Published on *Gooze* (http://www.gooze.eu)

Windows logon using smartcards

Here is a list of documentation and projects:

EIDauthentication

Website: https://sourceforge.net/projects/eidauthenticate/ [1]
GOOZE tutorial: EIDauthentication HOWTO [2]
Audience: single user authentication, small workgroups
Status: validated and working

While Microsoft has designed a smart card logon method in active directory, stand alone computer can't use smart cards. EIDauthentication allows smartcard logon, without the need of a domain controller.

This project works very well with the Feitian PKI and the Feitian ePass PKI token.

Active Directory

Website: Microsoft
Audience: workgroups using Active Directory
Status: validated and working

Microsoft has designed a smart card logon method in Active Directory, but this requires a Windows 2008 Server. The connection method using Windows 2008 Server is very described on Feitian CD.

A free software alternative to Active Directory server would be a Linux box running Kerberos + LDAP + Samba RPC. But our tutorial is not yet ready.

pGina open source authentication

Website: http://www.pgina.org [3]
Audience: workgroups using free software
Status: not validated

pGina is an open source authentication system that replaces the built in authentication of the Microsoft Windows operating system. pGina uses easy-to-write plugins that allow a system to authenticate against virtually any source. Some examples are LDAP, RADIUS, SSH, FTP, SMTP, POP3, and many more.

There used to be a smartcard plugin for pGina and the plugin needs to be revived. Please contact the developers for more information.

EIDauthentication HOWTO

This document describes how to set up smartcard logon in Windows 7/Vista.
We will be using EIDauthentication.

Why use EIDauthentication

Windows Vista and Windows 7 require an Active Directory Server (i.e. Windows 2008 Server) to manage smartcard logon. Microsoft is interested in the high-end market, not simple users.

But there is a simple and powerful alternative:
EIDauthentication [4] allows end-users to logon using a smarcard WITHOUT Active Directory Server.

EIDauthentication offers very nice features:

- Windows Desktop integration.
- Compliance with Windows standards.
- Nice wizards and intuitive interface.

EIDauthentication is free software released on SourceForge.

EIDauthentication is actively maintained. Its author offers custom services [5] on request.

GOOZE has no relation with EIDauthenticate, but only recommends using this software.

Before you start using EIDauthentication

Hardware prerequisites

As a prerequisite, we recommend using:

- A Feitian PKI card [6] and a Feitian R-301 reader [7]. We also offer pcsc+ccid smartcard readers [8].
- or a Feitian ePass PKI token [8].

Using a smartcard or a USB token is exactly the same solution, as both include the same smartcard chip.

The advantage of using our hardware is that it is very well tested under GNU/Linux, Mac OS X and Windows, which makes a nearly universal solution.

Software prerequisites

Read the Windows installation [9] section and follow the instructions.

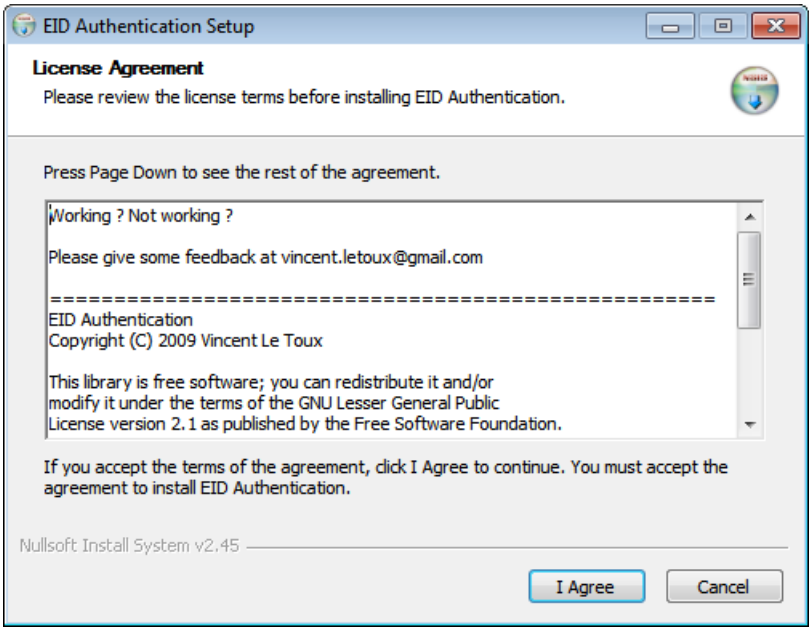
Because EIDauthentication relies on WinSCard Microsoft framework, you will need to initialize your card using Feitian utilities.

