



EIDVirtual

User Guide

A smart card on a USB key, for every Windows smart card scenario

Version 2.1

About this document

This guide explains how to install EIDVirtual 2.1, turn a USB key into a smart card, manage the certificates it holds and diagnose the most common problems. It is written for end users and for the administrators who deploy the product.

Item	Value
Product	EIDVirtual Enterprise Edition 2.1
Document	User Guide, revision 2.1
Publisher	My Smart Logon SAS
Audience	End users, desktop support, system administrators
Companion document	EIDVirtual 2.1 Functional Specification (architecture, storage, security model)
Support	support@mysmartlogon.com

Revision history

Version	Date	Author	Changes
1.0	21/02/2013	Vincent Le Toux	Creation
1.1	28/03/2013	Thierry Martin	Update
1.2	26/04/2013	Vincent Le Toux	Update to EIDVirtual 1.0.1.0
1.3	22/07/2013	Vincent Le Toux	Improved the troubleshooting paragraph
1.4	24/09/2015	Daniel Bhatoa	Minor adjustments to troubleshooting
2.0	17/05/2026	Vincent Le Toux	Update to EIDVirtual 2.0 (GIDS card, UMDF 2 driver)
2.1	29/09/2026	Vincent Le Toux	Complete rewrite for EIDVirtual 2.1: new layout, all screenshots retaken on Windows 11, installation without driver prompt, EIDVirtualCmd command-line tool, removable-device restriction and AllowNonRemovable setting, new tracing tool, Windows XP / Vista / 7 procedures removed

Conventions

Convention	Meaning
Bold	A button, a link or a label displayed on screen.
<code>Monospace</code>	A command, a file name, a registry value or text to type.
NOTE / TIP	Additional information that makes a task easier.
WARNING / IMPORTANT	An action that can destroy the content of a card or weaken its security.
NEW IN 2.1	A change since the previous edition of this guide (EIDVirtual 2.0, May 2026).

Contents

About this document	2
Revision history	2
Conventions.....	2
1 Introduction	5
1.1 What's new in version 2.1	5
2 System requirements	7
2.1 Operating systems	7
2.2 Storage devices	7
2.3 Smart card service	7
3 Installation	8
3.1 Interactive installation	8
3.2 Silent installation	9
3.3 Upgrade and removal.....	10
4 Creating a virtual smart card.....	11
4.1 The configuration wizard.....	11
4.2 Initializing the card	12
4.3 Inserting and removing the card.....	13
4.4 Clearing a card.....	13
5 Managing certificates.....	14
5.1 The Smart Card manager	14
5.2 Generate.....	15
5.3 Import	15
5.4 Request.....	16
5.5 View, delete and refresh	16
6 Using the virtual smart card	18
6.1 In Windows and in applications.....	18
6.2 Changing the PIN	18
6.3 Blocked PIN.....	19
6.4 Moving, copying and backing up a card.....	19
7 Command-line administration	20
7.1 EIDVirtualCmd.exe.....	20
8 Troubleshooting.....	21
8.1 Common problems.....	21



8.2	Checking the card with certutil	21
8.3	Checking the driver.....	23
8.4	Collecting traces with EIDVirtual Tracing	23
8.5	Capturing traces manually	24
8.6	Troubleshooting the installation	25
9	Appendix - reference	26
9.1	Files	26
9.2	Registry.....	26

1 Introduction

EIDVirtual turns an ordinary removable device - a USB key, an SD card - into a smart card. Windows sees a smart card reader with a standard smart card inserted, and every application that works with smart cards works with it, without any additional middleware.

The card is a **GIDS** card (Generic Identity Device Specification), the smart card profile Windows supports natively: the minidriver that drives it is part of Windows. Its content - the certificates, the private keys, the PIN - is kept in a single encrypted file on the removable device, bound to that device: a copy of the file on another key is not a card.

