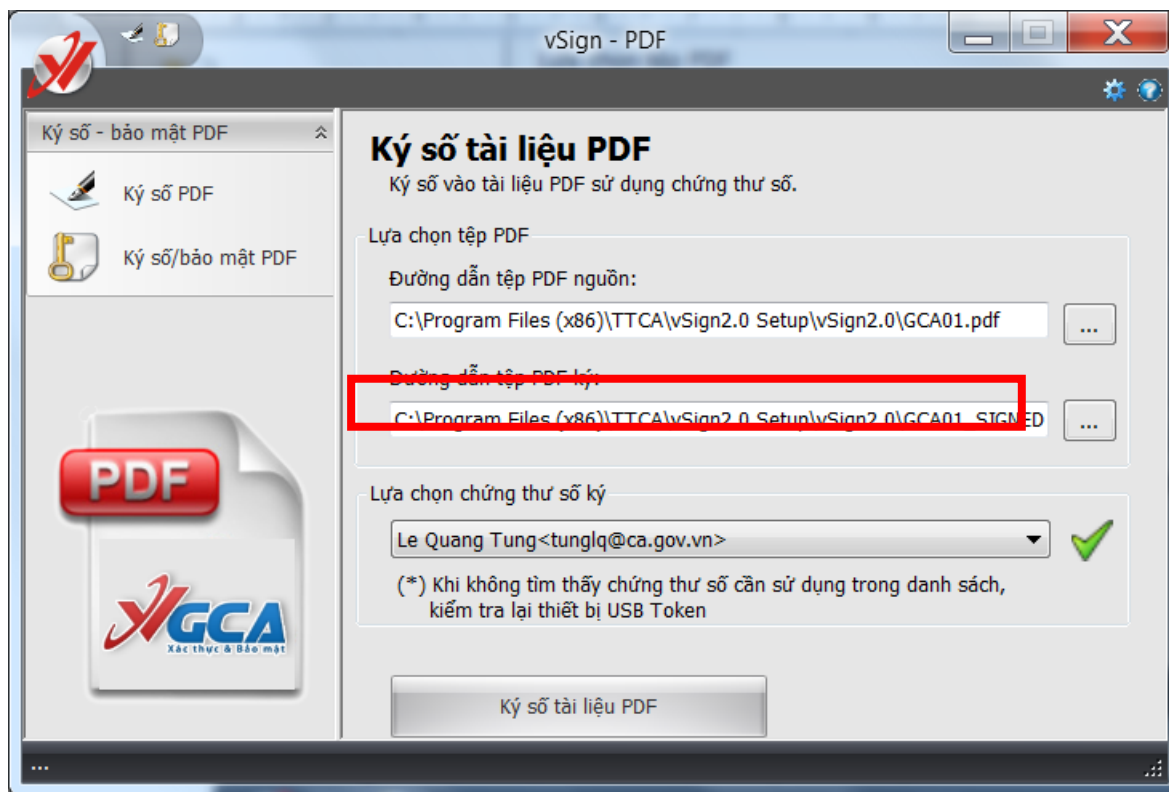
Chọn “Ký số PDF”: hiển thị giao diện ký số PDF.



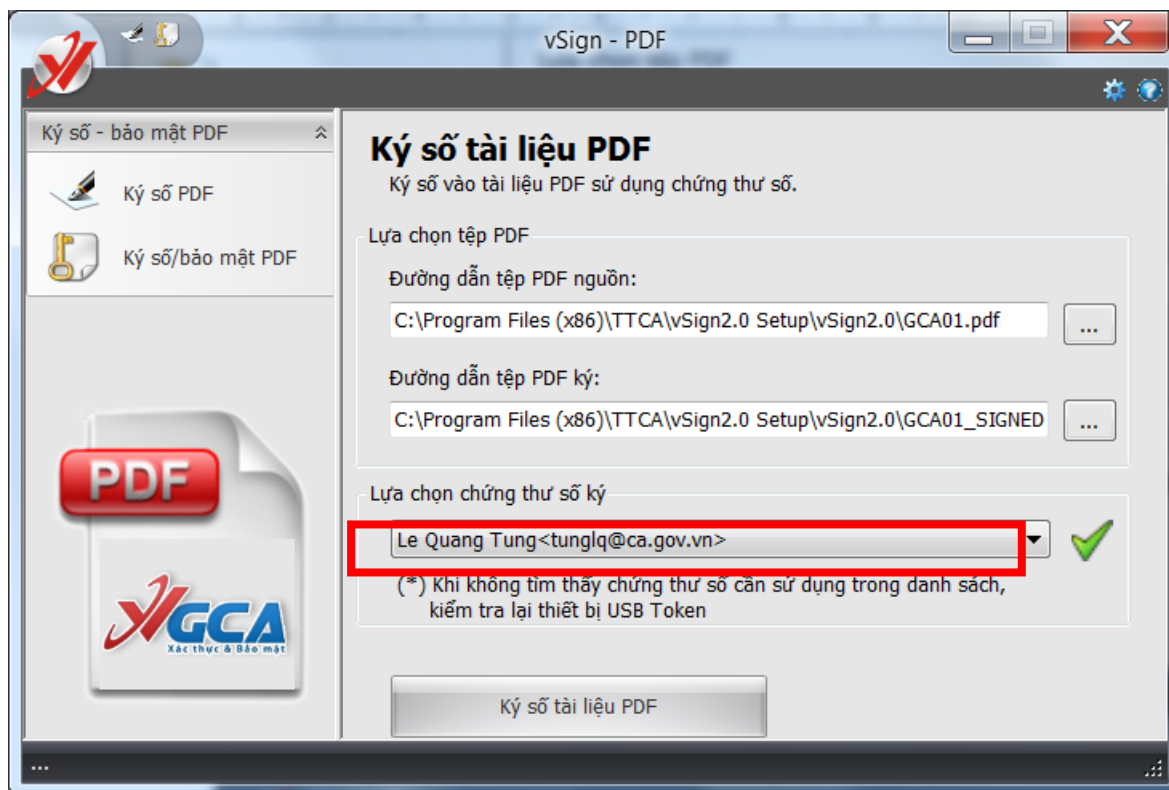
Chọn tệp nguồn(tài liệu PDF định ký số lên):



Chọn tệp đích(chọn vị trí lưu tài liệu PDF khi quá trình gắn chữ ký hoàn tất), mặc định chương trình tự động lưu thành tên tệp + SIGNED:



Chọn chứng thư số người ký :

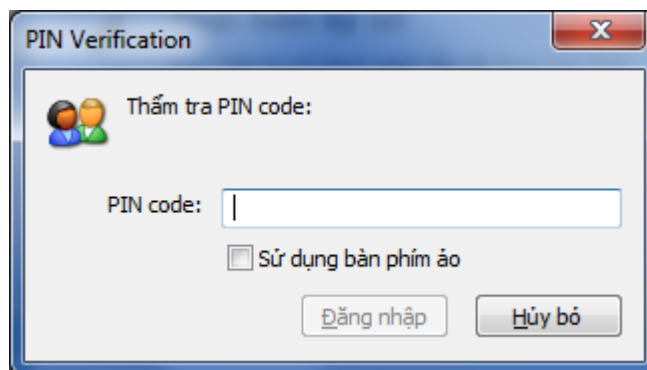


Nhấp vào nút “Ký số tài liệu PDF” để bắt đầu quá trình gắn hữ ký.
Nhập mật khẩu truy cập USB eToken.

- eToken



- ST3:



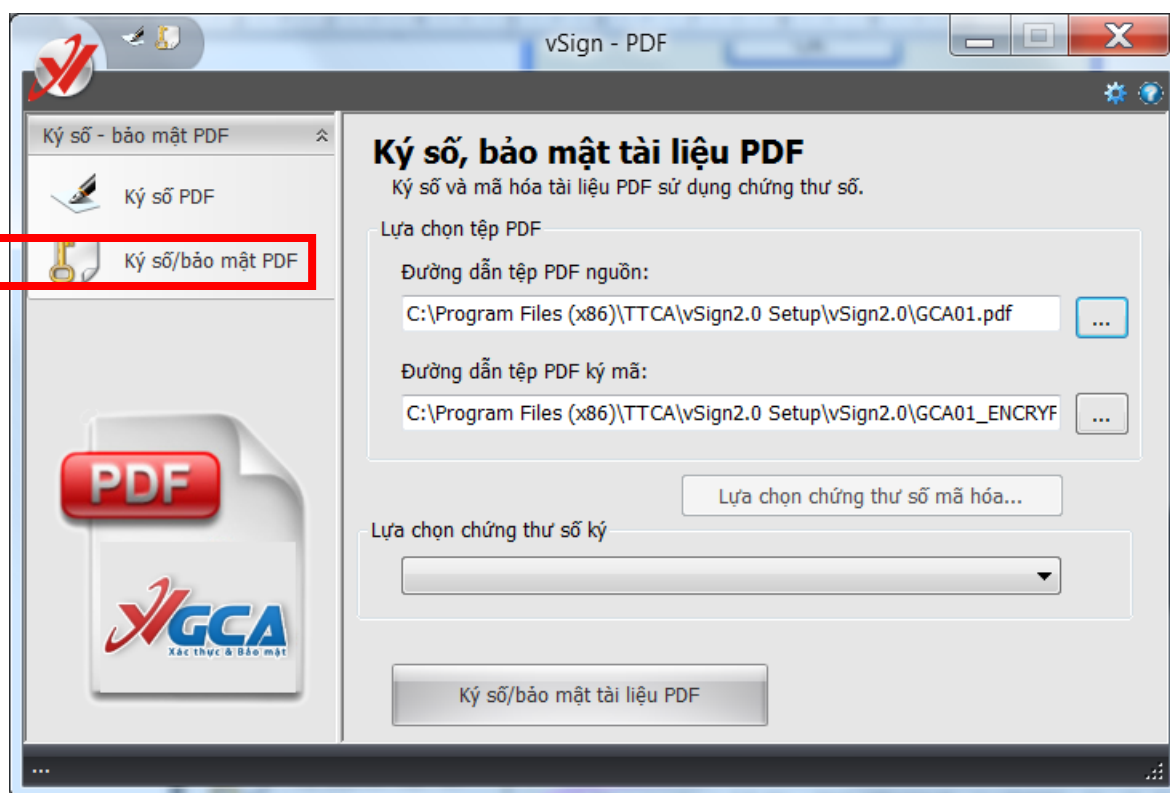
Hoàn tất quá trình gắn chữ ký:



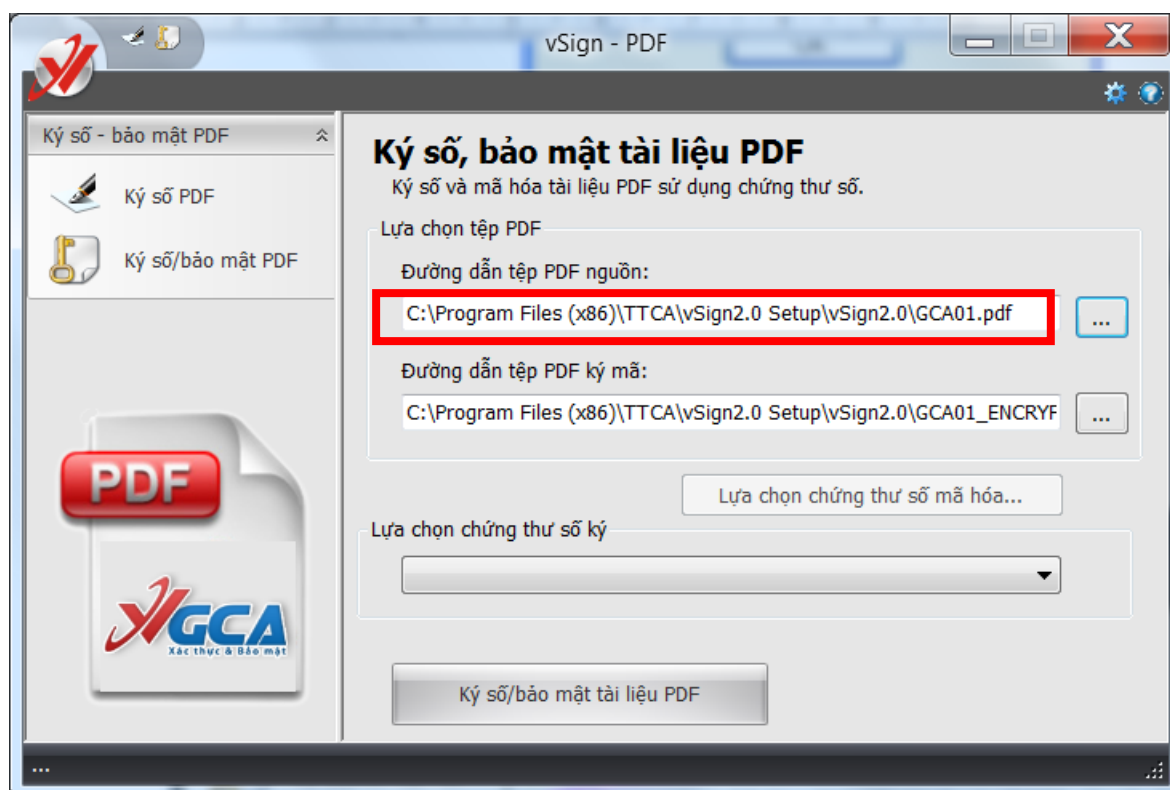
2.6.2 Ký số/bảo mật tài liệu PDF

Ký số/bảo mật tài liệu PDF giúp người sử dụng gắn chữ ký và mã hóa tài liệu PDF. Quy trình ký số/bảo mật như sau:

