User Documentation for "NFC CSP Light"

Version 1.0

Prepared by: "Vincent Le Toux"

Date: 03/02/2014

Table of Contents

Table of Contents

MySmartLogon

Revision History

This section records the change history of this document.

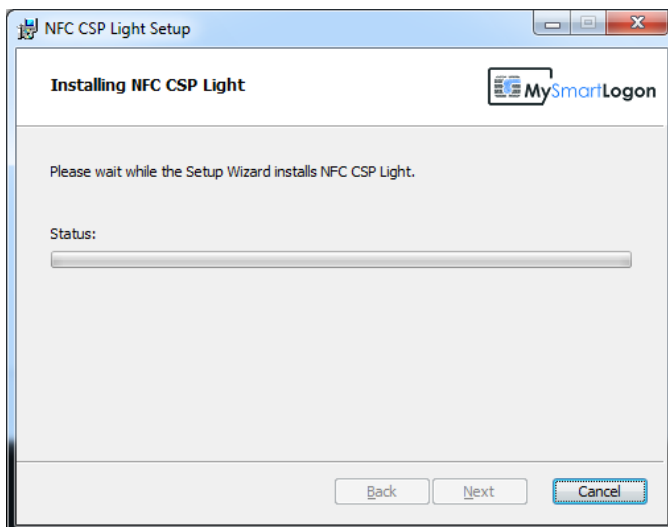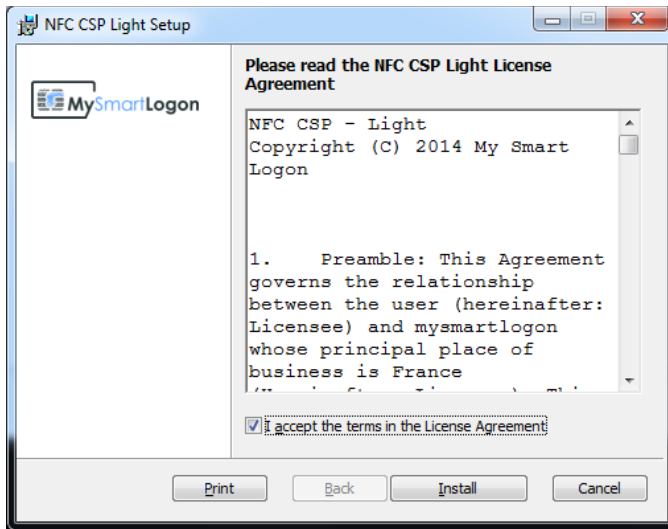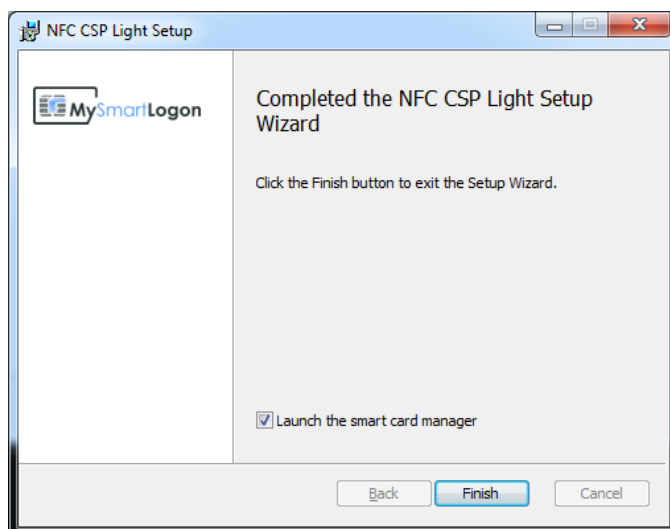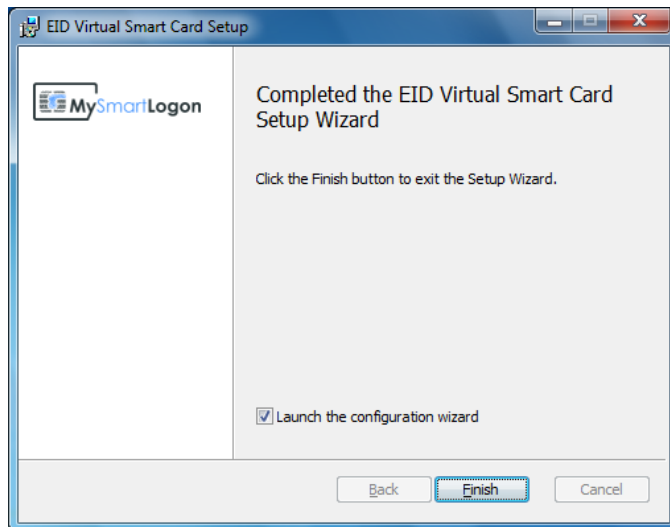| Name	Date	Reason For Changes	Version
Vincent Le Toux	03/02/2014	Creation	1.0

System Specifications

Operating system supported are :

