

User Documentation for EIDVirtual

Version 1.3

Prepared by: "Vincent Le Toux" Date: 21/02/2013



Table of Contents

Table	of	Contents

Revision History

System Specifications
Installing4
Create a virtual smart card
Manage Virtual Smart Card11
Generate12
Import
Request
Delete
Refresh13
Activation
PIN Change
On Windows Vista / Seven / Windows Server 2008 and Windows Server 2008 R2
On Windows XP / Windows 2003
Deployment on Active Directory
Creation of a MST file
Creation of a transformation
Disable the launch of the configuration wizard after the installation
Insert the serial number
Activate automatically
Optionally install only the minidriver
Save the MST file
Deployment of the MSI
Edit a group policy
Create a new package
Troubleshooting
Using certutil
Using EIDVirtual Trace27
Troubleshooting the setup



Revision History

This section records the change history of this document.

Name	Date	Reason For Changes	Version
Vincent Le Toux	21/02/2013	Creation	1.0
Thierry Martin	28/03/2013	Update	1.1
Vincent Le Toux	26/04/2013	Update to 1.0.1.0	1.2
Vincent Le Toux	22/07/2013	Improved the troubleshooting paragraph	1.3
Daniel Bhatoa	24/09/2015	Minor adjustments to troubleshooting	1.4



System Specifications

Operating system supported are:

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

On Windows XP and Windows 2003, the "Microsoft Base Smart Card Cryptographic Service Provider Package" must be installed before. It can be downloaded here:

http://www.microsoft.com/en-us/download/details.aspx?id=4670

Installing

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

🛃 EID Virtual Smart Card Setu		
	Welcome to the EID Virtual Smart Card Setup Wizard	
	The Setup Wizard will install EID Virtual Smart Card on your computer. Click Next to continue or Cancel to exit the Setup Wizard.	
	Back Next Cancel	



🖶 EID Virtual Smart Card Setup	
End-User License Agreement Please read the following license agreement carefully	
EID Virtual Smart Card - Enterprise E Copyright (C) 2009-2013 My Smart Logo	Edition 🔺
 Preamble: This Agreement govern relationship between the user (herein Licensee) and mysmartlogon whose prin place of business is France (Hereinaf Licensor). This Agreement sets the terrights restrictions and obligations I accept the terms in the License Agreement 	ns the nafter: ncipal fter: erms, on using
Print Back Next	t Cancel
븅 EID Virtual Smart Card Setup	×
EID Virtual Smart Card Setup Product Features Select the way you want features to be installed.	
EID Virtual Smart Card Setup Product Features Select the way you want features to be installed. Please select the feature to install.	MySmartLogon
Image: Big EID Virtual Smart Card Setup Product Features Select the way you want features to be installed. Please select the feature to install. Image: BIDVirtual Image: Virtual smart card minidriver only (for experts) This feature is designed for remote servers accessed by the RD installs the virtual smart card minidriver without the other programmer of the server s	P protocol only. It ams or the virtual

Note: the following dialog is not showed on Windows Home Editions or if the minidriver only is installed



🛃 EID Virtu	al Smart Card Setup
Serial nu	umber
1	A license must be purchased for use in Windows 'Server', 'Enterprise' or 'Professional' Editions.
	Please enter the serial number as found in your invoice. Serial Number :
•	If you don't have a serial number, you can evalute this software for 30 days. Don't forget to activate the software else it will stop working after the evaluation period.
	Back Next Cancel





EID Virtual Smart Card Setup	
Installing EID Virtual Smart Card	
Please wait while the Setup Wizard installs EID Virtual Smart Card.	
Status:	
<u>B</u> ack	Next Cancel

During the installation, 2 device drivers must be installed.

You must click on Install.

Windows Security
Would you like to install this device software? Name: EIDVirtual Smart cards Publisher: Vincent Le Toux
Always trust software from "Vincent Le Toux".
You should only install driver software from publishers you trust. <u>How can I</u> <u>decide which device software is safe to install?</u>



Windows Security
Would you like to install this device software? Name: MySmartLogon Smart card readers Publisher: Vincent Le Toux
Always trust software from "Vincent Le Toux". Install Don't Install
You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

On Windows XP, if the driver signing is activated (not by default) the following warning could be shown. You must click on "Continue Anyway".

Hardwa	re Installation
1	The software you are installing for this hardware: EIDVirtualSmartCardReader Device has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.) Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
	Continue Anyway



🛃 EID Virtual Smart Card Setu	ap qu
	Completed the EID Virtual Smart Card Setup Wizard
	Click the Finish button to exit the Setup Wizard.
	Launch the configuration wizard
	Back Einish Cancel

Create a virtual smart card

Entries has been added by the installer to the start menu:



You can launch the "Configuration Wizard" to create a new Virtual Smart card.