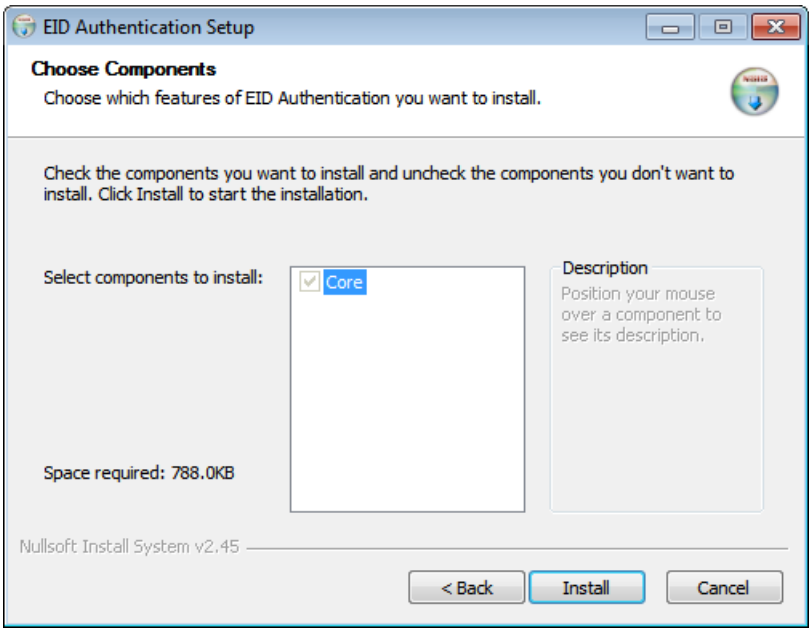
EIDauthentication Installation

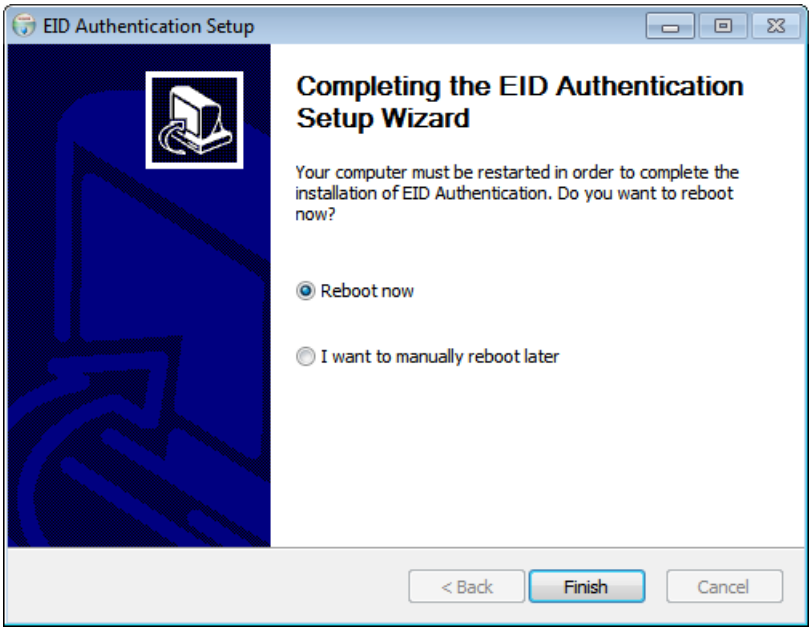
Downloading and installing EIDauthentication

Visit EIDauthenticate [4] Sourceforge project.

Download and install the latest version.


EID Authentication Setup
License Agreement
Please review the license terms before installing EID Authentication.
Press Page Down to see the rest of the agreement.
Working ? Not working ?
Please give some feedback at vincent.letoux@gmail.com
==========
EID Authentication
Copyright (C) 2009 Vincent Le Toux
This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License version 2.1 as published by the Free Software Foundation.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install EID Authentication.
Nullsoft Install System v2.45
I Agree
Cancel


EID Authentication Setup
Choose Components
Choose which features of EID Authentication you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Install to start the installation.
Select components to install:
Core
Description
Position your mouse over a component to see its description.
Space required: 788.0KB
Nullsoft Install System v2.45
< Back
Install
Cancel

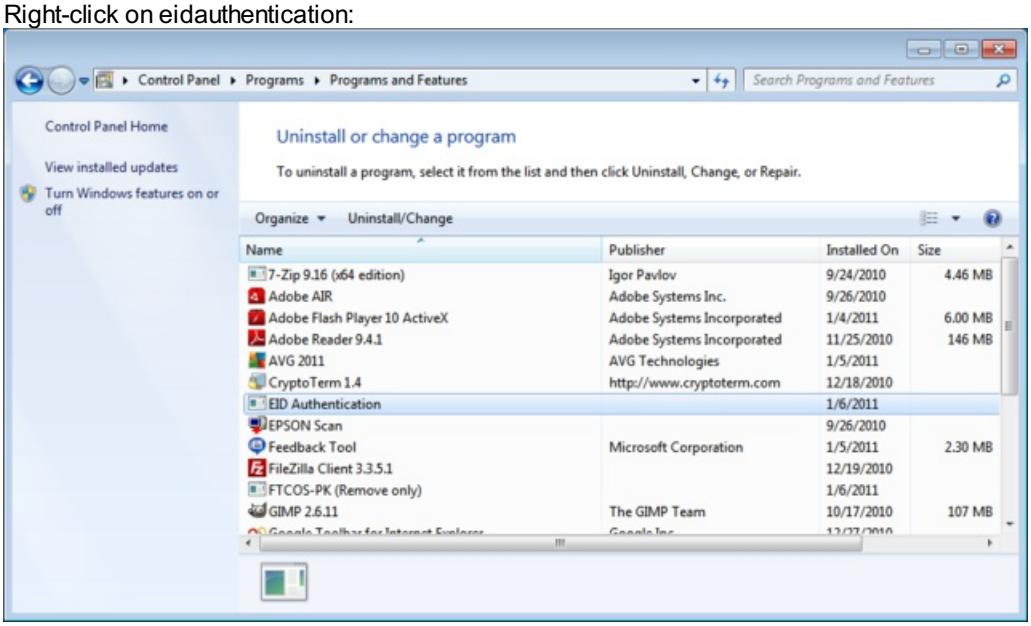


After installation, click the Reboot button.

