BAN CƠ YẾU CHÍNH PHỦ

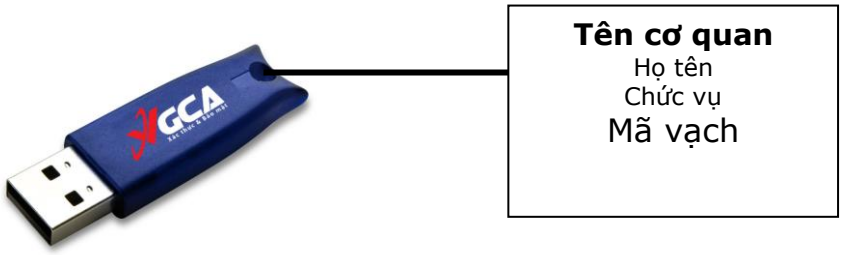
TÀI LIỆU HƯỚNG DẪN SỬ DỤNG BỘ CÔNG CỤ KÝ SỐ GCA-01

Người ký: Phạm Công Thảo
Email: pcthao@bcy.gov.vn
Cơ quan: Cục Chứng thực số và Bảo mật Thông tin, Ban Cơ yếu Chính phủ
Thời gian ký: 13.04.2016 13:02:44 +07:00

Mục lục

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 512MB, có cổng USB, sử dụng hệ điều hành: Windows XP SP3, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012, Windows 8.0, 8.1, Windows 10.

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

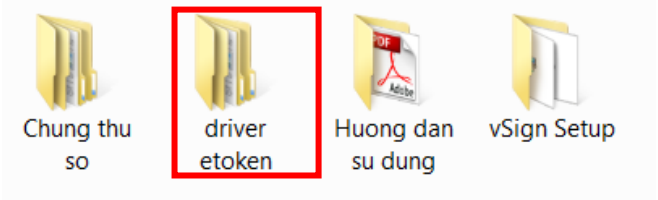
1.2.2.1 Thiết bị eToken

Thiết bị eToken Pro

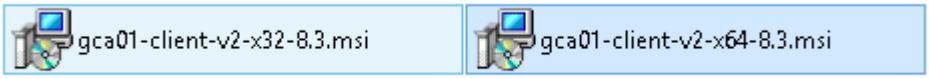
Thiết bị eToken 5100

1.2.2.2 Cài đặt trình điều khiển thiết bị eToken

Bước 1: Mở đĩa CD được cấp phát



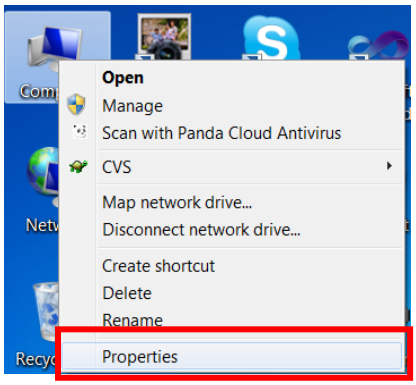
Chọn thư mục driver etoken → chọn bộ cài đặt "*gca01-client-v2-x32-8.3.msi*" cho hệ điều hành 32-bit hoặc "*gca01-client-v2-x64-8.3.msi*" cho hệ điều hành 64-bit.



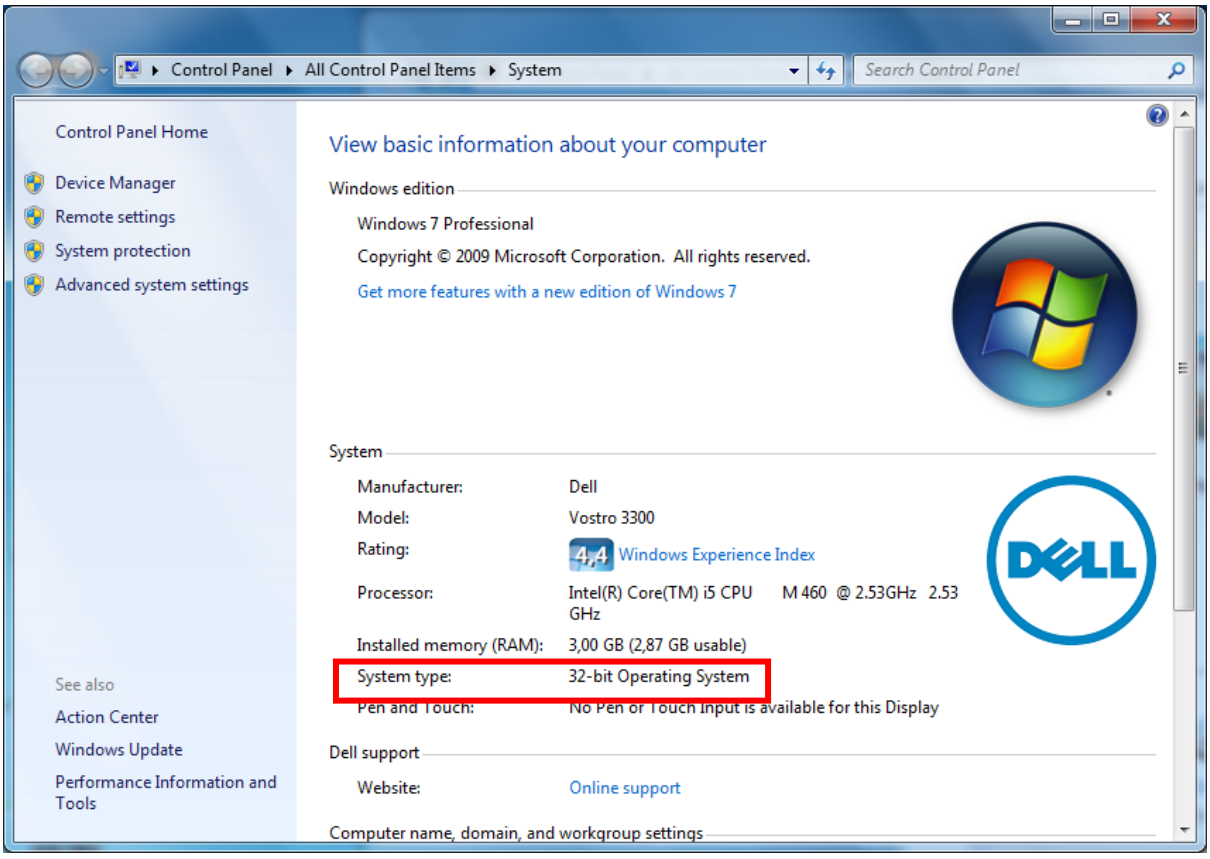
Nhấp đúp chuột để chạy chương trình cài đặt.

Chú ý:

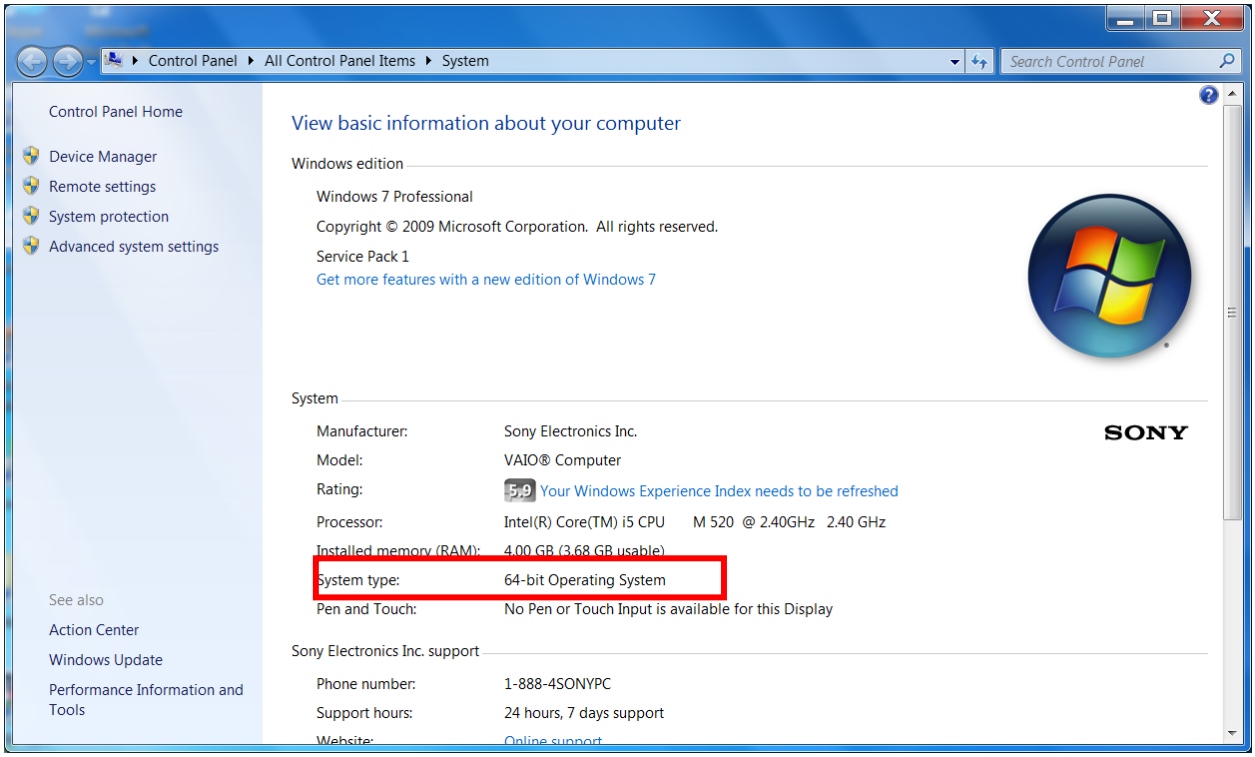
- ***Để biết được hệ điều hành mình đang sử dụng là hệ điều hành 32bit hay 64bit, bấm chuột phải vào biểu tượng My Computer (trên màn hình) → Properties.***



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

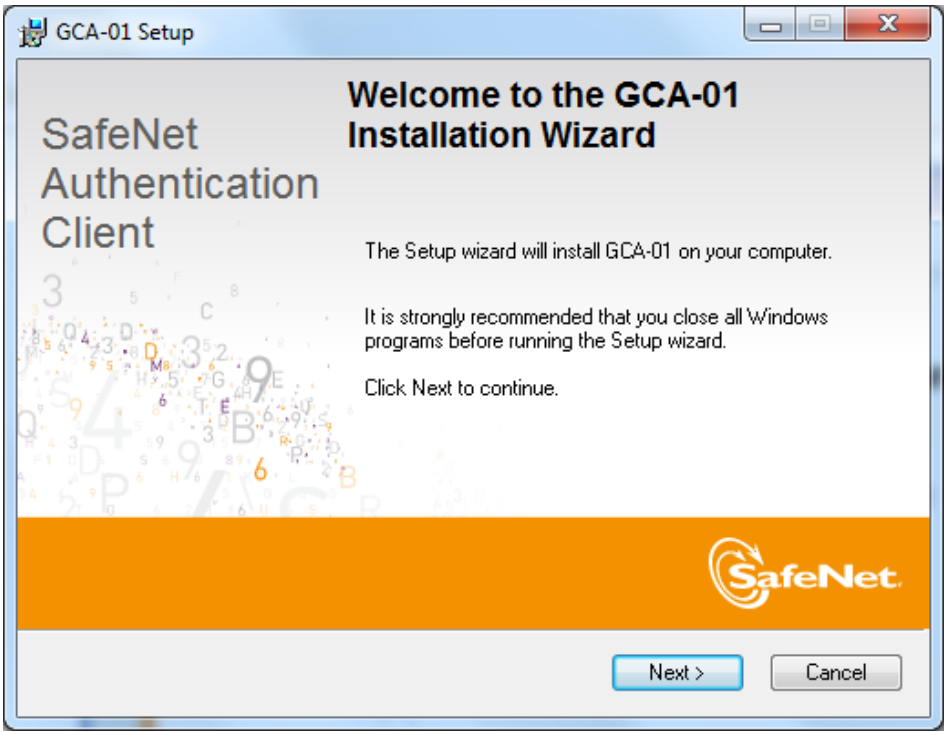


- ***Hệ điều hành 64 bit (Windows 7):***

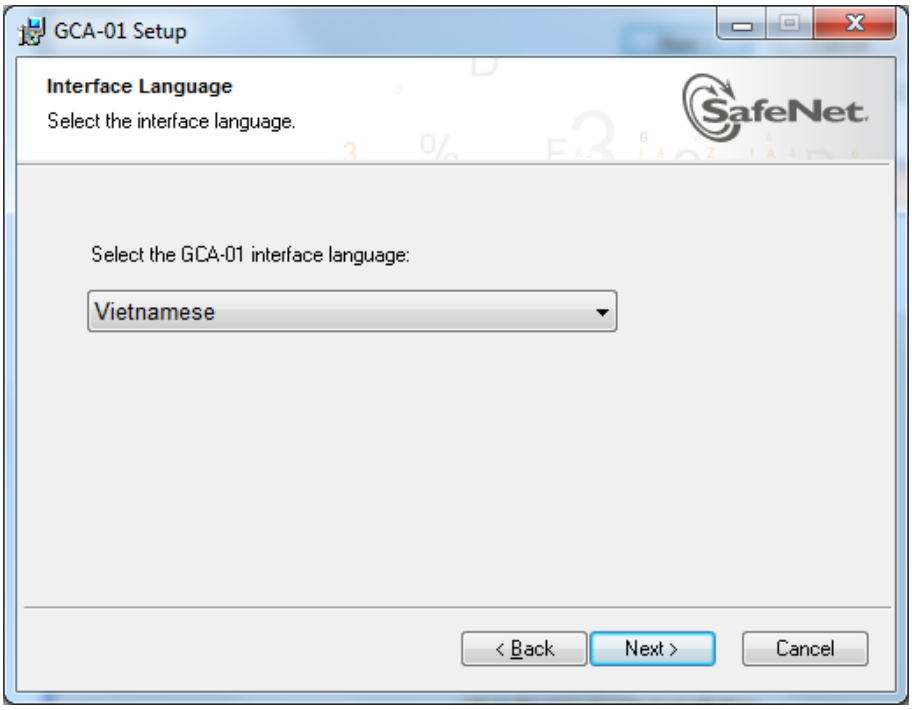


- ***Đối với Windows XP chủ yếu là hệ điều hành 32bit, Windows Vista 32bit và 64bit giao diện kiểm tra có khác hơn một chút nhưng vẫn có thể kiểm tra được bằng phương pháp trên.***
- ***Bộ công cụ ký số GCA-01 chủ yếu sử dụng hệ điều hành Windows 32bit, đối với hệ điều hành Windows 64bit, chức năng chuột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

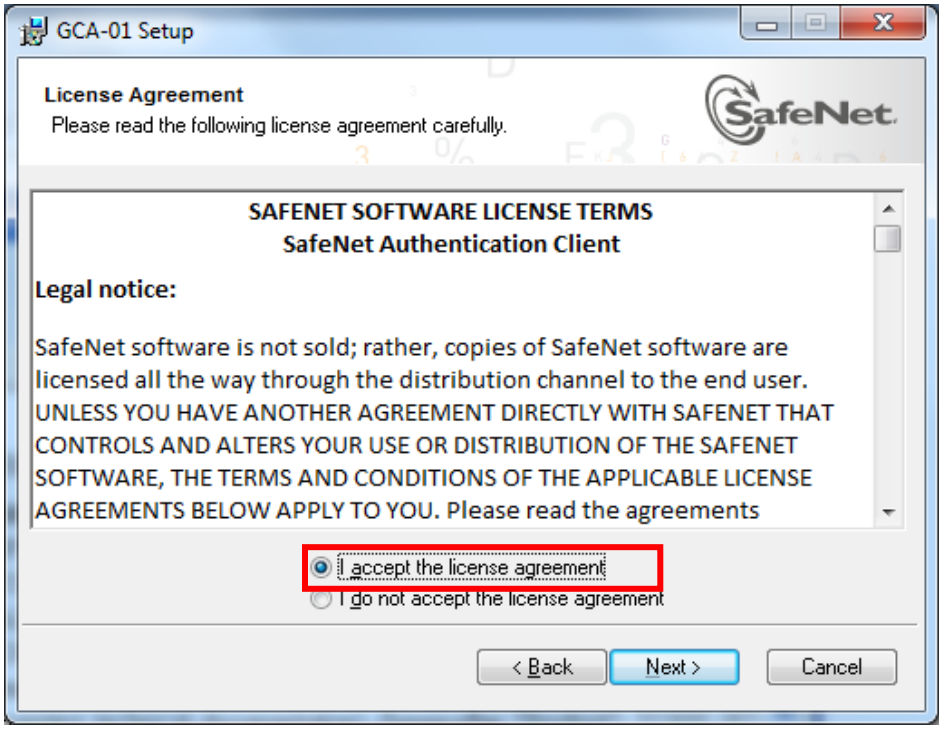
Bước 2: Cài đặt driver USB Token



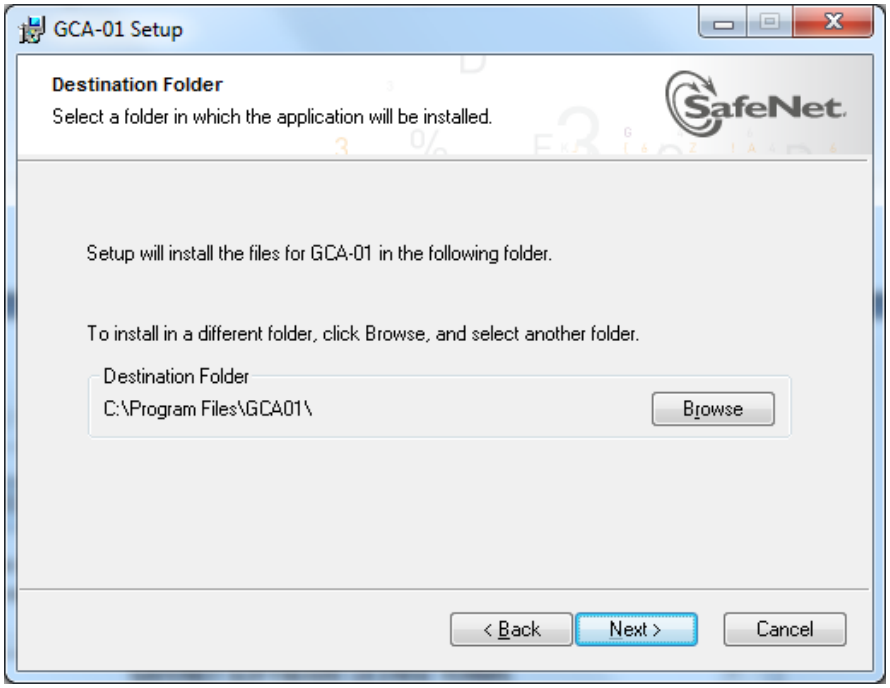
Chọn Next



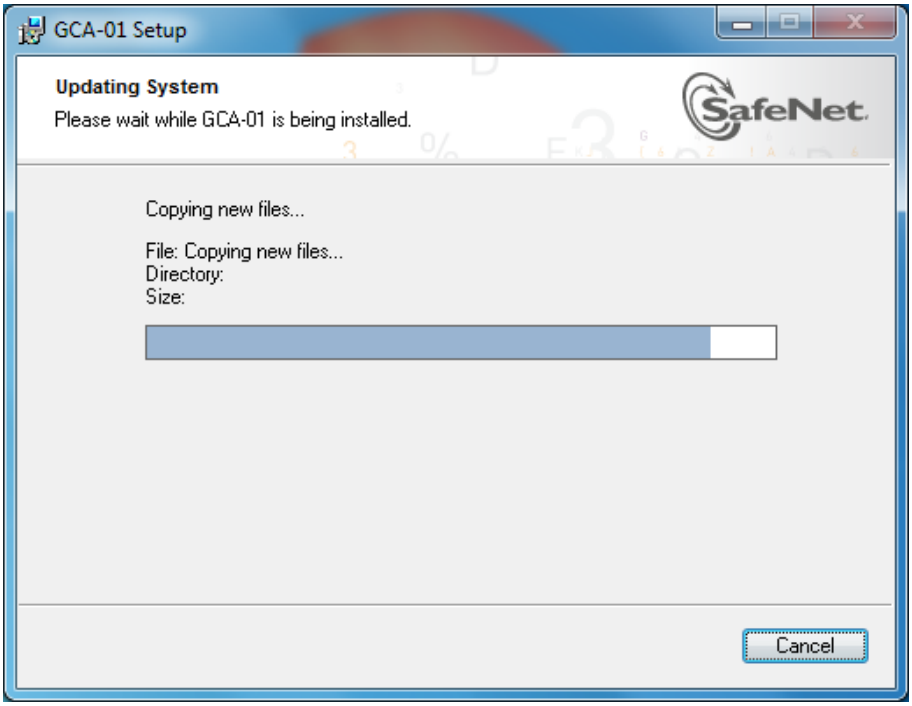
Chọn ngôn nhữ "Vietnamese" và chọn Next



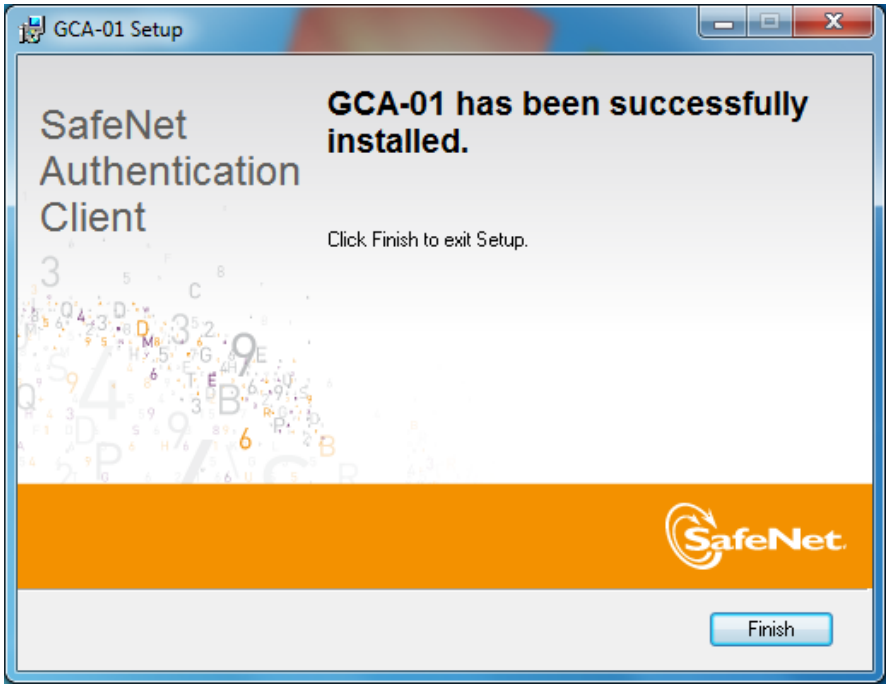
Chọn "I accept the lecense agreement", chọn Next



Chọn Next



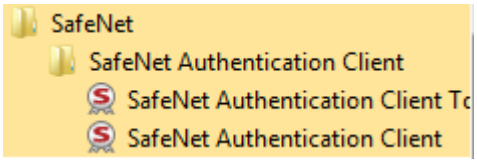
Chọn Next



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

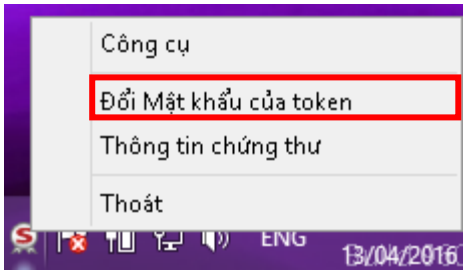
Hoặc vào menu Start → SafeNet → SafeNet Authentication Client



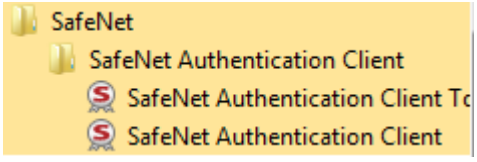
1.2.2.3 Đổi mật khẩu cho thiết bị eToken

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

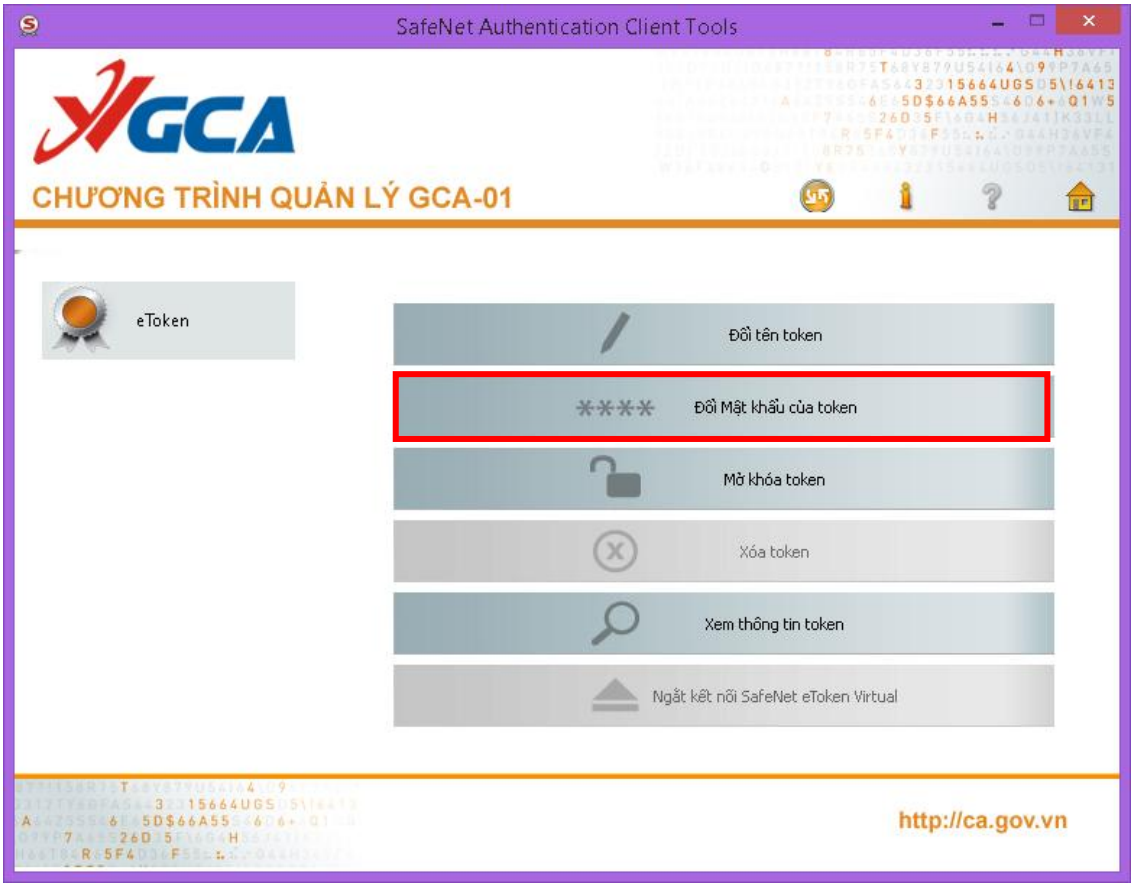
Bước 2: Nhấp chuột phải vào biểu tượng USB Token ở góc phải màn hình và chọn "Đổi Mật khẩu của token".