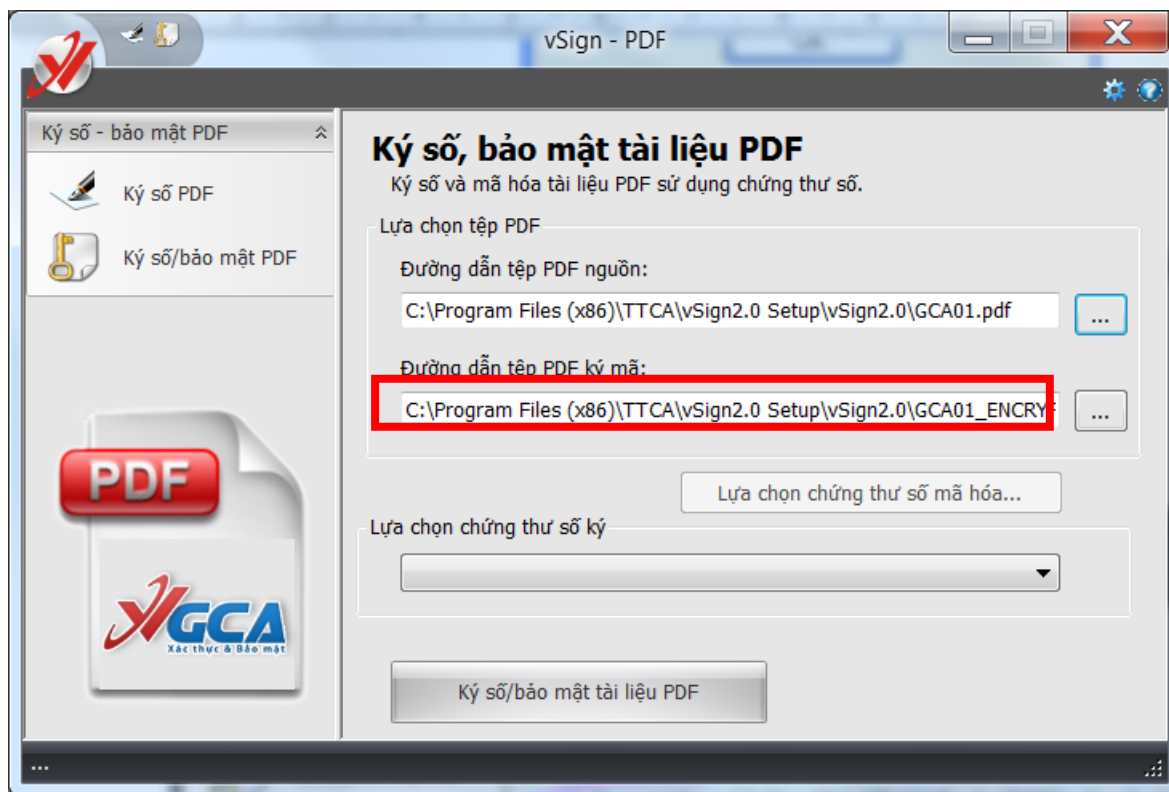
Từ giao diện chính chọn “Ký số/bảo mật PDF”:



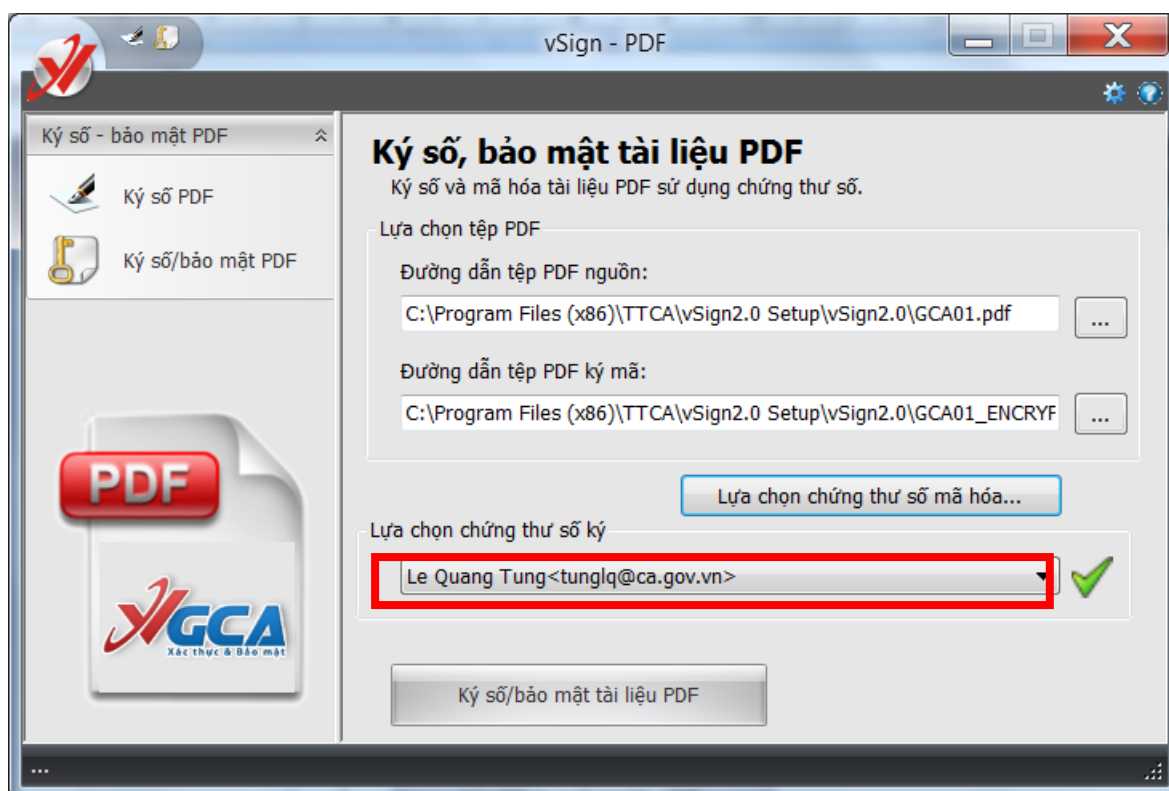
Chọn tệp PDF nguồn (tệp dự định ký số/bảo mật) :



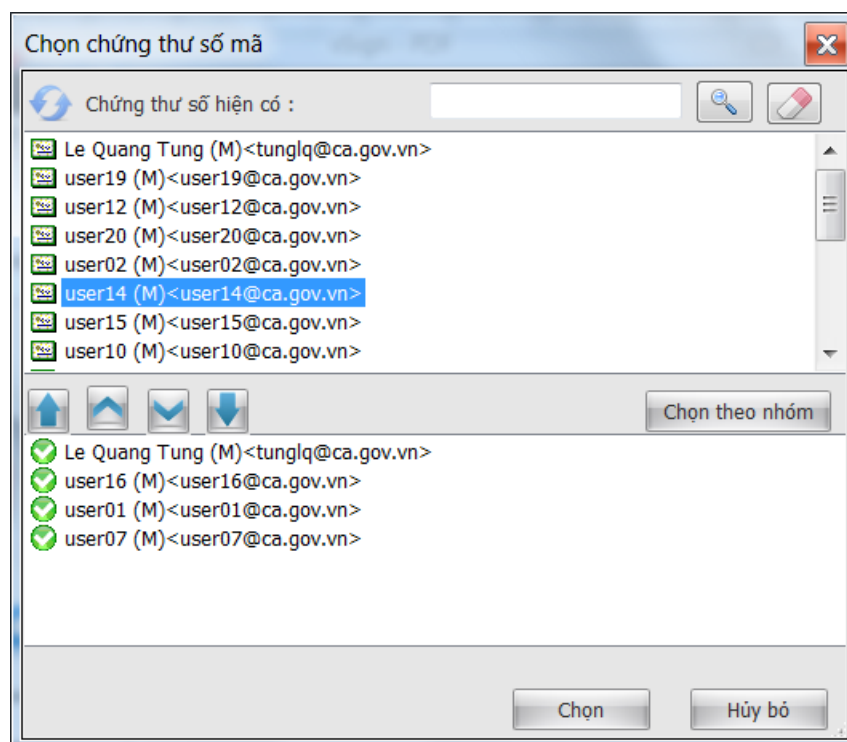
Chọn tệp PDF đích (vị trí lưu tệp PDF khi đã gắn chữ ký và bảo mật hoàn thành), mặc định chương trình tự động lưu tệp với tên tệp + ENCRYPTED.



Chọn chứng thư số người ký:

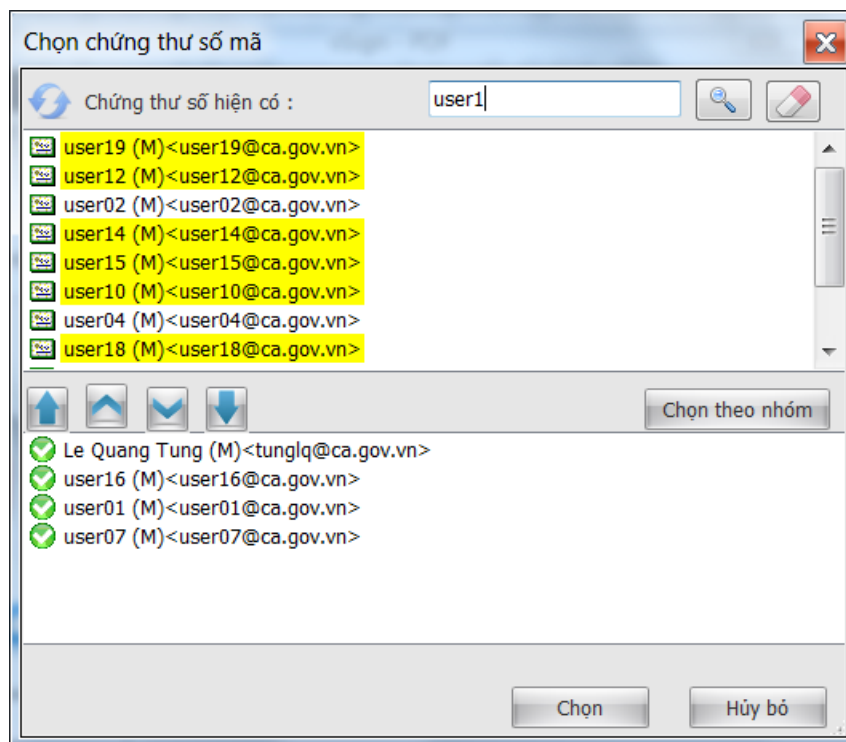


Chọn danh sách chứng thư số được phép giải mã tệp PDF:



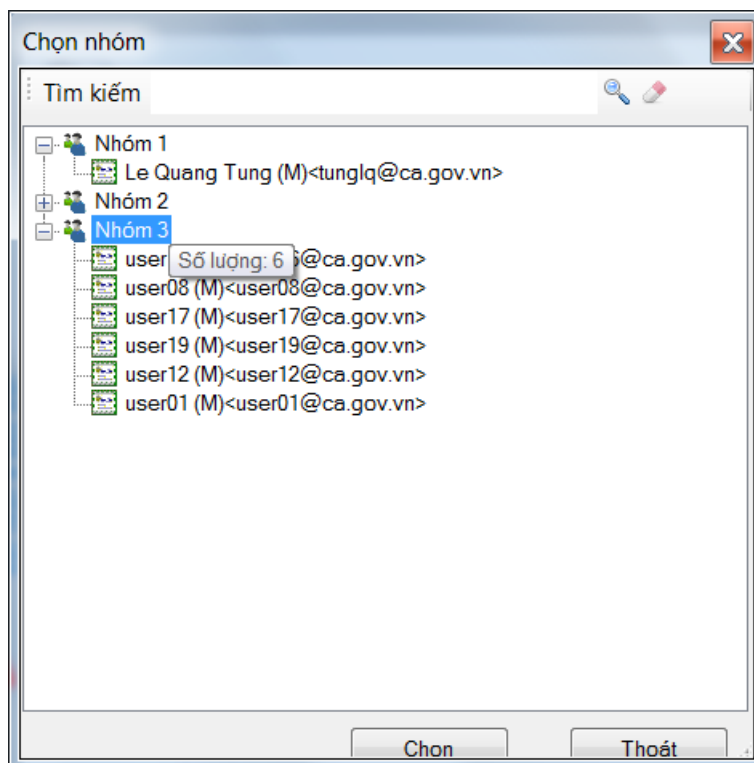
Nếu danh sách chứng thư số quá dài, có thể sử dụng chức năng tìm kiếm để tìm các chứng thư số cần sử dụng, để sử dụng chức năng tìm kiếm người sử dụng gõ tên

cần tìm kiếm để tìm kiếm chứng thư số mong muốn, các chứng thư số phù hợp với tên tìm kiếm sẽ được đánh dấu màu vàng:

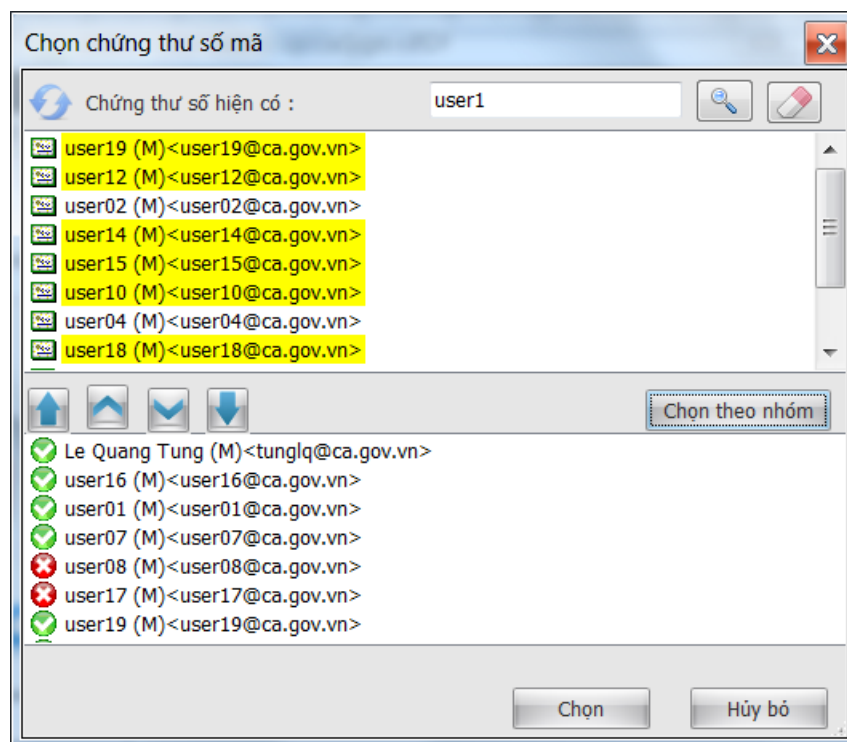


Chọn chứng thư số thích hợp để đưa xuống danh sách bên dưới.

Có thể chọn chứng thư số theo nhóm để có thể quản lý chứng thư số một cách dễ dàng hơn. Để chọn chứng thư số theo nhóm, chọn nút “chọn theo nhóm”:

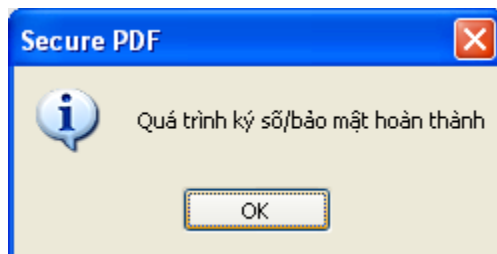


Chọn nhóm chứng thư số cần chọn, bấm chọn để kết thúc quá trình chọn nhóm, toàn bộ chứng thư số trong nhóm sẽ được lựa chọn để mã tệp dữ liệu:



Những chứng thư số có biểu tượng dấu "x" đỏ là các chứng thư số bị hủy bỏ hoặc lỗi cần loại bỏ, kích đúp chuột vào chứng thư số này để loại bỏ.

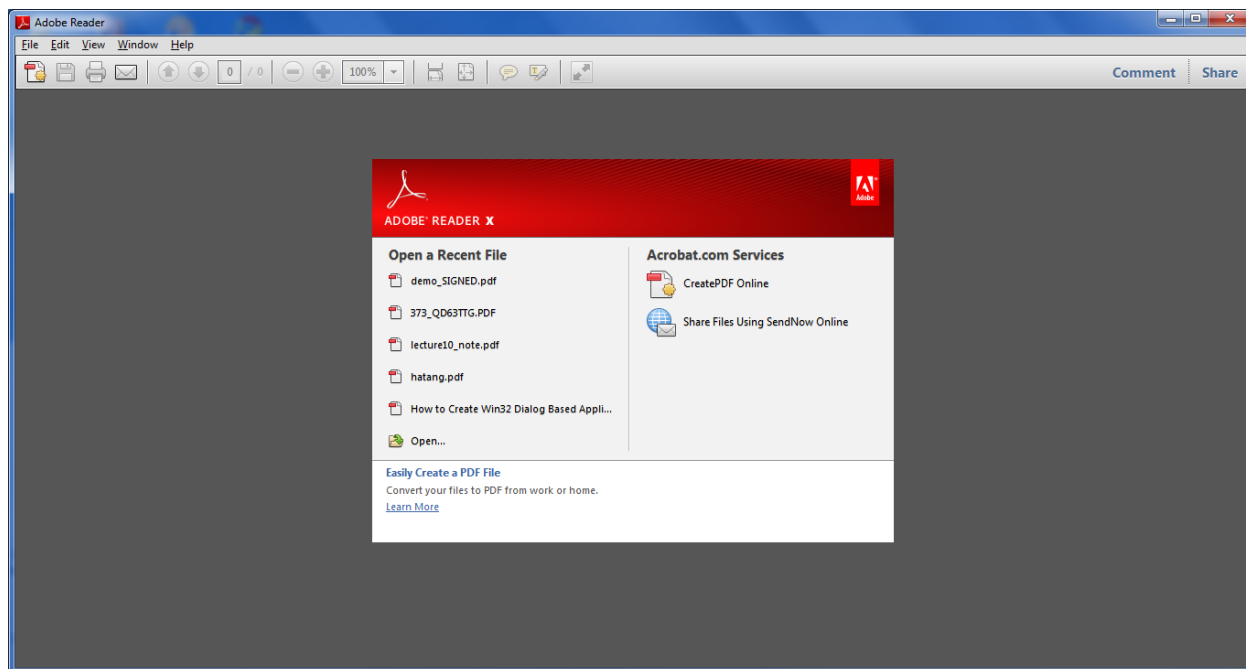
Nhấp nút “Ký số/bảo mật tài liệu PDF” để quá trình gắn chữ ký và mã hóa tiến hành.



2.6.3 Kiểm tra chữ ký số và giải mã tài liệu PDF

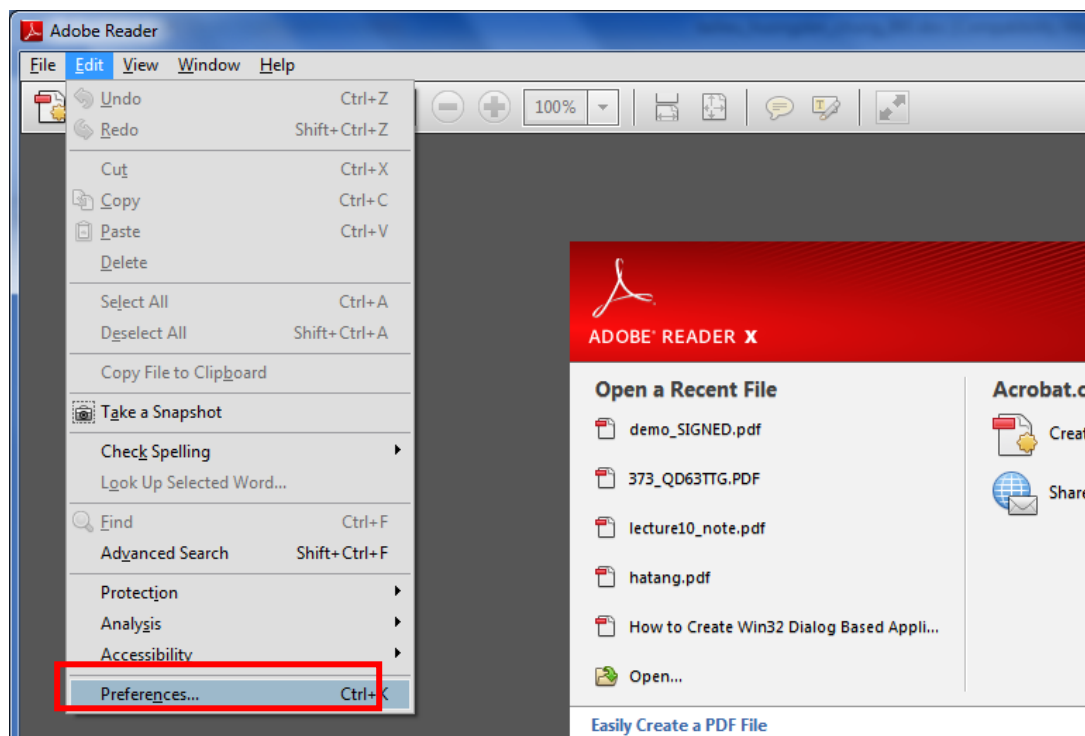
2.6.3.1 Cấu hình Adobe Reader

Trước khi kiểm tra chữ ký số trên tài liệu PDF cần phải cấu hình phần mềm PDF. Sau khi cài đặt Adobe Reader, chạy chương trình Adobe Reader để cấu hình, tùy từng phiên bản sẽ có giao diện hiển thị khác nhau.