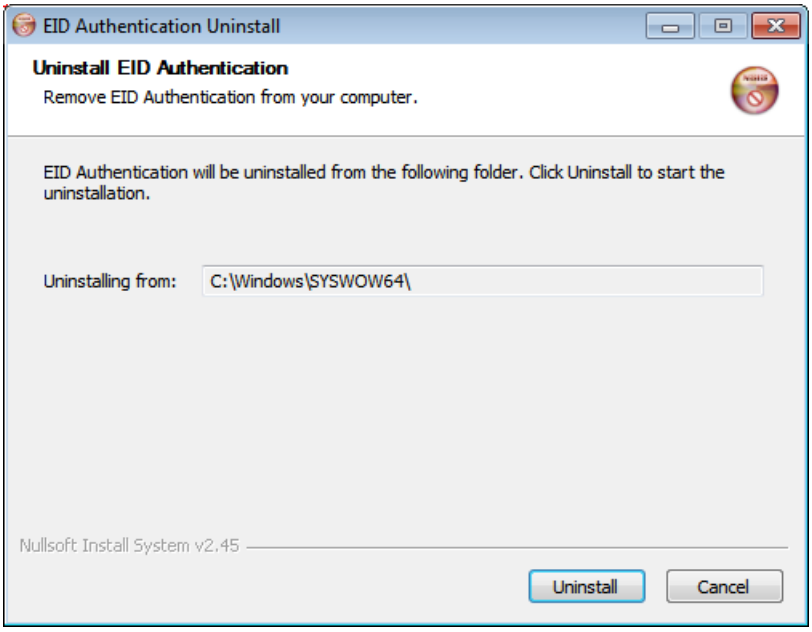
Uninstalling EIDauthenticate

In Control Panel, click Uninstall a program.

Right-click on eidauthentication:



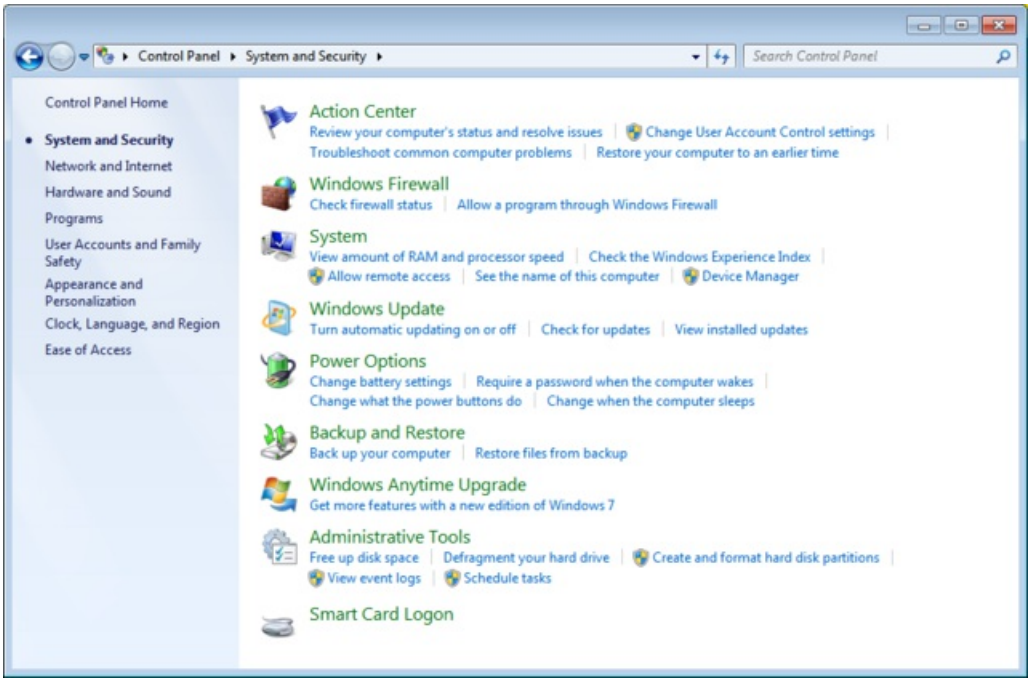
Click the Uninstal button, follow the process and reboot:



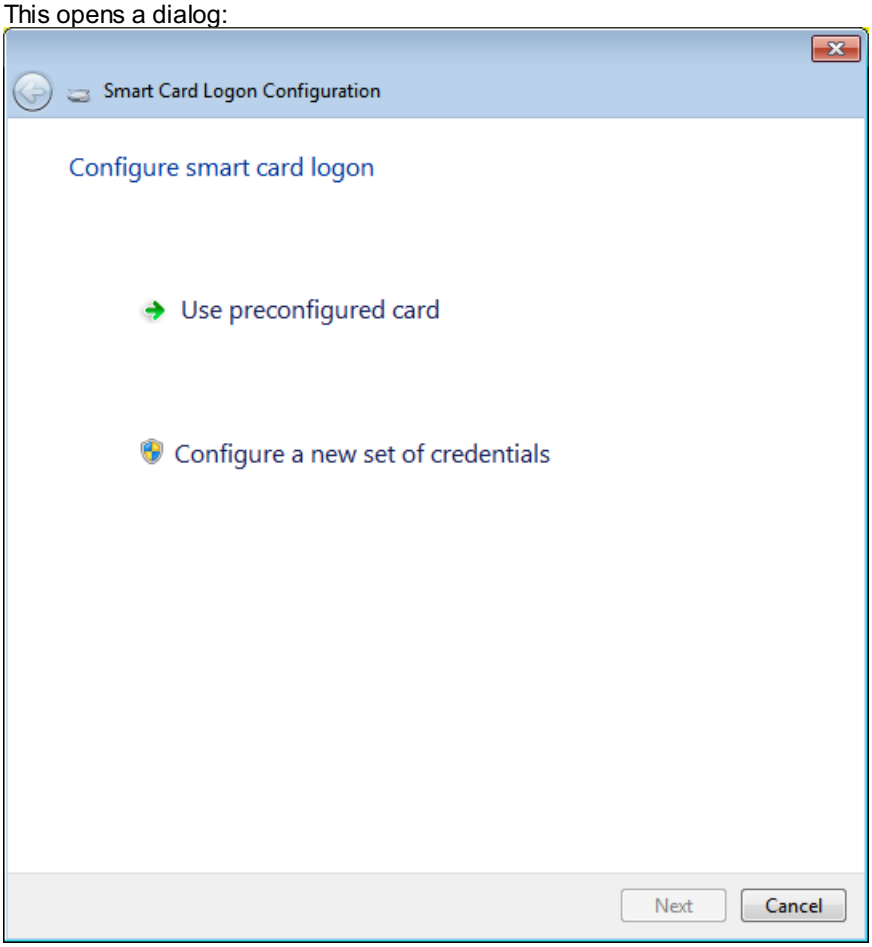
EIDauthentication configuration

Open the Control Panel and click on System and Security:

In the bottom, click the Smart Card Logon icon:



This opens a dialog:



Basically, there are two scenarios:

- Your smartcard / token is bank. Click on Configure a new set of credentials.
- Your smartcard / token contains certificates. Click on Use preconfigured card.

In the next page, we will demonstrate these scenarios.

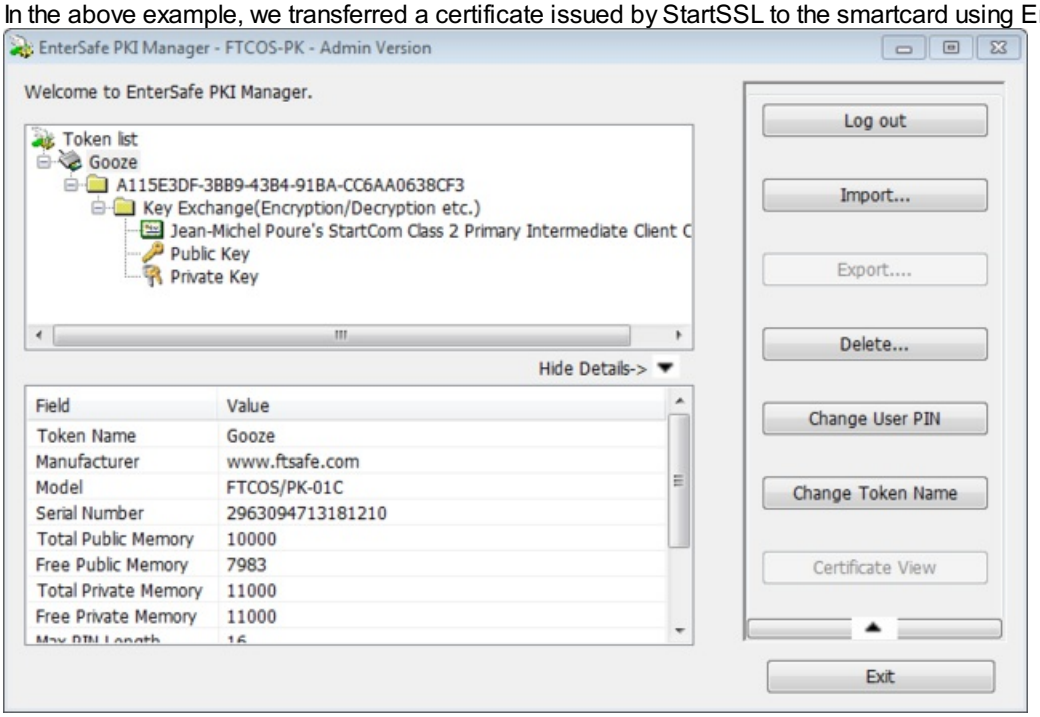
Scenario 1: Use a preconfigured card

In this sections, you should have your own PKI, including RSA key and X.509 certificate. Visit CAcert.org or StartSSL to create your own certificates. Using CAcert.org is recommended and covered in one of our guides.

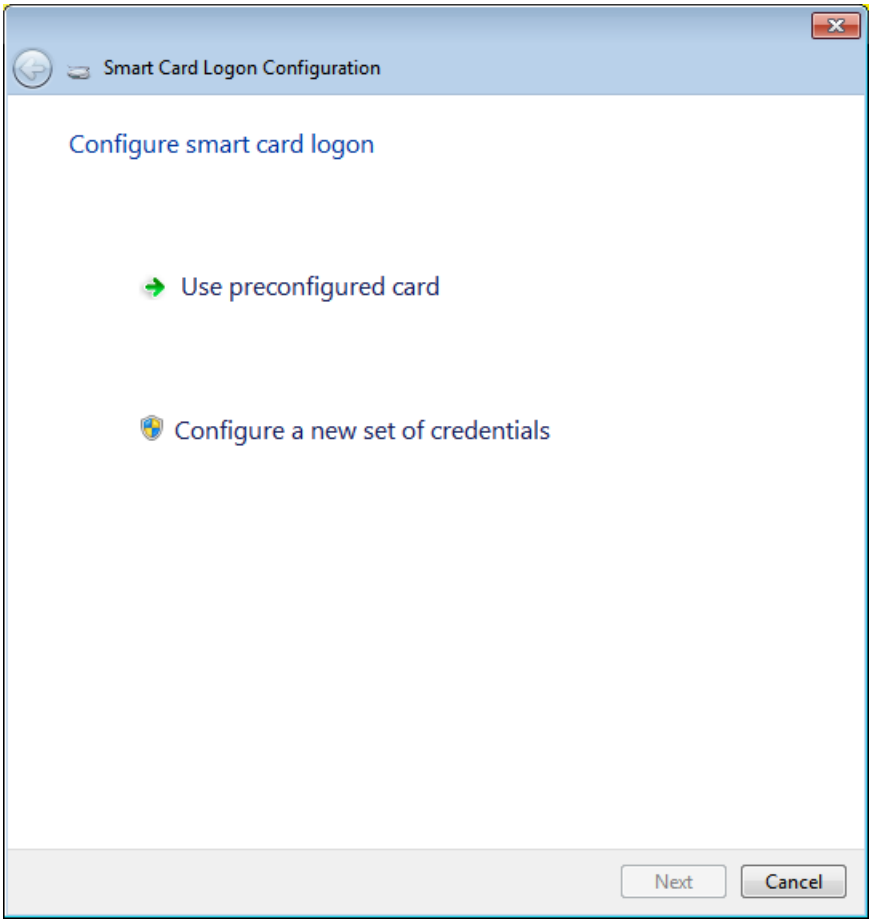
As a prerequisite:

- Your smarcard/token has been initialized using Feitian utilities.
- RSA keys and X.509 certificates have been transferred using Feitian utilities.

In the above example, we transferred a certificate issued by StartSSL to the smartcard using Entersafe PKI manager:

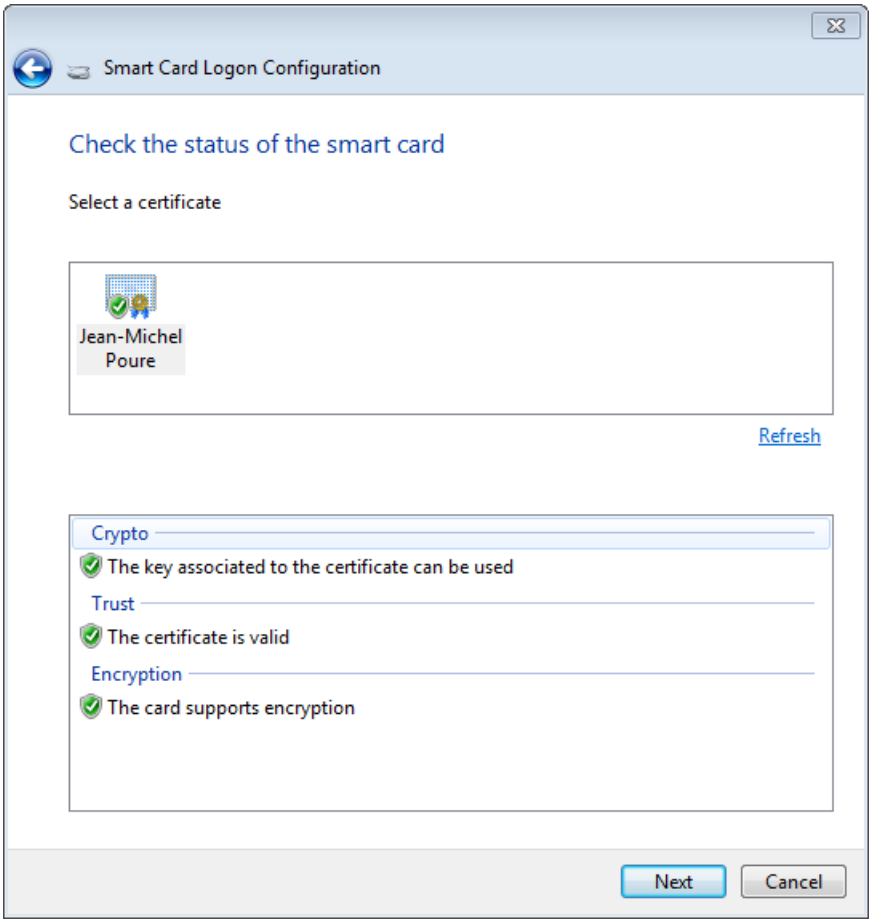


Now we are back to EIDauthenticate dialog:

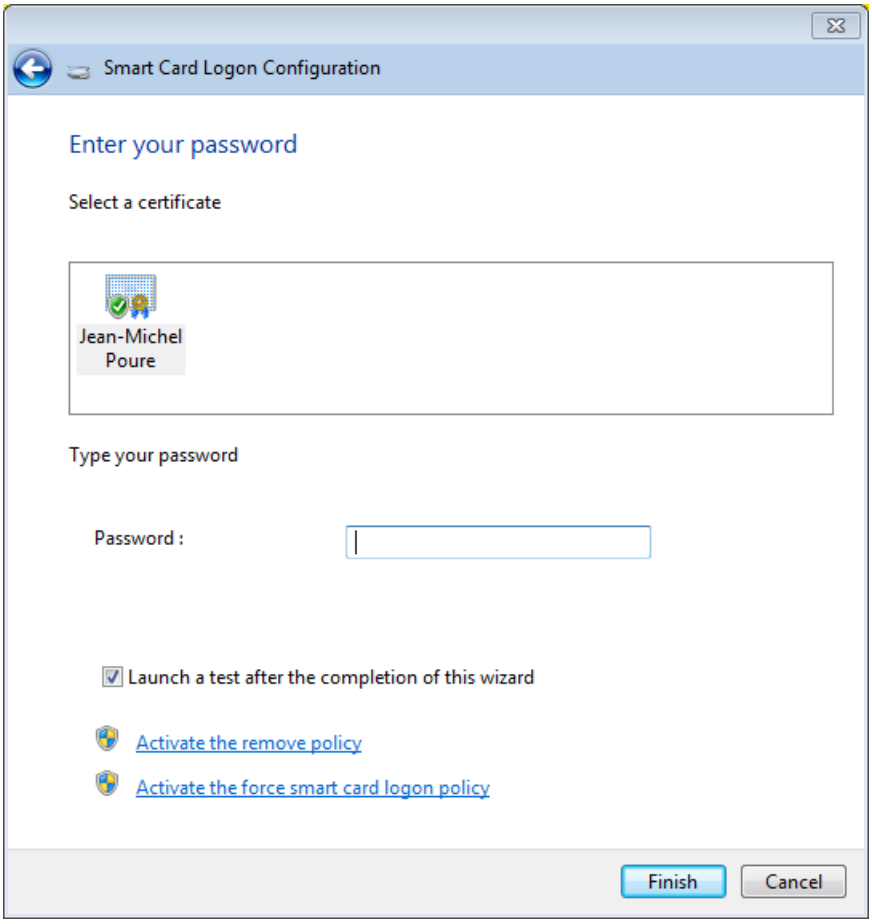


Click the "Use preconfigured card" button.

You may now check the status of your certificate:

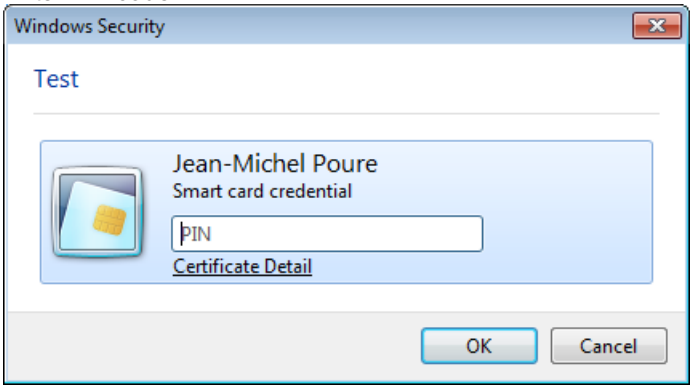


Click Next. The following dialog opens:

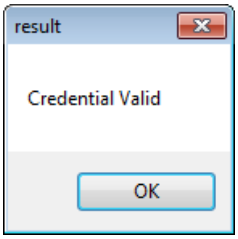


Enter your account password and enable "Launch a test" and click finish.

Enter PIN code:



The test is successful, your station is ready for smartcard logon!



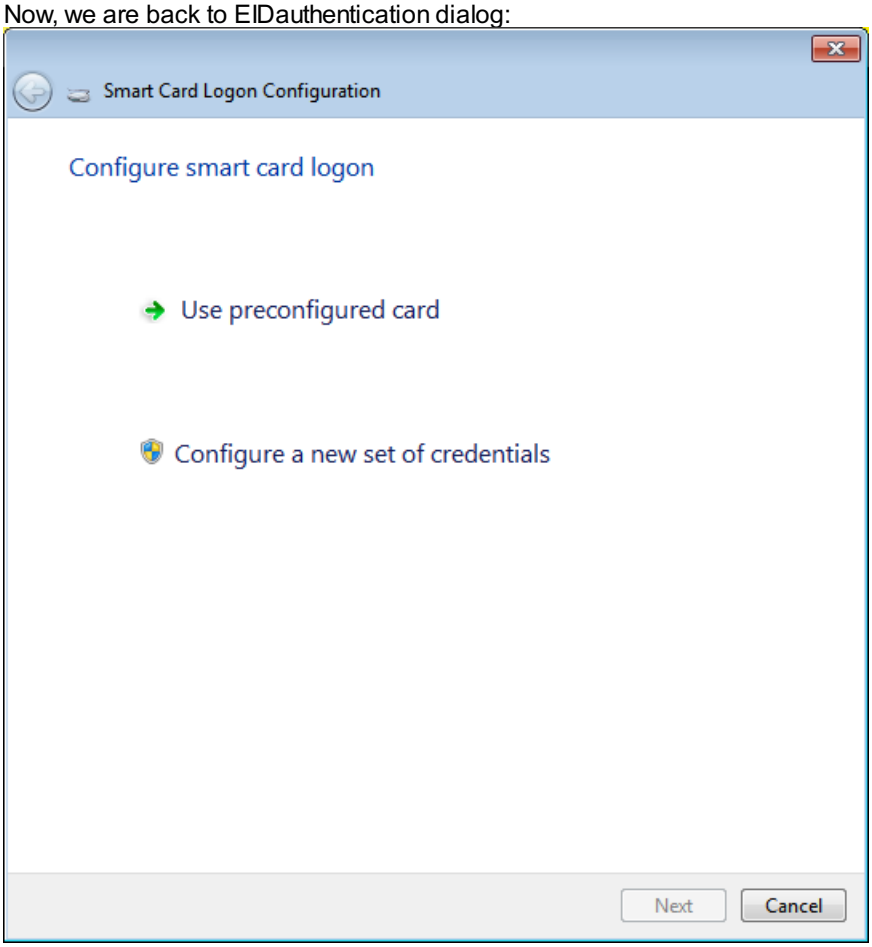
Scenario 2: Configure a new set of credentials

In this section, we will configure Windows smartcard logon using a blank card.