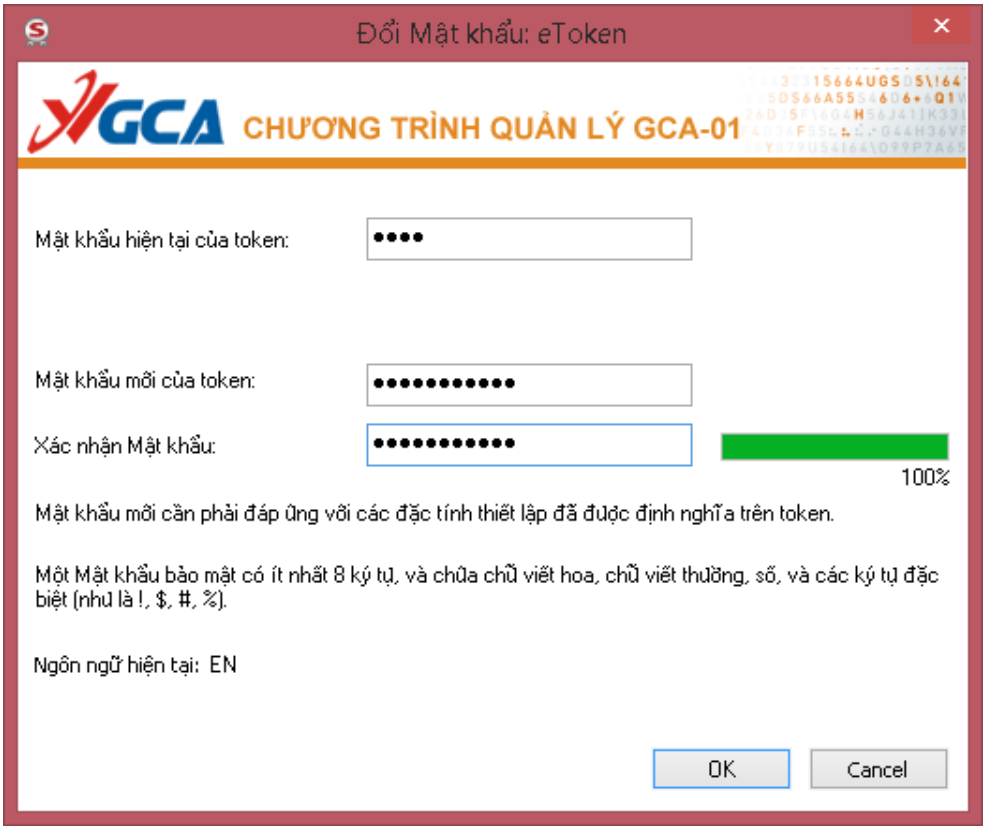
Hoặc vào menu Start → SafeNet → SafeNet Authentication Client → SafeNet Authentication Client Tools



Nhấp chuột trái vào mục "Đổi Mật khẩu của token"

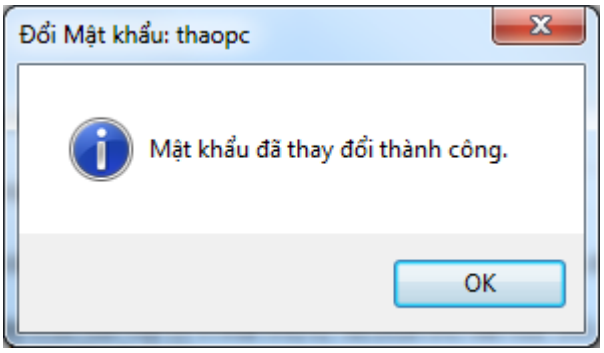


Bước 3: Thay đổi mật khẩu



Nhập mật khẩu hiện tại vào ô “Mật khẩu hiện tại của token”. Nhập mật khẩu mới vào ô “Mật khẩu mới của token” và “Xác nhận Mật khẩu”. Sau khi nhập xong nhấn “Đồng ý” để xác nhận sự thay đổi trên.

Giao diện thông báo thay đổi mật khẩu thành công

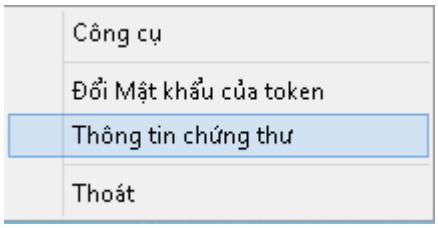


Chú ý:

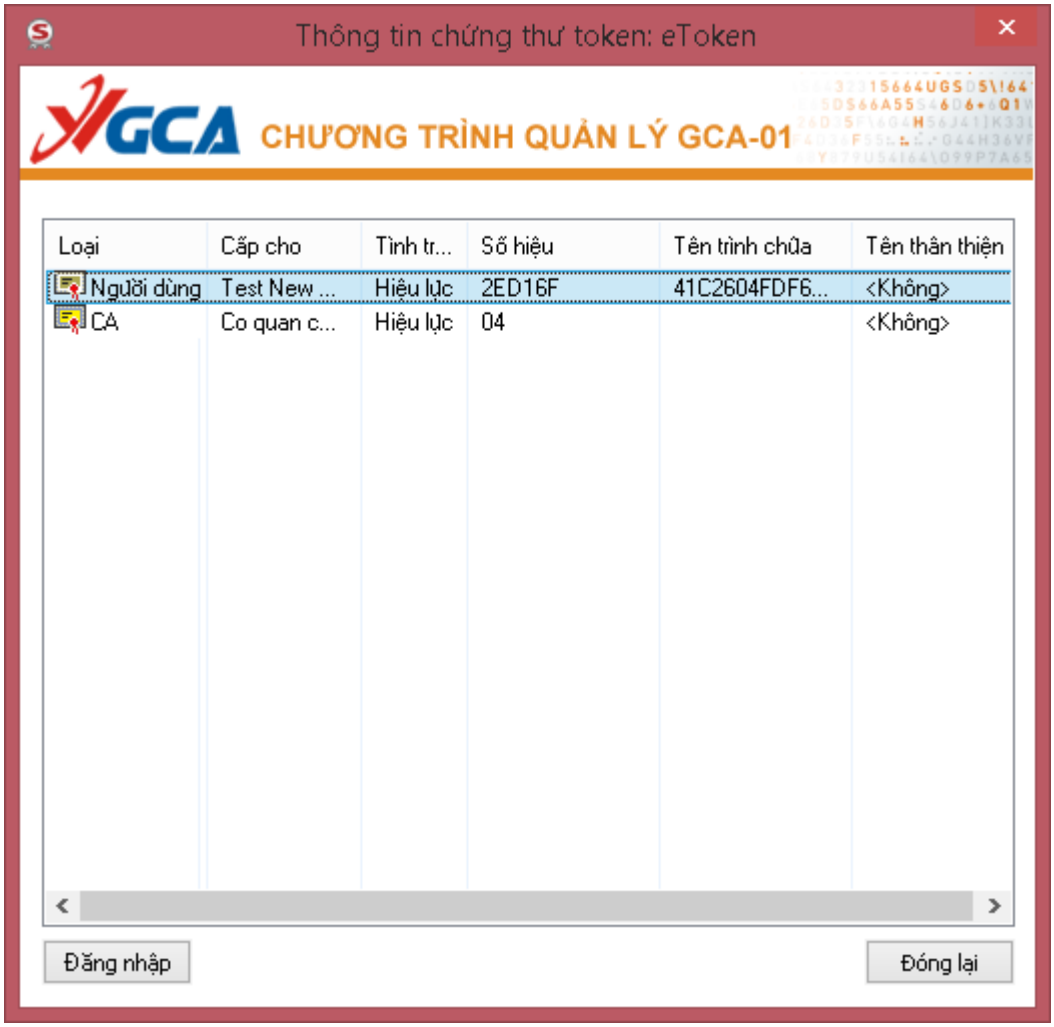
- ***Mật khẩu mới phải có độ dài ít nhất 8 ký tự, phải chứa chữ hoa, chữ thường và số.***
- ***Người sử dụng phải nhớ kỹ mật khẩu của mình.***
- ***Theo mặc định của thiết bị USB Token, người dùng nhập sai mật khẩu liên tiếp quá 15 lần, thì USB Token sẽ tự động khóa và người dùng sẽ không tiếp tục sử 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.***

1.2.2.4 Hướng dẫn xuất (export) chứng thư số từ trong Token

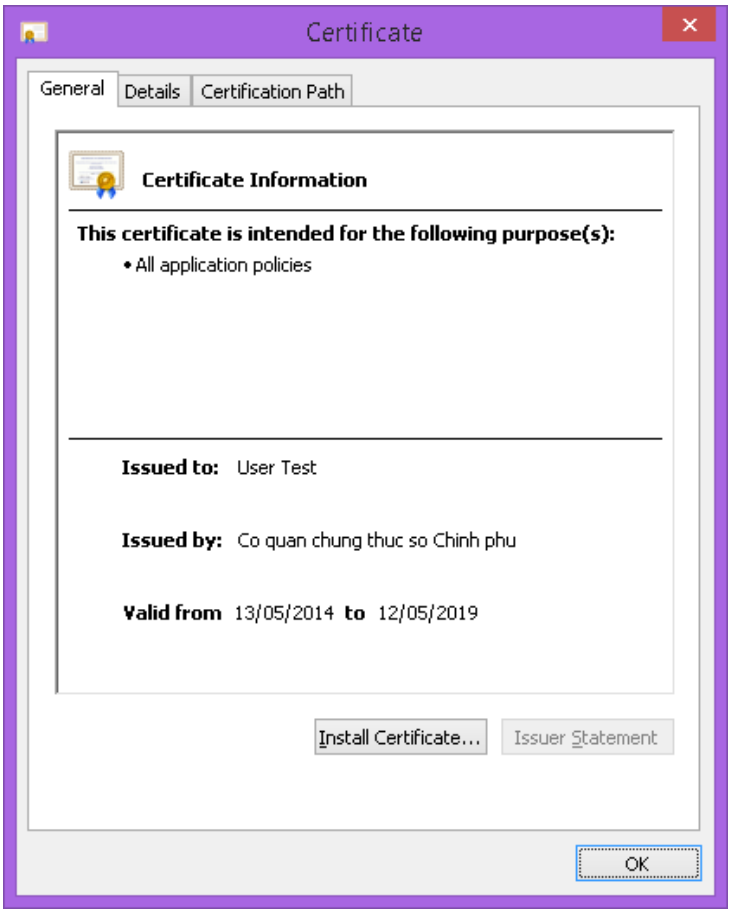
Bước 1: Cắm thiết bị vào máy tình. Bấm chuột phải vào biểu tượng trình điều khiển thiết bị (chữ S màu đỏ) ở "Tray icons" phía góc phải bên dưới màn hình:



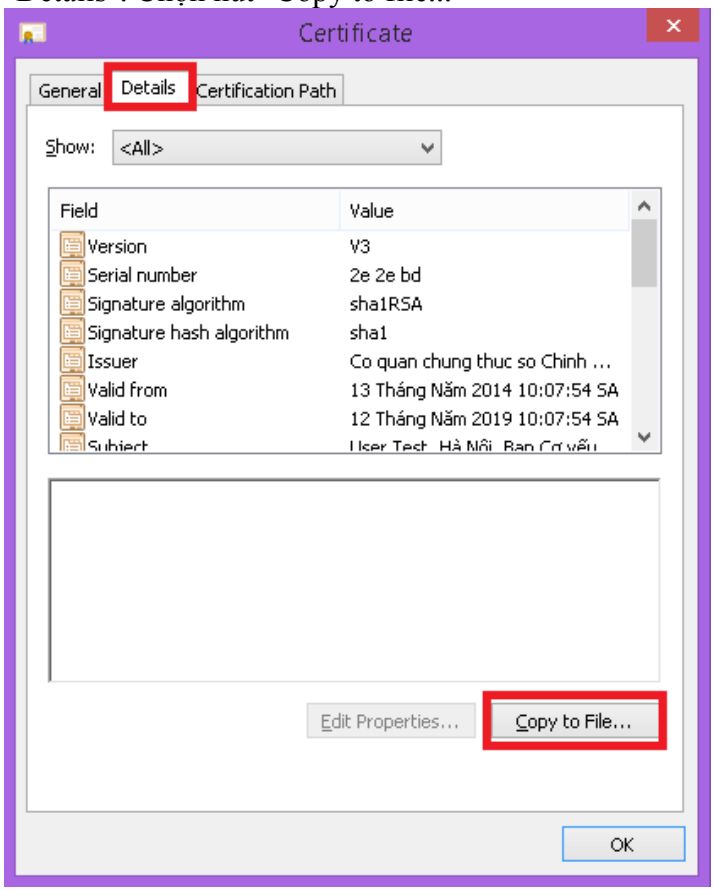
Bước 2: Chọn Menu "Certificate Infomation":



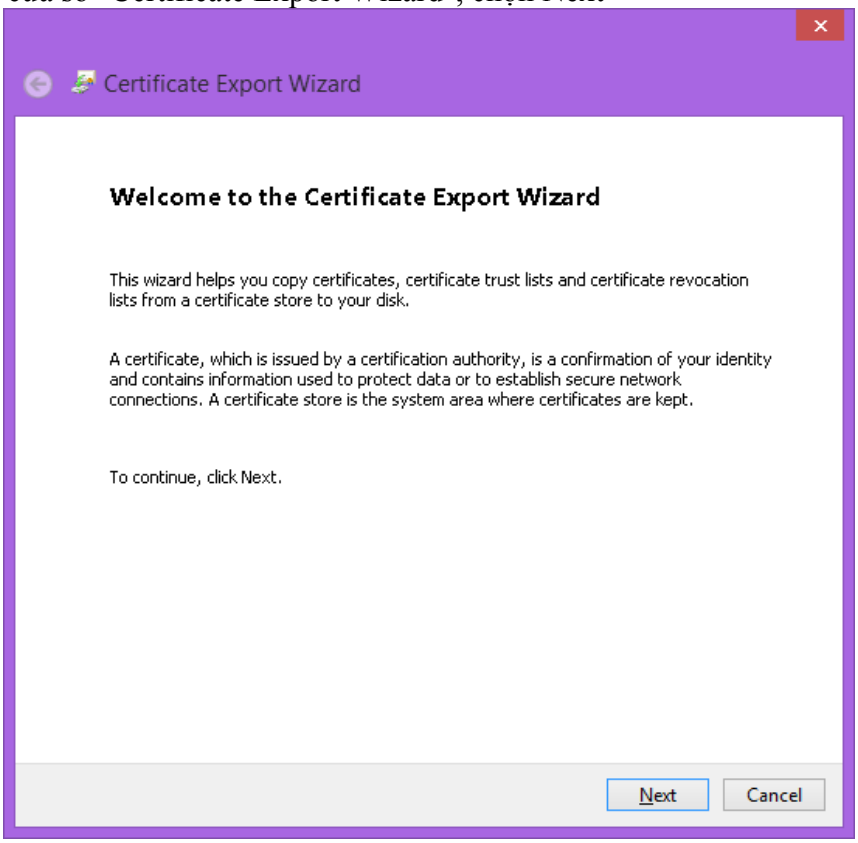
Bước 3: Bấm đúp chuột trái vào chứng thư số muốn xuất ra tệp để mở cửa sổ thông tin chứng thư số.



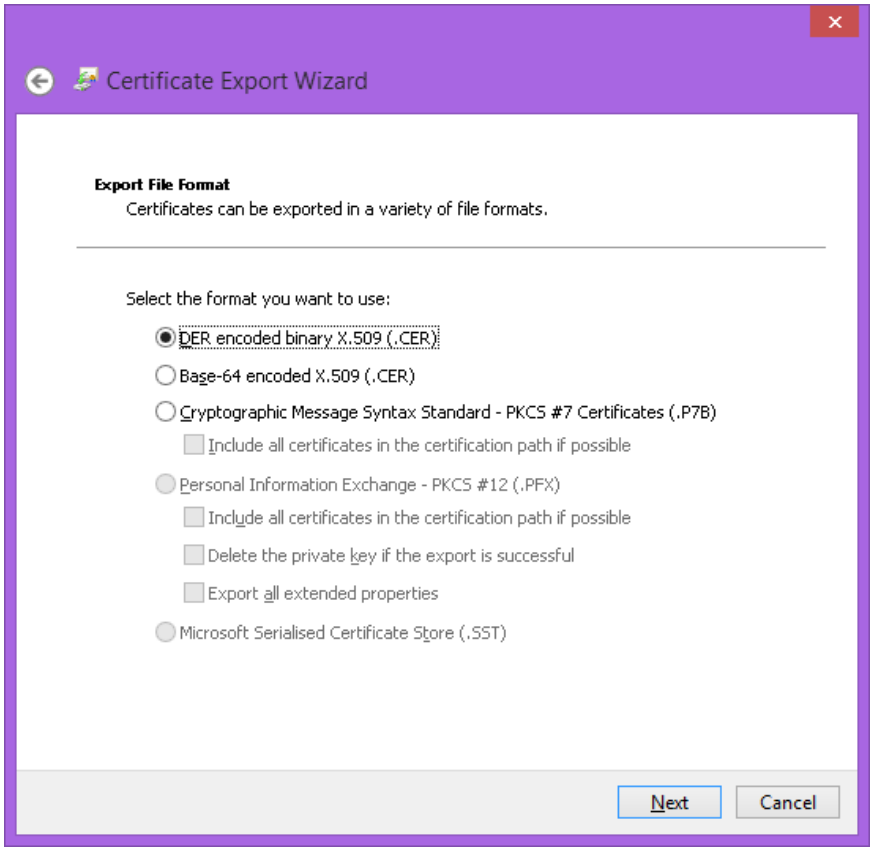
Bước 4: Chọn Tab "Details". Chọn nút "Copy to file..."



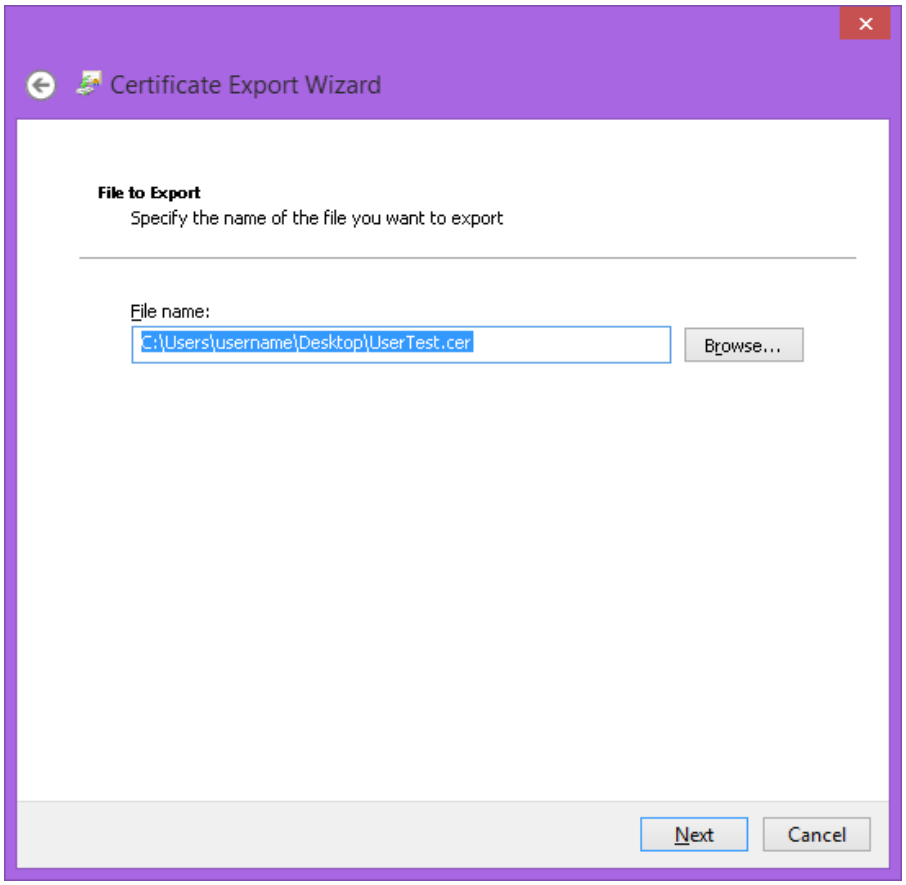
Bước 5: Trên cửa sổ "Certificate Export Wizard", chọn Next



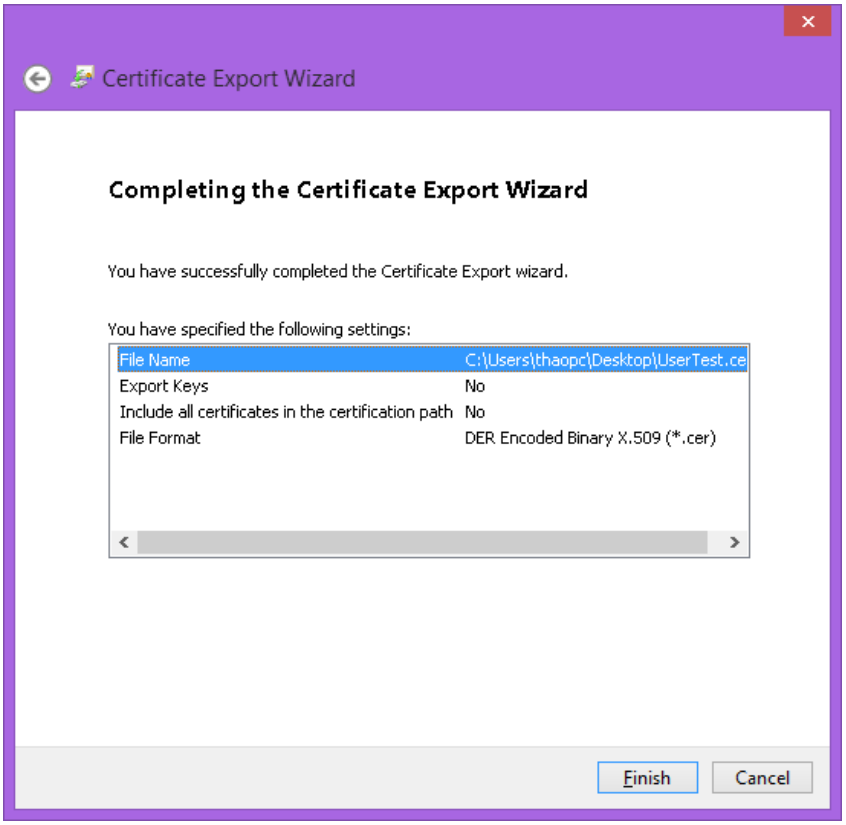
Bước 6: Chọn Export File Format là DER, hoặc Base-64, chọn Next:



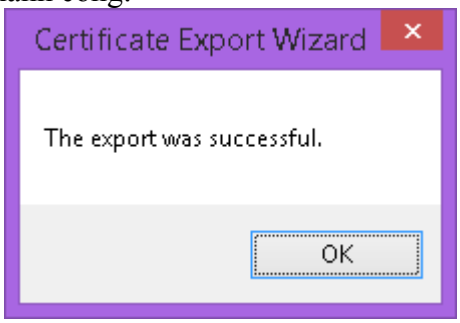
Bước 7: Chọn đường dẫn File to export, chọn Next:



Bước 8: Chọn Finish, trên cửa sổ "Completing the Certificate Export Wizard":



Bước 9: Thông báo Export thành công:

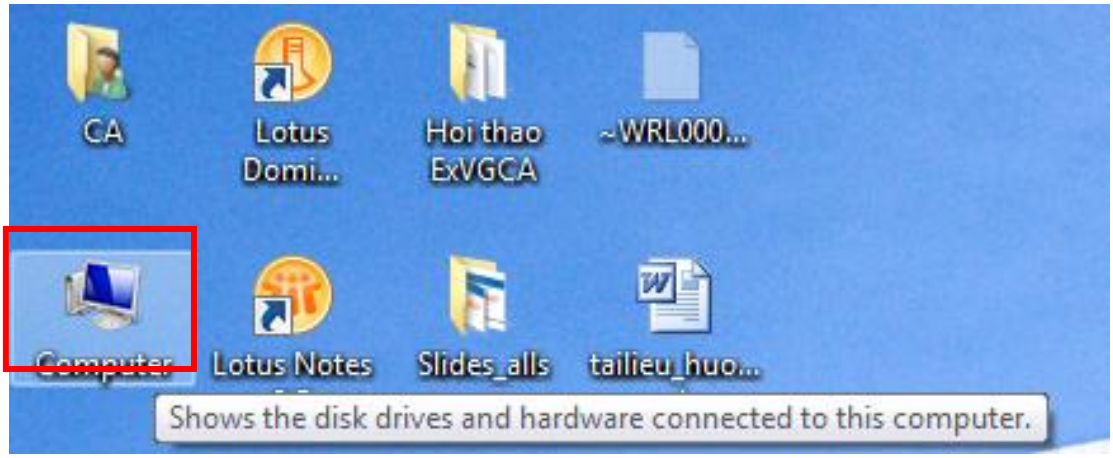


1.2.3 Cài đặt trình điều khiển và thay đổi mật khẩu thiết bị ST3

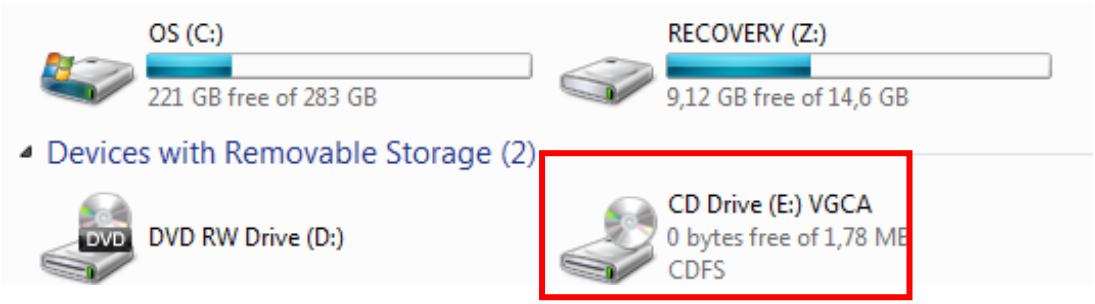
1.2.3.1 Thiết bị ST3

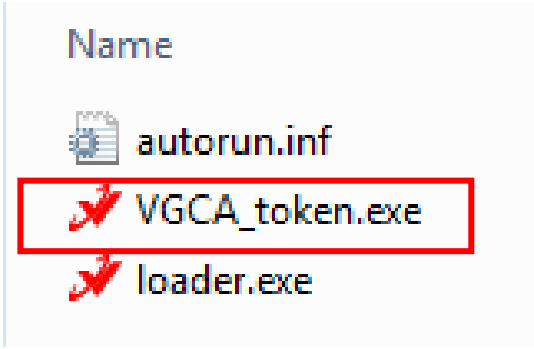
1.2.3.2 Cài đặt trình điều khiển thiết bị ST3