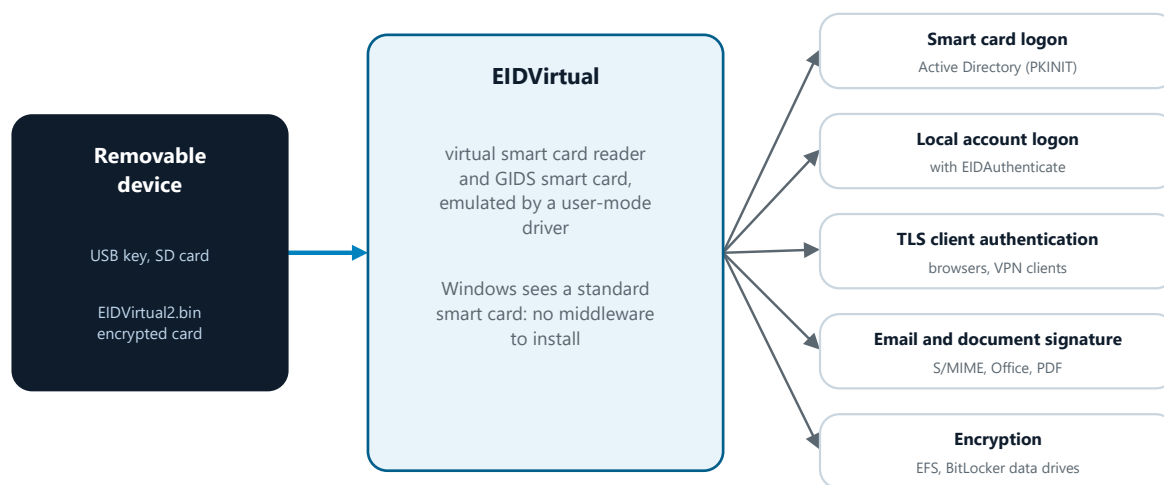


Figure 1 – What an EIDVirtual card can be used for

Typical uses are smart card logon (with Active Directory, or on standalone computers with EIDAuthenticate), TLS client authentication, signature of emails and documents, and file encryption. EIDVirtual is also a convenient way to test and develop smart card applications without buying hardware.

NOTE

A virtual card is protected by software, not by a secure chip: the private keys are encrypted on the removable device, and the PIN is checked by the EIDVirtual driver. The functional specification describes the security model in detail; read it before using EIDVirtual where a certified hardware token is required.

1.1 What's new in version 2.1

Area	What changed
Installation	No more "Would you like to install this device software?" prompt: the installer registers the publisher certificate of the driver before installing it. The setup is now fully unattended, and fast. See chapter 3.
Command line	New EIDVirtualCmd tool: initialize a card, import a PFX, eject or re-insert the card, change the device policy - from scripts and deployment tools. See chapter 7.

Area	What changed
Device policy	By default only removable devices (removable media, or any disk on the USB bus) can carry a card. The new AllowNonRemovable setting accepts fixed disks too. See section 2.2.
Card insertion	A card is available immediately after its initialization: no need to unplug and plug the device again. A card can also be ejected and re-inserted by command, without touching the device.
Device identification	The device identity is read from the physical disk (and, for disks without a serial number, from the SCSI device identifiers): USB disks that report themselves as fixed disks are recognized.
Certificate import	PFX files are imported through the Smart Card Key Storage Provider (CNG), as Windows 11 requires.
Reliability	Card insertion, removal and state changes are serialized inside the reader: no more conflicts with the Windows certificate propagation service, no more spurious errors in the event log.
User interface	Dark mode (follows the Windows app setting), version and copyright displayed in every tool, certificate list with sortable columns and context menu, redesigned tracing tool with live tracing window.
Older Windows	On Windows versions older than Windows 8.1, the installer automatically installs a UMDF 1 compatibility driver. The version of the driver now equals the version of the product.

2 System requirements

2.1 Operating systems

Windows version	Architecture	Driver
Windows 11, Windows 10	x64	UMDF 2 (native)
Windows Server 2025, 2022, 2019, 2016	x64	UMDF 2 (native)
Windows 8.1, Windows Server 2012 R2	x64	UMDF 2 (native)
Windows 7 SP1, Windows 8, Windows Server 2008 R2 / 2012	x64	UMDF 1 compatibility driver (legacy)
32-bit editions of Windows, Windows XP and Vista	-	Not supported

The installer selects the driver from the build number of Windows (9600 = Windows 8.1 and later: UMDF 2). Installing the product requires administrator rights; using the card does not.