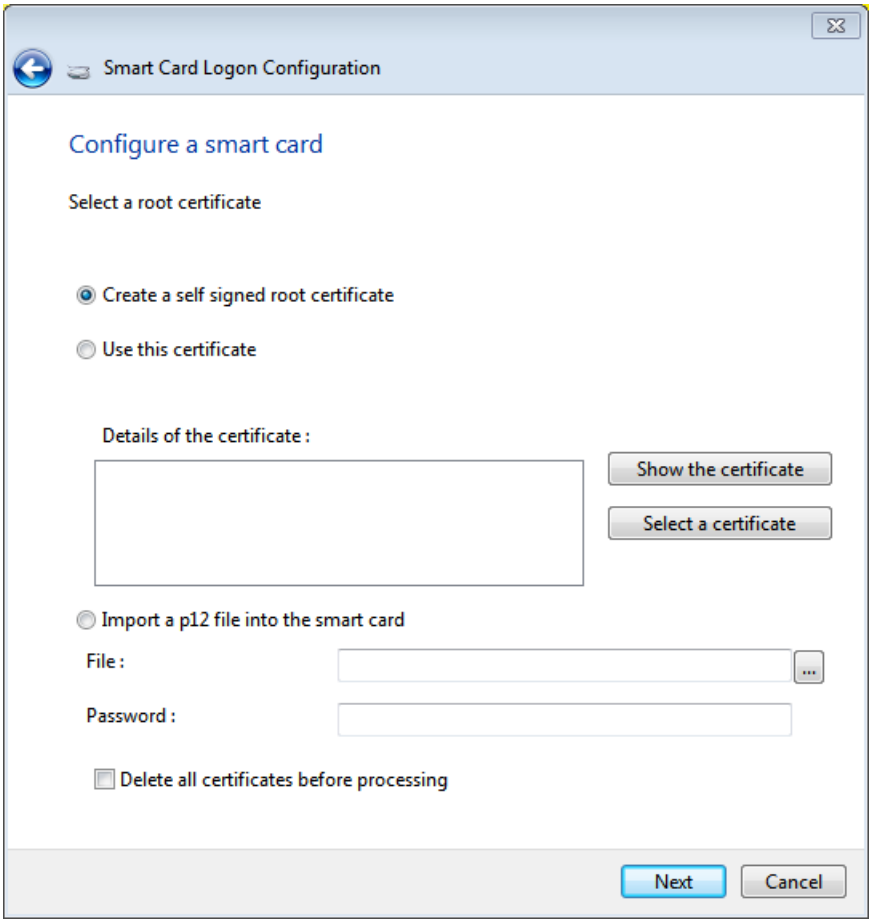
As a prerequisite:

- Your smarcard/token should be blank.
- Your smarcard/token has been initialized using Feitian utilities.

Now, we are back to EIDauthentication dialog:



Click Configure a new set of credentials:



You have three choices:

- First choice: **Create a self-signed certificate**

  Creating a self-signed certificate is a very neat feature of EIDauthentication, which allows to create your own Certificate Authority (CA) and certificates automatically.

  If you don't use an online Certificate authority like CAcert.org or StartSSL, choose this option.

- Second choice: **Use an existing certificate**

  The second option is to use a certificate stored on your computer.

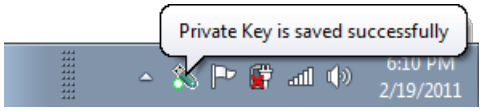
- Third choice: **Import a certificate in p12 format**

  The third option is to import a certificate on smartcard. It is very similar to using Feitian tools to import a certificate on smartcard.

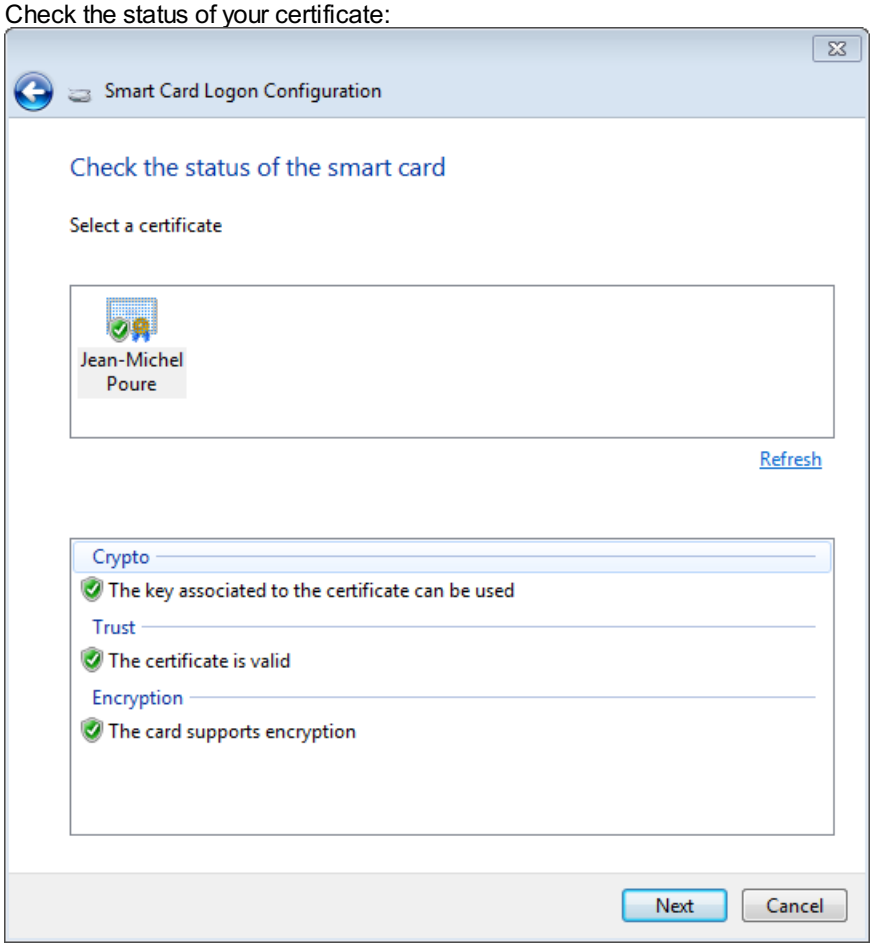
We choose to create a self-signed certificate. Other options are quite straighforward.