- Windows XP, 2003, 8
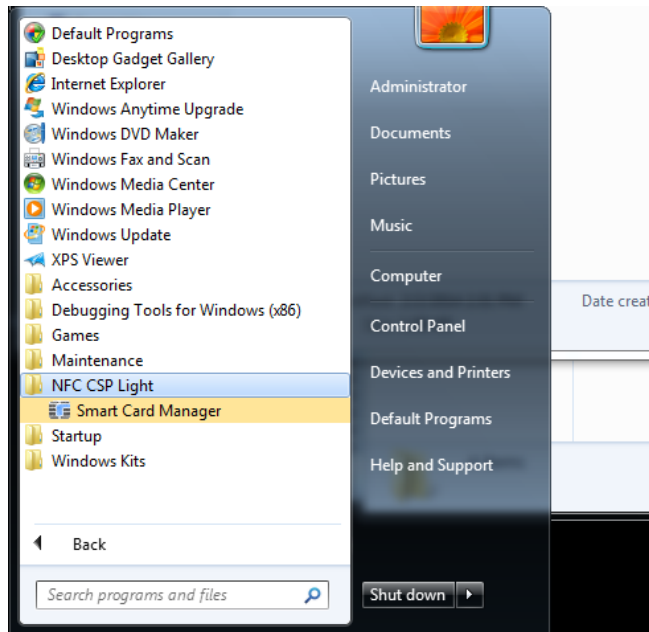- Windows Vista, Seven, 2008, 2012

Installing

Run the installer. The user performing the installation must have administrator privileges.

Launch the smart card manager

An Entry has been added by the installer to the start menu :

You can launch the "Smart Card Manager" to create a new Virtual Smart card.

Manage NFC Virtual Smart Card

You can launch the "Smart Card Manager" to edit the content of your smart card or any CAPI compliant tool, like Internet Explorer or the mmc certificate snap-in. In this documentation, only the "Smart Card Manager" will be described.

Run the "Smart Card manager" using its shortcut in the start menu. When launched, the manager will try to read a virtual smart card. The following dialog can be showed if there are no NFC tag present.
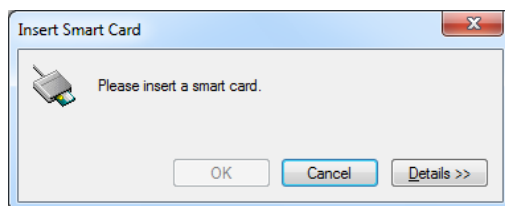

Press Details to get more information and wait for a compatible NFC tag.
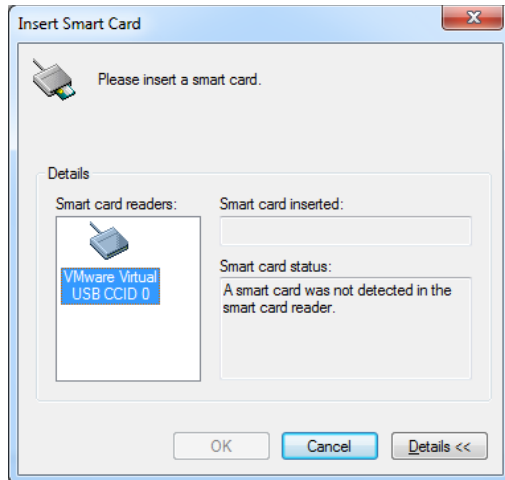
Important : if you see "*Smart card inserted : Unknown*", the NFC tag is missing its registration. If the tag is compatible and if the tag is still connected to the reader, the registration dialog will be shown after Cancel has been pressed. This procedure requires to run the program as administrator.
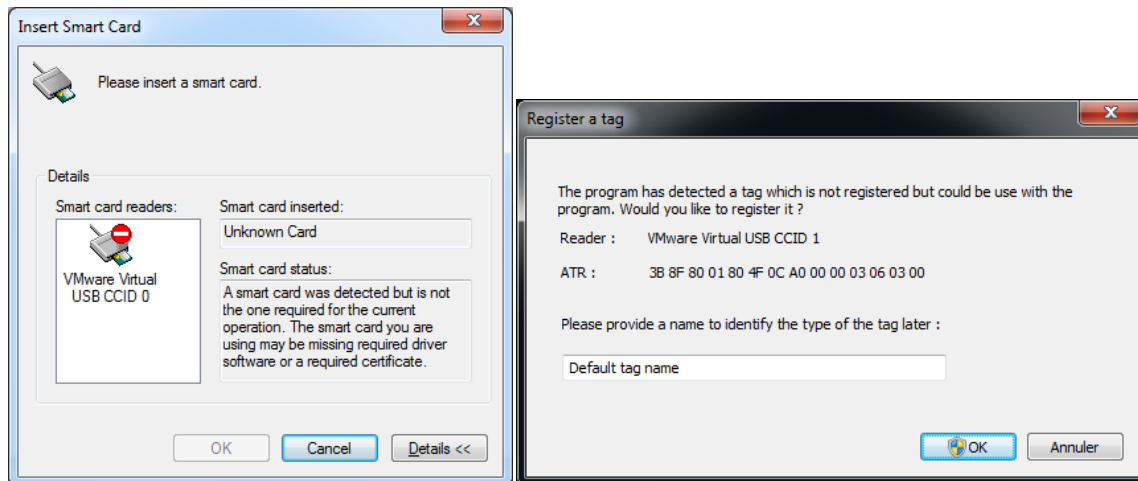

When a registered tag has been found, the OK button will become enabled. Press OK to continue. In our example, we used a Mifare 1k tag.