2.2 Storage devices

The card is stored in a file, `EIDVirtual12.bin`, at the root of a volume of the device. The device must:

- be writable and hold a file system Windows can read and write (FAT32, exFAT or NTFS). CD, DVD and Blu-ray drives are never offered;
- report an identity (vendor, product, revision and serial number): the card is encrypted with a key derived from it. Almost every USB key and memory card reader does;
- be **removable**: removable media, or any disk connected to the USB bus - many USB disks declare themselves as fixed disks and are accepted all the same;
- not be the Windows volume.

NEW IN 2.1

Fixed disks (internal disks, virtual machine disks, some card readers) are refused by default. An administrator can accept them with `EIDVirtualCmd nonremovable on`, which sets the `AllowNonRemovable` value under `HKLM\SOFTWARE\MySmartLogon\EIDVirtual1`. The setting applies at the next arrival of a volume (plug the device again or restart the reader).

Refusing fixed disks by default avoids turning a disk that never leaves the computer into a "card" that never leaves the computer either.

2.3 Smart card service

The Windows **Smart Card** service (SCardSvr) must be allowed to run. The installer sets it to start automatically as soon as a reader - the EIDVirtual reader - is present.

3 Installation

The package is a Windows Installer (MSI) file, `EIDVirtualSetup.msi`. The same file is used for an interactive installation and for a silent deployment. The installation requires administrator rights.

3.1 Interactive installation

- 1 Run `EIDVirtualSetup.msi`. Read the license agreement, select **I accept the terms in the License Agreement** and click **Install**.

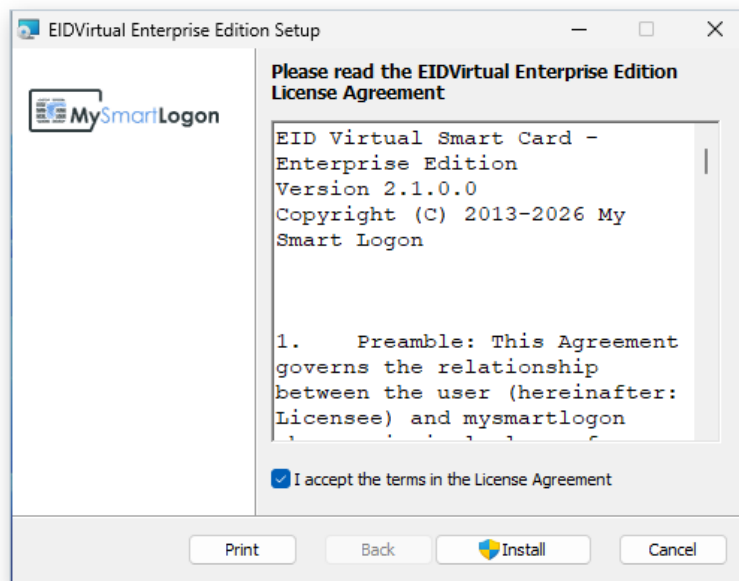


Figure 2 – License agreement

- 2 Accept the User Account Control prompt. The installer is signed by **My Smart Logon SAS**.

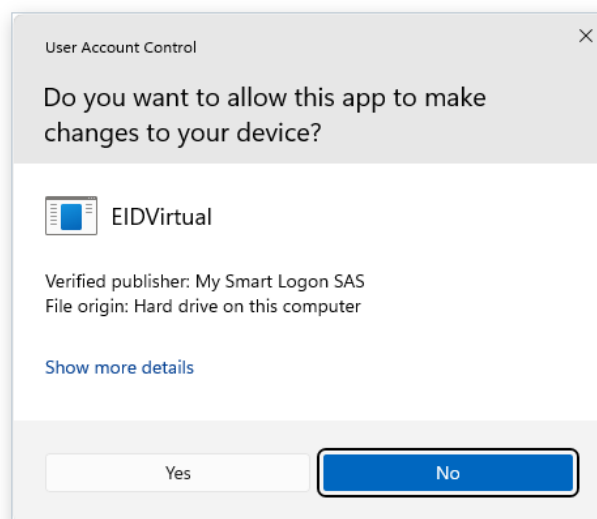


Figure 3 – User Account Control prompt of the installer

- 3 Click **Finish**. Leave **Launch the configuration wizard** checked to create a card right away (chapter 4).