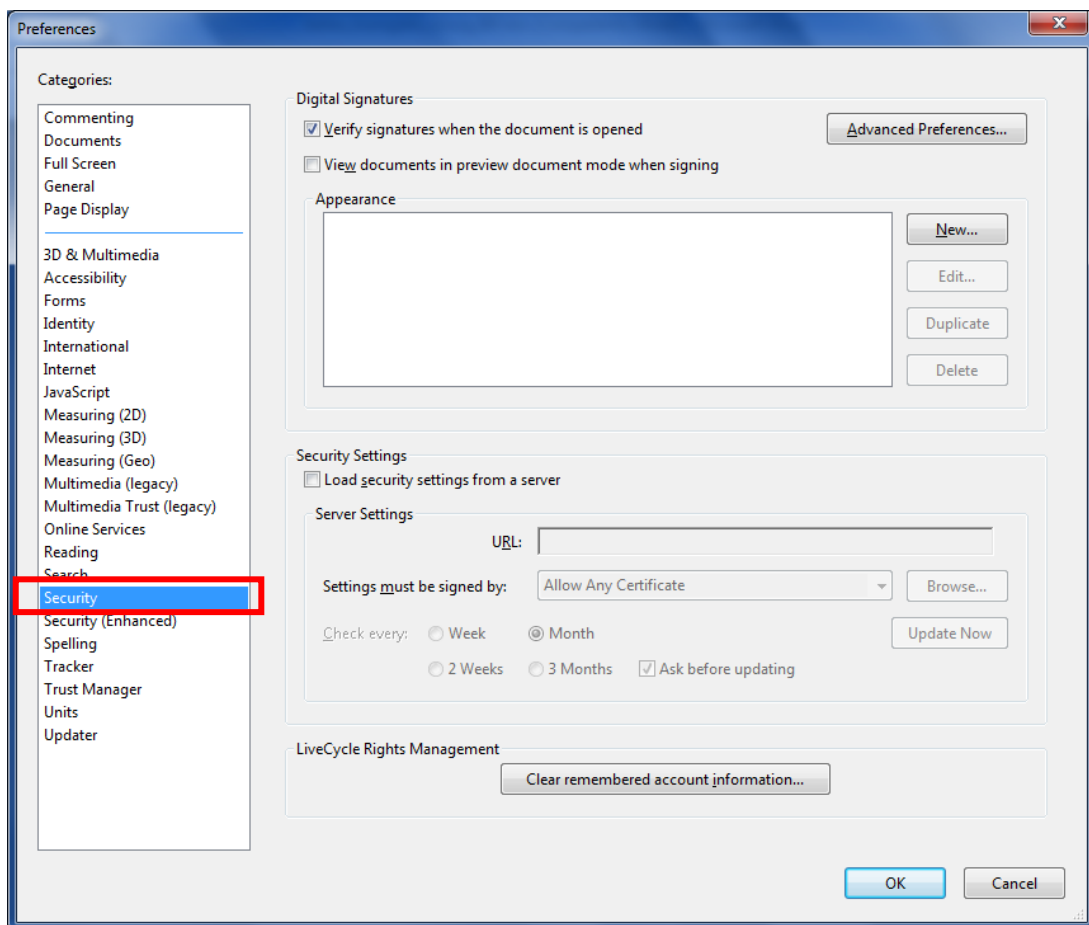


Mục đích cấu hình phần mềm Adobe Reader để sử dụng và kiểm tra được dấu thời gian gắn trên chữ ký và làm cho phần mềm tin tưởng (trust) vào các chứng thư số (chứng thư số Root, sub, timestamp, user,...).

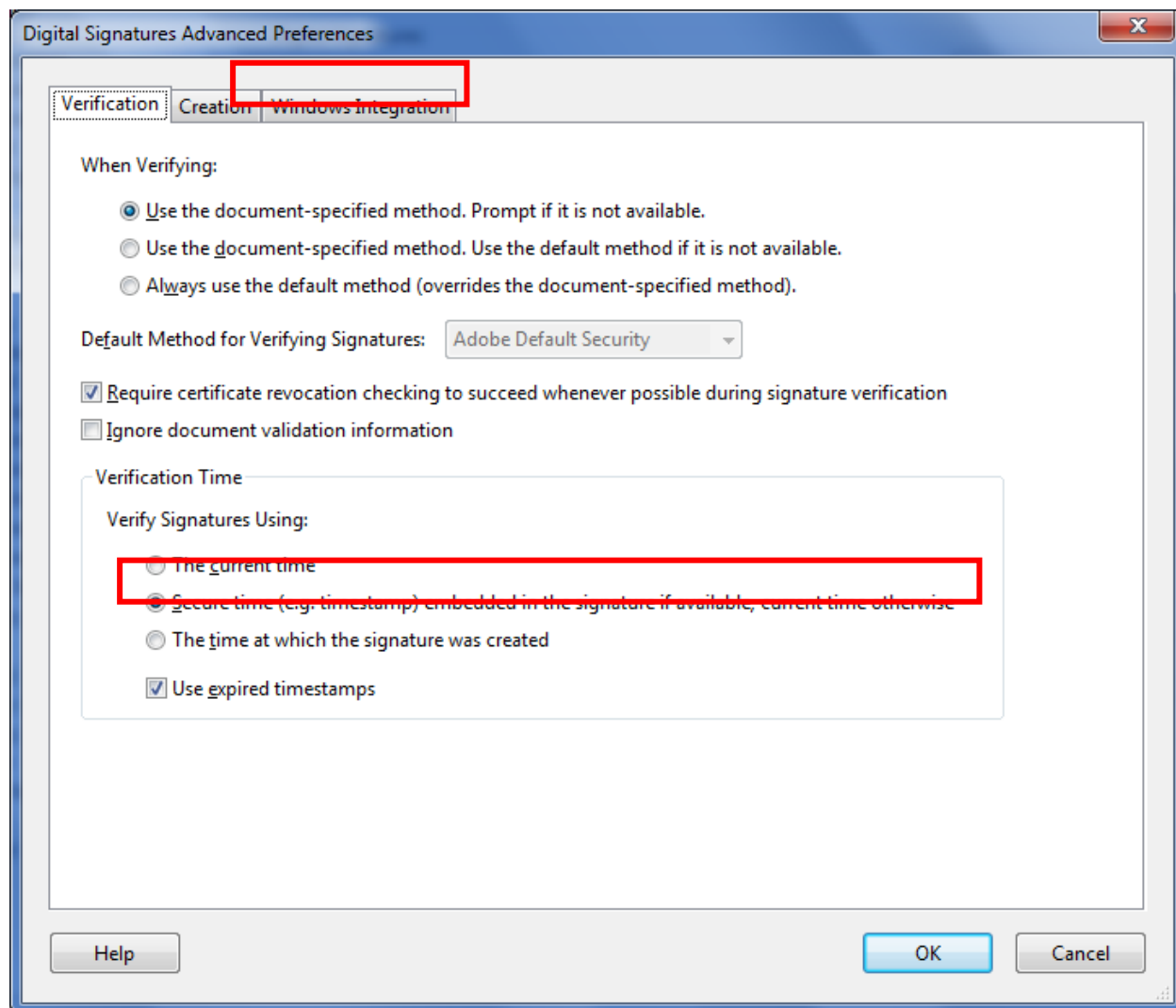
Để cấu hình vào Edit->Preferences...



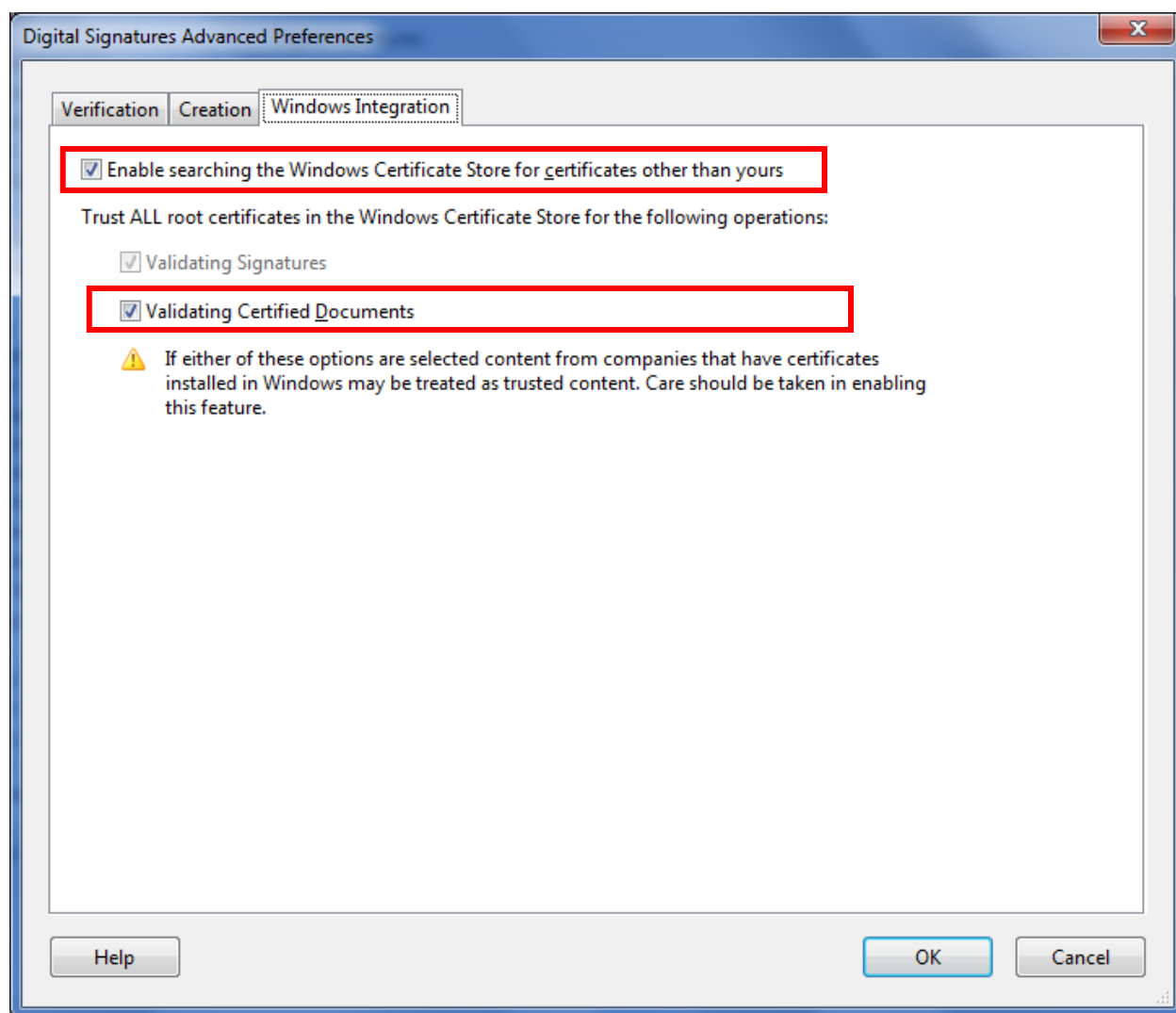
Giao diện hiển thị, chọn Security.



Trong giao diện trên chọn Advanced Preferences.... chọn ô “Secure Time (e.g.timestamp) embedded in the signature if available, current time otherwise”.



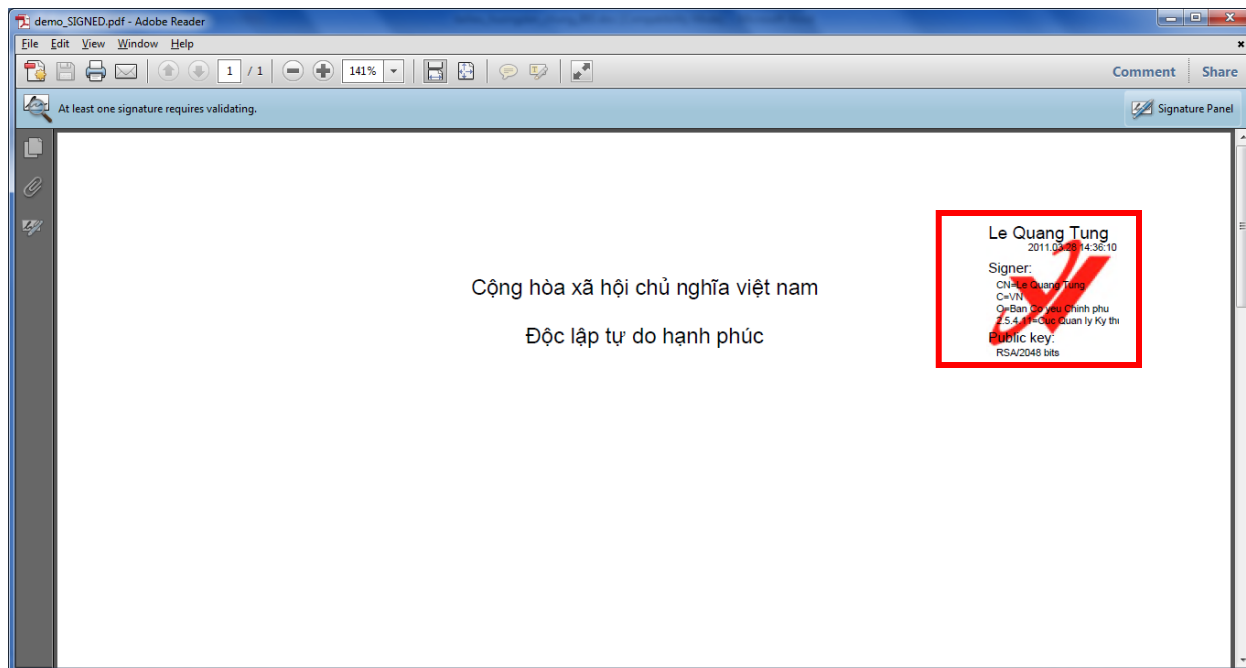
Chọn tab “Windows Intergration” để cấu hình tiếp:



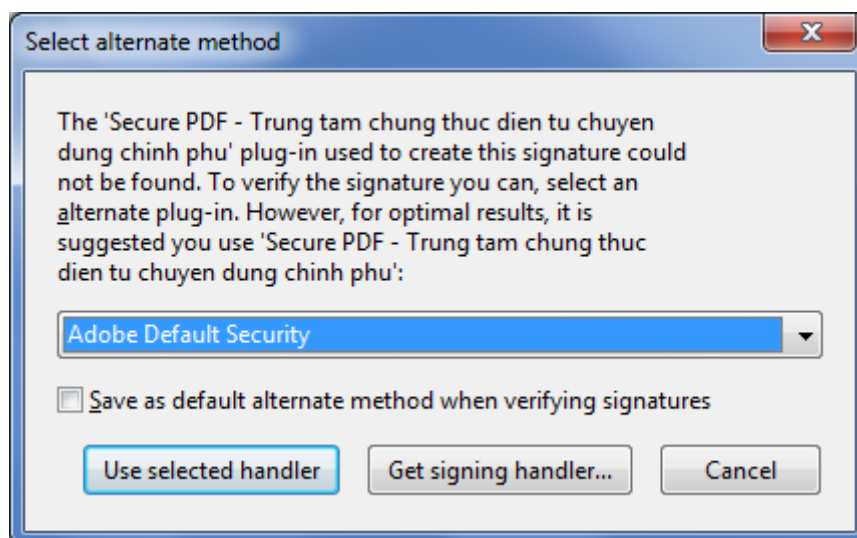
Tích vào ô “Enable searching the Windows Certificate Store for certificates other than yours” và ô “Validating Certified Documents”. Chọn OK để kết thúc việc cấu hình Adobe Reader.