MySmartLogon
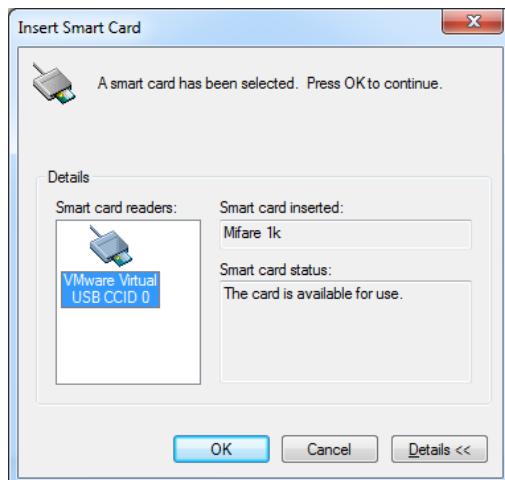
If a tag which has not being already configured is being read, the message "the smart card is empty" will be shown.

The smart card is empty
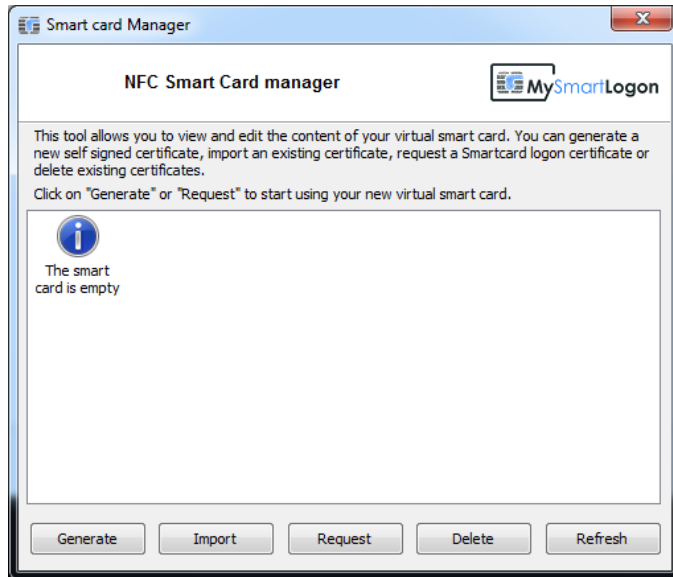
If you generate, import or request a certificate and if the PIN has not been set, the initialization dialog will be shown.
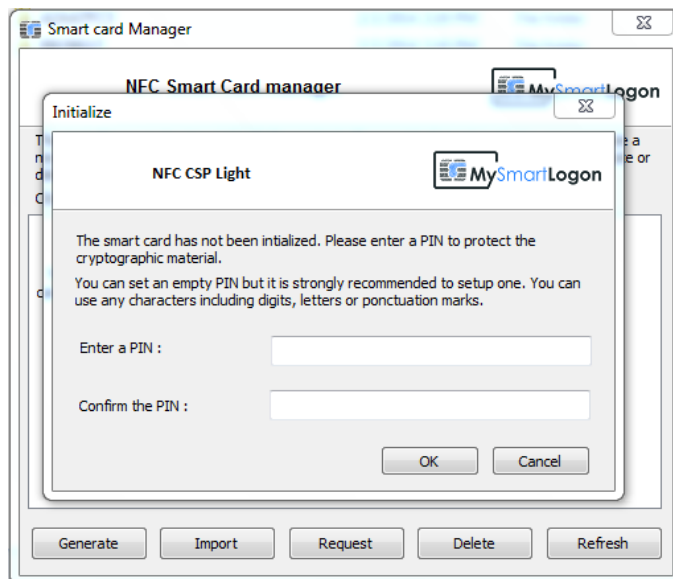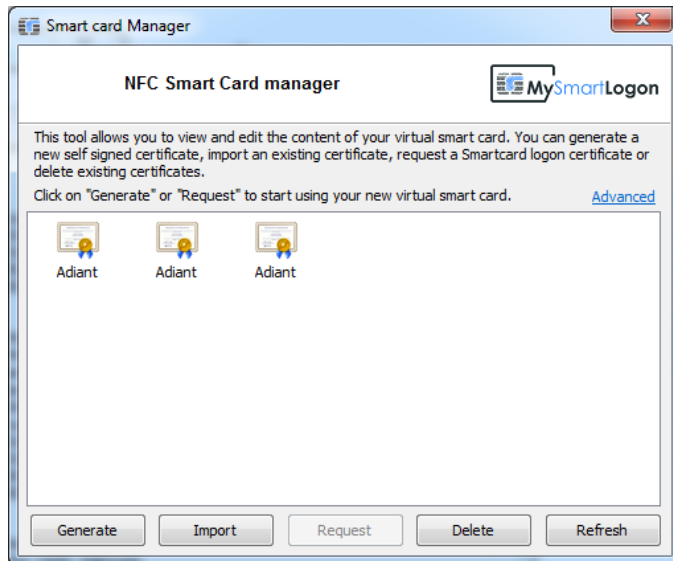

Enter twice the PIN and the NFC tag will be initialized as a virtual smart card.

Note: the PIN can be empty, but it is recommended to setup a PIN to mitigate software attacks.