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



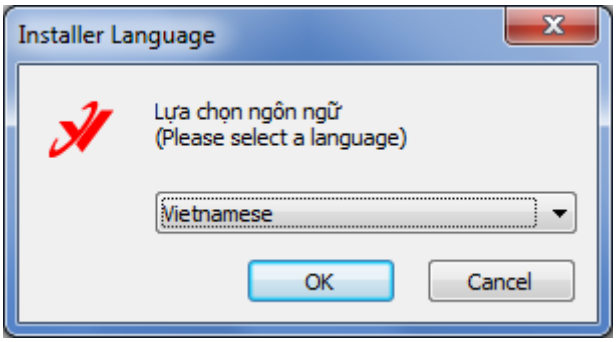
Mở ổ đĩa VGCA:



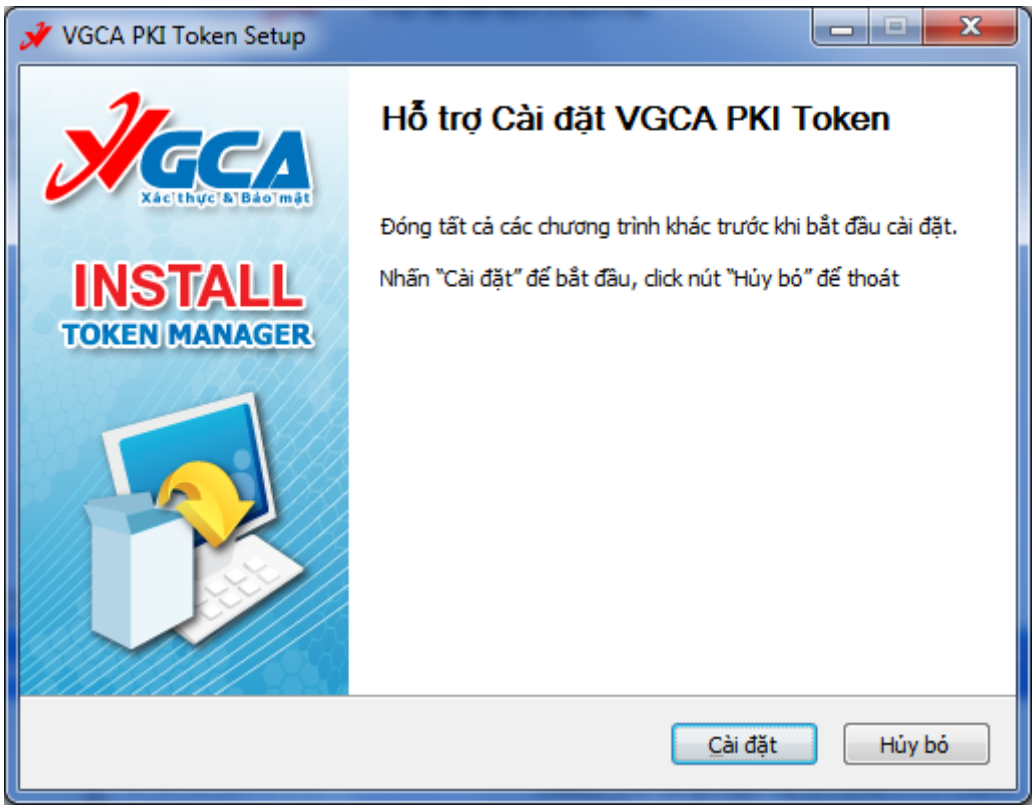


Kích đúp chuột vào tệp VGCA_token.exe để cài đặt.

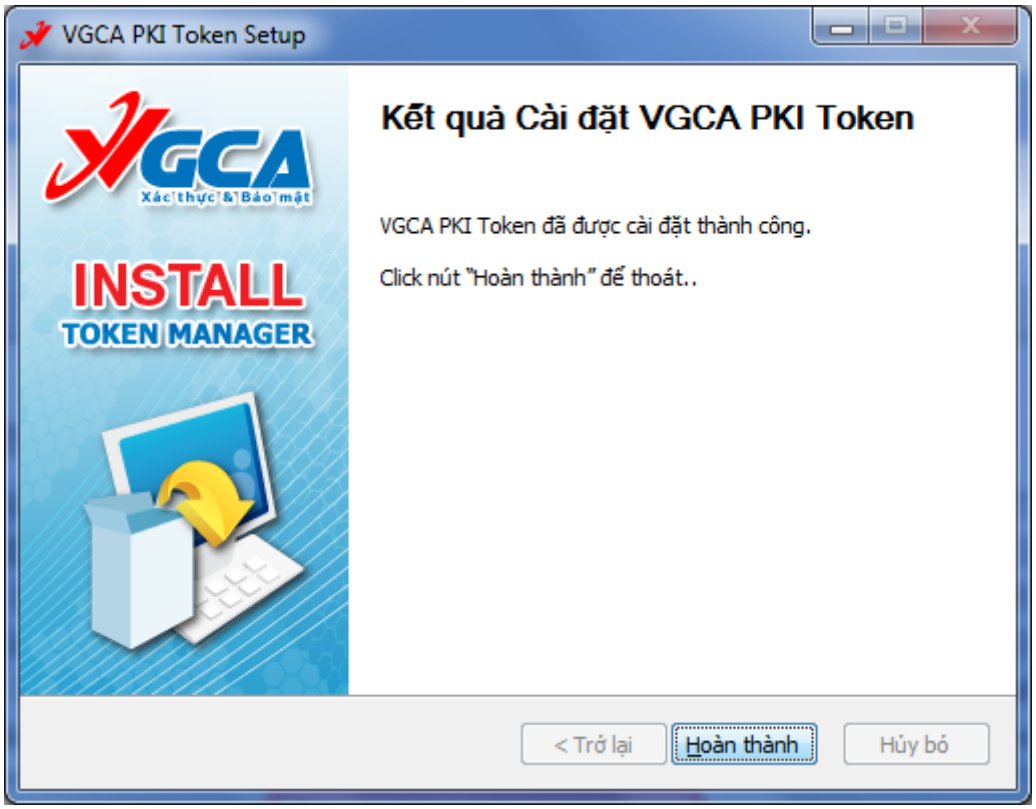
Bước 2: Cài đặt driver USB Token



Chọn OK



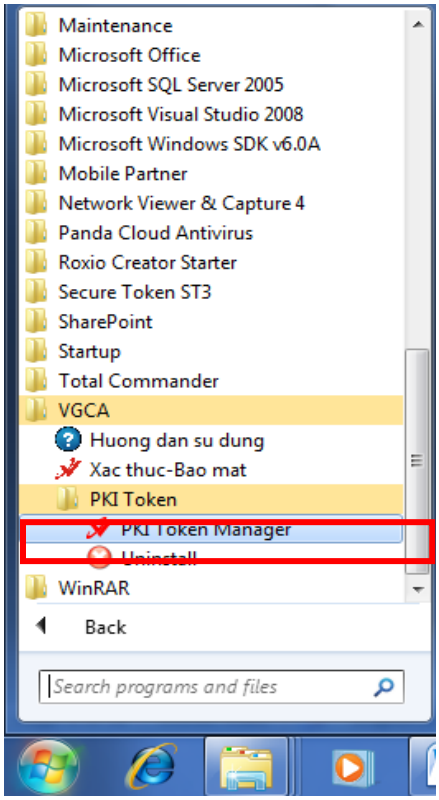
Chọn Cài đặt



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.

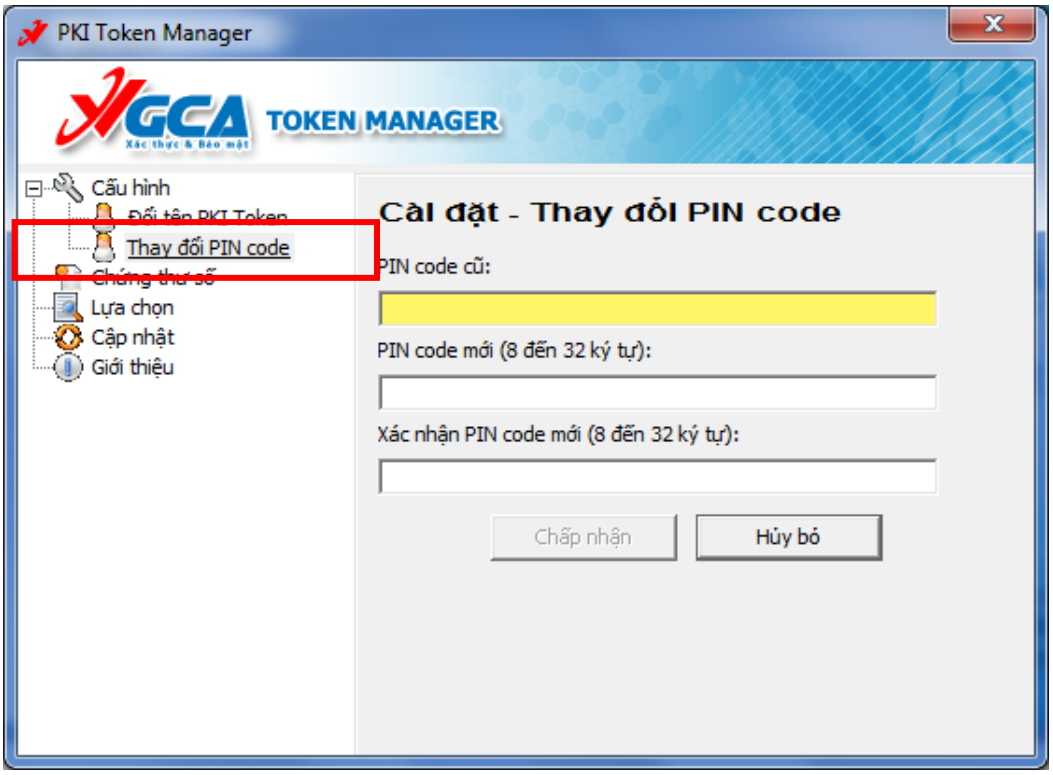
Hoặc vào menu start → VGCA → PKI Token → PKI Token Manager.



Giao diện PKI Token Manager:

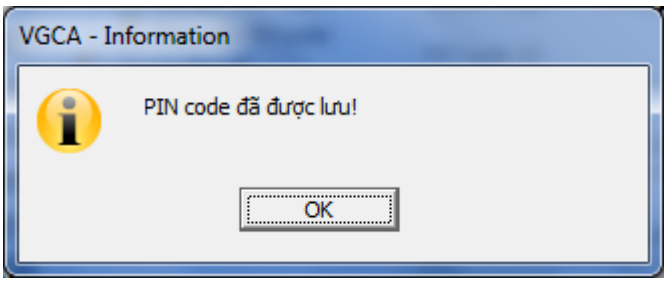
1.2.3.3 Đổi mật khẩu cho thiết bị USB Token ST3

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 ký số và xác thực 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 2.3.
- 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 ký số 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 bằng các thuật toán mật mã an toàn.

vSign đảm bảo toàn bộ các yêu cầu về xác thực 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.

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, PKC#7, ...
- 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 xác thực 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 xác thực 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 xác thực tất cả các định dạng tệp dữ liệu trên môi trường Windows.
- vSign - Mail có thể ký số và xác thực 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.

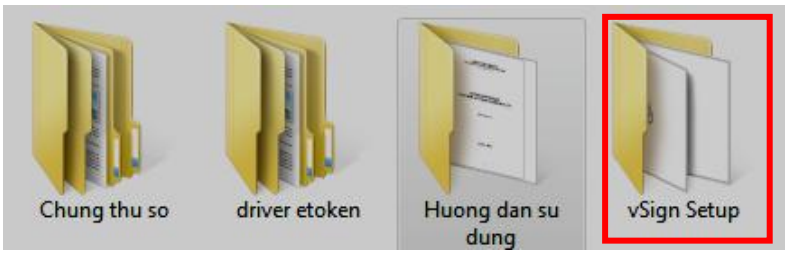
2.1.3 Các chuẩn đáp ứng

- 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.

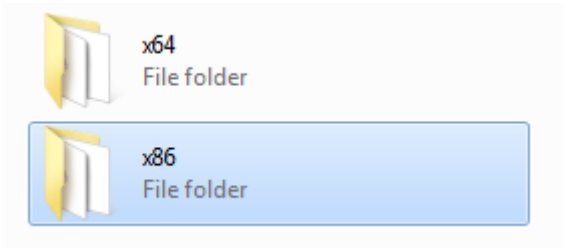
- Chuẩn khuôn dạng chữ ký số PKCS#7 (CMS – Cryptography Message Syntax).
- Chuẩn gắn dấu thời gian theo giao thức TSP RFC3161 Time-Stamp Protocol (TSP).
- Chuẩn ký số tài liệu PDF theo ISO 32000-12.

2.2 Cài đặt phần mềm vSign2.3

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

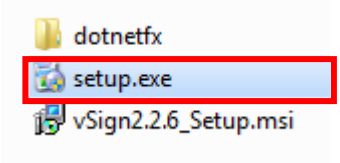


Bước 2: Chọn bộ cài x86 (cho 32-bit) hoặc x64 (cho 64-bit) phù hợp với hệ điều hành đang sử dụng.



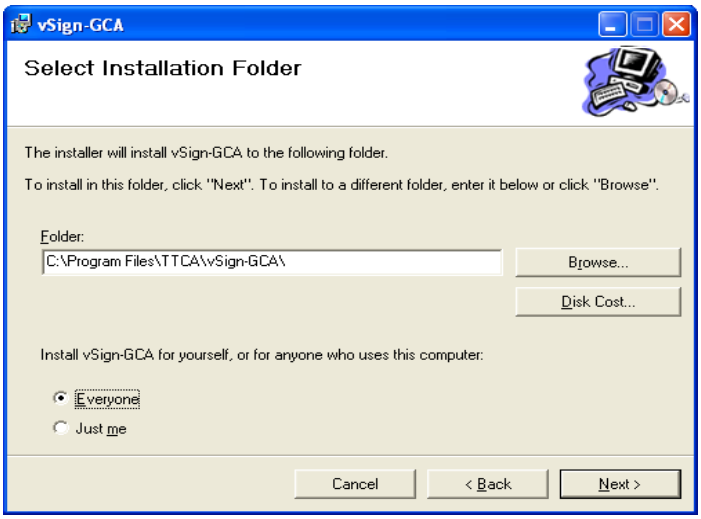
Bước 3: Cài đặt chương trình vSign Setup

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

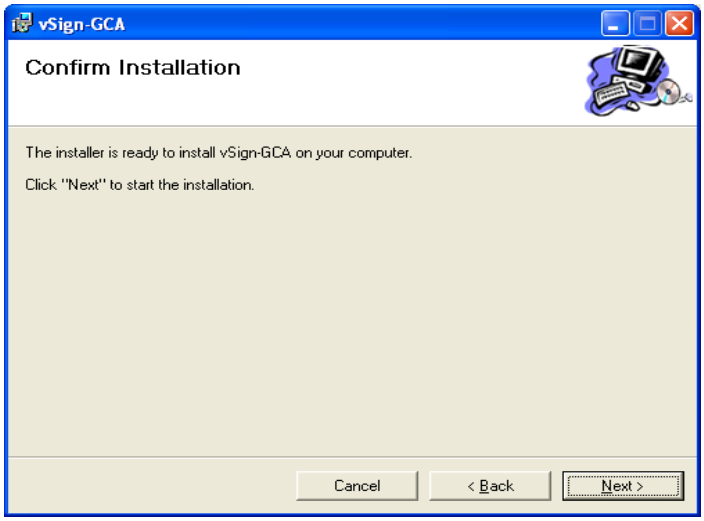


- Giao diện cài đặt

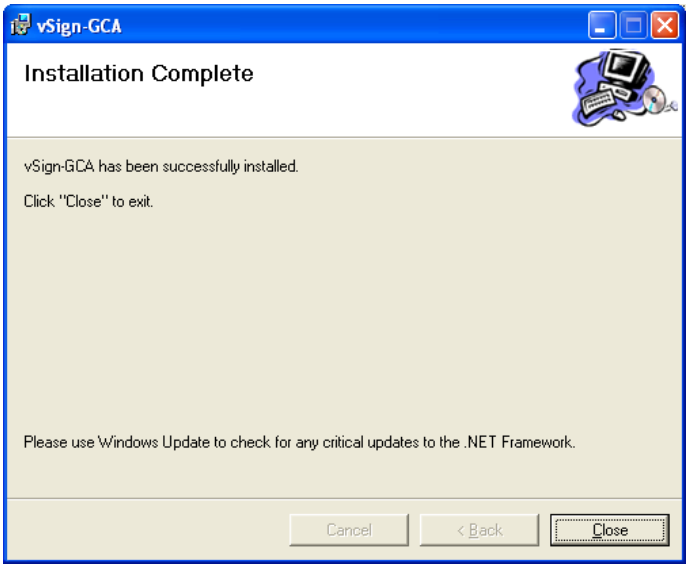
- Chọn Next



- Chọn **Next**



- Chọn **Next**



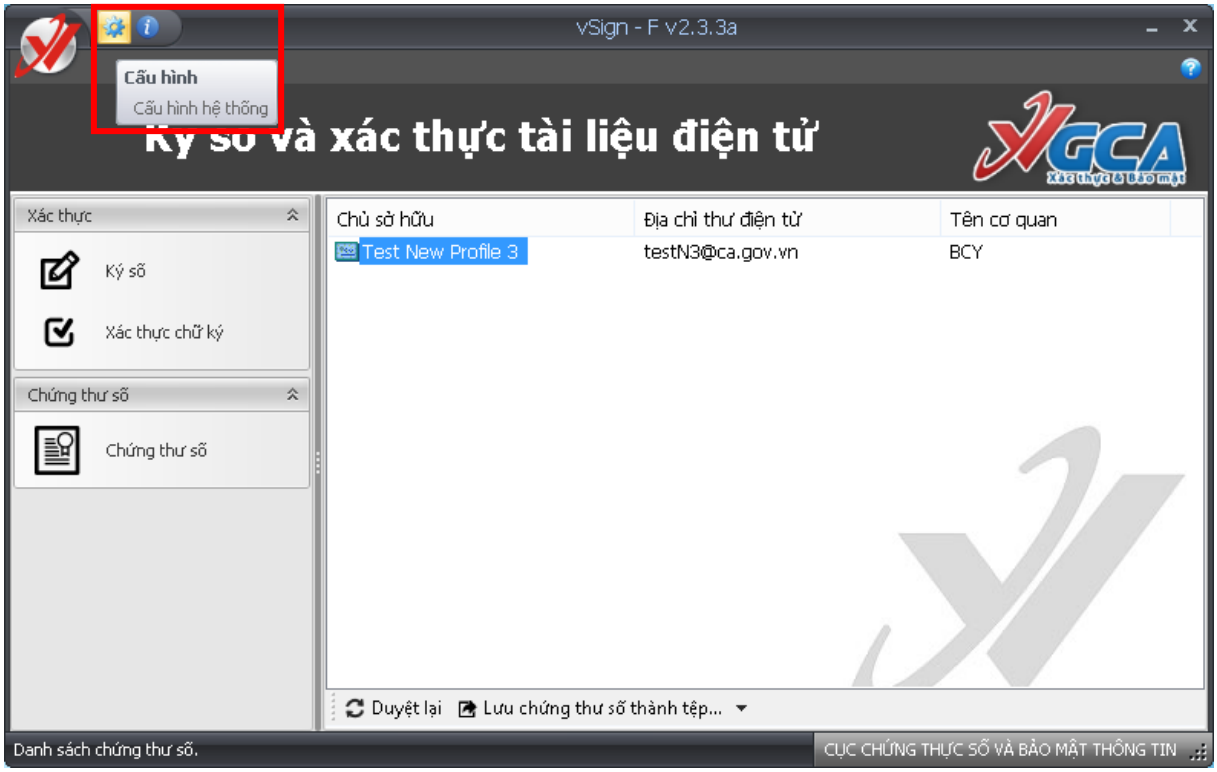
Chọn **Close** để kết thúc quá trình cài đặt.

2.3 Cấu hình cho phần mềm vSign2.3

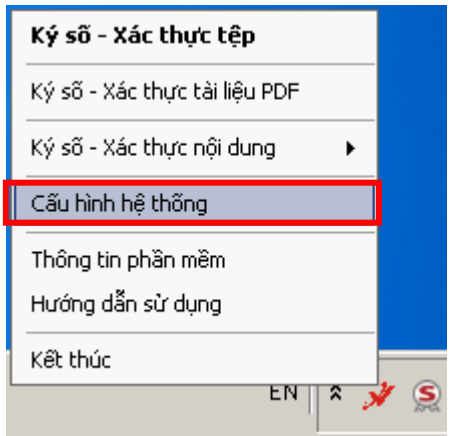
Chức năng cấu hình hệ thống giúp người sử dụng có thể sử các dịch vụ chứng thực chữ ký số khi ký số dữ liệu và xác thực chữ ký số.

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

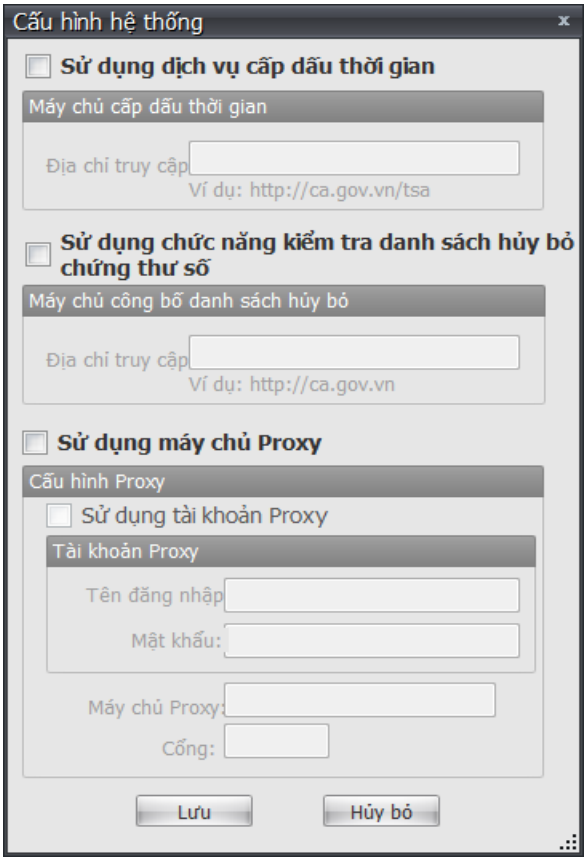
Cách 1: Từ giao diện chính click vào chức năng cấu hình.



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

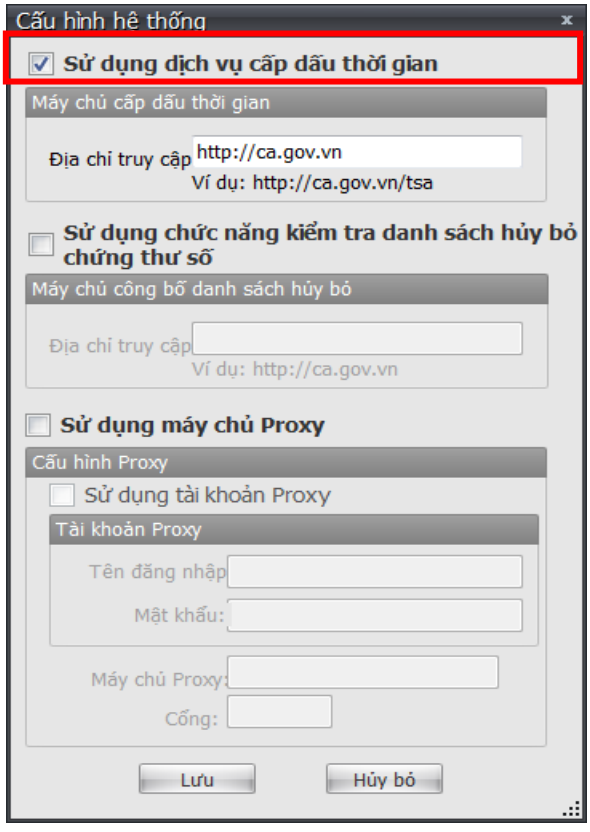


Thực hiện một trong hai cách trên giao diện cài đặt sẽ như sau:



2.3.1 Cấu hình tự động gắn dấu thời gian

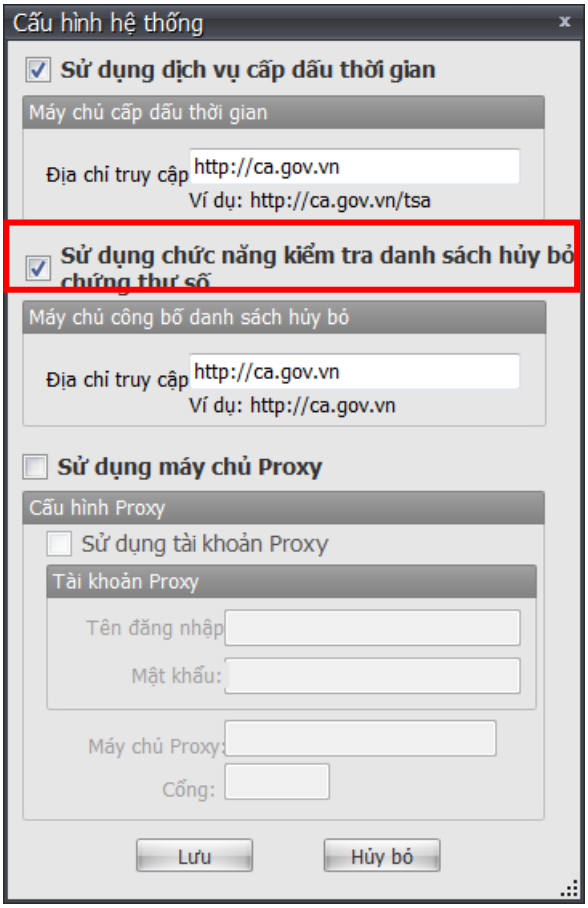
Đánh dấu vào mục "Sử dụng dịch vụ tem thời gian" để cấu hình cho phép hệ thống tự động gắn dấu thời gian vào văn bản ký số.