EIDVirtual Smart Card Configur	ration Wizard	×	
EIDVirtual Configura	ation Wizard	MySmartLogon	
Please select (or insert) a removable device, choose a strong PIN then click on Format.			
A secure container will be created allowing the emulation of a smart card. This virtual smart card can be used to store a certificate. You will be ready to sign, encrypt your data or authenticate yourself.			
Drive	e: 🔻	Clear the card	
The PIN must be 4 digits long but we are recommending 8 digits to be resistant to offline attacks.			
PIN	12345678]	
You can enable an Admin Key to unblock the card if you lost the PIN. This feature is recommended for security professionals only.			
Enable Ad	dmin Key		
Admin Key	000000000000000000000000000000000000000	C	
	Form	at Cancel	

Insert a removable device and the letter associated to this device will be refreshed instantly.

Note: The "Drive" list is automatically updated when a new removable device is inserted.

Choose a PIN and click on Format.

Success	
()	Congratulation ! Your container has been succesfully configured.
	IMPORTANT: You MUST unplug and replug your usb key so the virtual smart card can be recognized.
	Would you like to launch the Smart Card manager ?
	Yes <u>N</u> o

Remove and insert the device again to trigger the container load.

Congratulation ! Your virtual smart card has been created.



Manage 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 virtual smart card present.

Insert Smart Card	
A smart card has	been selected. Press OK to continue.
Details	Smot and inseted:
	EIDVirtual
	Smart card status:
MySmartLogon Virtual Smart Card Reader 0	The card is available for use.

Important: if you see "Smart card inserted: Unknown", look at our troubleshooting section.

To continue further, you must insert a token previously formatted by the "Configuration Wizard". Note: if no virtual smart card reader is present, you can restart the "Smart Card" service.



📑 Smart card Manager	×
EIDVirtual Smart Card manager	MySmartLogon
This tool allows you to view and edit the content of your virtual smart new self signed certificate, import an existing certificate, request a Sm delete existing certificates.	card. You can generate a artcard logon certificate or
Click on "Generate" or "Request" to start using your new virtual smart	card.
Administrator	
Generate Import Request Dele	ete Refresh

Note: by default, no certificate is present and the following icon is showed:



Generate

This button will create a self signed certificate. The key length 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.



Import a certificate with its priv	vate key	×
Important note :		
Windows denies by default the import of private keys to smart card. The policies involved are AllowPrivateSignatureKeyImport and AllowPrivateExchangeKeyImport.		
This wizard will temporary alter is not run as administrator, it wi	these policies to import the file. Ho I fail with the error "Access Denied	owever if this wizard d".
File :		
Password :		
	ОК	Annuler

Important: by default importing a certificate is prohibited by the Windows default Policy. Don't forget to run the tool as administrator to import a file.

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* (the default template must be loaded, using a custom or duplicated template will not work).

In addition, each domain controller must have a valid "Domain Controller" certificate and a valid "Domain Controller Authentication" certificate.

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.



Activation

If EIDVirtual is free on Windows Home Editions, a license must be purchased on other Editions of Windows. EIDVirtual can be used as a trial for 30 days. After this period, all authentication attempts will be blocked.

Windows Security	J
Microsoft Smart Card Provider Please enter your digital signature PIN.	
PIN PIN Click here for more information	
😣 A wrong PIN was presented to the card	
OK Cancel	

You must activate EIDVirtual using the "Activation Wizard" and can launch this tool by its shortcut in the Start Menu:

Activation	×
This Wizard will activate EIDVirtual	
Step 1 : Enter the serial number of your product (you can find it on your invoice) Serial Number]
Step 2 : Choose to activate your product on line (in this case, the registration process will be done automatically) or off line (in this case, you will have to enter registration data manually)	
< Back Next > Car	ncel



You can activate the software Online of Offline.

Activation		×
Manual activation		Arten Kinda Billio Arten Billio
Go to http://downloa	ad.mvsmartlogon.com/activate.php, fill on the website	
the serial number an	d the challenge zones and copy back the response.	
Challenge	00426-068-3830275-86439]
Response]
	< <u>B</u> ack <u>N</u> ext > Ca	ncel

The following screen is show if the activation is successful.

Activation		×
The activa	ition was successful	
i	The activation was successful. Your serial number is :	
	1234567890	
	< <u>P</u> récédent Terminer Ann	nuler

This screen is also shown directly if the software has been previously activated.

Note: The activation wizard can also be run from the command line.



PIN Change

This procedure describes how to change the user PIN (not the admin PIN) of a smart card using the Microsoft Base Smart Card Cryptographic Provider.