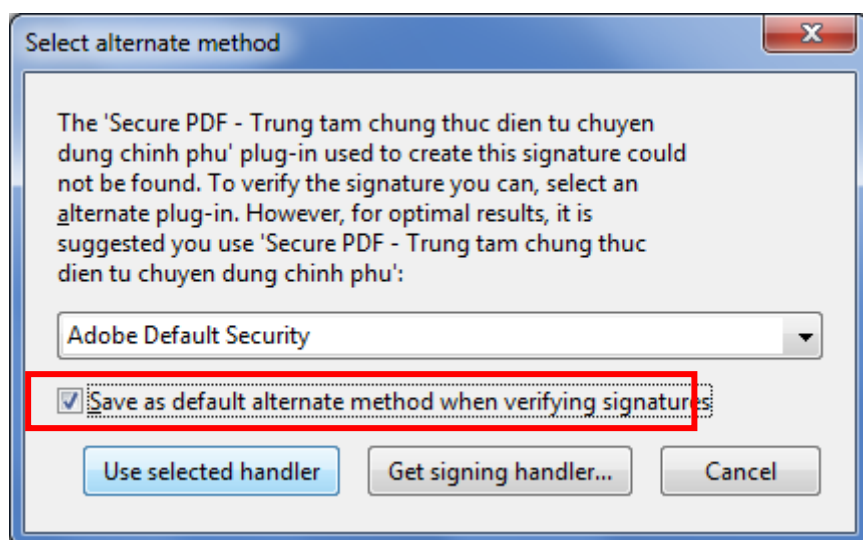
2.6.3.2 Kiểm tra chữ ký số trên tài liệu PDF

Mở tài liệu PDF đã được ký (kích đúp chuột lên tệp PDF được ký).

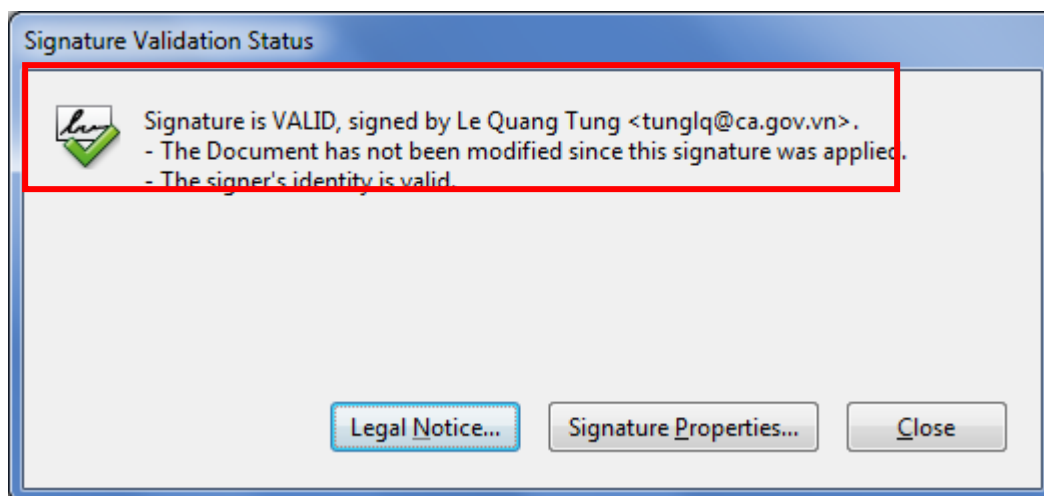


Kích đúp chuột lên chữ ký số trên tài liệu PDF (ô màu đỏ).

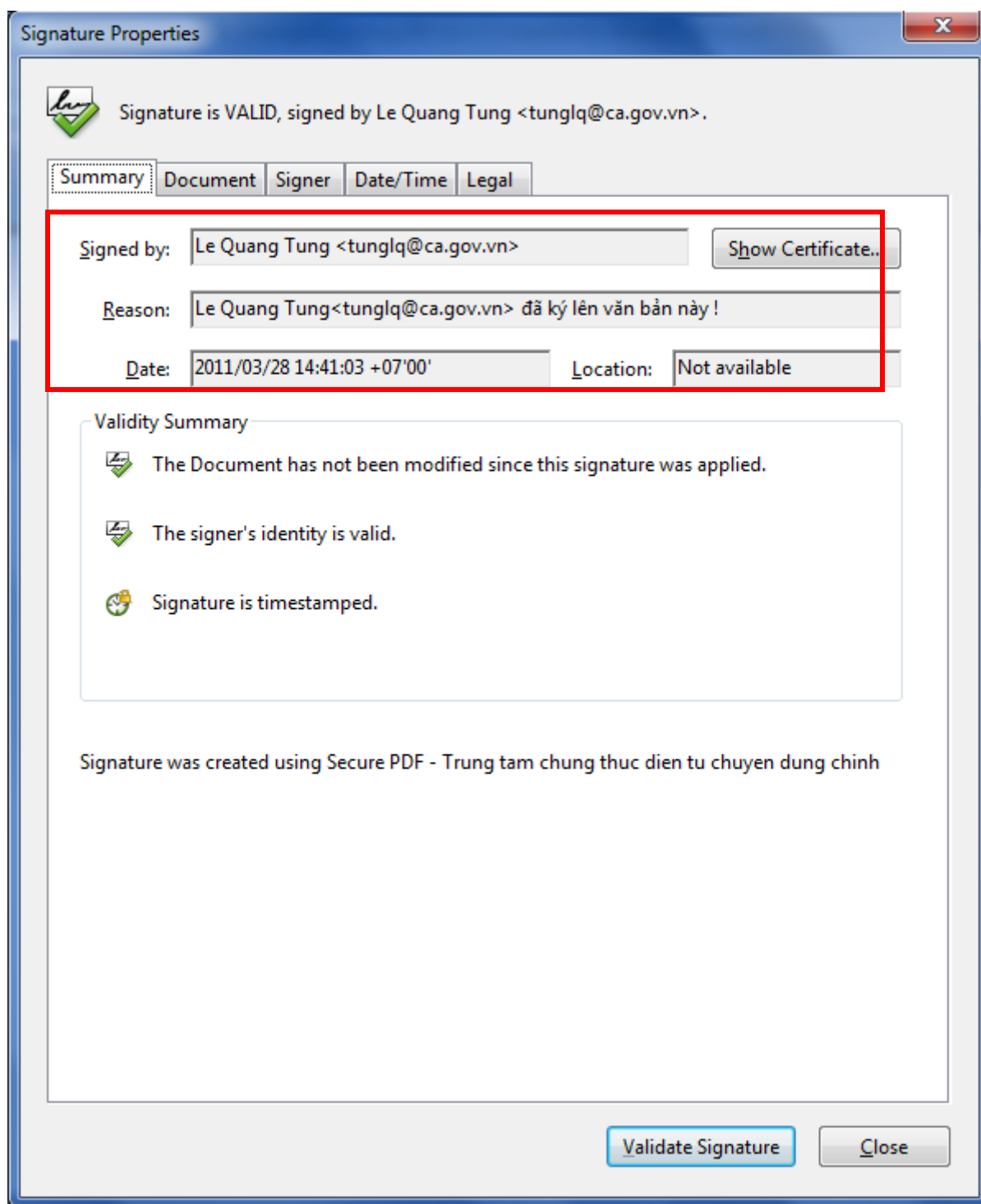




Chọn ô “Save as default.....” và chọn “Use selected handler”.

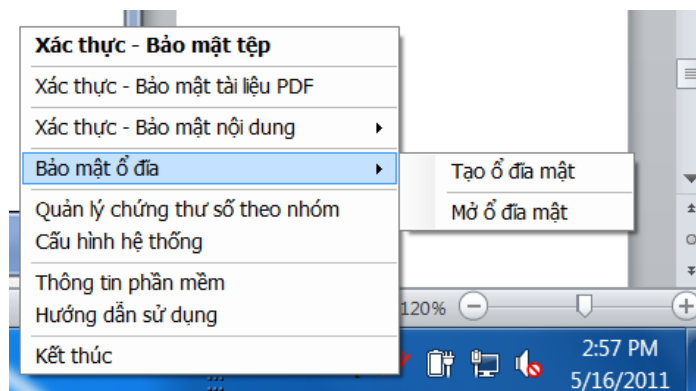


Để xem chi tiết nội dung chữ ký số chọn “Signature Properties...”.



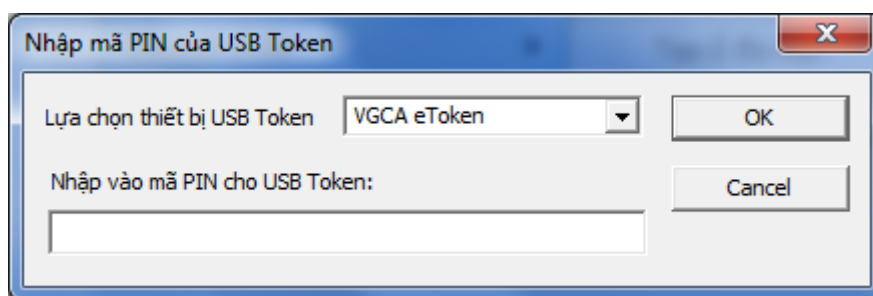
2.7 Bảo mật ổ đĩa

Chương trình bảo mật ổ đĩa giúp người sử dụng tạo các ổ đĩa mật để lưu trữ các tài liệu quan trọng. Chương trình có 02 chức năng chính đó là tạo ổ đĩa mật và mở ổ đĩa mật. Để chạy chương trình, kích chuột phải vào biểu tượng chữ "V" màu đỏ ở góc phải dưới màn hình chọn "Bảo mật ổ đĩa".