Once a NFC tag has been configured, the Smart card manager displays each certificate it has found.
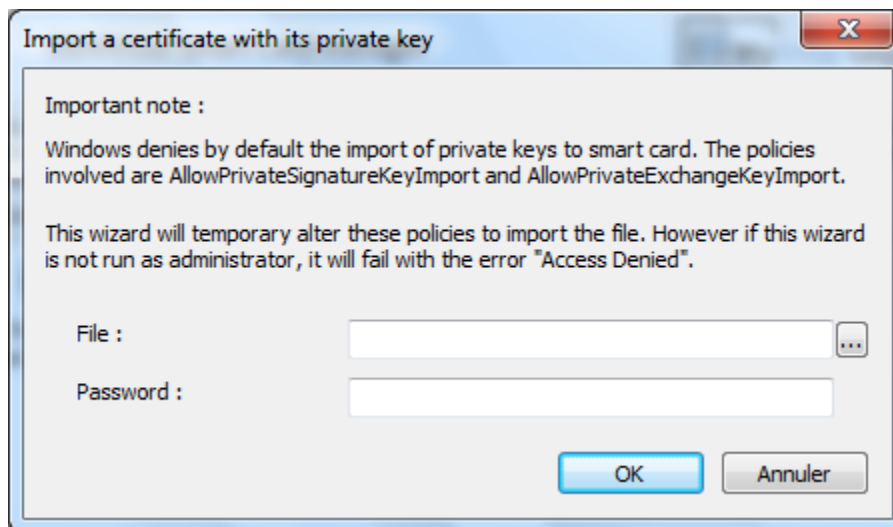
Generate

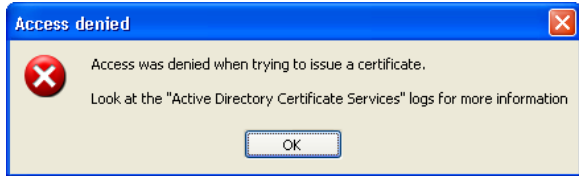This button will create a self signed certificate. The key length used is 2048 bits.

Import

This button will import a p12 or pfx file. A p12 file includes a set of one certificate and the associated public / private key pair. This file is protected by a password.
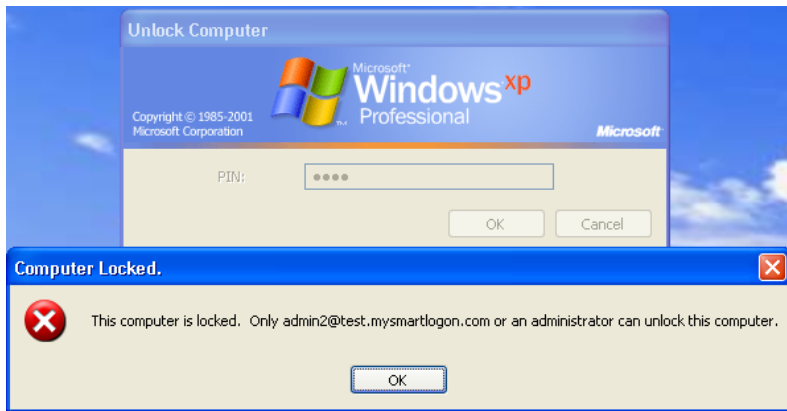

Request

This button will request a smart card logon certificate on behalf of the current user from the certificate authority installed on the active directory if it has been installed. The key length is 2048 bits.

Note : The *Enterprise PKI* component must be installed and the user MUST have the right to request a certificate using the template *Smart Card Logon* else an error message will be shown.

MySmartLogon

Access denied

Access was denied when trying to issue a certificate.

Look at the "Active Directory Certificate Services" logs for more information

[OK]

On Windows XP, the certificate requested for the smart card logon MUST be the first certificate displayed. If the first certificate has not been requested for smart card logon, the login will fail.

Unlock Computer

Microsoft
Windowsxp
Professional

Copyright © 1985-2001
Microsoft Corporation

Microsoft

PIN: ●●●●

[OK] [Cancel]

Computer Locked.

This computer is locked. Only admin2@test.mysmartlogon.com or an administrator can unlock this computer.

[OK]

Delete

This button will delete the selected certificates and their associated private keys. This operation can't be cancelled.

Refresh

This button will refresh the screen if modifications outside of this tool has been done.

Test the compatibility of a NFC card reader

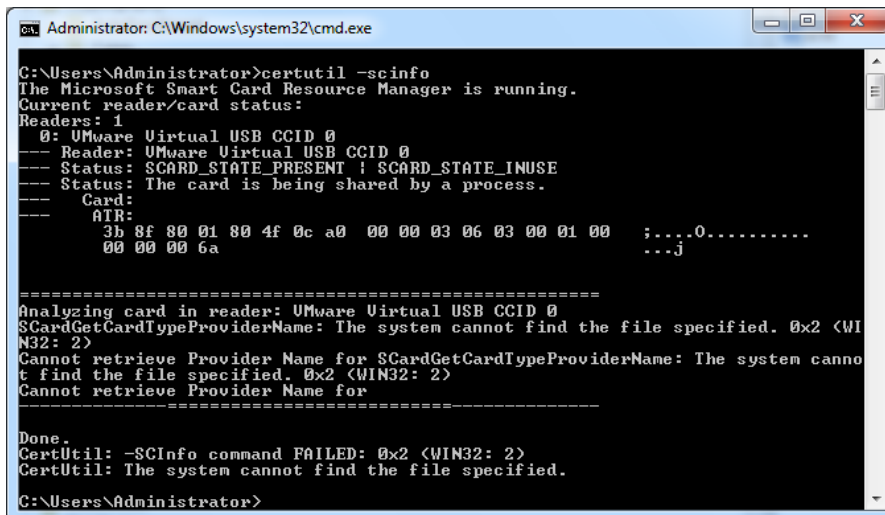The following tests need that the NFC card reader is plugged, and that a NFC tag is ready to be read.