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

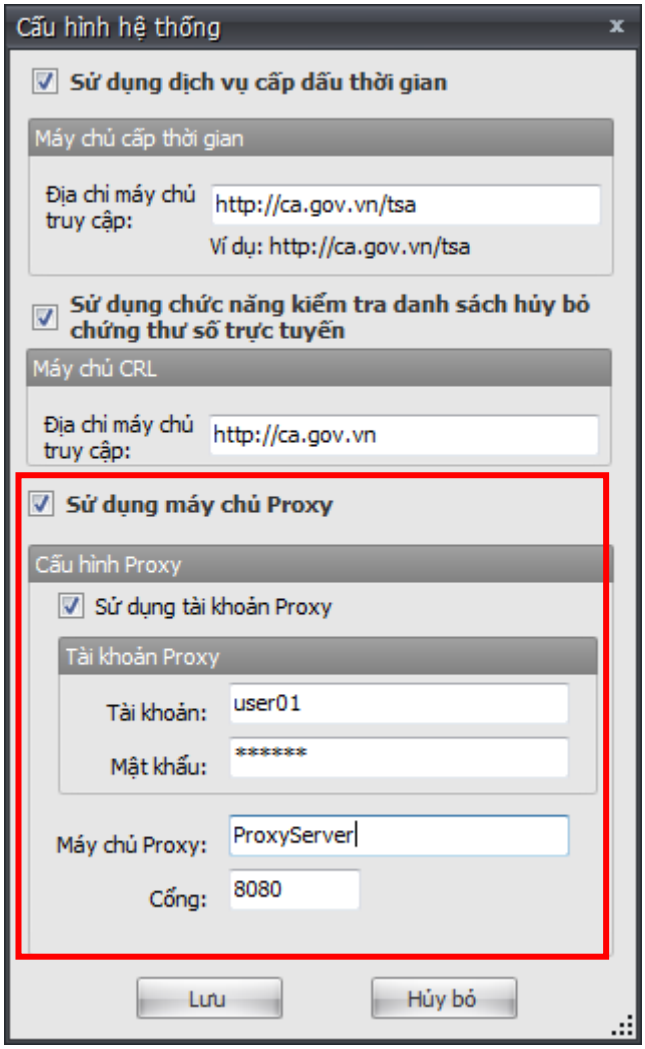
Đánh dấu vào mục "Sử dụng kiểm tra danh sách hủy bỏ chứng thư số" để cấu hình cho phép hệ thống tự động truy cập danh sách hủy bỏ chứng thư số xác định tình trạng chứng thư số.



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

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. Nếu có thiết lập tài khoản để đăng nhập Proxy thì nhập tài khoản và mật khẩu cho tài khoản.

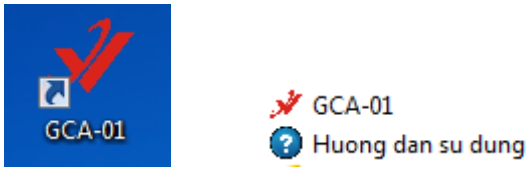


Chú ý: với Proxy ISA người quản trị hệ thống cần cài đặt thêm một số phương thức xác thực kiểu Basic để chương trình hoạt động đúng.

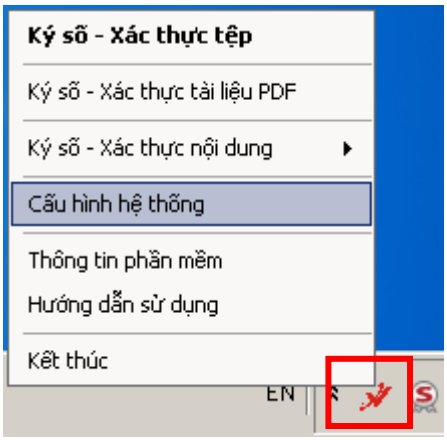
2.4 Hướng dẫn sử phần mềm vSign2.3 để ký số và xác thực tài liệu điện tử

2.4.1 Khởi động chương trình ký số và xác thực tệp

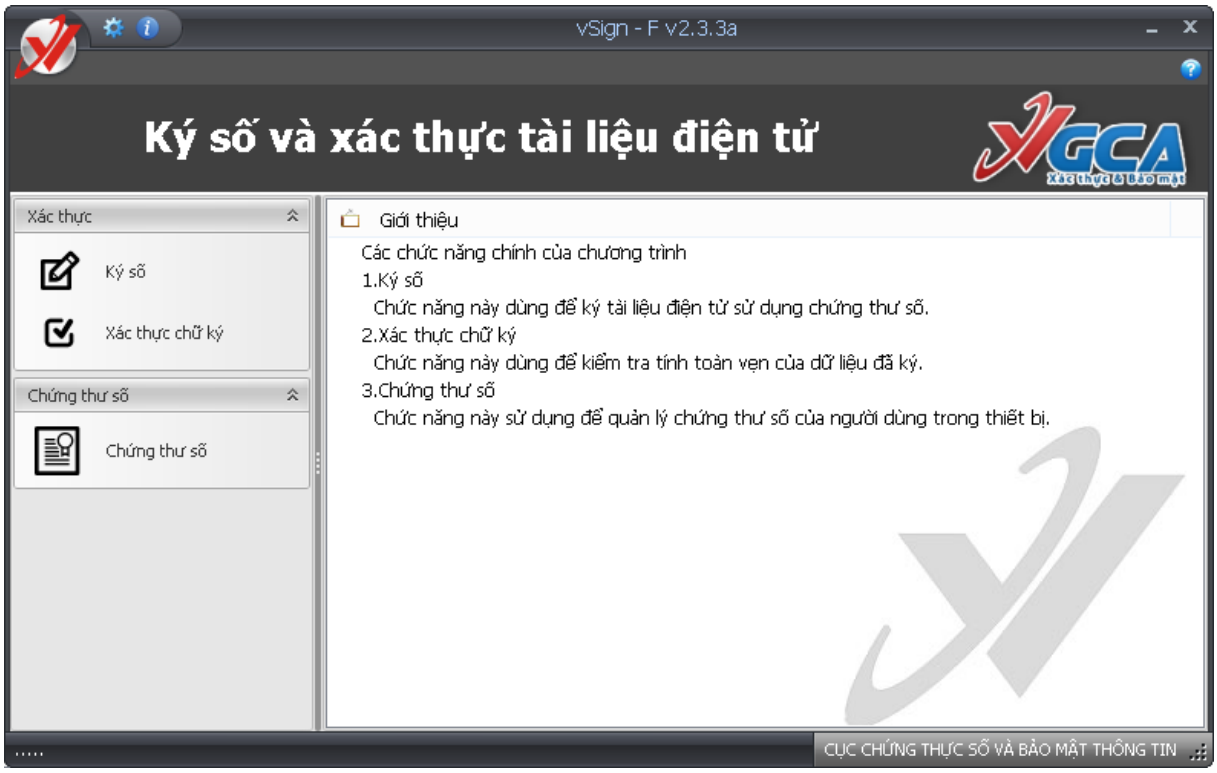
Để khởi động phần mềm kích đúp vào biểu tượng chữ "V" màu đỏ trên màn hình, hoặc chọn Start → Programs → GCA-01.



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.



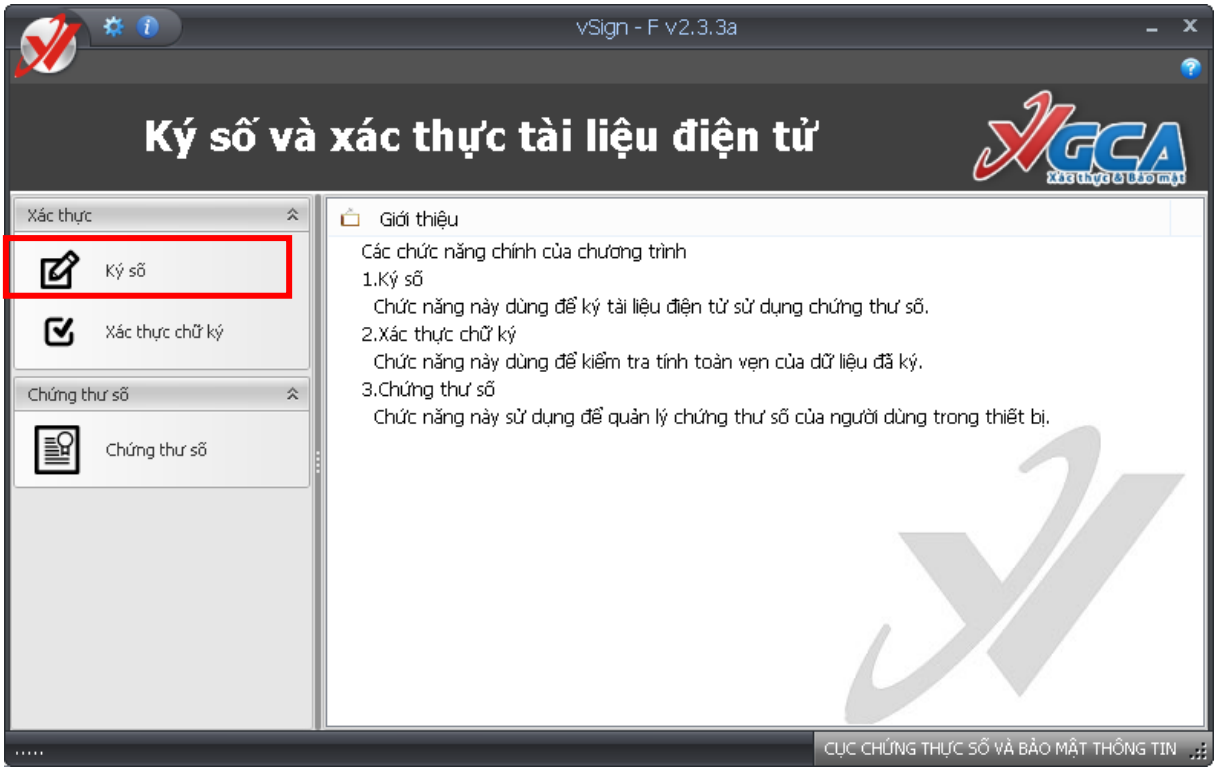
2.4.2 Các chức năng chính của ký số và xác thực tệp

2.4.2.1 Ký số tệp dữ liệu

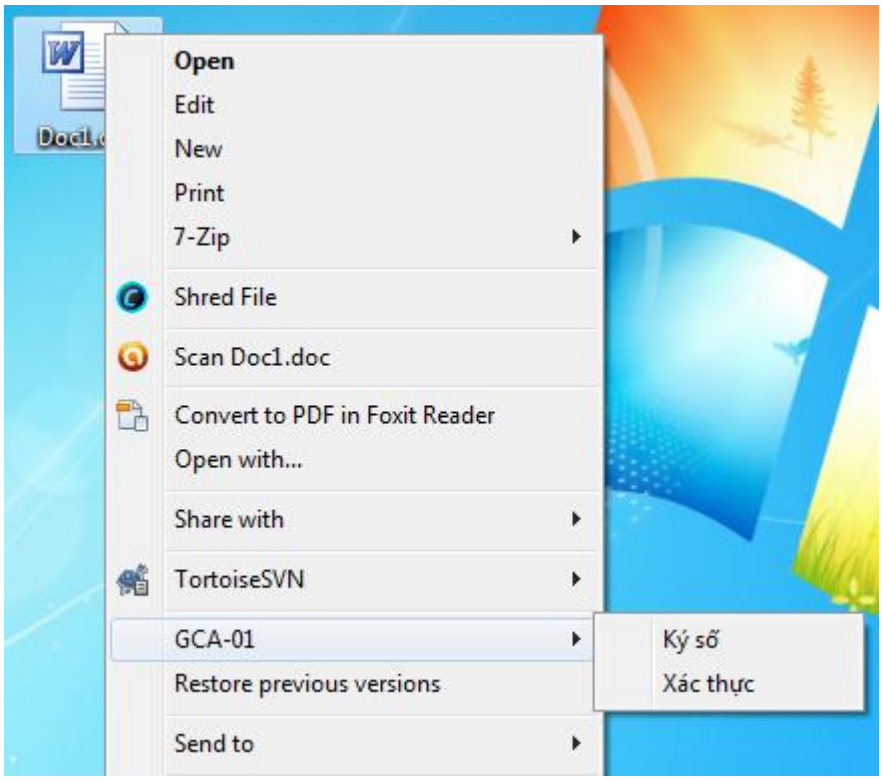
Có 2 cách để ký số tệp dữ liệu bao gồm: sử dụng chức năng "Ký số " trong giao diện chính của chương trình, hoặc từ thực đơn ngữ cảnh của Windows nhấp chuột phải vào tệp chuẩn bị ký số sau đó chọn "GCA-01" -> "Ký số".

Bước 1: chọn cách ký số tệp dữ liệu.

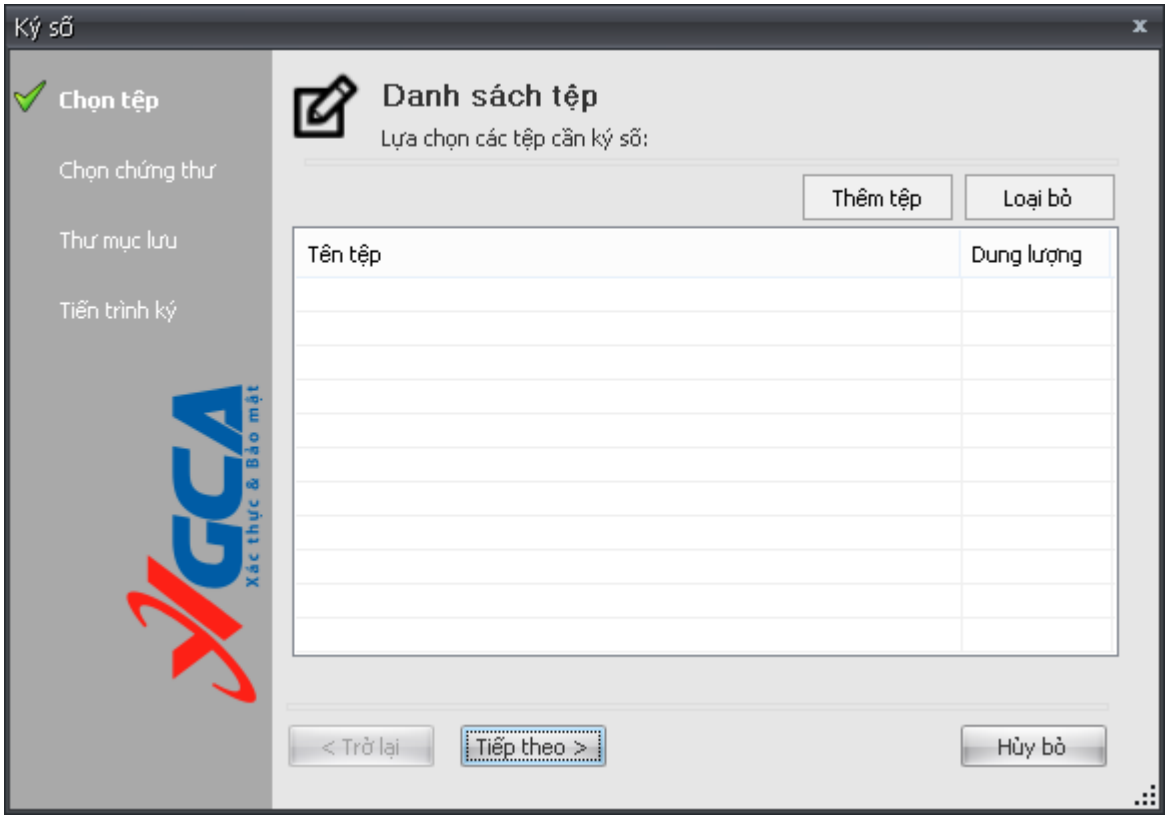
Cách 1 : ký số trong giao diện chính của chương trình.



Cách 2 : Ký từ thực đơn chuột phải.



Giao diện ký hiển thị như sau :

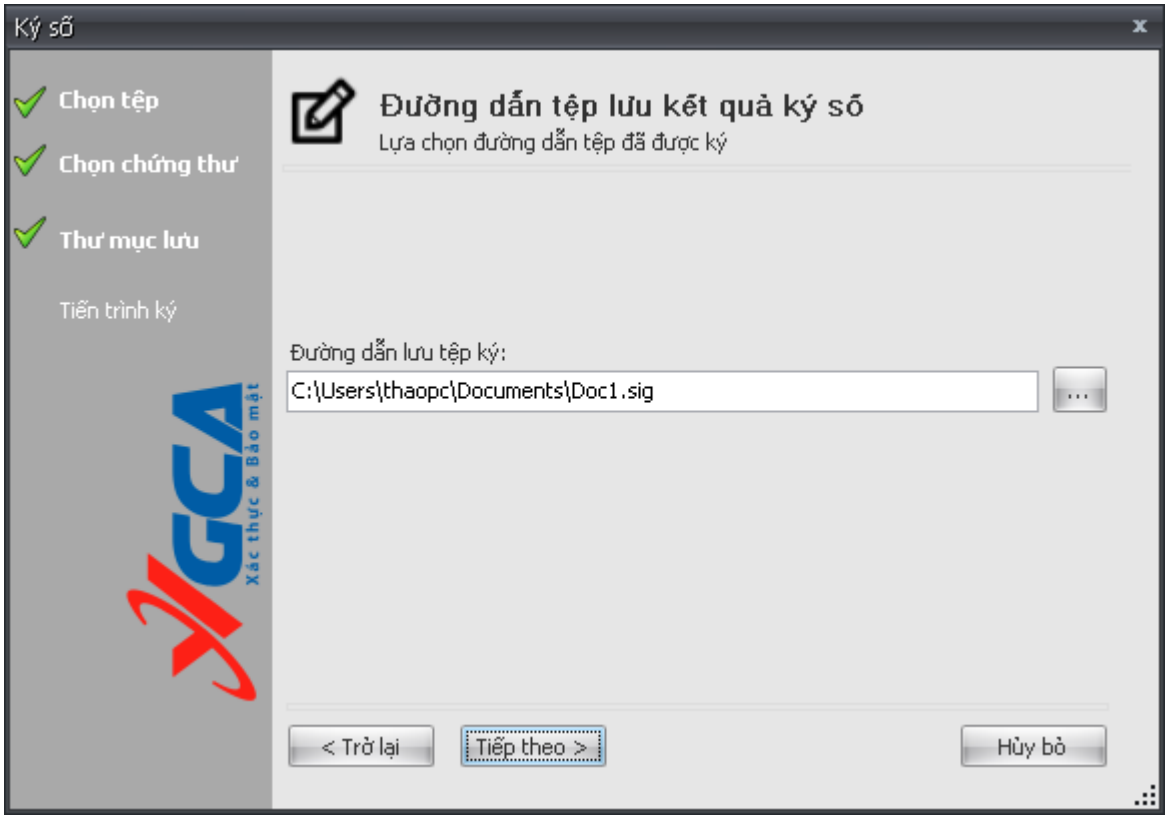


Bước 2: Thêm tệp, xóa tệp vào danh sách.

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.

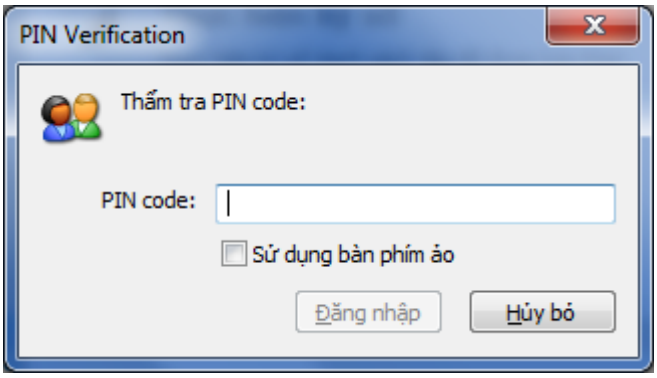


Nhấp "Tiếp theo" để tiến trình ký số được tiếp tục.

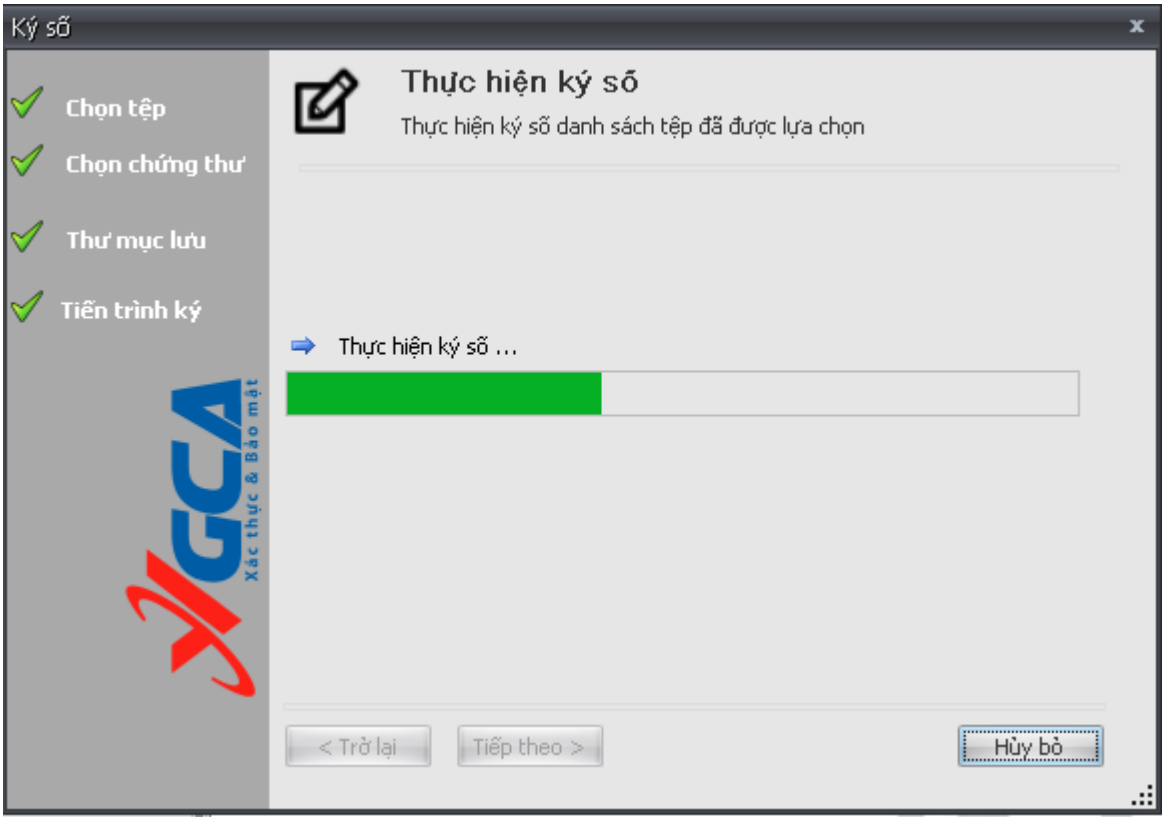
Bước 4: Nhập mật khẩu đăng nhập thiết bị USB Token:

- eToken:

- ST3:

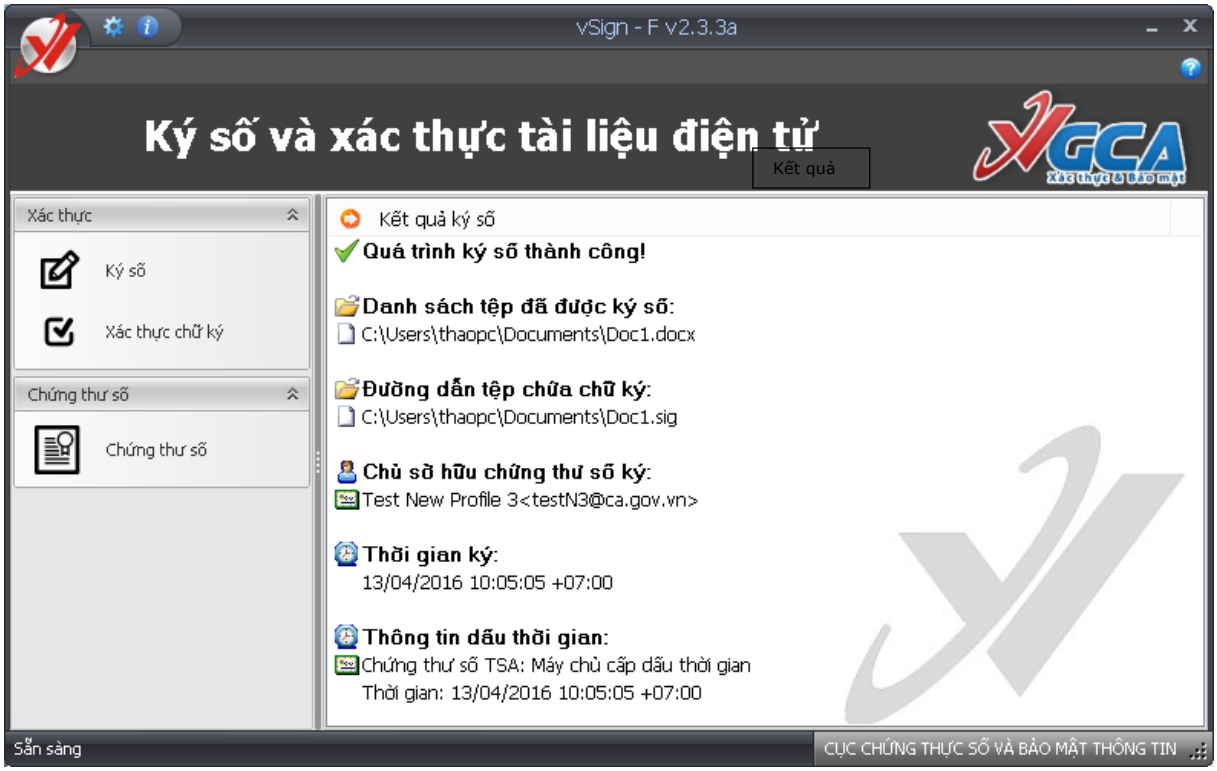


Nhập mật khẩu truy cập USB Token.