On Windows Vista / Seven / Windows Server 2008 and Windows Server 2008 R2

Press Ctrl+Alt+Del and choose "Change a password"

 Lock this computer Switch User Log off 	×+
 Change a password Start Task Manager 	
Cancel	0 -

Click on "Other credentials"



Adiant
DId password
New password
Confirm password
Create a password reset disk
Other Credentials Cancel
Servindows ⁻⁷ Ultimate

Click on the icon which represents your smart card reader





Enter the old PIN, the new PIN and press Enter.

Smart card PIN change	
Enter your old PIN and your new PIN. PIN	
New PIN New PIN confirmation	
Other Credentials Cancel	
💐 Windows [:] 7 Ultimate	

Reference: http://msdn.microsoft.com/en-us/library/bb905527.aspx

On Windows XP / Windows 2003

Clic on start -> run then enter "pintool"

Smart Card PIN Tool	×
Change PIN Unblock	
To change your Smart Card PIN, enter the old PIN and the desired new PIN and press the 'Change PIN' button below.	
Old <u>P</u> IN	
New PIN	
Confirm New PI <u>N</u>	
Change Pin	
Close	;

Reference: <u>http://download.microsoft.com/download/f/4/f/f4f3c957-057c-4acb-b10c-bb6087045025/WSCFDepl.doc</u>



Deployment on Active Directory

Creation of a MST file

Creation of a transformation

Download and install Orca. The installer, Orca.msi, can be found in the Windows SDK.

Launch Orca and open the MSI file of EIDVirtual.

~	Orca			

Select Transform, New Transform.

Trar	sform	Tools	View	Help		
	New Tr	ansforn	n			
	Apply Transform					
	View Patch					
	Genera	te Trans	form			

Open the tables *Property*.

Tables	
MsiFileHash	
Property	
RadioButton	

Disable the launch of the configuration wizard after the installation

Disable the autorun by selecting the property *WIXUI_EXITDIALOGOPTIONALCHECKBOX* then right click, then *drop row*.

Add Row	Ctrl+R
Drop Row	

Insert the serial number

Enter the license by add a new property named *SERIALNUMBERPROPERTY* (tables -> Add Row).

Tab	es Transform	Tools	View	Help
	Add Table		Ctrl-	۰T
	Add Custom Ta			
	Drop Table			
	Add Row		Ctrl	⊦R

Enter the serial number as Value.



A	dd Row	×
Γ		
	Name	Value
	Property	SERIALNUMBERPROPERTY
	Value	
	Column	
	Value - Loo	calizable String[0], Required
	12345678	90
		OK Cancel

Activate automatically

Create a new property named ACTIVATEPROPERTY (tables -> Add Row) and set its value to 1.

Optionally install only the minidriver

Open the table *Feature*.

EventMapping Feature

FeatureComponents

Feature	Feature	Title	Description	Display	Level	Directo	Attribu
VirtualReader	DefaultFeat	Virtual smart card reader	This feature install the	2	2		0
Wizard	DefaultFeat	Configuration Wizard	This feature contains	8	2		0
Manager	DefaultFeat	Smart Card Manager	This feature contains	10	2		0
Activation	DefaultFeat	Activation Wizard	This feature contains	12	2		0
Shortcuts	DefaultFeat	Programs' shortcuts	This feature contains	14	2		0
DefaultFeature		EIDVirtual	This feature contains	1	1		16
MiniDriver	DefaultFeat	smart card minidriver	This features install th	4	1		0
Tracing	DefaultFeat	Tracing tools	This feature contains	6	1		0

Change the Level of all features except DefaultFeature, MiniDriver and Tracing from 1 to 2.

Note: Changing the *Level* disable the installation of these features if the *INSTALLLEVEL* property is not changed.

Save the MST file

Save the changes as *Transform* -> *Generate Transform* and save the MST file.

Transform	Tools	View	Help				
New T	New Transform						
Apply	Apply Transform						
View P	View Patch						
Genera	ate Trans	form					
Close	Transfor	m					



Deployment of the MSI

Edit a group policy

Select administrative tool then Group Policy management.

Choose the group policy which control the computers were you want to deploy the package.

🔜 Group Policy Management

- Forest: test.mysmartlogon.com
 - a 📑 Domains
 - ▲ i test.mysmartlogon.com
 - 🛒 Default Domain Policy
 - 🛒 MySmartLogon Policy
 - Domain Controllers
 - a 📑 Group Policy Objects
 - Default Domain Controllers Policy
 - Default Domain Policy
 - MySmartLogon Policy

Edit the policy by right clicking on the policy then choose *edit*.

Create a new package.

Select Computer Configuration, Policies, Software Settings, Software installation.



Choose the msi file of EIDVirtual.

Note: Don't forget that there are one msi per processor architecture.