Click Create a self-signed certificate.
After entering PIN code, a self-signed certificate is created on your smartcard/token.

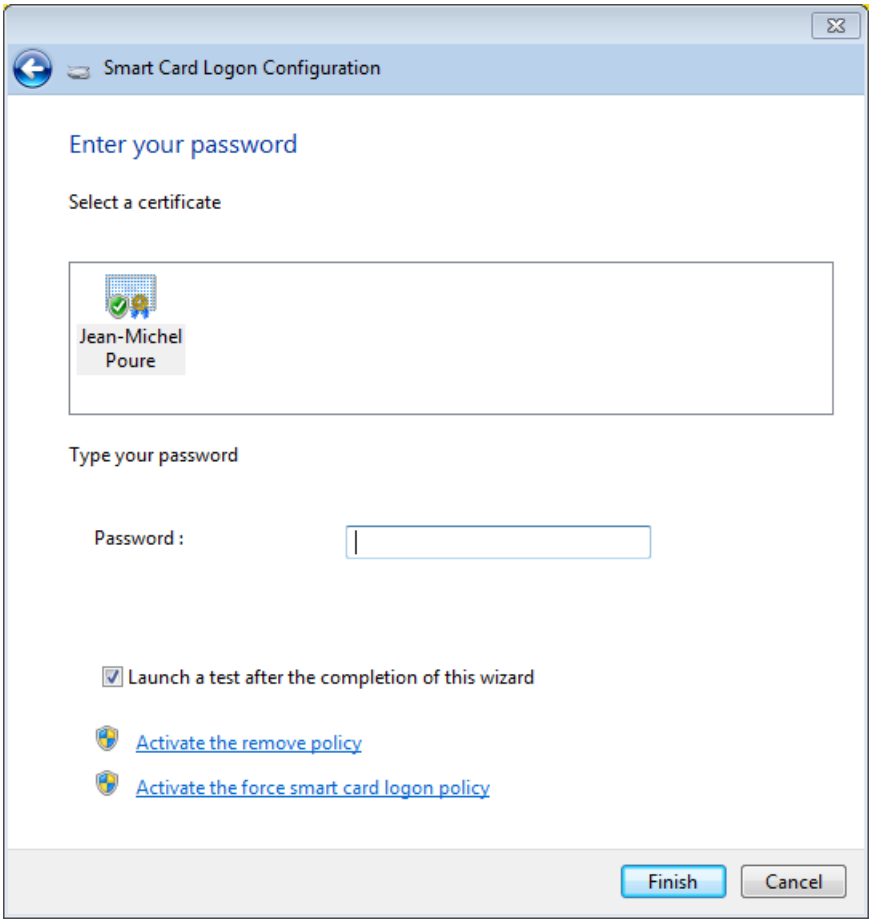
Please note that the certificates are created using the chip processor. Therefore it is a very secure option. After creation of certificate, a dialog is displayed in the menu bar:



Check the status of your certificate:

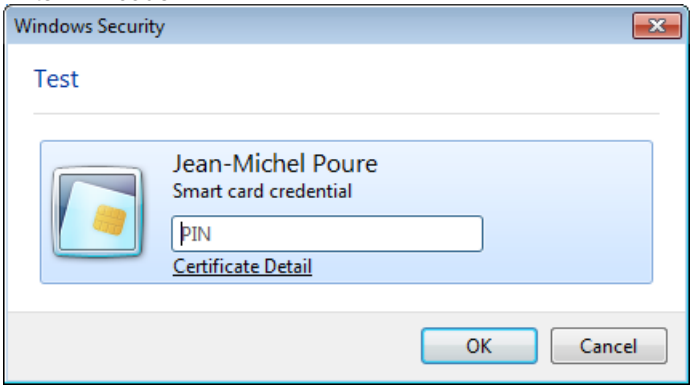


Click Next. The following dialog opens:

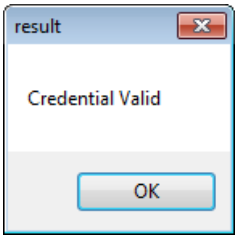


Enter your account password and enable "Launch a test" and click finish.

Enter PIN code:



The test is successful, your station is ready for smartcard logon!



Smartcard logon in action

Log off your Windows session and log on.

You should see this connection screen:

Enter your PIN code and you are connected.

Copyright GOOZE.EU 2011.

Source URL: http://www.gooze.eu/howto/windows-logon-using-smartcards

Links:
[1] https://sourceforge.net/projects/eidauthenticate/
[2] http://www.gooze.eu/howto/windows-logon-using-smartcards/eidauthentication-howto
[3] http://www.pgina.org
[4] http://sourceforge.net/projects/eidauthenticate/
[5] http://www.mysmartlogon.com/services.html
[6] http://www.gooze.eu/feitian-pki-card-ftcos-pk-01c
[7] http://www.gooze.eu/feitian-r-301-v2
[8] http://www.gooze.eu/catalog/smart-card-readers
[9] http://www.gooze.eu/howto/smartcard-quickstarter-guide/windows-installation