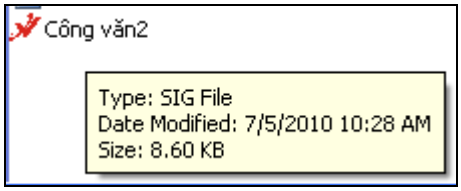


Thực hiện tác vụ ký số. Chờ trong giây lát và xem bảng tổng kết quá trình ký số tệp dữ liệu.

Bước 5: 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".



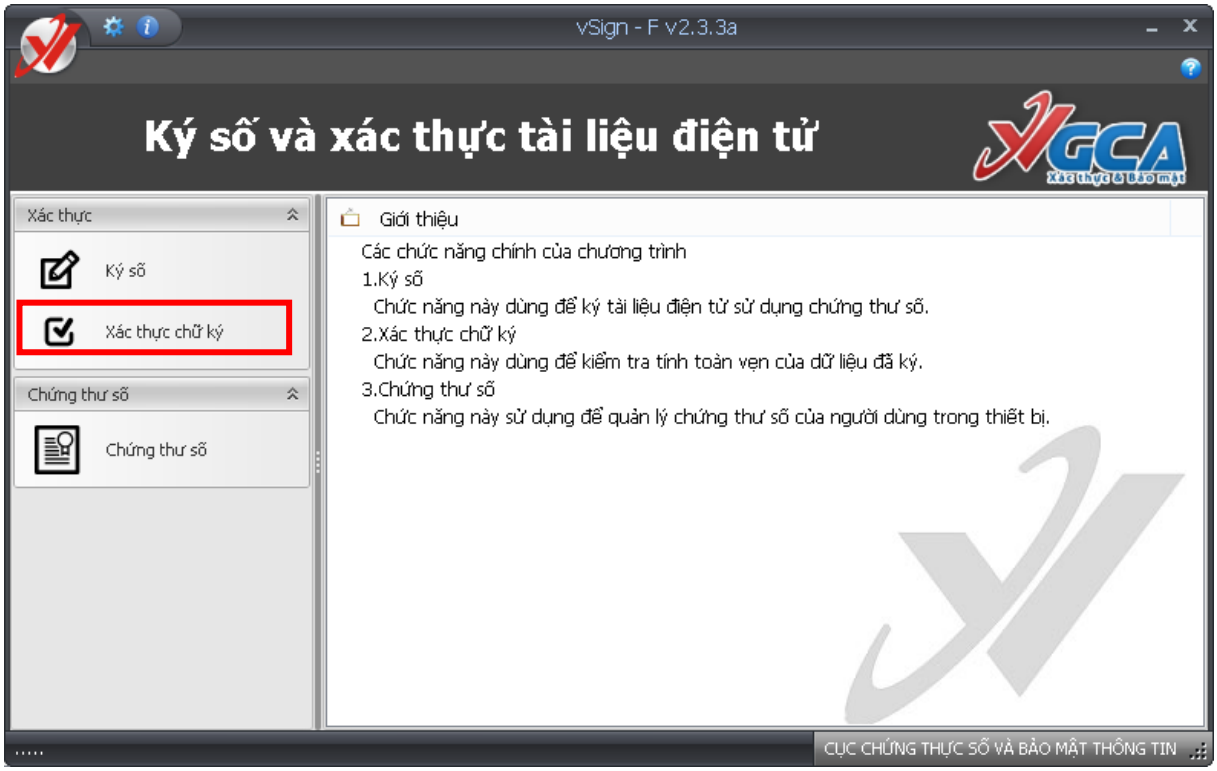
Tệp ký đầu ra có đuôi là ".sig" và có biểu tượng chữ "V" màu đỏ.

2.4.2.2 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 "GCA-01" -> "Xác thực", kích đúp vào tệp cần xác thực(tệp có phần mở rộng là sig).

Bước 1: chọn cách xác thực chữ ký.

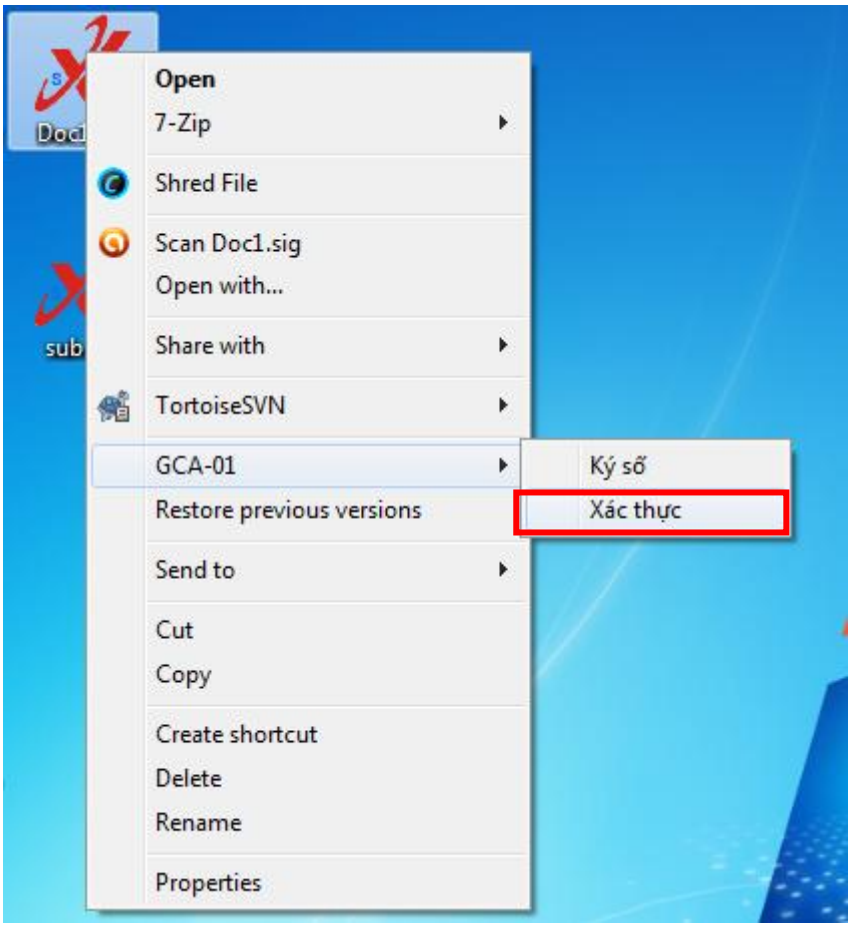
Cách 1: từ giao diện chính của chương trình.



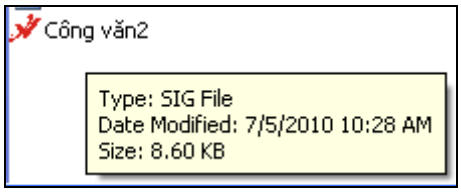
Chọn tệp cần xác thực chữ ký.

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.

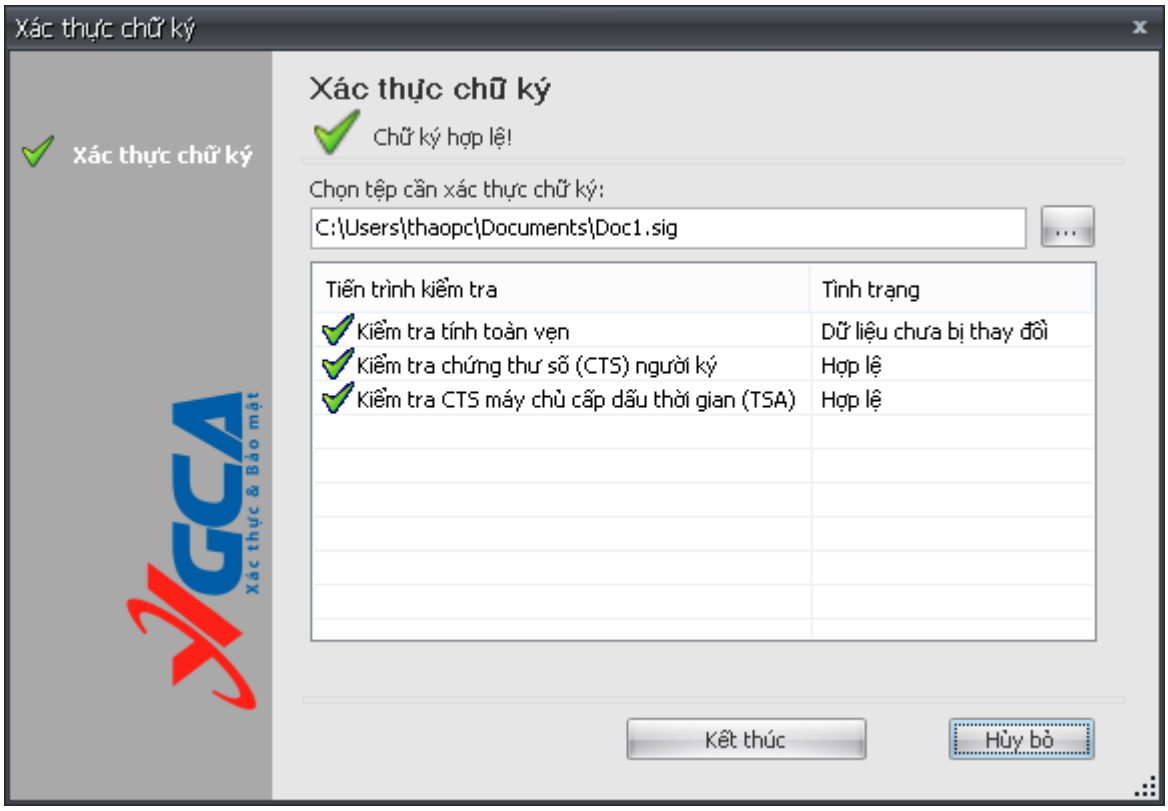


Cách 3: kích đúp vào tệp cần cần xác thực chữ ký.



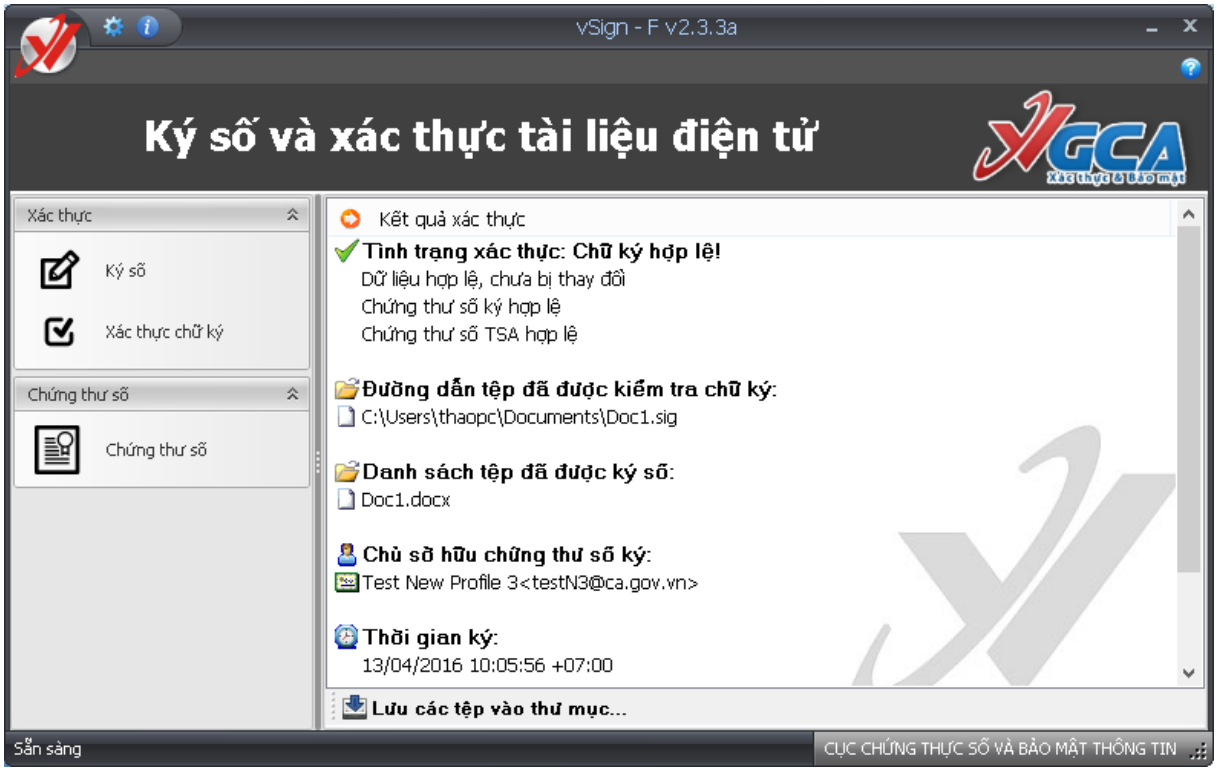
Bước 2: Xác thực chữ ký.

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



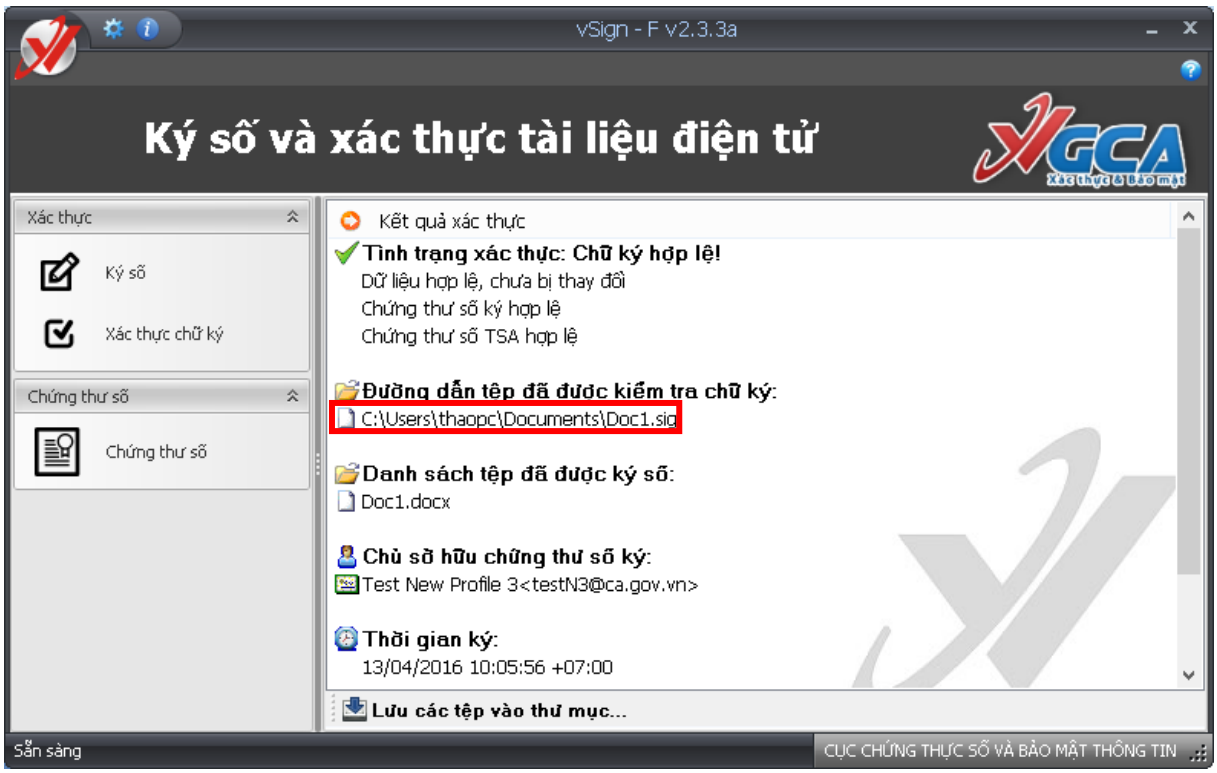
Nhấp "Kết thúc" để xem tổng kết quá trình xác thực.

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

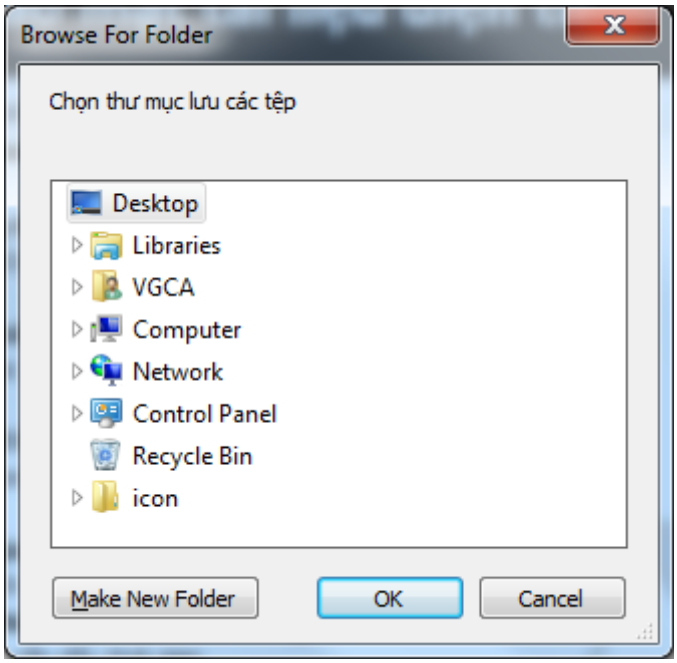


Bước 4: Xem và lưu tệp đã xác thực.

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



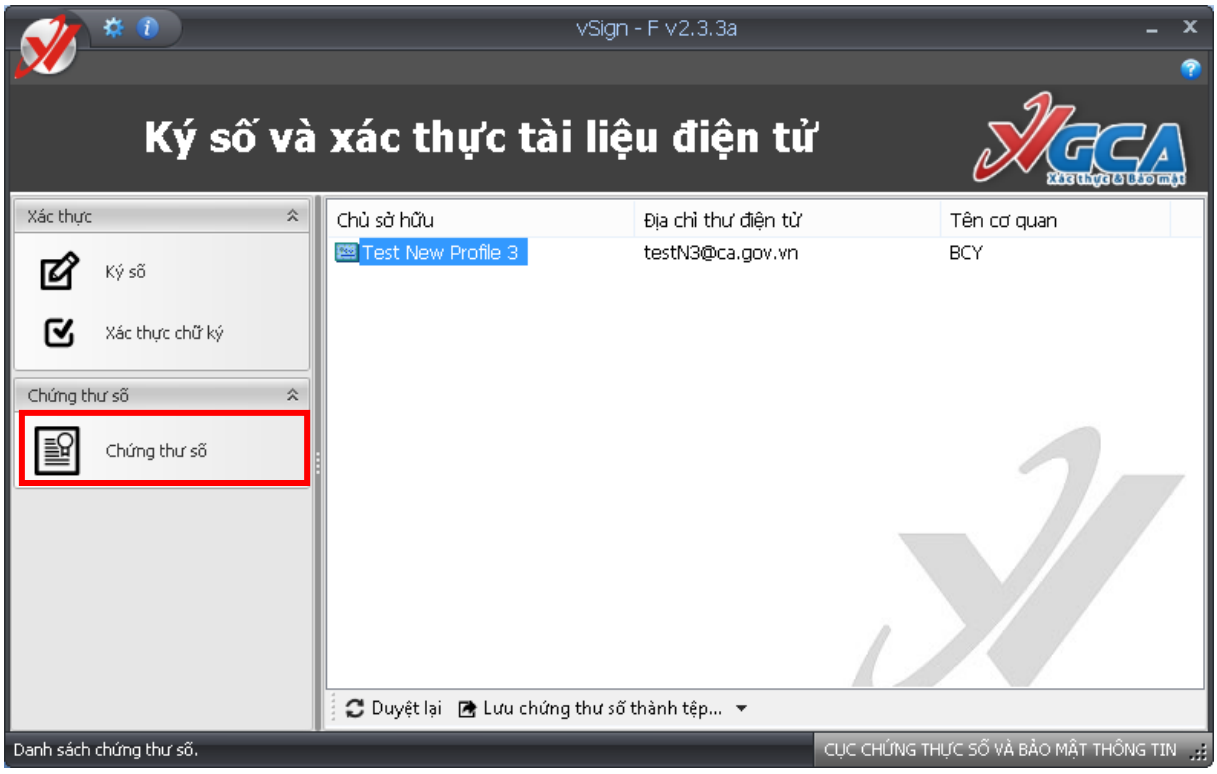
Hoặc lưu tệp lại để xem, nhấp "Lưu các tệp vào thư mục…" để thực hiện việc lấy danh sách các tệp ký số ra khỏi tệp chữ ký.



2.4.2.3 Xuất chứng thư số trong thiết bị ra tệp

Bước 1: Cắm thiết bị Token vào máy tính

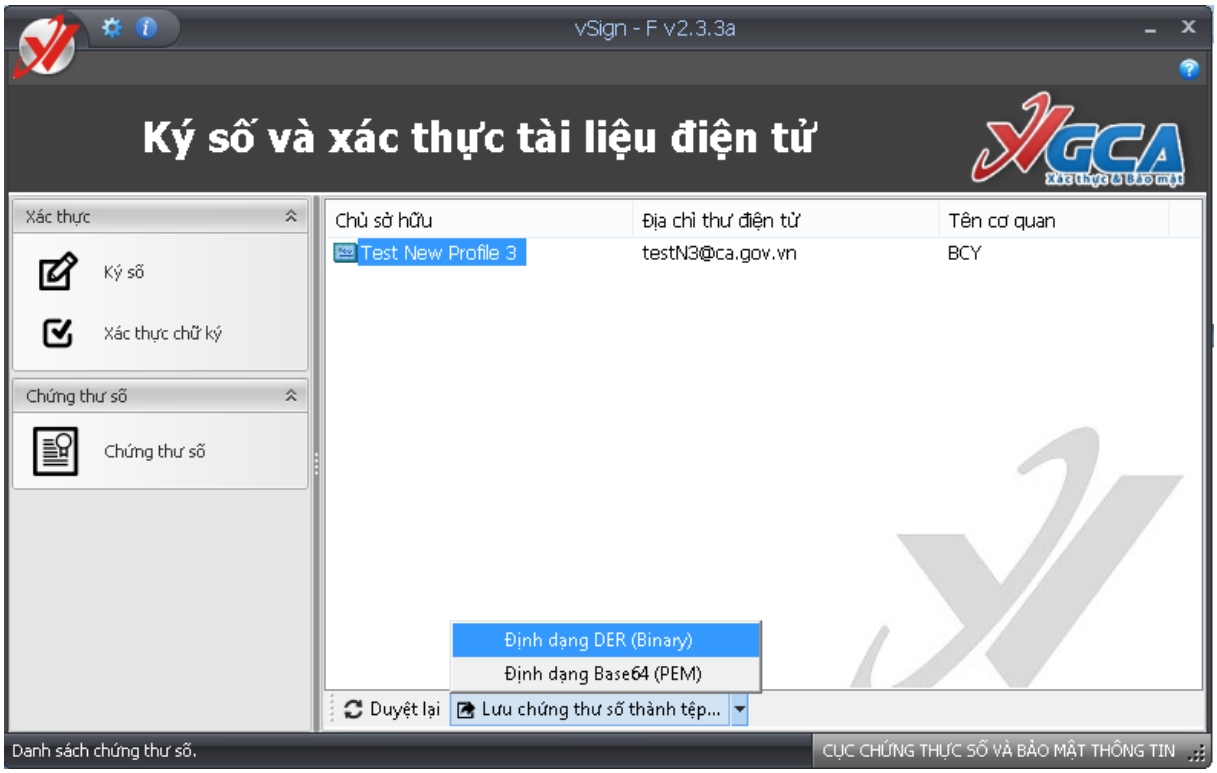
Bước 2: Trên giao diện chương trình, chọn menu "Chứng thư số"



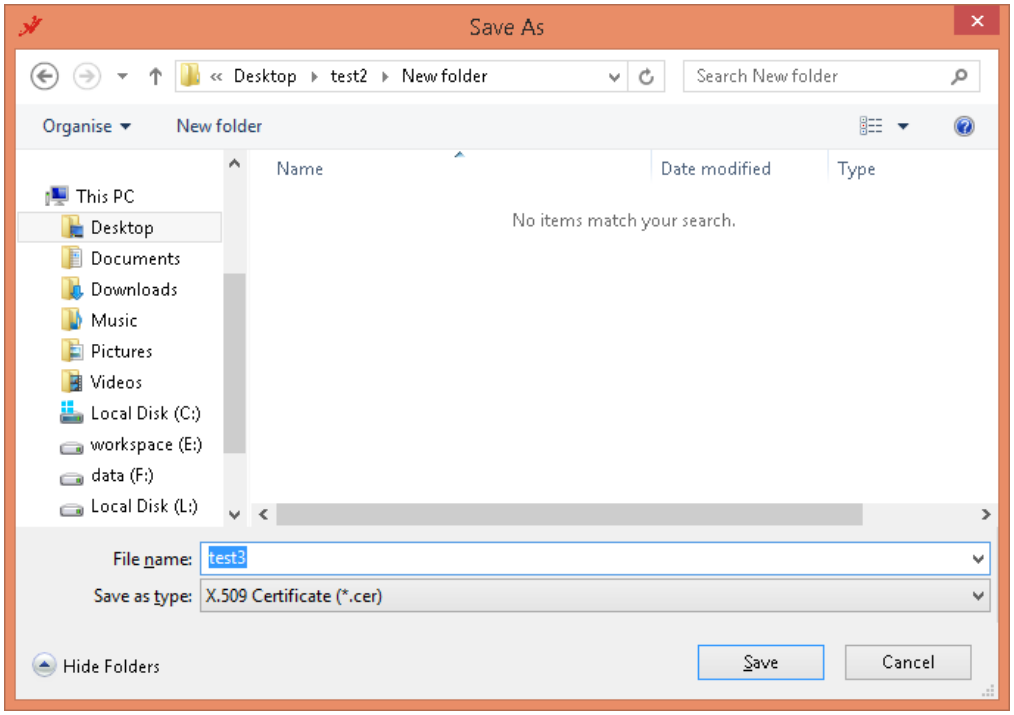
Bước 3: Chọn chứng thư số trong danh sách muốn lưu. Ví dụ: "Test New Profile 3" như trên hình.