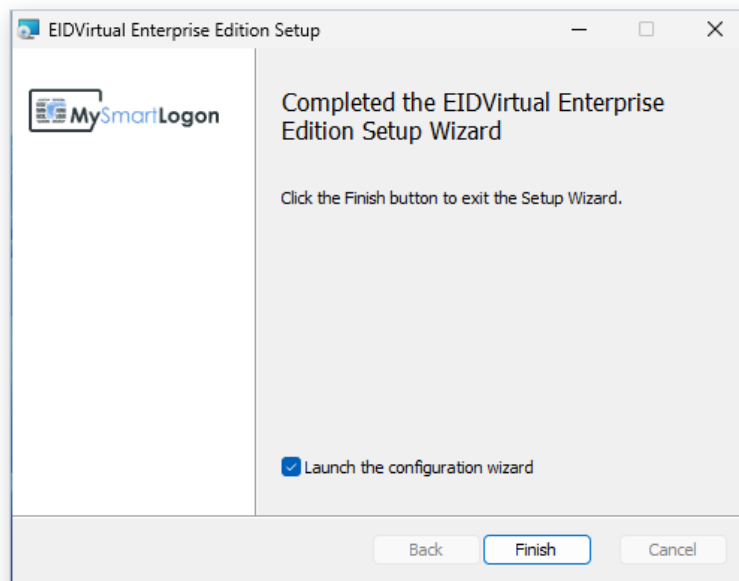


Figure 4 – End of the installation

NEW IN 2.1

The installation no longer displays the Windows Security prompt **"Would you like to install this device software?"** that previous versions required the user to accept. The installer registers the certificate that signs the driver in the **Trusted Publishers** store of the computer before installing the driver, so Windows installs it silently. The certificate is left in place at uninstallation.

The installation adds:

- the **EIDVirtual2SmartCardReader Device** in Device Manager, under **Smart card readers**. Windows names the reader **MySmartLogon Virtual Reader 0**;
- the programs `EIDVirtualWizard.exe` (configuration wizard), `EIDVirtualManager.exe` (smart card manager), `EIDVirtualCmd.exe` (command line) and `EIDVirtualTrace.exe` (tracing) in `C:\Program Files\EID Virtual Smart Card`;
- a Start menu folder **EID Virtual Smart Card** with **Configuration Wizard** and **Smart Card manager**.

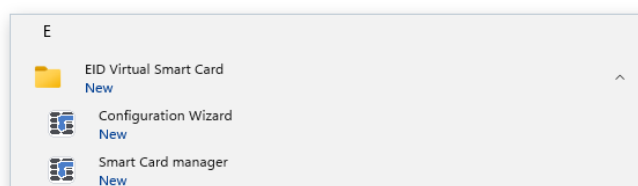


Figure 5 – Start menu entries

3.2 Silent installation

From an elevated prompt, or from a software distribution tool:

SILENT INSTALLATION

```
msiexec /i EIDVirtualSetup.msi /qn /norestart /l*v install.log
```

UNINSTALL

```
msiexec /x EIDVirtualSetup.msi /qn /norestart /l*v uninstall.log
```

A silent installation can be followed by `EIDVirtualCmd format` to initialize a card without any user interaction (chapter 7).

3.3 Upgrade and removal

- Installing a newer version upgrades the product in place; the cards already created stay valid.
- Uninstalling removes the reader and its driver package from the driver store. The cards on the removable devices are not touched and can be used again after a new installation.

4 Creating a virtual smart card

A card is created once on a device with the **Configuration Wizard**. The wizard creates the GIDS card, sets its PIN, its admin key and its serial number, and writes it, encrypted, on the device.

4.1 The configuration wizard

Plug in the device, then start **Configuration Wizard** from the Start menu (it also opens at the end of the installation). The **Drive** list shows the compatible volumes and is updated as soon as a device is plugged in or removed.

Figure 6 – The configuration wizard with its default values

Field	Content
Drive	The volume that will carry the card.
PIN	4 to 16 digits. Default 0000: change it.
Admin Key	48 hexadecimal characters (a 24-byte 3DES key). It unblocks the card when the PIN is blocked. Default: all zeros - change it, and keep it in a safe place.
Serial number	32 hexadecimal characters, generated at random. It identifies the card; click Generate for a new one.
Clear the card	Deletes the card present on the selected volume (see 4.4).