1. Test the existance of a PCSC reader

You can test the presence of a minidriver or a CSP by running the command "certutil - scinfo".

Certutil.exe is a diagnostic tool provided by Microsoft and is installed by default since Windows Vista and Windows 2003. It must be installed on Windows XP using the Windows Server 2003 Administration tool pack.

Positive test

There is a smart card (SCARD_STATE_PRESENT) and the ATR is not empty (3b 8f 80 ... 00 6a)

Negative test

If the smart card resource manager is not running, the following message will be shown :

If the smart card reader is empty, aka if the token is not recognized, or if there are other readers (in this case our product EIDVirtual) the following output will be produced :

2. Test for the APDU used to catch the card ID

Retrieve the program scarddemo from codeproject.com and run it.

Select the reader you want to test, then click on Open. The connection should succeed if the previous steps were successful.

Enter the APDU "FFCA000000" and click on APDU.

Positive test

The zone bellow the APDU field must change and its content must be terminated by (9000). The unique ID of the card tested (a Mifare 1k) is FD4D0A31.
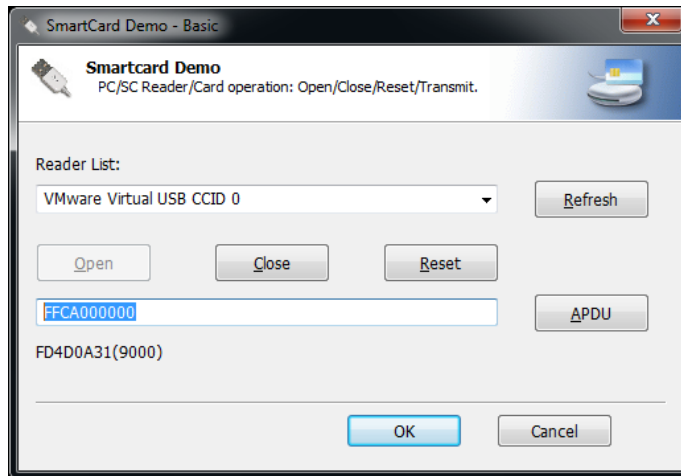
Negative test

The field bellow the ATR field is not changed. It is like nothing happened. This is related to the fact that the first byte of the APDU (FF), is an escape command which is in this case not understood by the smart card reader.
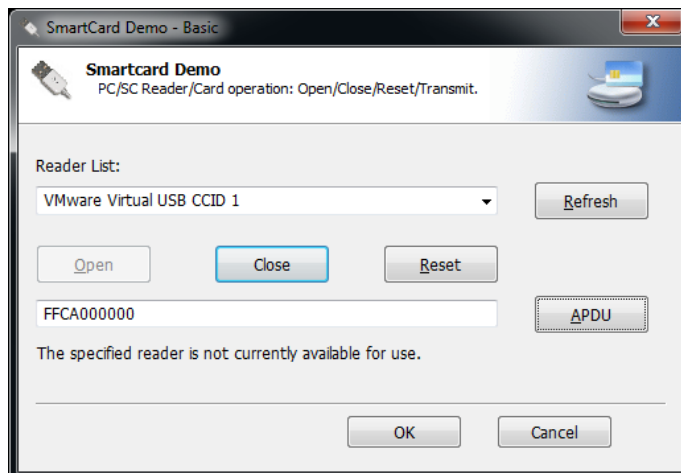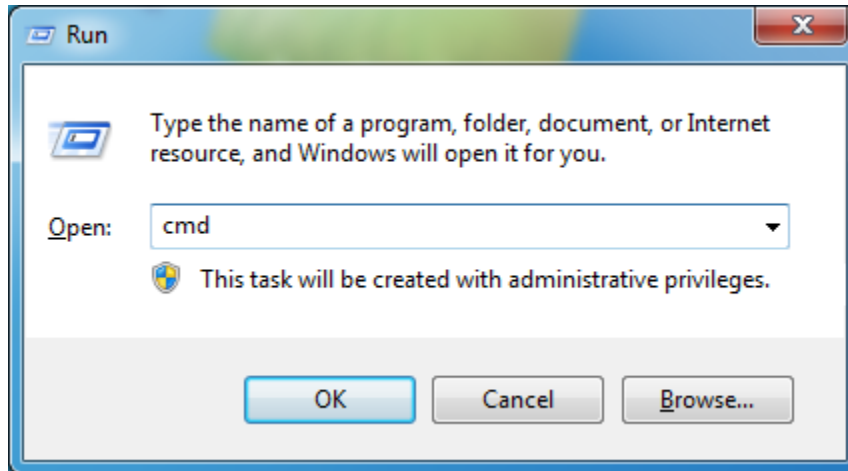
Troubleshooting