Bước 4: Chọn "Lưu chứng thư số thành tệp ..." dưới thanh công cụ. Ở đây có hai định dạng cho phép người dùng lựa chọn để lưu chứng thư số ra tệp là:

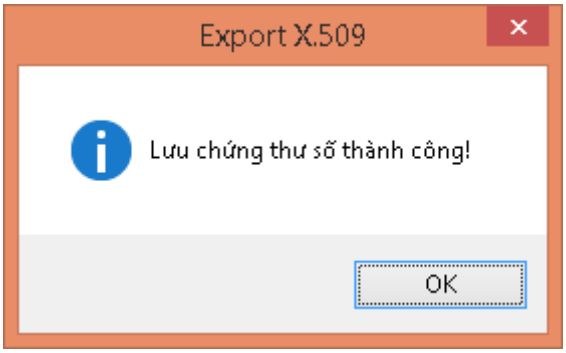
- Định dạng DER: đây là định dạng mảng byte nhị phân (binary) nội dung chứng thư số.
- Định dạng Base64: Chứng thư số sẽ lưu dưới dạng chuỗi Base64, có các tag đánh dấu Header (-----BEGIN CERTIFICATE-----) và Footer (-----END CERTIFICATE-----) của chứng thư số, đây còn gọi là định dạng PEM (Privacy Enhanced Mail).



Bước 5: Chọn đường dẫn lưu tệp chứng thư số:



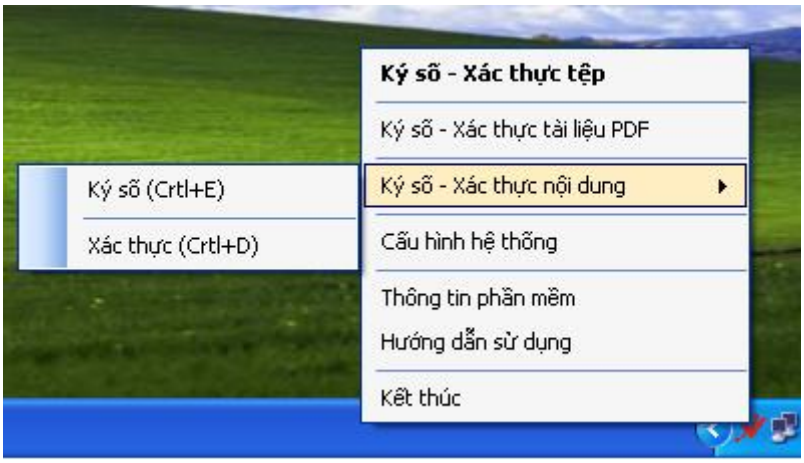
Thông báo xuất chứng thư số ra tệp thành công:



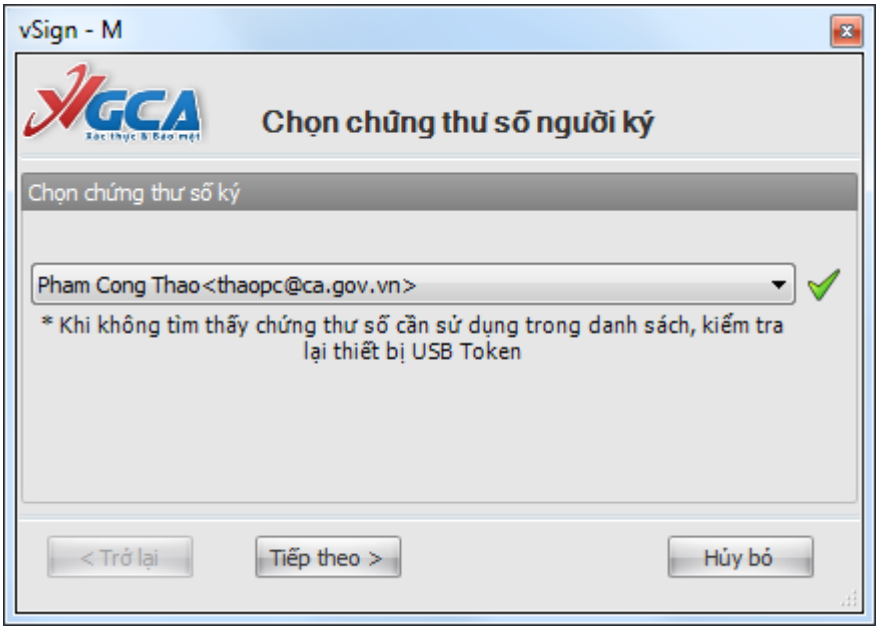
2.5 Ký số và xác thực nội dung thư

2.5.1 Ký số nội dung thư

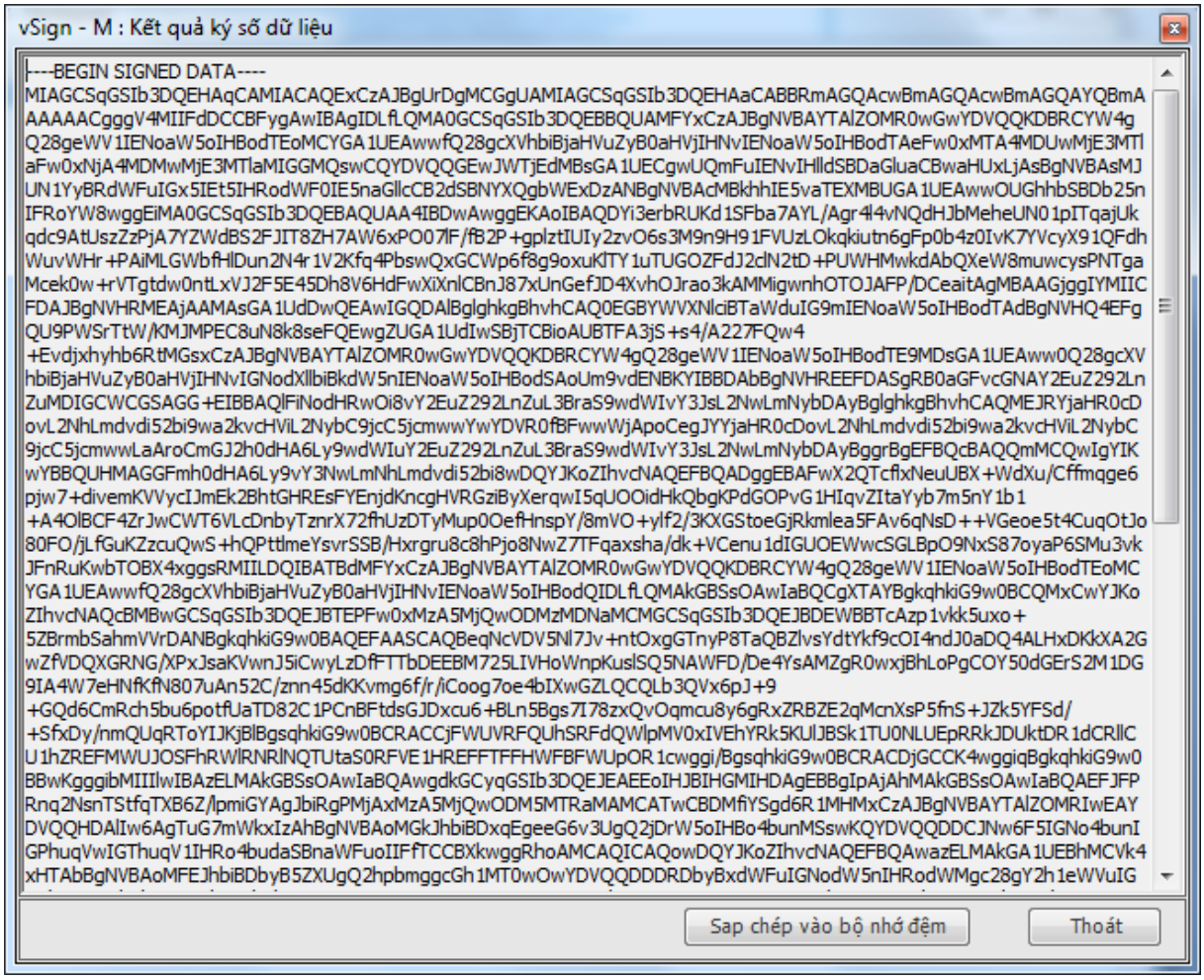
Có hai cách để ký số nội dung thư như sau: từ trình soạn thảo thư sử dụng phím tắt Ctrl + E, từ TrayIcon của hệ thống chọn "Ký số - Xác thực nội dung" -> "Ký số (Ctrl+E)".



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.

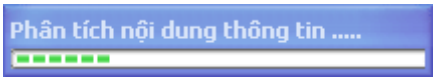


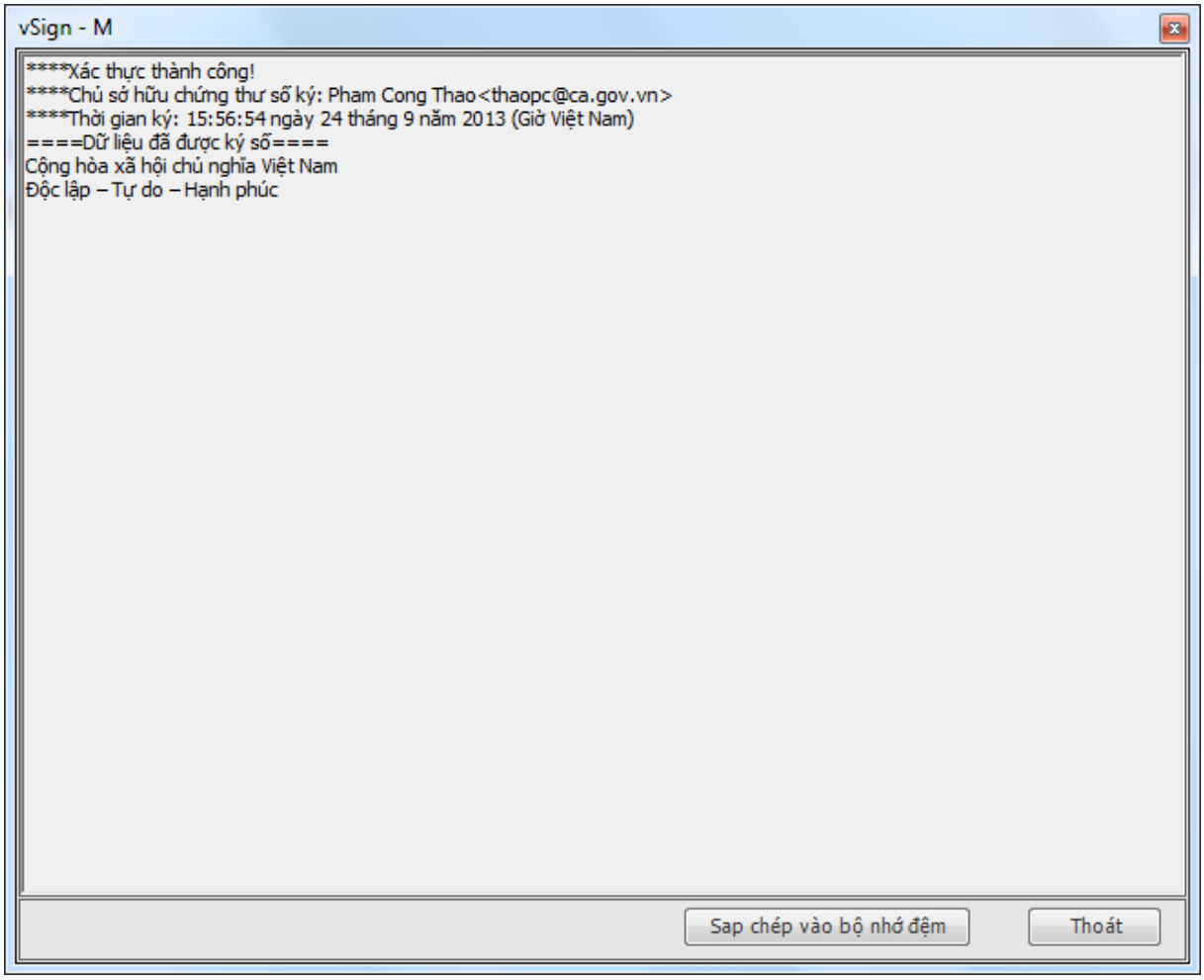
Kết quả ký số sẽ được hiển thị trên cửa sổ, người dùng sẽ thực hiện sao chép vào bộ nhớ đệm và gán vào trình soạn thảo thư để gửi đi.

2.5.2 Xác thực chữ ký trên nội dung thư

Khi nhận được thư đã ký người dùng sẽ copy nội dung vào bộ nhớ đệm và thực hiện xác thực bằng cách sau: nhấp Ctrl +D hoặc từ biểu tượng của chương trình trên khay hệ thống chọn "Ký số – Xác thực nội dung" -> "Xác thực (Ctrl + D)".

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

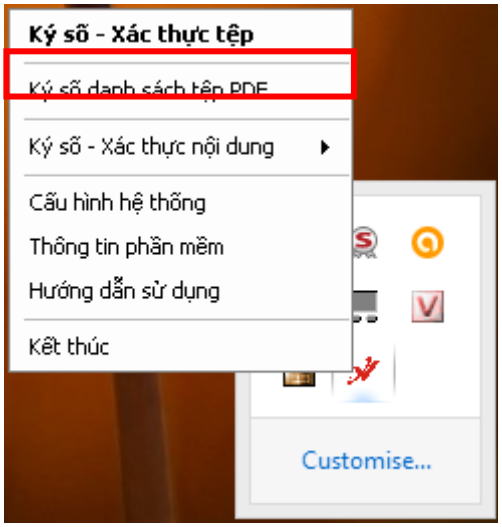




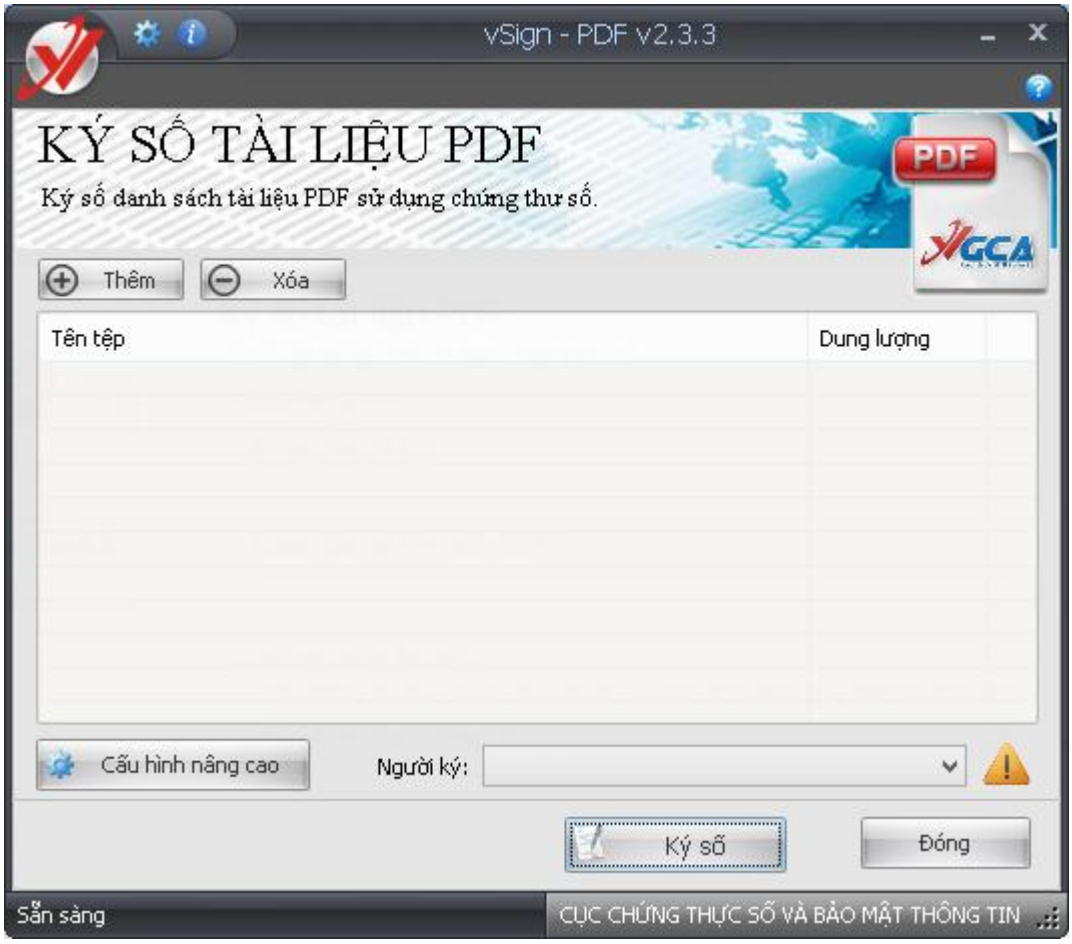
Giao diện hiển thị kết quả quá trình phân tích nội dung thông tin.

2.6 Ký số danh sách tệp PDF

Để khởi động chương trình ký số danh sách tệp PDF, từ thực đơn trên khay hệ thống chọn "Ký số danh sách tệp PDF".



Giao diện chính của chương trình như sau:

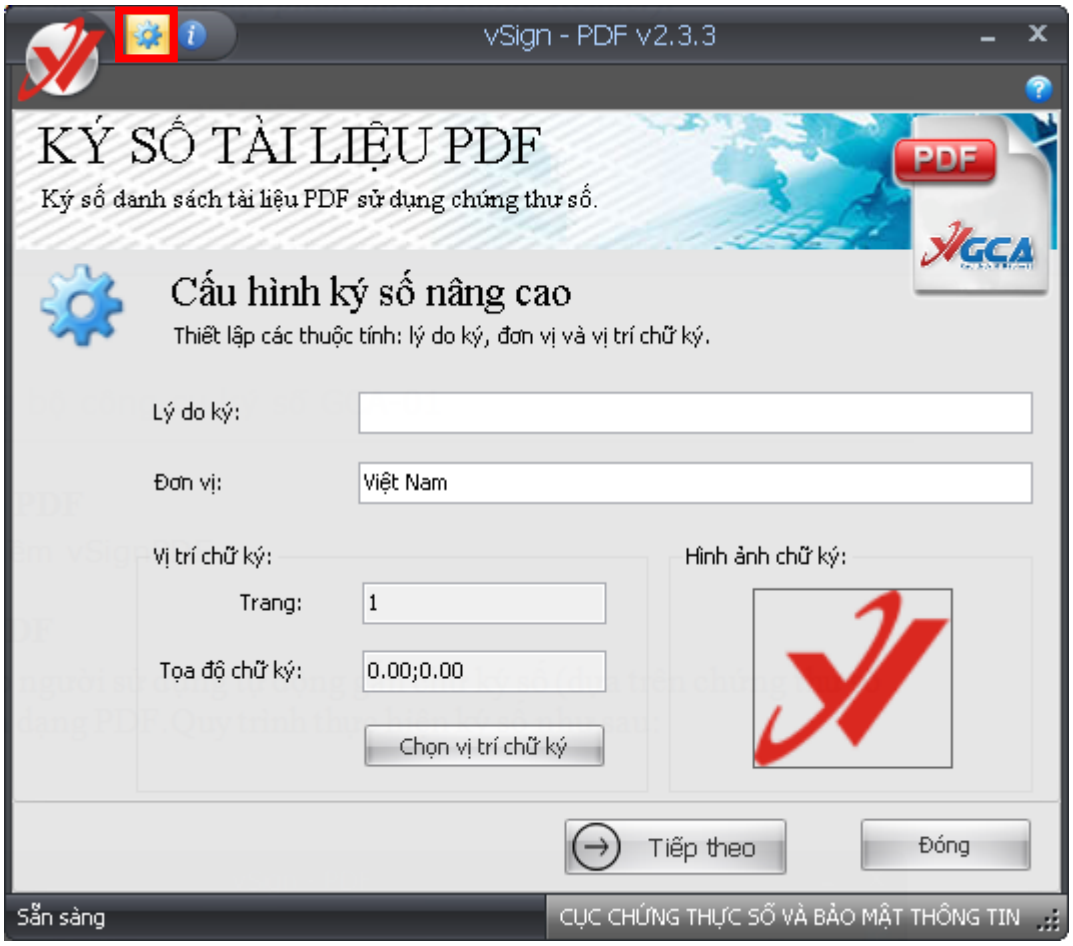


Chú ý:

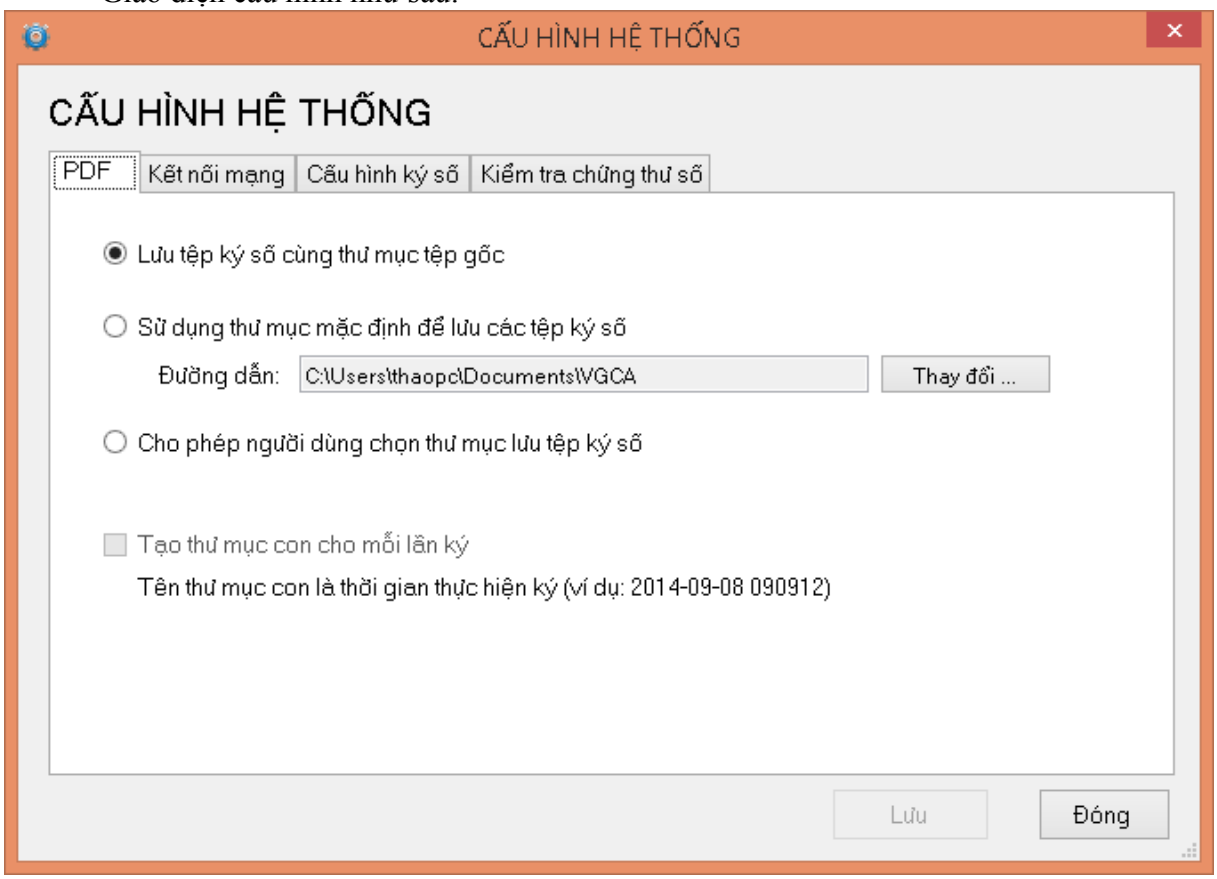
- ***Phần mềm vSign2.3 không thiết kế chức năng giải mã và xác thực chữ ký cho tài liệu PDF, người dùng sẽ sử dụng phần mềm Adobe Reader để giải mã xác thực tài liệu PDF.***
- ***Sử dụng phần mềm Adobe Reader phiên bản 8.0 trở lên để tạo tệp PDF và kiểm tra xác thực chữ ký.***
- ***Cần phải cấu hình 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 Cấu hình ký số PDF

Trên giao diện phần mềm ký số danh sách tệp vSign-PDF, bấm chọn nút cấu hình phía trên bên trái để mở giao diện cấu hình:



Giao diện cấu hình như sau:



Trên đây cho phép người dùng thiết lập thư mục lưu trữ tệp pdf sau khi đã ký số:

1. Lưu tệp ký số cùng thư mục tệp gốc: tệp sau khi ký sẽ được lưu cùng thư mục với tệp đầu vào

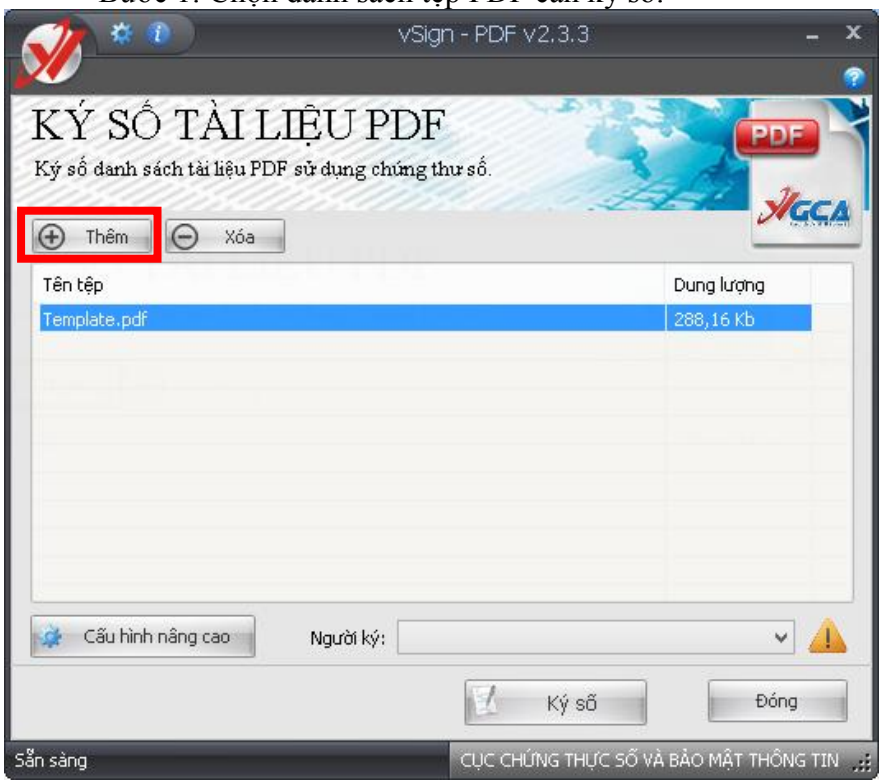
2. Sử dụng thư mục mặc định để lưu các tệp ký số: Nếu người dùng chọn thiết lập này, các tệp sau khi ký sẽ được lưu vào đường dẫn thư mục mặc định.