4.2 Initializing the card

- 1 Select the **Drive**.
- 2 Type the **PIN** and the **Admin Key**. Keep the generated **Serial number** unless your organization assigns them.
- 3 Click **Initialize card**.

EIDVirtual GIDS Card Configuration Wizard

Version 2.1.0.0

EIDVirtual GIDS Card Configuration Wizard MySmartLogon

This tool initializes a card where the GIDS applet has just been installed. It configures the PIN, the admin key and installs the file system. This operation is performed once.

Drive: e: Clear the card

The PIN must be between 4 and 16 characters long. It can include digits only.

PIN: 123456

The Admin Key is present to unblock the card if the PIN is lost. The Admin Key must be an hexadecimal string containing 48 characters.

Admin Key: 7E3A91C04BD25F68A0137C9E52D4B86F1A09E3C7D5B2486F

The serial number is used to identify the card uniquely. It is an hexadecimal string having 32 characters.

Serial number: F80CAB2A0D82564DC85FA7AFFA4AB614 Generate

© 2013-2026 MySmartLogon.com Initialize card Cancel

Figure 7 – Wizard ready to initialize a card

The wizard asks for confirmation when the volume already holds a card - initializing it again destroys its certificates and keys - and when the PIN or the admin key still have their default value.

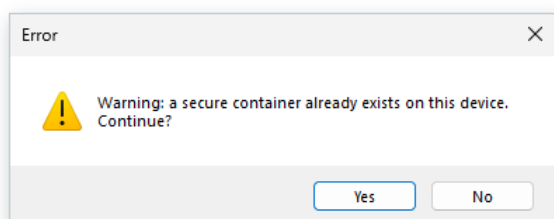


Figure 8 – The volume already holds a card

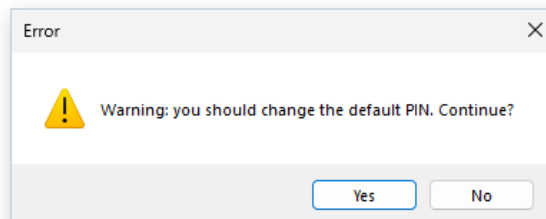


Figure 9 – The default PIN is still in place

A few seconds later the card is ready. The wizard offers to open the Smart Card manager (chapter 5).

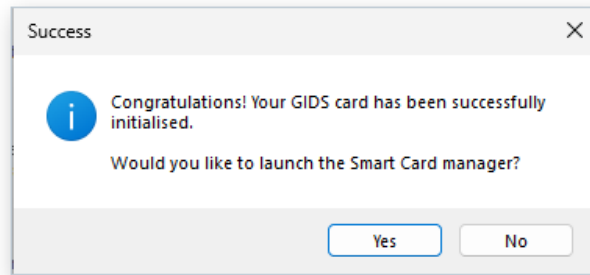


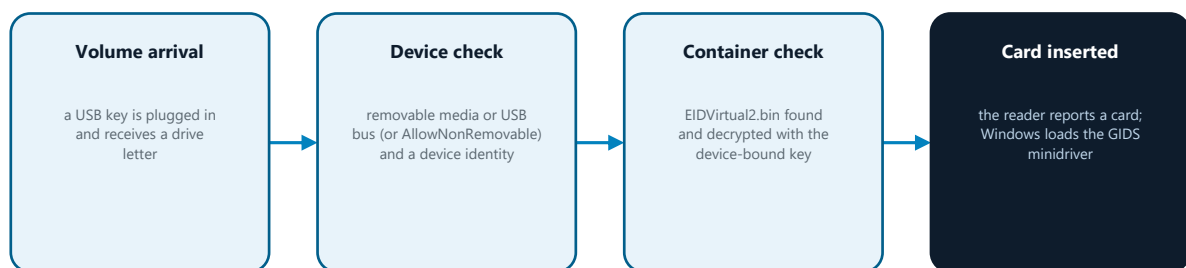
Figure 10 – Card initialized

NEW IN 2.1

The card is available at once: the wizard hands the volume to the reader, which inserts the card. Previous versions required the device to be unplugged and plugged in again.