Choose the advanced deployment method to configure the license.

Deploy Software						
Select deployment method:						
<u>P</u> ublished						
Assigned						
Advanced						
Select this option to configure the Published or Assigned options, and to apply modifications to a package.						
OK Cancel						



Select *Modifications* and add the MST file to customize the setup.

EID Virtua	Smart Card	Properties			? 🗙
General	Deployment	Upgrades	Categories	Modifications	Security
Modification	ations or transf to the packag	orms allow ye e in the orde	ou to customi r shown in th	ze the package e following list:	and are
Modific	ations:				
					M <u>o</u> ve Up lo <u>v</u> e Down
Ad	d	Remove			
Importa correct then cli	nt! Do not pres ly. For more inf ck What's this	ss OK until al ormation, rig ?	l transforms a ht-click on th	ire added and o e Modifications	rdered list box, and
			(ОК	Cancel



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

📼 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	cmd 🗸
	This task will be created with administrative privileges.
	OK Cancel <u>B</u> rowse

Then "cmd" then "certutil -scinfo"

Expected diagnostic of a healthy virtual smart card

Administrator: C:\Windows\system32\cmd.exe	
C:\SmartCardMinidriverTest>certutil -scinfo The Microsoft Smart Card Resource Manager is running. Current reader/card status: Readers: 1 Ø: MySmartLogon Virtual Smart Card Reader Ø Reader: MySmartLogon Virtual Smart Card Reader Ø Status: SCARD STATE PRESENT : SCARD STATE UNPOWERED Status: The card is available for use. Card: EIDVirtual, EIDVirtualSmartCard ATR: 3b 8c Ø1 4d 79 53 6d 61 72 74 4c 6f 67 6f 6e a5 ;MySmartLogon.	< III
Analyzing card in reader: MySmartLogon Virtual Smart Card Reader Ø Missing stored keyset Missing stored keyset 	
CertUtil: -SCInfo command FAILED: 0x80090016 <-2146893802> CertUtil: Keyset does not exist	
C:\SmartCardMinidriverTest>	Ŧ

The previous screenshot shows an <u>empty</u> smart card, without any certificate or private key stored (the KeySet does not exist)

(Look at the ATR and the mention "SCARD STATE PRESENT")



Virtual smart card not formatted or corrupted

A container not loaded will produce the following output:



(Look at the mention "SCARD_STATE_EMPTY")

In this case, the program has not found an USB having a secure container.

Causes:

- USB key not formatted
- Secure container copies from one USB key to another
- Secure container corrupted (probable cause: usb key removed without having warned the system)

Solutions:

- Run the configuration wizard to create a new container
- Run the log tool and check for errors related to corrupted container

The minidriver has not been installed

A minidriver (the driver of the smart card and not for the reader) not installed BUT with a container recognized will produce the following results:





An ATR entry, here present, means that a smart card (aka an USB key) has been inserted.

However the empty line for "Card" means that the system couldn't find a driver.



Also the "CALAIS" database in the registry won't show an entry for the virtual smart card.



Causes:

• The Plug&play manager didn't launch the installation of the driver at the installation

Solutions:

- 1. Open the program files folder and look for the EIDVirtual installation.
- 2. Search for .inf files
- 3. Right click on the inf file which name contains "minidriver" and select "install"

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 running, the following error will be shown:



Causes:

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

Solutions

- Go to "service" (administrative tools), find the service and start it
- Reinstall the program



Using EIDVirtual Trace

By default the Tracing tool named "EIDVirtualTrace" is installed in "C:\Program Files\EID Virtual Smart Card"

Log Level for live tracing :
Live Tracing

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

Or you can view live tracing.

Monitoring Active WndProcStep1(34) : Activate CMyDevice::IoSmartCardGetState(332) : [GSTA]IOCTL_SMARTCARD_GET_STATE SCARD_SWALLOWED CMyDevice::IoSmartCardGetState(332) : [GSTA]IOCTL_SMARTCARD_POWER SCARD_COLD_RESET CMySmartCardInterface::Reset(35) : INFO : Change state from 3 to 6 CMyDevice::IoSmartCardGetState(335) : [GSTA]IOCTL_SMARTCARD_GET_STATE SCARD_SPECIFIC CMyDevice::IoSmartCardGetState(335) : [GSTA]IOCTL_SMARTCARD_GET_STATE SCARD_SPECIFIC CMySmartCardInterface::FormatResponse(802) : INFO: return 9000 CMyDevice::IoSmartCardGetState(335) : [GSTA]IOCTL_SMARTCARD_GET_STATE SCARD_SPECIFIC CMySmartCardInterface::FormatResponse(802) : INFO: return 900	

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 <u>Process Monitor</u> 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