Using certutil

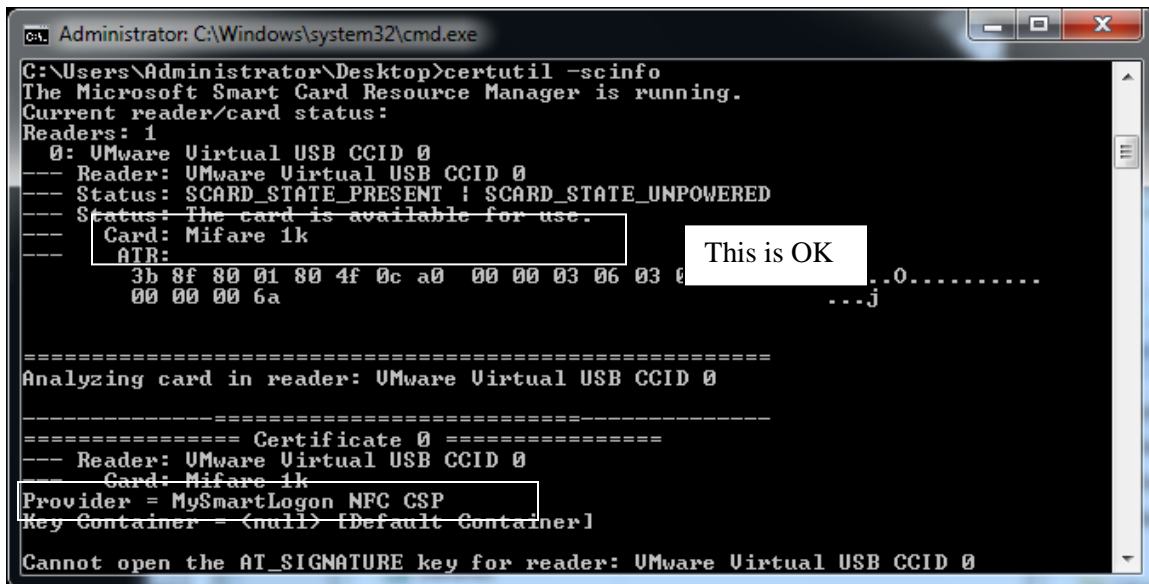Certutil is a troubleshooting tool edited by Microsoft.

Note : certutil.exe is installed by default starting Windows Vista and Windows 2008. Certutil can be installed on Windows XP by the package "WindowsServer2003-KB304718-AdministrationToolsPack"

You can run certutil by typing Windows +R

Then "cmd" then "certutil -scinfo"

Expected diagnostic of a healthy virtual smart card
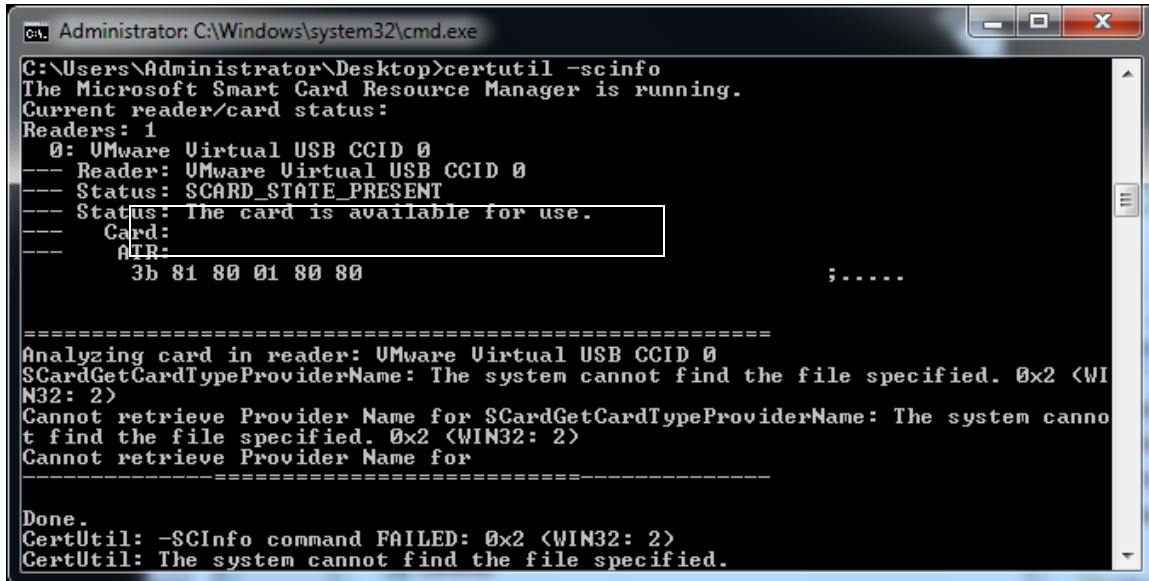

The previous screenshot shows an <u>empty</u> smart card

The smart card is recognized by Windows because the Card name is not empty.

Also the CSP is well set becasue the Provider is "MySmartLogon NFC CSP".

NFC tag unrecognized

A tag not recognized by the system will produce the following output :

(Look at empty card name)

In this case, the smart card configuration is missing.