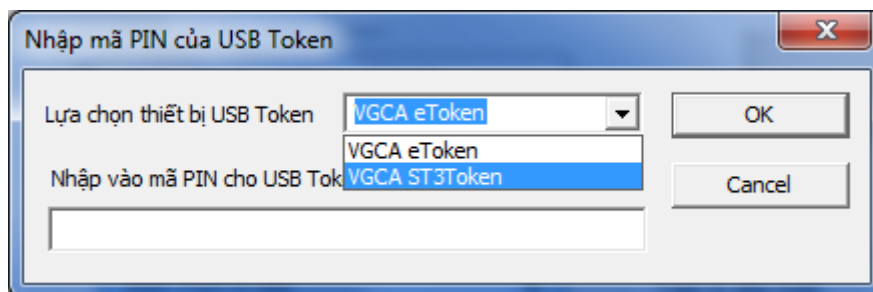


2.7.1 Tạo ổ đĩa mật

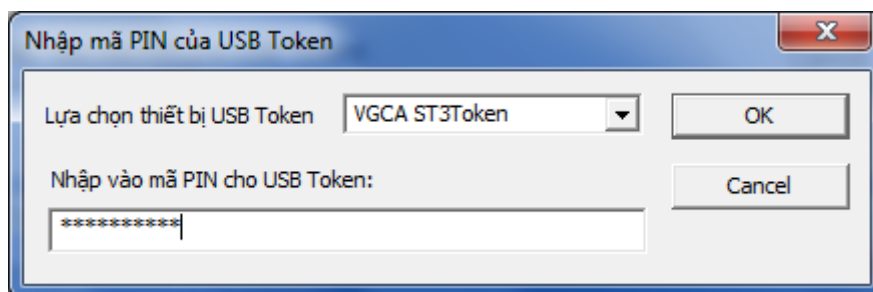
Bước 1: Chọn menu “Bảo mật ổ đĩa”→ “Tạo ổ đĩa mật”.



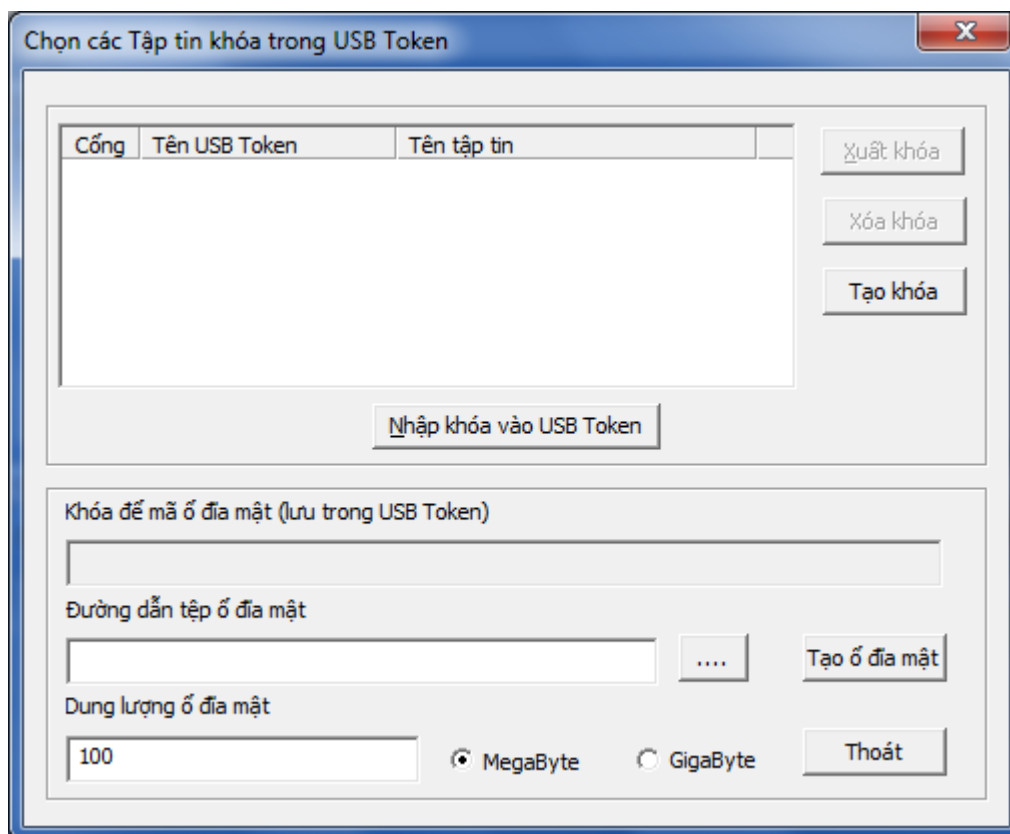
Bước 2: Lựa chọn thiết bị USB Token thích hợp.



Bước 3: Nhập mã PIN cho thiết bị USB Token, chọn OK.

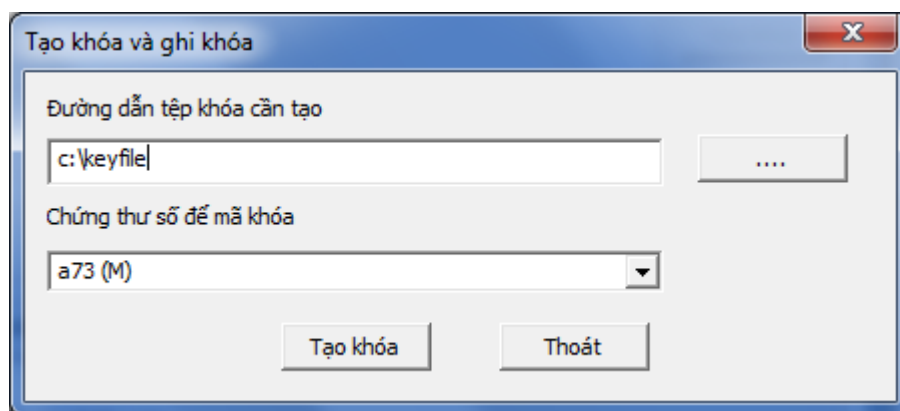


Giao diện chương trình tạo ổ đĩa mật:

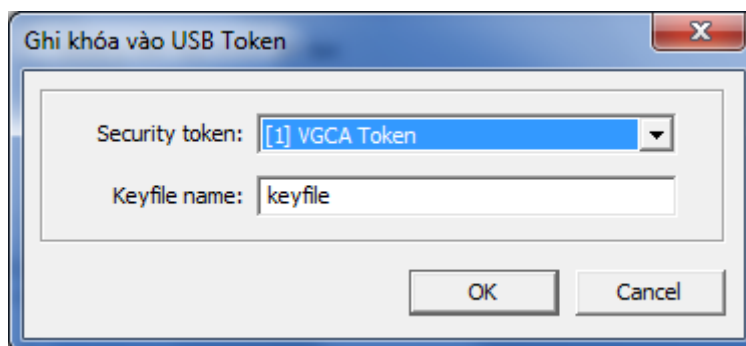


Nếu chưa tạo khóa để mã hóa ổ đĩa mật hoặc muốn tạo khóa mới để mã hóa ổ đĩa tiếp tục bước 5, nếu có khóa sẵn và muốn sử dụng khóa có sẵn thì bỏ qua bước 5 sang bước 6.

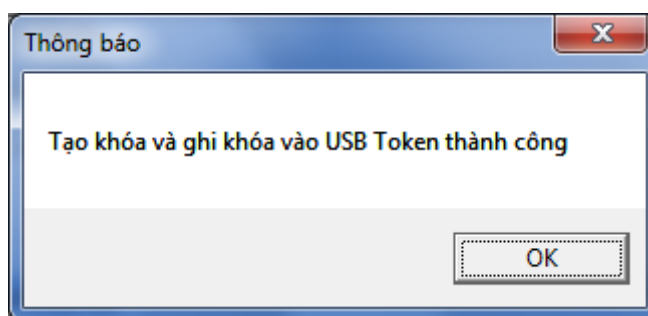
Bước 5: Để tạo khóa chọn nút “Tạo khóa”:



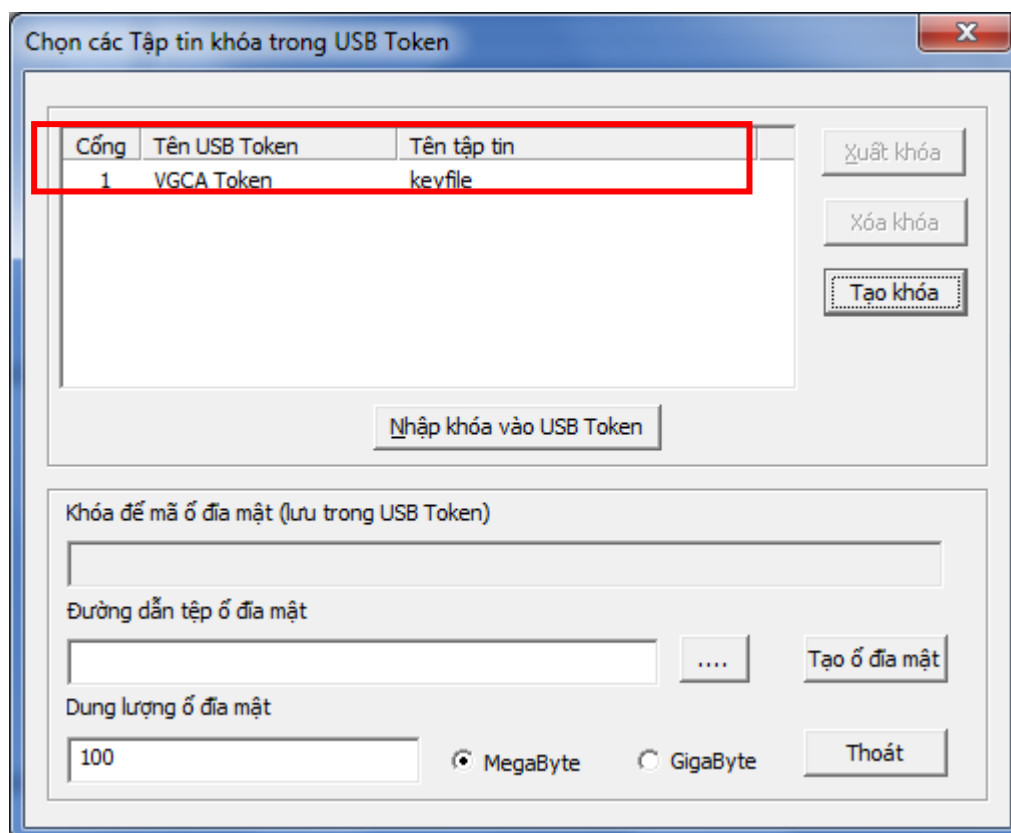
Chọn đường dẫn để lưu tệp khóa mã, chọn chứng thư số để mã khóa (chứng thư số nằm trong thiết bị USB Token), sau đó “tạo khóa”.



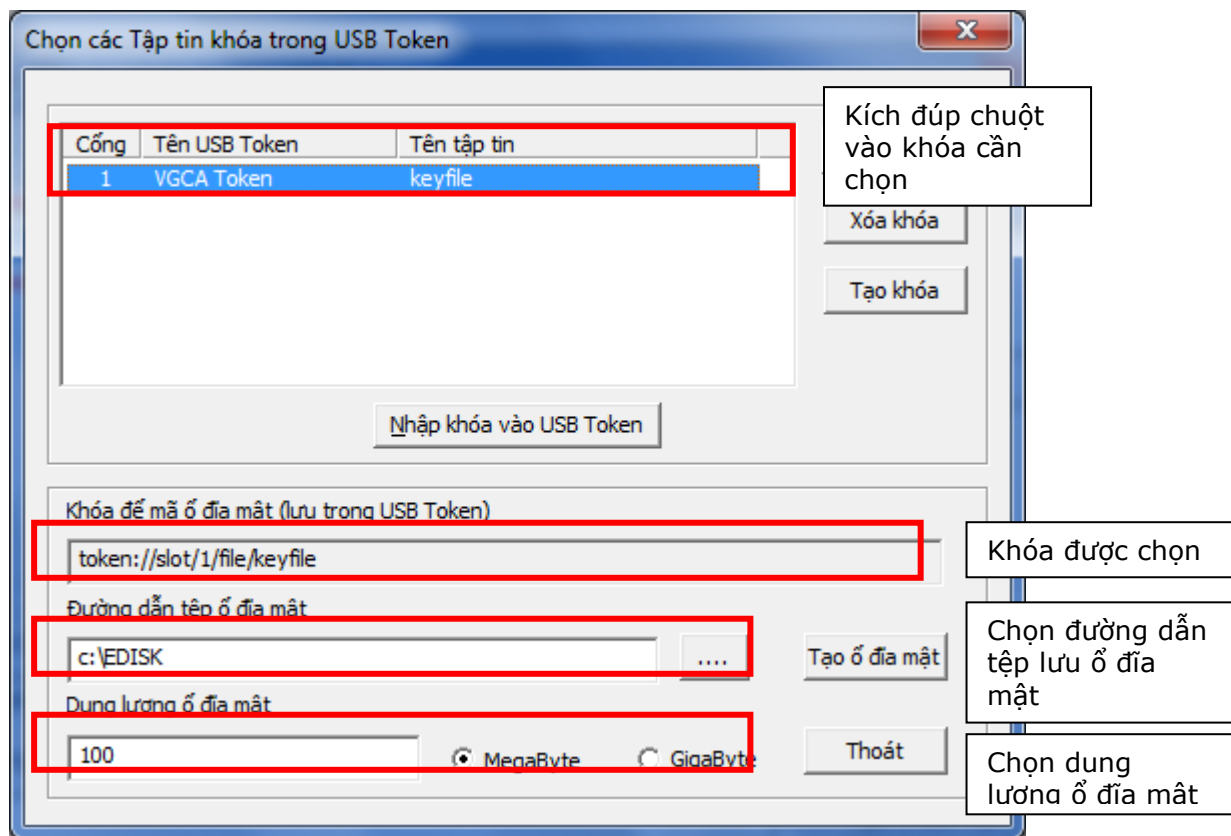
Chọn OK, thông báo tạo và ghi khóa vào USB Token thành công.