3. Cho phép người dùng chọn thư mục lưu tệp ký số: Trước khi quá trình ký số được bắt đầu, người dùng sẽ phải chọn đường dẫn thư mục lưu

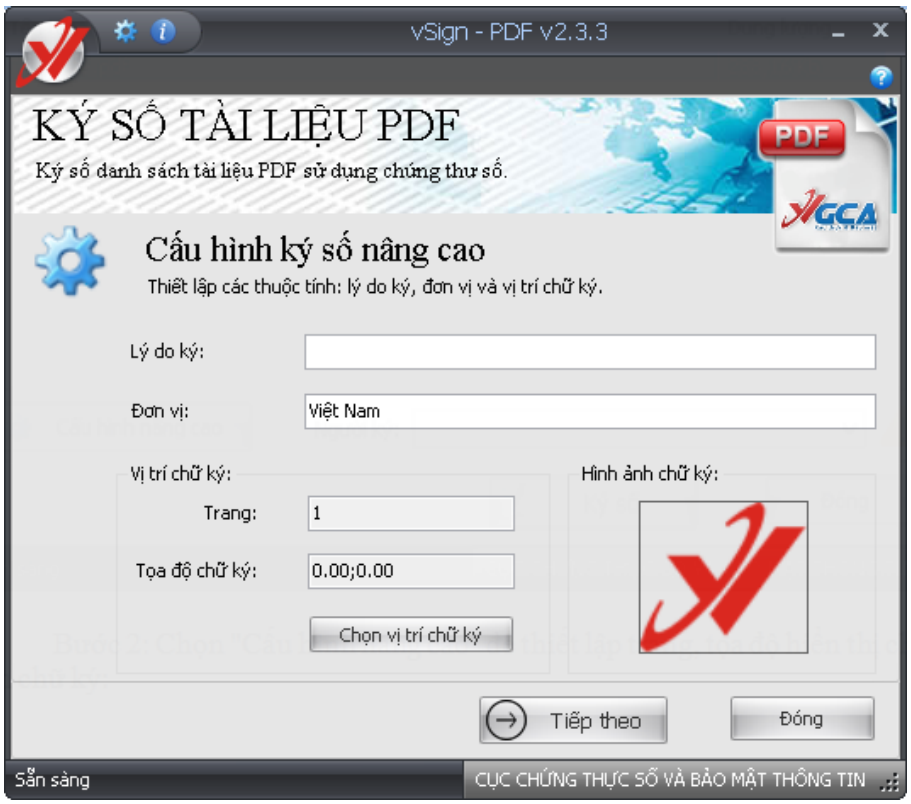
4. Tạo thư mục con cho mỗi lần ký: Thiết lập này chỉ có tác dùng khi ở chế độ người dùng tự chọn thư mục lưu. Nếu được chọn, thì chương trình sẽ tự động tạo ra một thư mục con với tên là thời gian tạo, ví dụ "2014-09-08 090912" và các tệp sau khi ký số sẽ được lưu tại đây.

2.6.2 Ký số danh sách tệp PDF

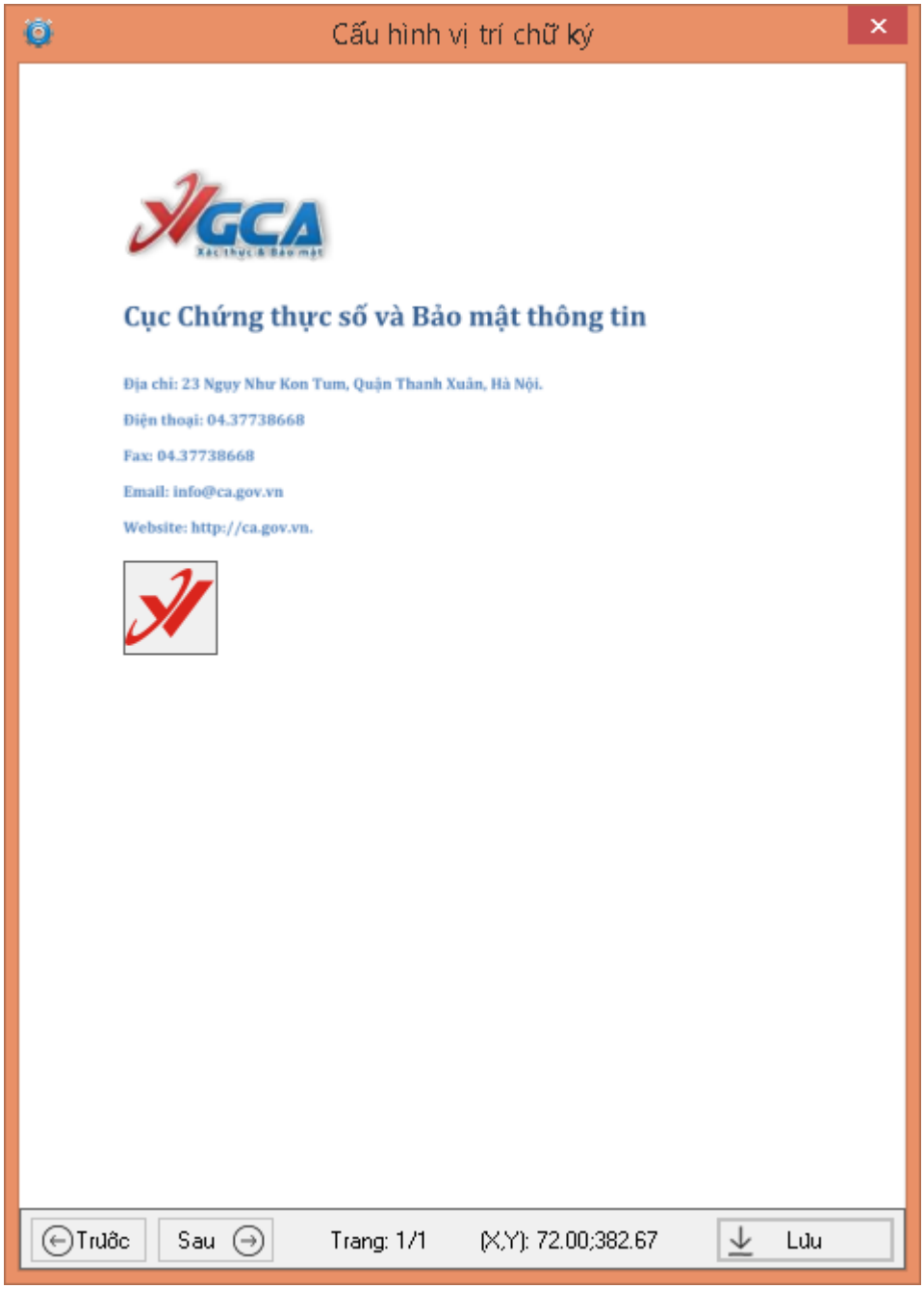
Bước 1: Chọn danh sách tệp PDF cần ký số:



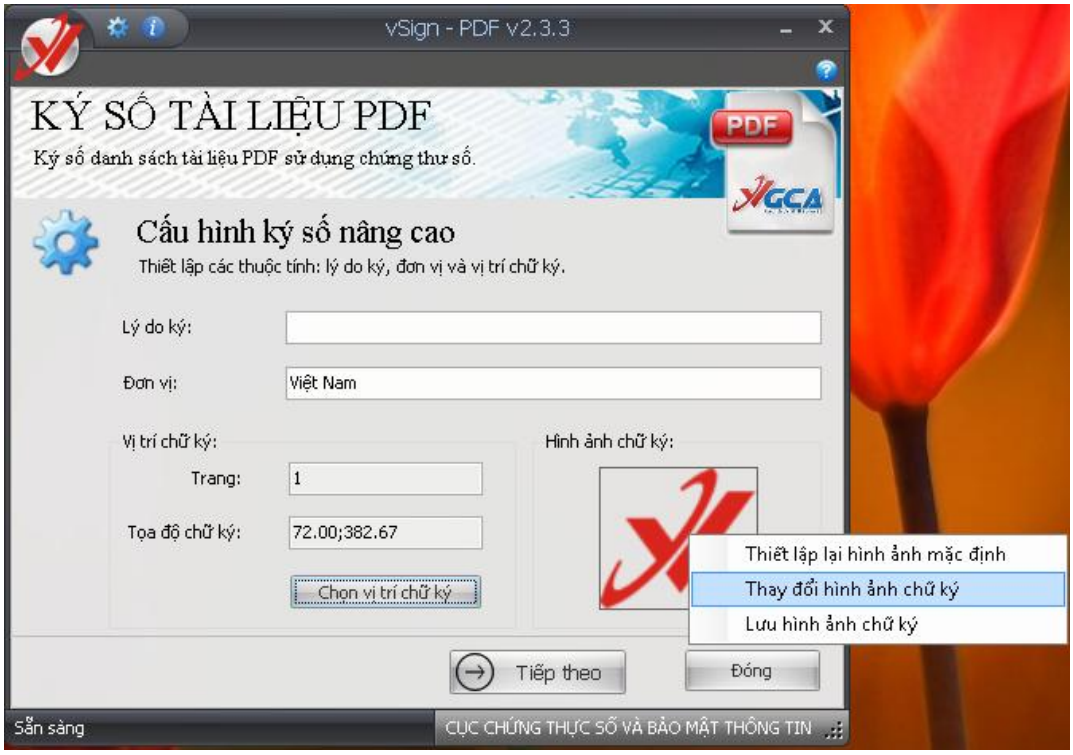
Bước 2: Chọn "Cấu hình nâng cao" để thiết lập lý do ký, đơn vị, trang, tọa độ hiển thị chữ ký và hình ảnh chữ ký:



- Lý do ký, và đơn vị người dùng nhập trực tiếp vào ô tương ứng
- Để thay đổi vị trí chữ ký người dùng bấm chọn "Chọn vị trí chữ ký", trên giao diện người dùng di chuyển hình ảnh chữ ký đến vị trí thích hợp và bấm "Lưu":

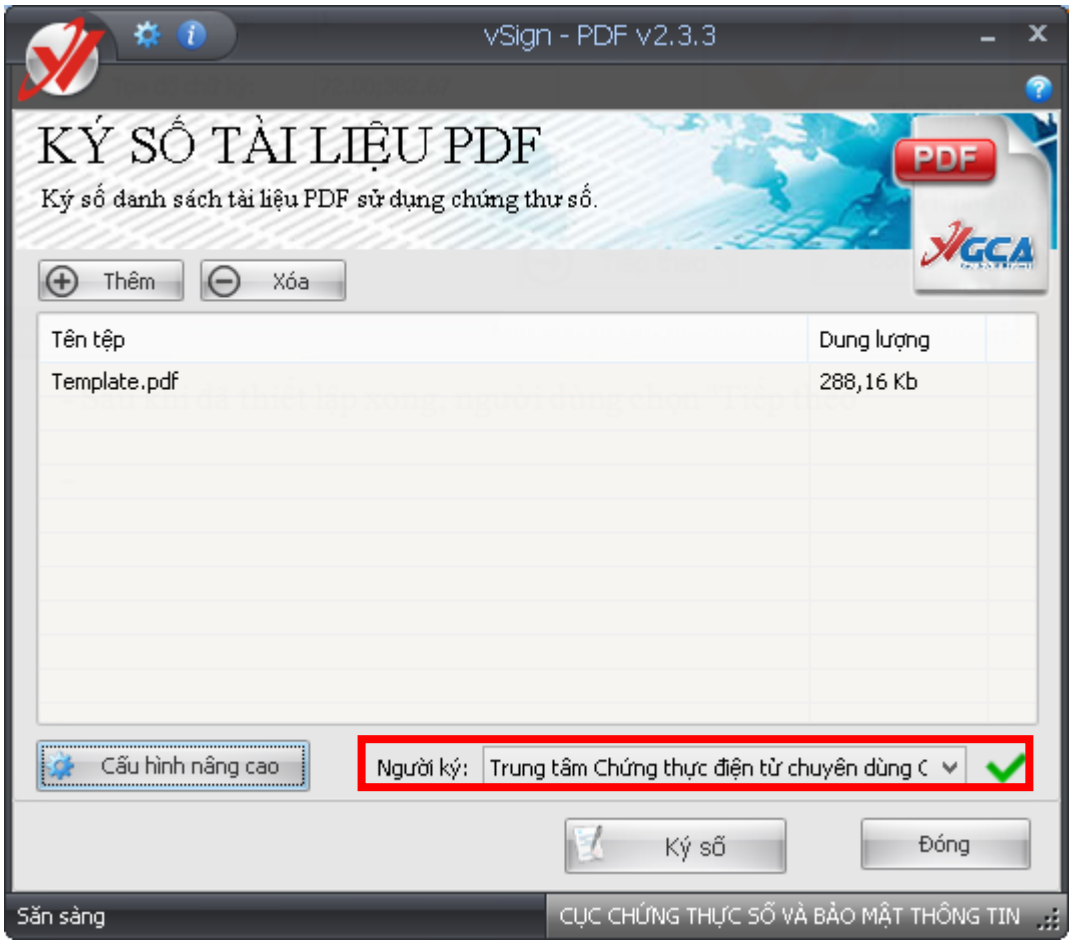


- Để thay đổi hình ảnh chữ ký, người dùng bâm phải chuột vào khung hình ảnh chữ ký, chọn menu "Thay đổi hình ảnh chữ ký"; nếu muốn sử dụng hình ảnh mặc định chọn "Thiết lập lại hình ảnh mặc định"; để lưu lại hình ảnh chữ ký chọn "Lưu hình ảnh chữ ký";

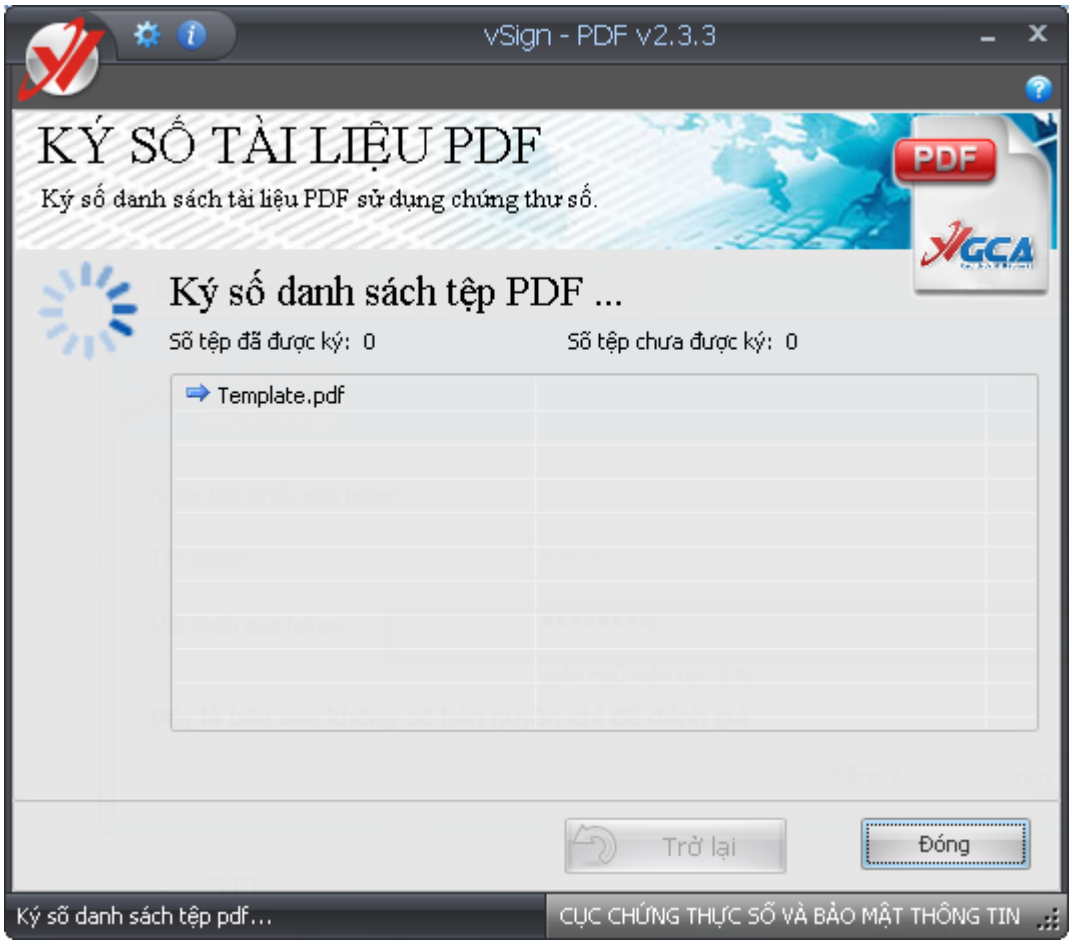


- Sau khi đã thiết lập xong, người dùng chọn "Tiếp theo"

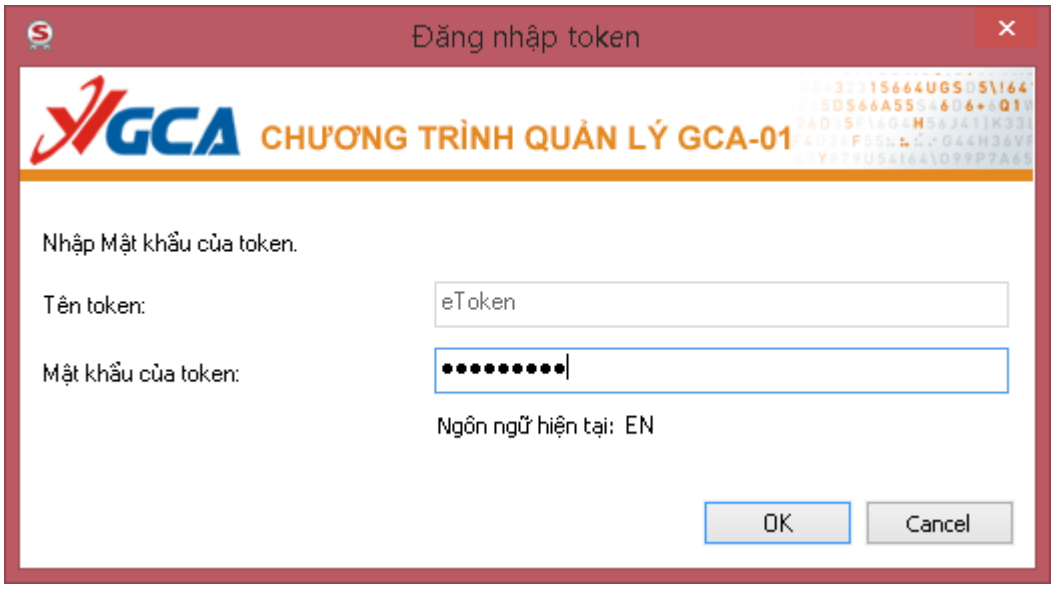
- Chọn chứng thư số ký:



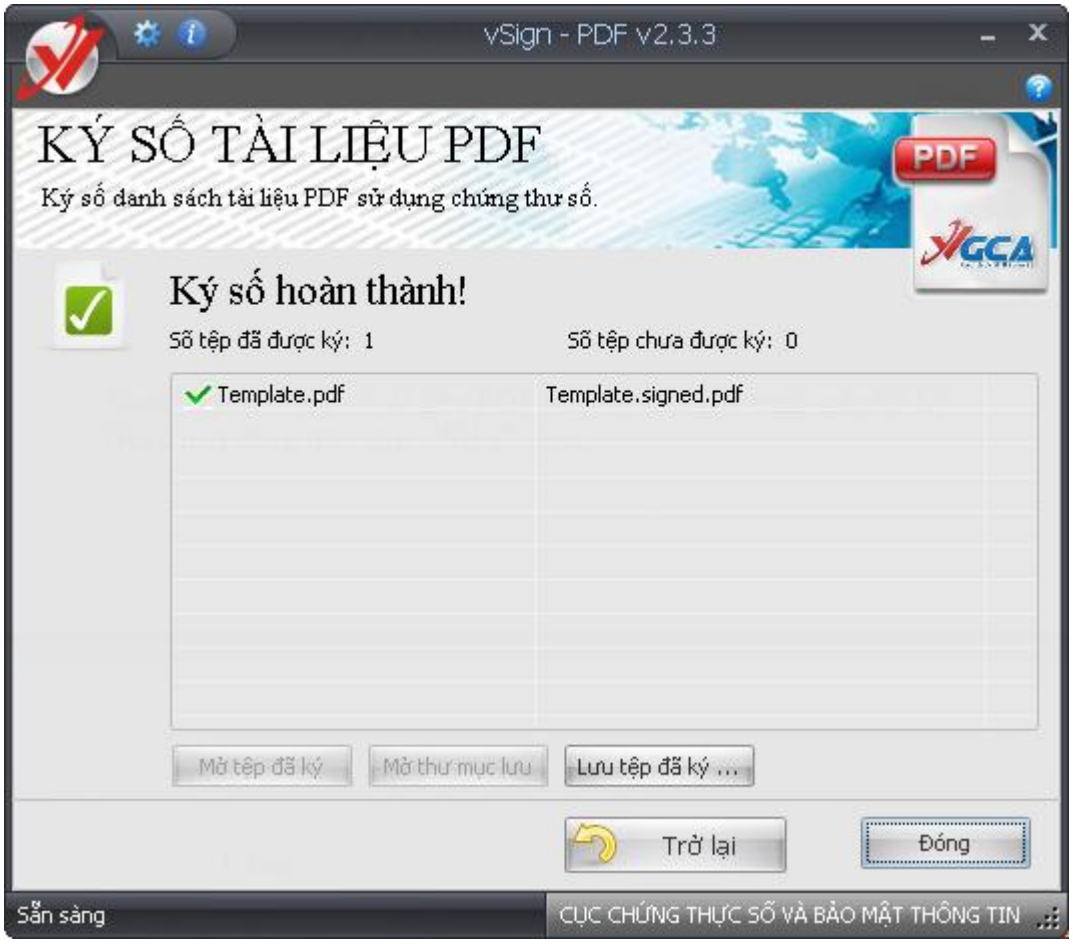
- Bấm ký số để bắt đầu:



- Nhập mật khẩu thiết bị:



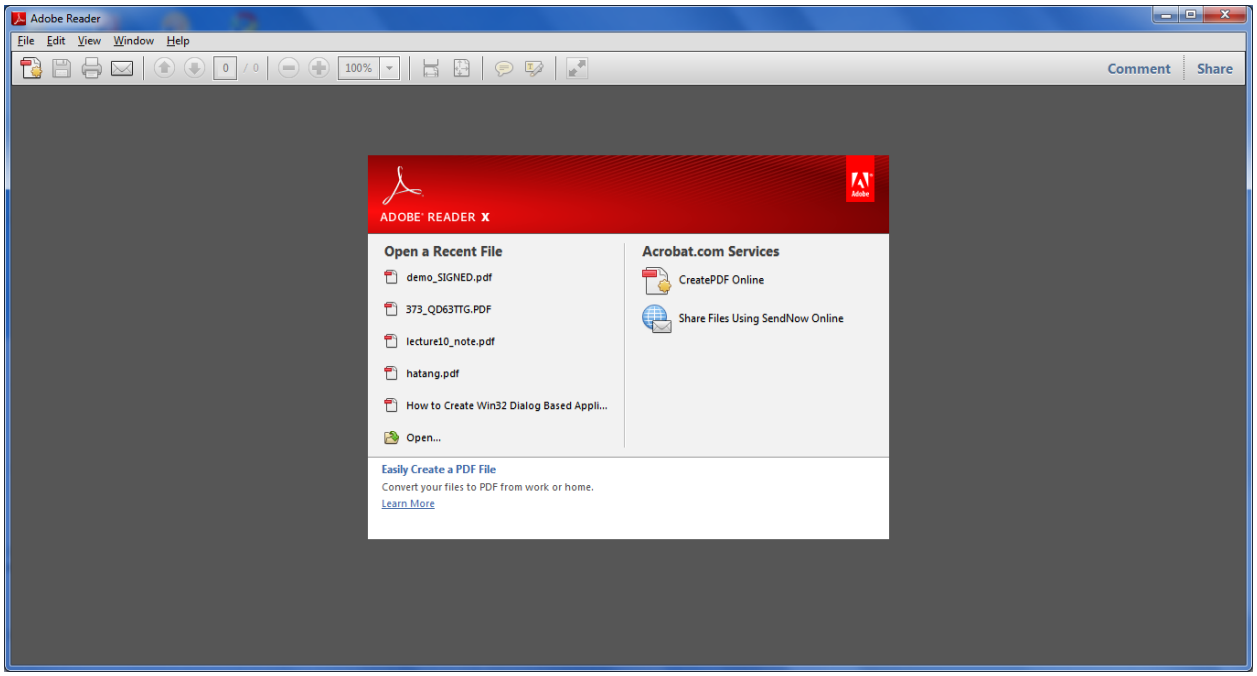
- Ký số thành công:



2.6.3 Kiểm tra chữ ký số trên tài liệu PDF

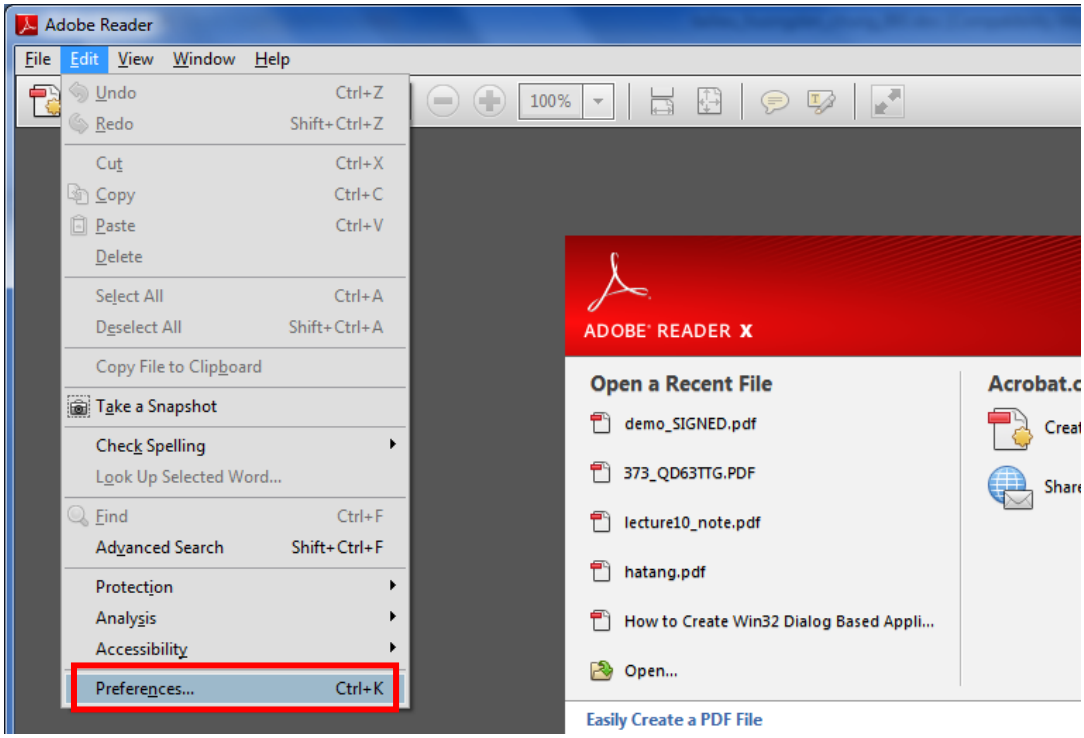
2.6.3.1 Cấu hình Adobe Reader

Trước khi kiểm tra chữ ký số trên tài liệu PDF cần phải cấu hình phần mềm Adobe Reader. 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.