Solutions:

Launch the registry editor:
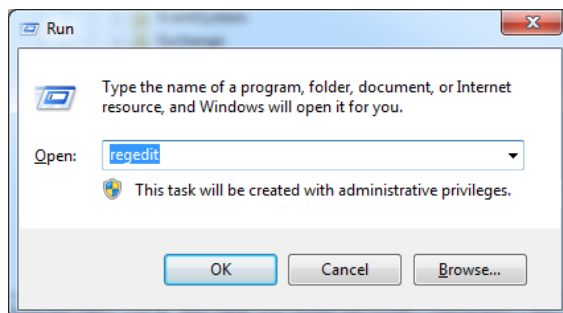
Go to SOFTWARE\Microsoft\Cryptography\Calais\SmartCards and create the following registry keys :

Name	Type	Data
(Default)	REG_SZ	(value not set)
ATR	REG_BINARY	3b 81 80 01 80 80
ATRMask	REG_BINARY	ff ff ff ff ff ff
Crypto Provider	REG_SZ	MySmartLogon NFC CSP

Copy paste the ATR data which MUST be the same than displayed by certutil.
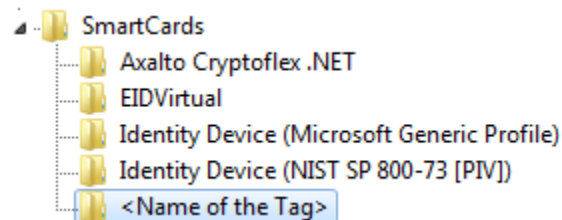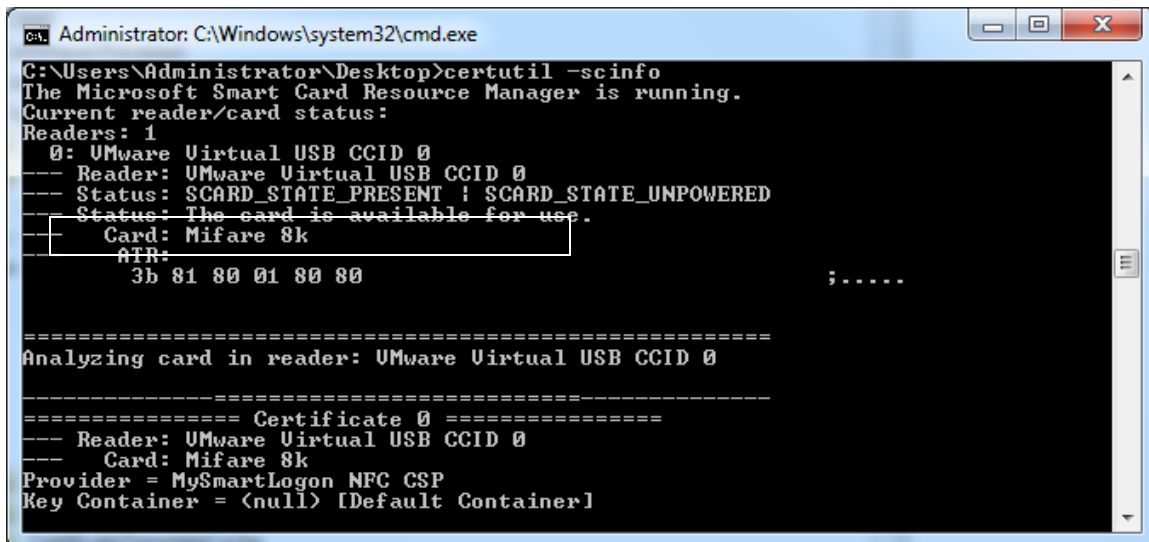
Then complete the ATRMask. The lenght must be exactly the same than the ATR.

On x64 system, proceed the same on the following registry key :

SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards

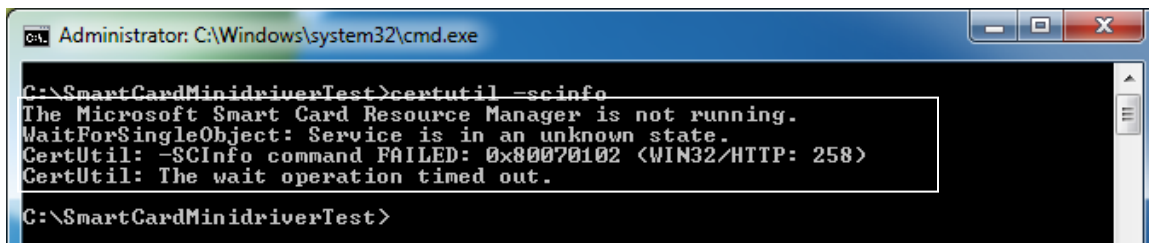The certutil output will change and display the name of the Tag.

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator\Desktop>certutil -scinfo
The Microsoft Smart Card Resource Manager is running.
Current reader/card status:
Readers: 1
  0: VMware Virtual USB CCID 0
--- Reader: VMware Virtual USB CCID 0
--- Status: SCARD_STATE_PRESENT | SCARD_STATE_UNPOWERED
--- Status: The card is available for use.
--     Card: Mifare 8k
         ATR:
         3b 81 80 01 80 80                                        ;.....


===========================================
Analyzing card in reader: VMware Virtual USB CCID 0

------------------------------------------
================ Certificate 0 ================
--- Reader: VMware Virtual USB CCID 0
---     Card: Mifare 8k
Provider = MySmartLogon NFC CSP
Key Container = <null> [Default Container]
```

The smart card resource manager is not running

If the Virtual Smart Card reader is not loaded or if the smart card service is not runing, the following error will be showed :

```
Administrator: C:\Windows\system32\cmd.exe

C:\SmartCardMinidriverTest>certutil -scinfo
The Microsoft Smart Card Resource Manager is not running.
WaitForSingleObject: Service is in an unknown state.
CertUtil: -SCInfo command FAILED: 0x80070102 (WIN32/HTTP: 258)
CertUtil: The wait operation timed out.