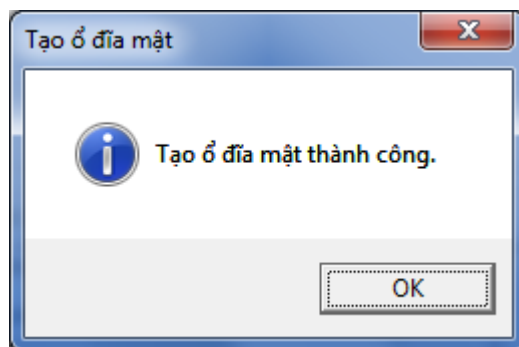
Chọn OK và thoát. Giao diện chương trình sau khi tạo khóa xong.



Bước 6: Tạo ổ đĩa mật, kích đúp chuột vào khóa lưu trong thiết bị USB Token, nhập các thông số cần thiết để tạo ổ đĩa mật.



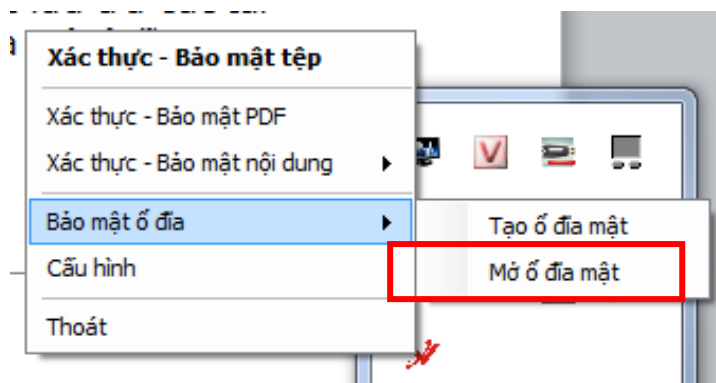
Chọn nút “Tạo ổ đĩa mật” để tạo ổ đĩa mật:



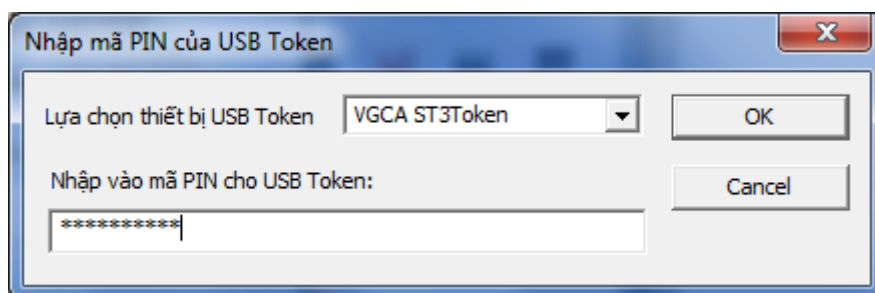
Sau khi tạo xong, tệp ổ đĩa mật sẽ được lưu vào “đường dẫn tệp ổ đĩa mật”. Trước khi sử dụng phải sử dụng chương trình “Mở ổ đĩa mật” để sử dụng.

2.7.2 Mở ổ đĩa mật

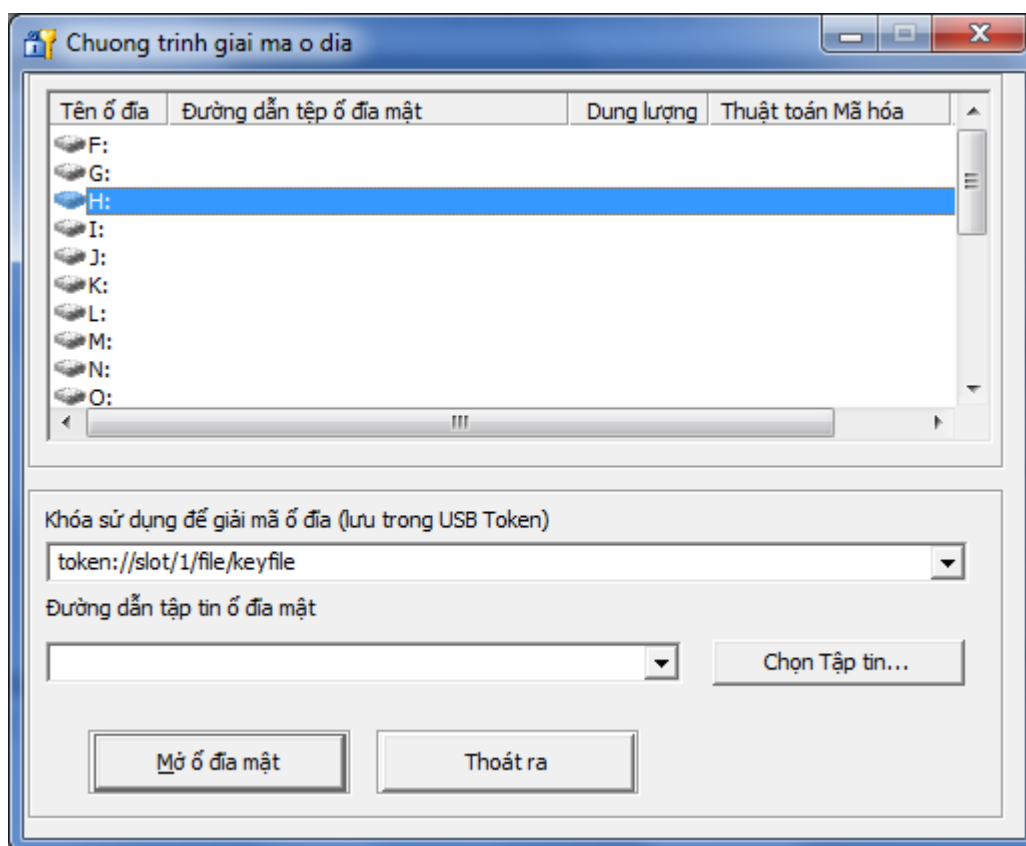
Để mở ổ đĩa mật chọn menu “Bảo mật ổ đĩa” → “Mở ổ đĩa mật”.



Bước 1: Đăng nhập (giống phần đăng nhập của chương trình tạo ổ đĩa mật).

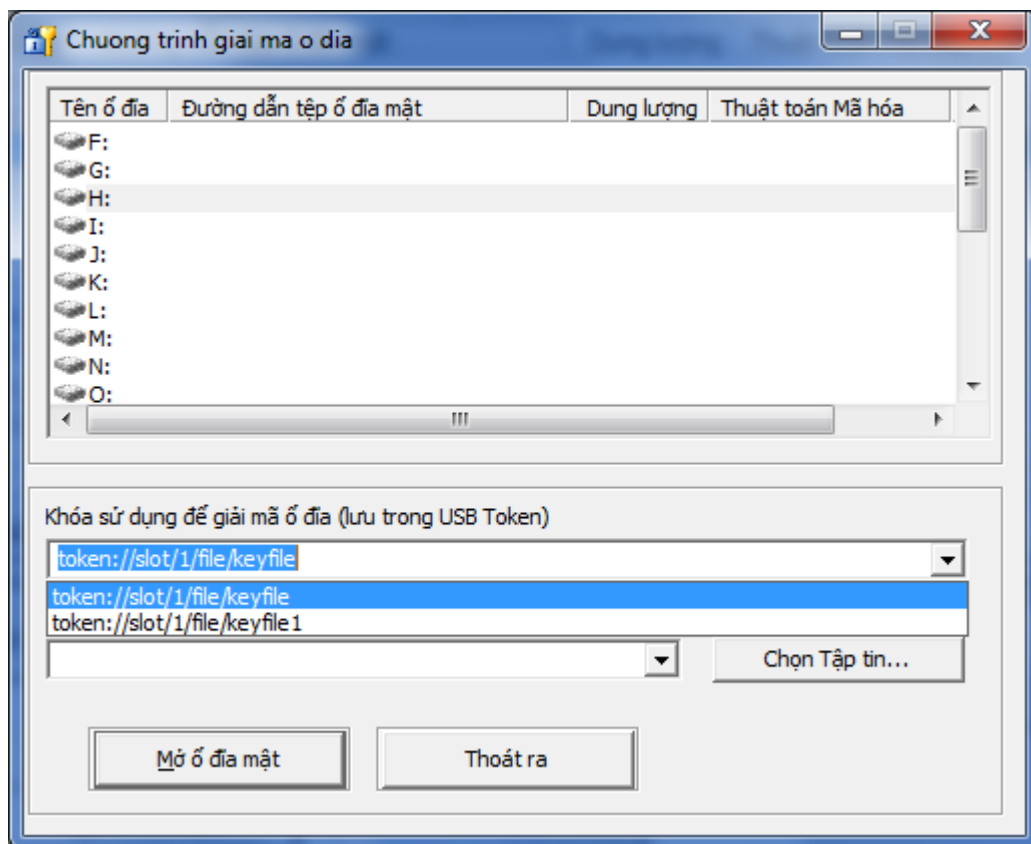


Chọn thiết bị USB Token tương ứng và nhập mã PIN cho thiết bị USB Token.



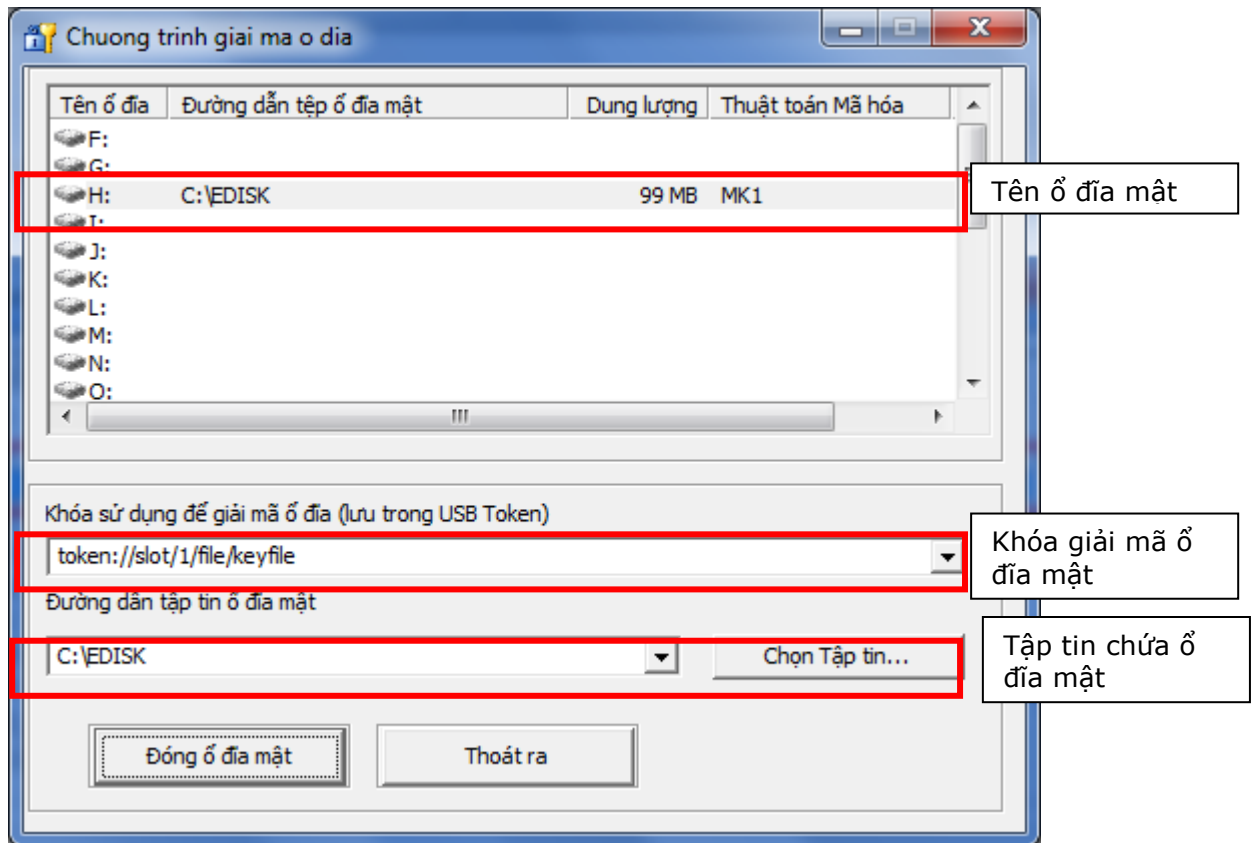
Bước 2: chọn tên ổ đĩa trong danh sách “tên ổ đĩa”.