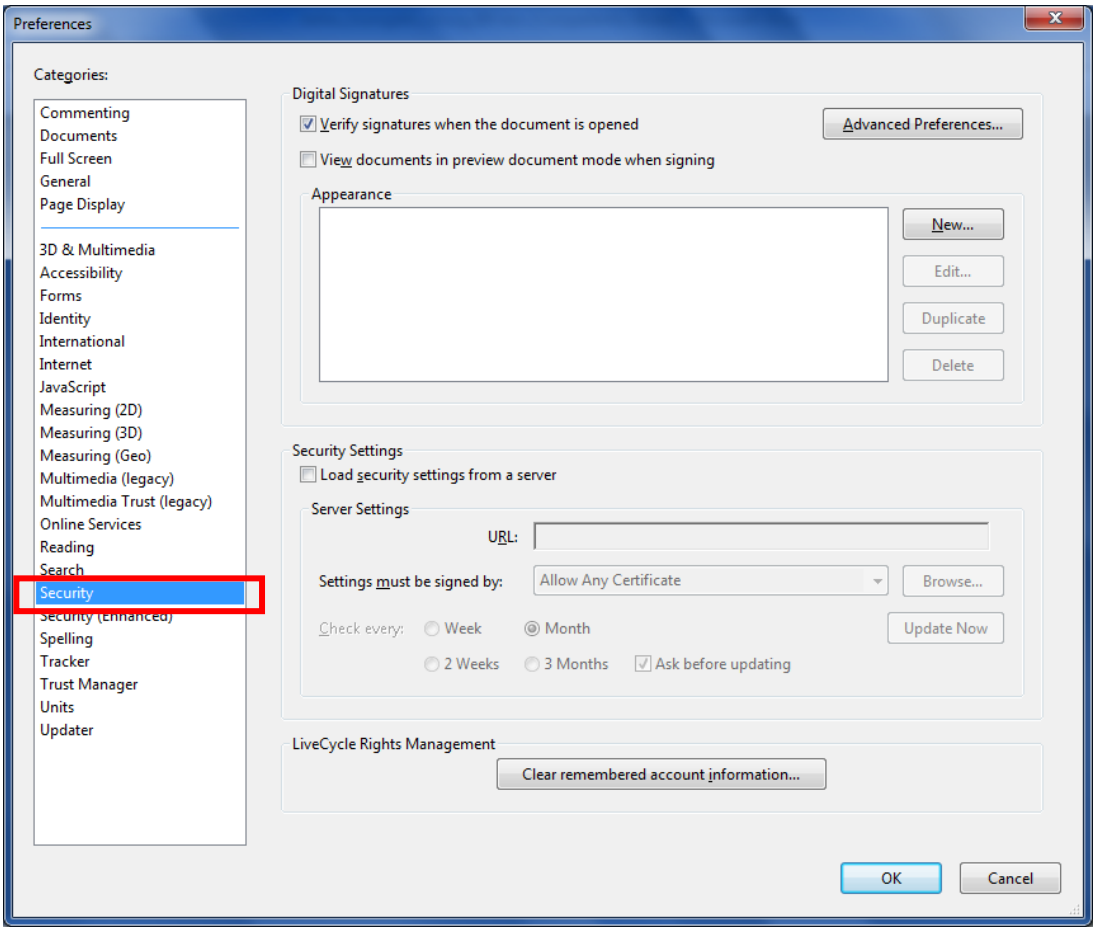


Mục đích cấu hình phần mềm Adobe Reader để sử dụng và kiểm tra được dấu thời gian gắn trên chữ ký và làm cho phần mềm tin tưởng (trust) vào các chứng thư số (chứng thư số Root, sub, timestamp, user,…).

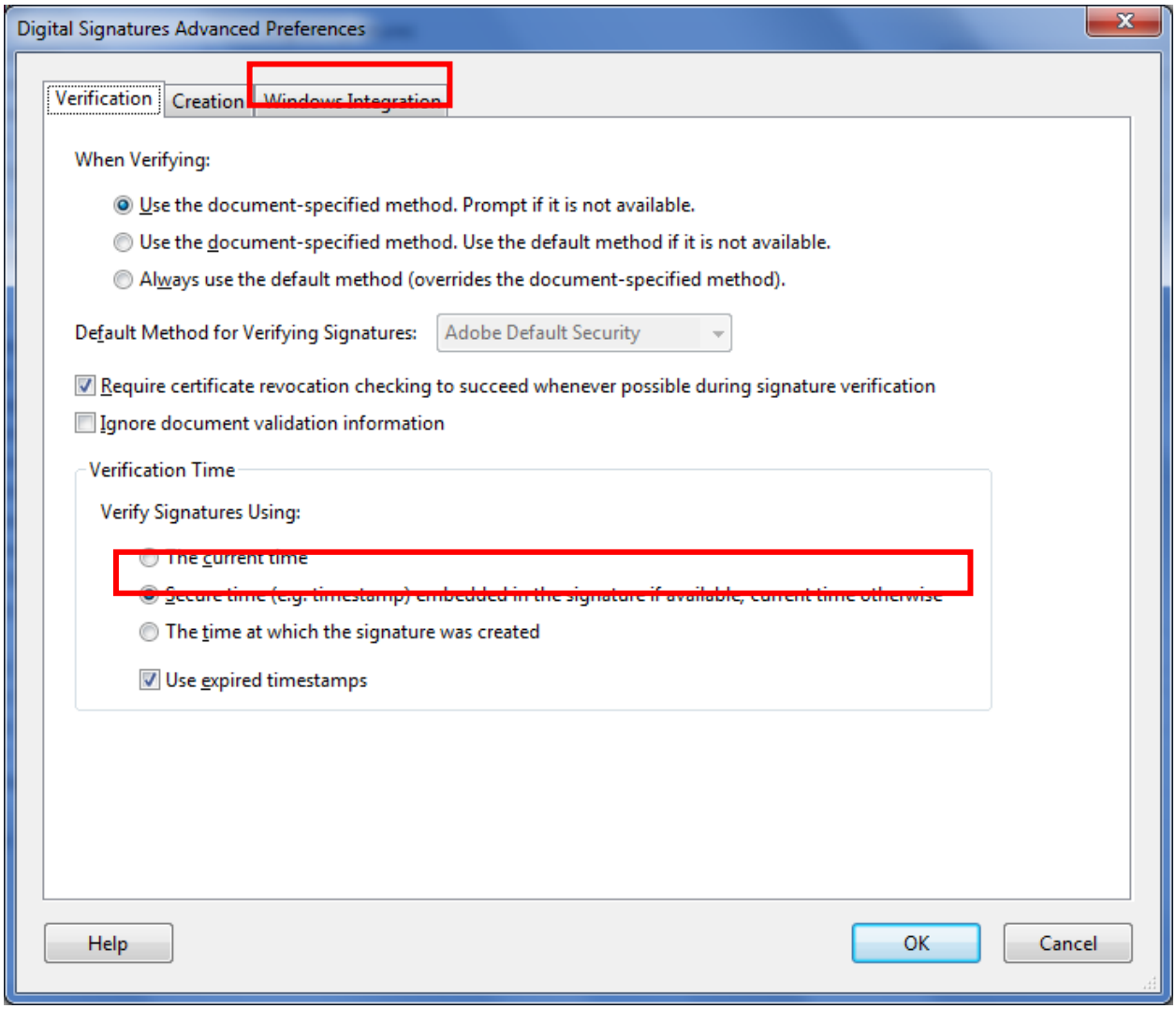
Để cấu hình vào Edit->Preferences…



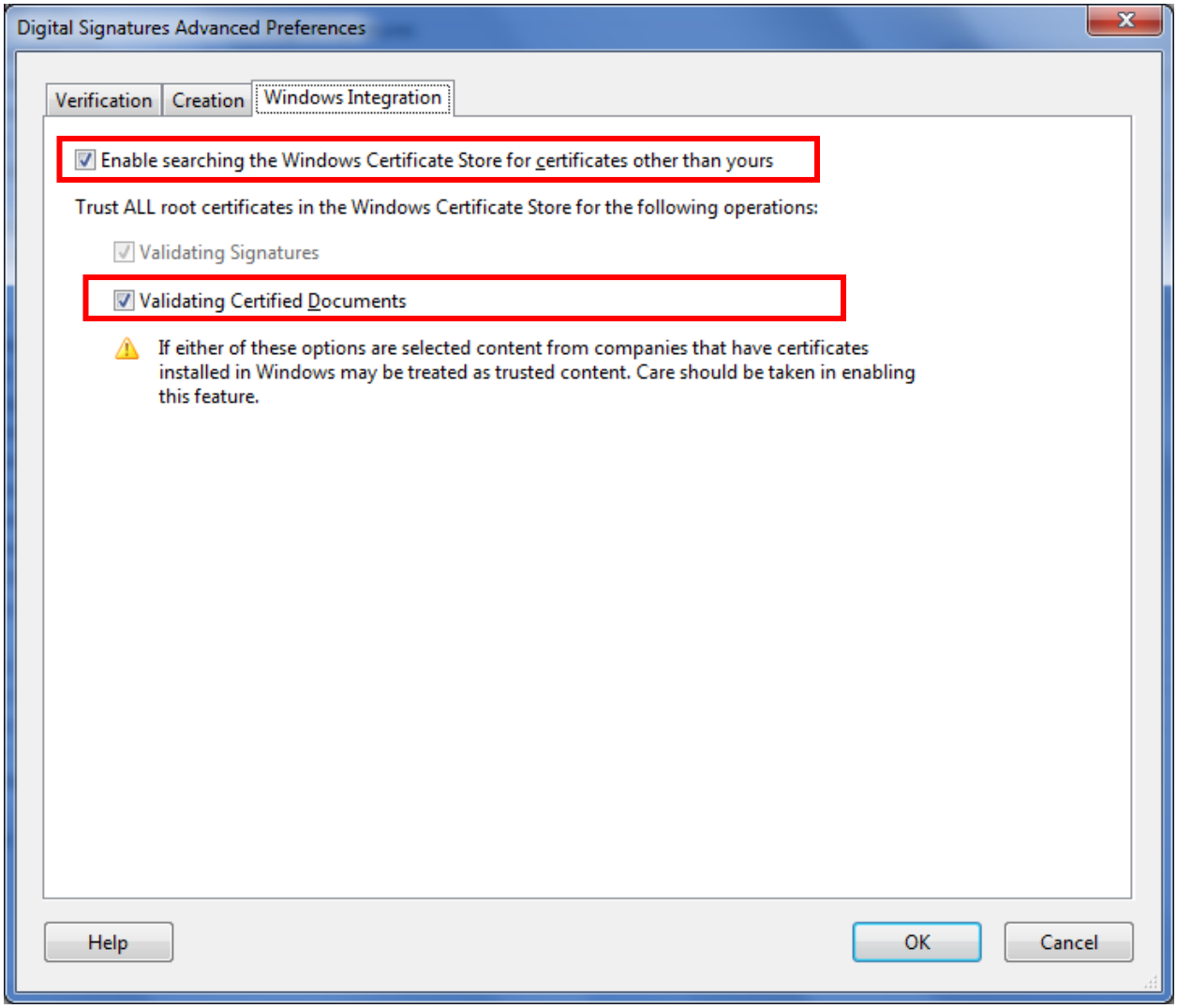
Giao diện hiển thị, chọn Security.



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



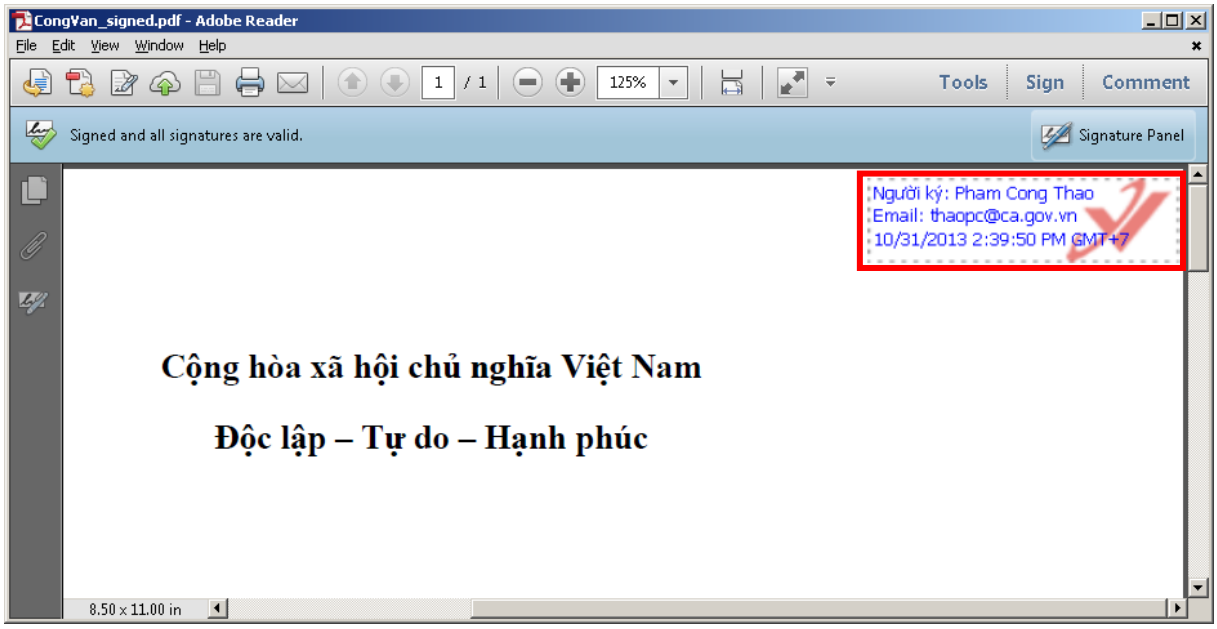
Chọn tab "Windows Intergration" để cấu hình tiếp:



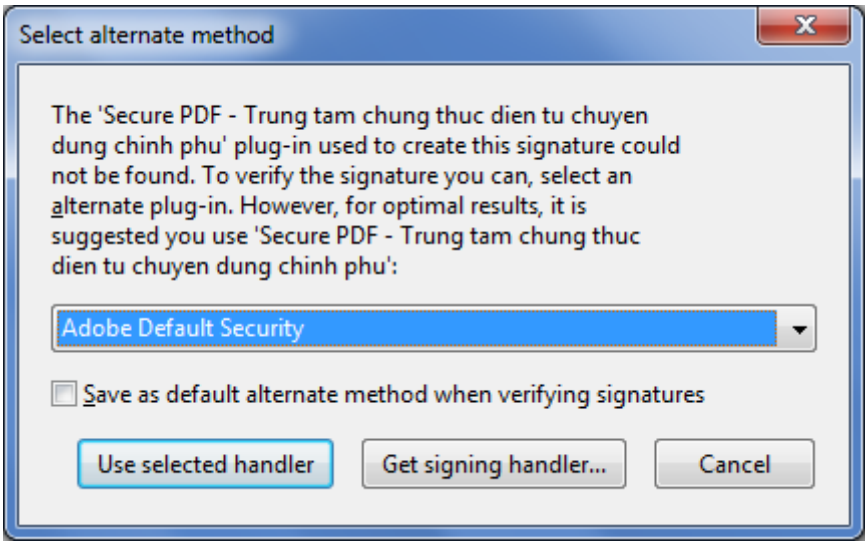
Tích vào ô "Enable searching the Windows Certificate Store for certificates other than yours" và ô "Validating Certified Documents". Chọn OK để kết thúc việc cấu hình Adobe Reader.

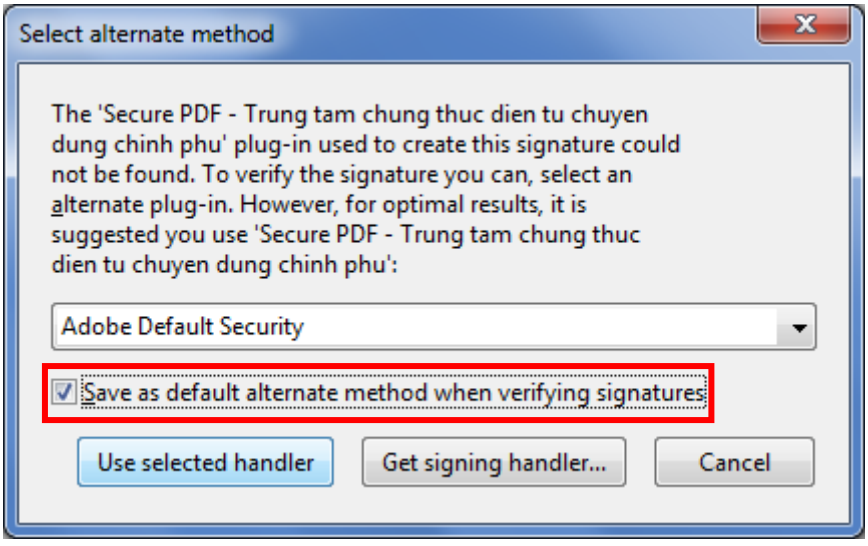
2.6.3.2 Kiểm tra chữ ký số trên tài liệu PDF

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

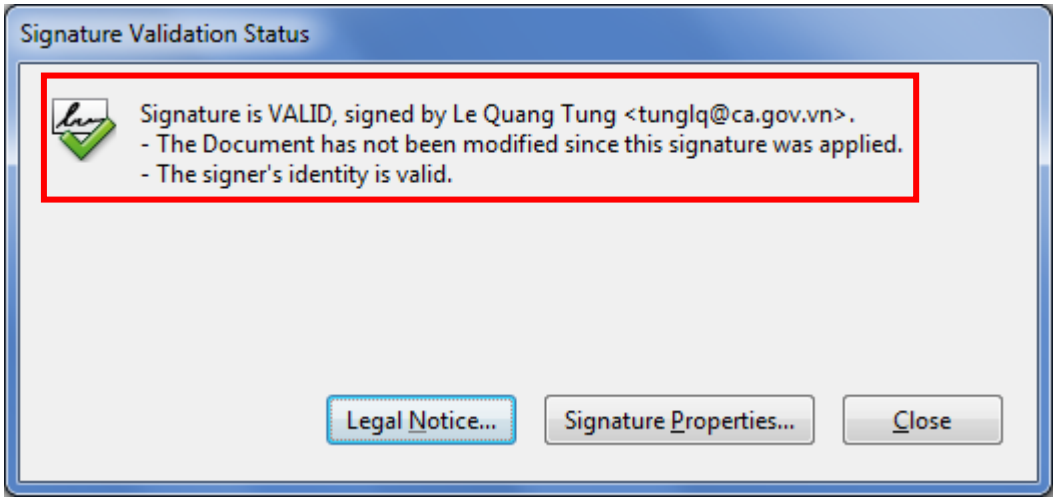


Kích đúp chuột lên chữ ký số trên tài liệu PDF (ô màu đỏ).

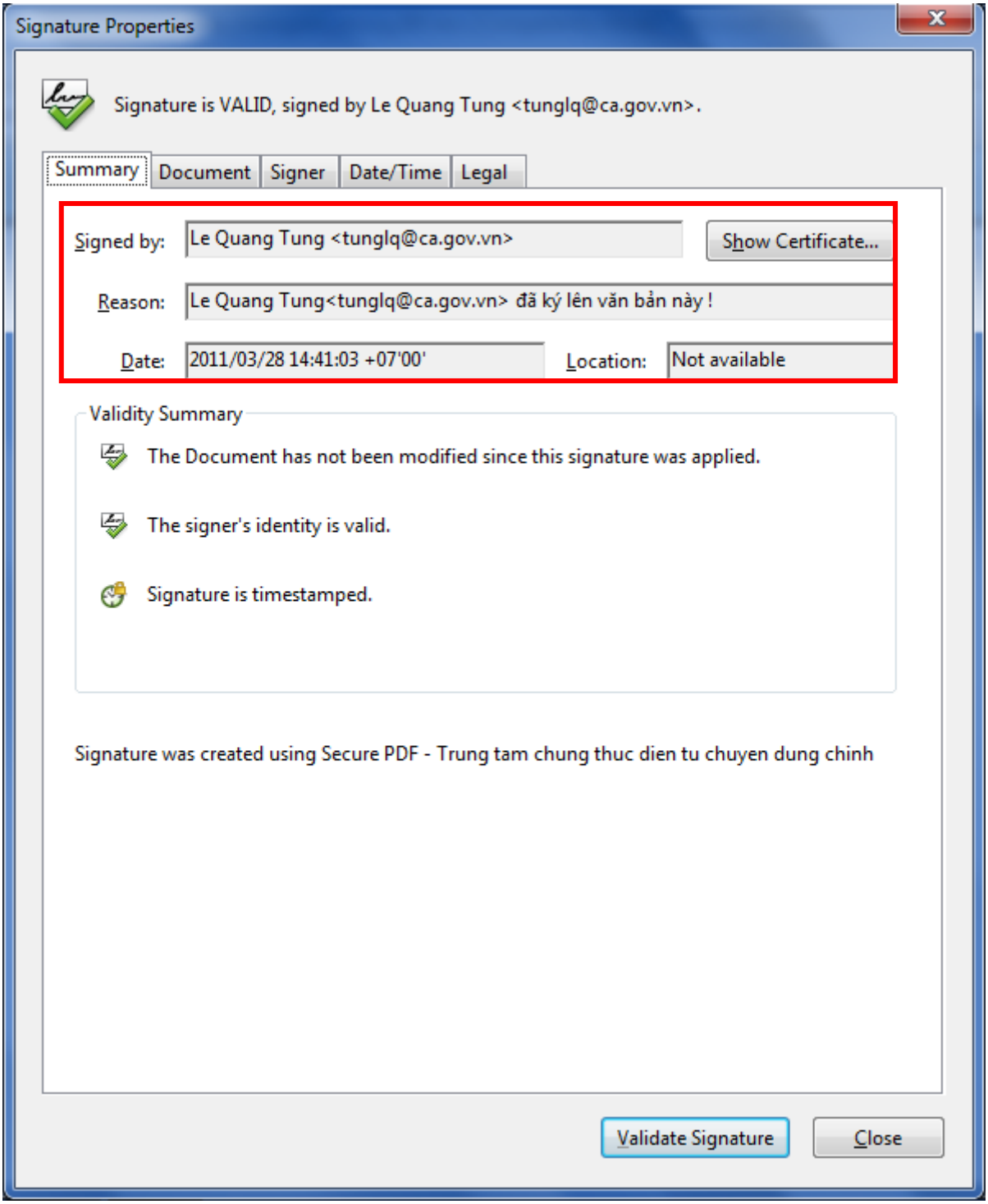




Chọn ô "Save as default….." và chọn "Use selected handler".



Để xem chi tiết nội dung chữ ký số chọn "Signature Properties…".


Signature Properties
Signature is VALID, signed by Le Quang Tung <tunglq@ca.gov.vn>.
Summary
Document
Signer
Date/Time
Legal
Signed by:
Le Quang Tung <tunglq@ca.gov.vn>
Show Certificate...
Reason:
Le Quang Tung<tunglq@ca.gov.vn> đã ký lên văn bản này !
Date:
2011/03/28 14:41:03 +07'00'
Location:
Not available
Validity Summary
The Document has not been modified since this signature was applied.
The signer's identity is valid.
Signature is timestamped.
Signature was created using Secure PDF - Trung tam chung thuc dien tu chuyen dung chinh
Validate Signature
Close

3 Kết luận

Bộ công cụ ký số GCA-01 có thể đáp ứng tốt các nhu cầu ký số 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 ký số và xác thực tài liệu điện tử cho các cơ quan thuộc hệ thống chính trị.

Địa chỉ liên hệ:

Cục Chứng thực số và Bảo mật thông tin
Địa chỉ: Số 23, Ngụy Như Kon Tum, Thanh Xuân, Hà Nội
Điện thoại: 04.37738668
Fax: 04.37738668
Email: ca@bcy.gov.vn
Website: http://ca.gov.vn