C:\SmartCardMinidriverTest>
```

Causes :

- The "Smart card" service has been disabled
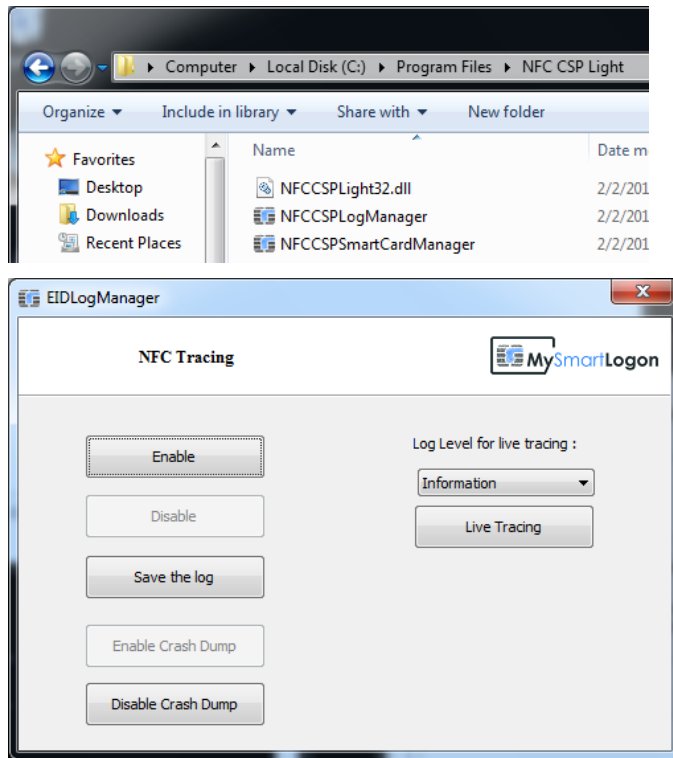- The smart card reader has been installed

Solutions

- Go to "service" (administrative tools), find the service and start it
- Reinstall the program
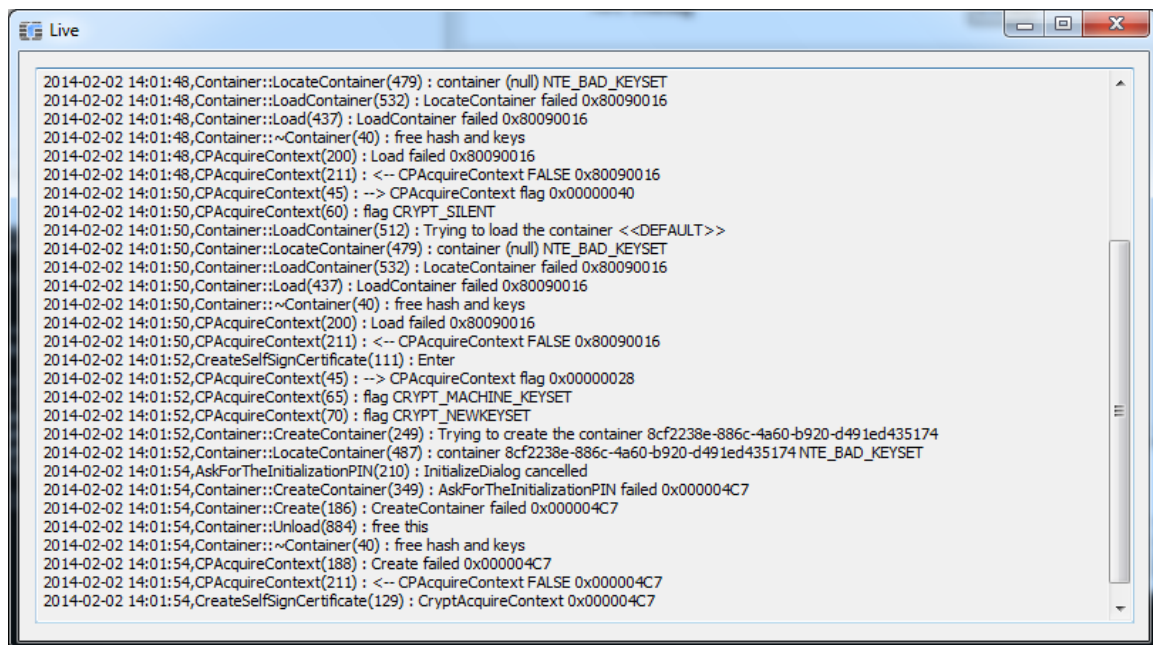
![MySmartLogon logo]

Using NFCCSP Trace

By default the Tracing tool named "EIDVirtualTrace" is installed in "C:\Program Files\NFC CSP Light"


You can record a trace by clicking on "Enable", doing some actions, then click on "Save the log".

Or you can view live tracing.

A recorded trace is the preferred way when contacting the support.

If the live trace can't start, you may have not the permission to run ETW (event tracing). This happens in large organization were permissions are restricted. You can run Process Monitor on the tracing process to look for errors.
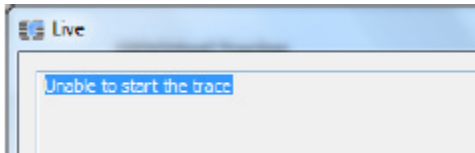
Troubleshooting the setup

You can run the msi tracing procedure :

msiexec /i EIDVirtualpackage.msi /L*v log.txt