Bước 3: chọn khóa giải mã ổ đĩa được lưu trong thiết bị USB Token.

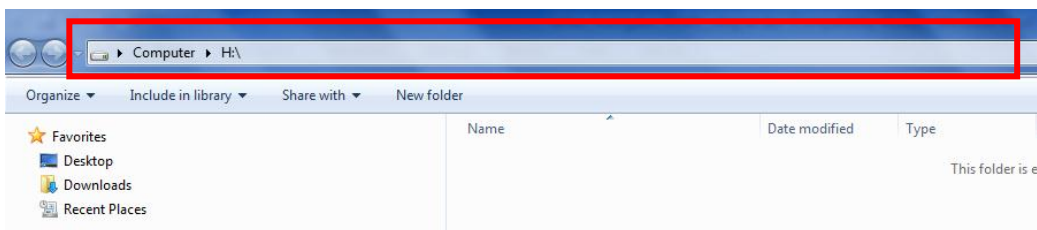


Trong trường hợp có nhiều khóa mã, phải chọn đúng khóa mã cần dùng, nếu không sẽ không mở được ổ đĩa mật.

Bước 4: Chọn tập tin ổ đĩa mật và giải mã ổ đĩa.

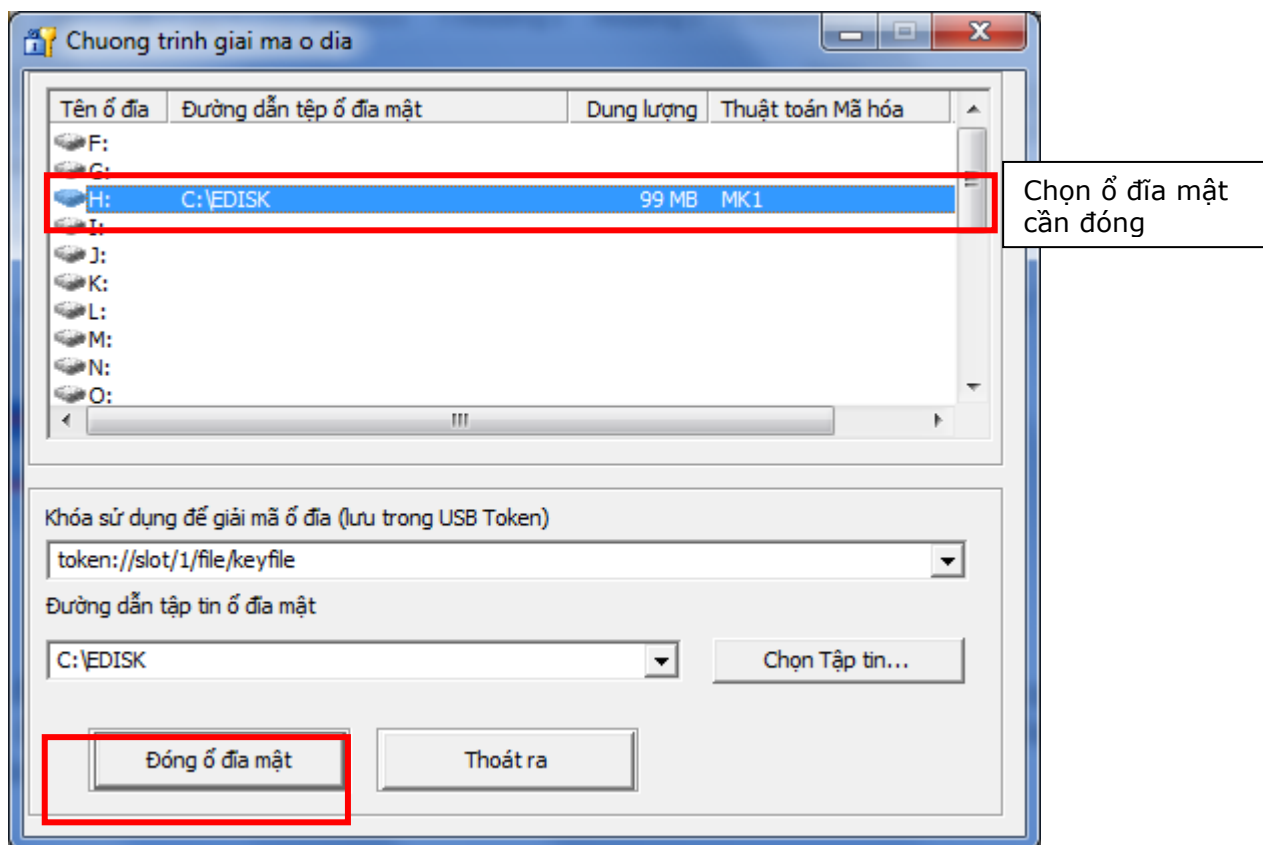


Bước 5: mở ổ đĩa mật kích đúp chuột vào phần tên ổ đĩa mật đang ở, hoặc mở “My Computer”:



Sau khi ổ đĩa mật được mở người dùng có thể sao chép hoặc tạo những dữ liệu quan trọng cần bảo mật vào ổ đĩa này. Khi không dùng ổ đĩa mật này, phải đóng ổ đĩa mật lại.

Bước 6: Đóng ổ đĩa mật, chọn ổ đĩa mật cần đóng và chọn nút “Đóng ổ đĩa mật”.

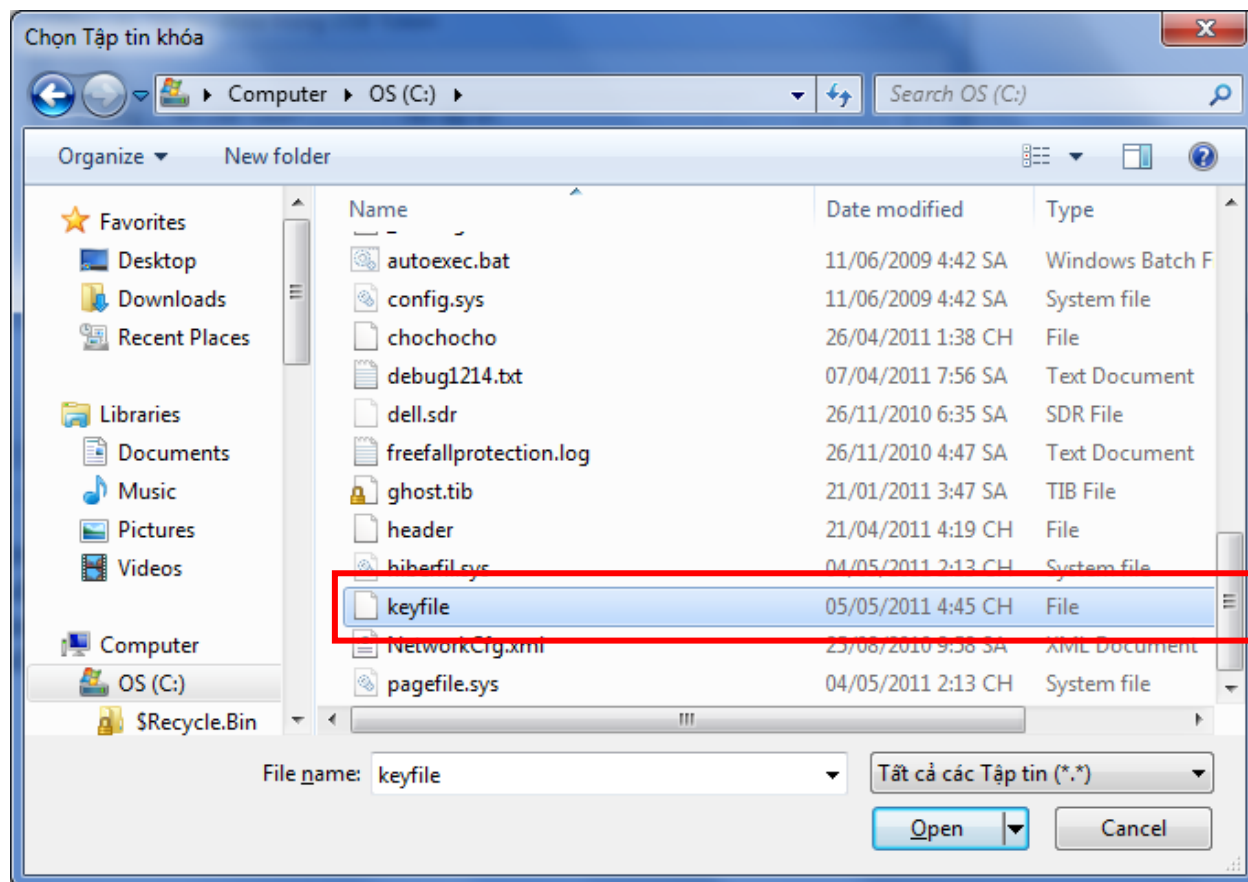


Khi thoát khỏi chương trình, toàn bộ ổ đĩa mật đang mở sẽ tự động đóng lại.

Chú ý:

Khóa bảo mật ổ đĩa được mã hóa bằng chứng thư số mã của người sử dụng và người sử dụng phải lưu lại khóa để tránh trường hợp hỏng hoặc mất thiết bị USB Token và không mở lại được ổ đĩa mật.

Nếu trường hợp mất hoặc hỏng thiết bị có thể xin cấp thiết bị mới và nhập chứng thư số mã cũ vào thiết bị USB Token (xin cấp lại chứng thư số mã được lưu tại Trung tâm Chứng thực điện tử chuyên dùng Chính phủ), sau đó sử dụng chức năng nhập khóa vào thiết bị USB Token, tìm khóa đã lưu để nhập lại.



Sau đó mở ổ đĩa mật như phần “mở ổ đĩa mật”.

3 Kết luận

Bộ công cụ ký số GCA-01 có thể đáp ứng tốt các nhu cầu bảo mật và xác thực tài liệu điện tử trong các cơ quan nhà nước, tuy nhiên trong quá trình xây dựng và triển khai bộ công cụ ký số GCA-01 sẽ không tránh khỏi một số lỗi, sai sót, do vậy chúng tôi rất mong muốn các cơ quan đơn vị trong quá trình triển khai, sử dụng bộ công cụ ký số GCA-01 đóng góp các ý kiến, nhận xét để chúng tôi phát triển và hoàn thiện sản phẩm hơn nữa để phục vụ tốt nhiệm vụ bảo mật và xác thực tài liệu điện tử cho các cơ quan thuộc hệ thống chính trị.

Địa chỉ liên hệ:

Trung tâm chứng thực điện tử chuyên dùng Chính phủ
Địa chỉ: 105 Nguyễn Chí Thanh, Đống Đa, Hà Nội
Điện thoại: 04.37738668
Fax: 04.37738668
Email: info@ca.gov.vn
Website: http://ca.gov.vn

Bộ phận hỗ trợ triển khai:

Lê Quang Huy
Mobile: 0918.491930

Email: lequanghuy@ca.gov.vn

Bộ phận hỗ trợ tích hợp ứng dụng:

Lê Quang Tùng

Mobile: 0913.062590

Email: tunglq@ca.gov.vn

Bộ phận hỗ trợ cấp chứng thư số:

Nguyễn Hoàng Điệp

Mobile: 0915.981708

Email: diepnh@ca.gov.vn