4.3 Inserting and removing the card

From then on, plugging the device in inserts the card in the reader, and removing the device removes the card. Windows reacts exactly as with a physical card: lock on removal if the policy requires it, certificate propagation to the user store, and so on.



Unplugging the volume, or EIDVirtualCmd eject, removes the card. EIDVirtualCmd swallow inserts it again without unplugging.

Figure 11 – From the volume arrival to the inserted card

WARNING

Remove the device with **Safely Remove Hardware** (or `EIDVirtualCmd eject` first). Pulling a USB key out while the card is being written can corrupt the card file.

4.4 Clearing a card

Clear the card ejects the card and deletes `EIDVirtual2.bin` from the selected volume. The other files of the volume are not touched.

IMPORTANT

Clear the card acts immediately, without confirmation. The certificates and private keys of the card are lost. Check the selected drive before clicking.

5 Managing certificates

The **Smart Card manager** lists the certificates of the card and creates, imports and deletes them. Any tool that works with smart cards (the certificate snap-in, `certreq`, `certutil`, enrollment in a browser) can also be used: the card is a standard smart card.

5.1 The Smart Card manager

Start **Smart Card manager** from the Start menu. When no card is present, Windows asks for one:

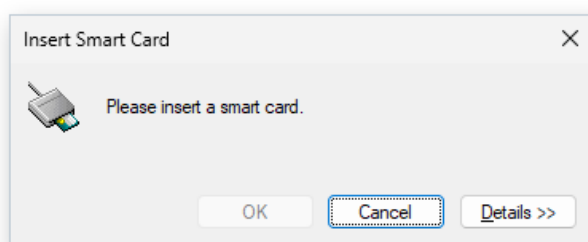


Figure 12 – No card in the reader

Plug in a device that holds a card, or cancel. A new card is empty:

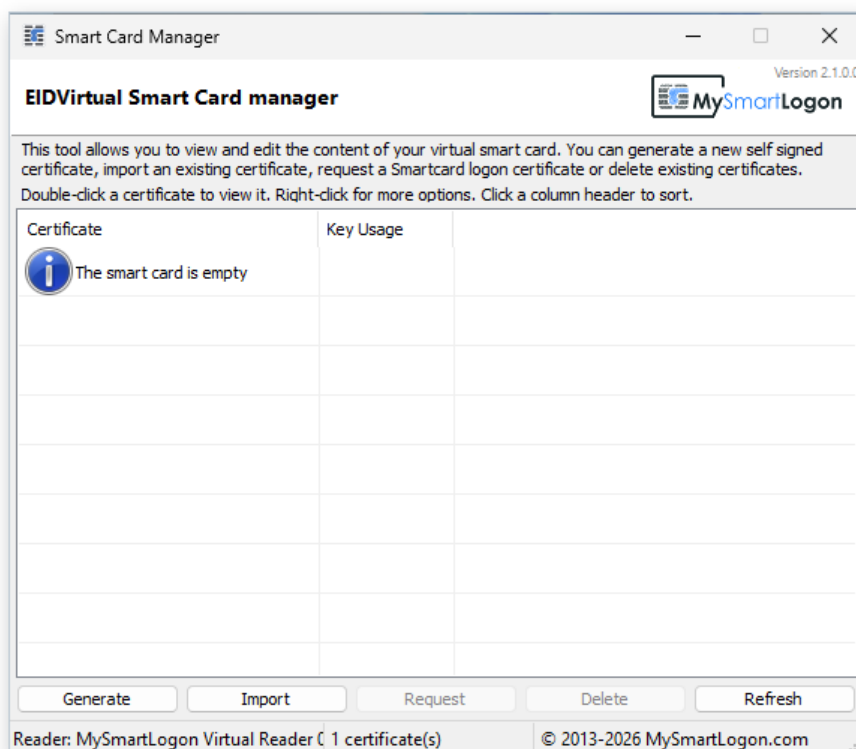


Figure 13 – An empty card

The status bar shows the reader and the number of certificates. Double-click a certificate to display it, right-click for the context menu, click a column header to sort.

5.2 Generate

Generate creates a 2048-bit RSA key on the card and a self-signed certificate for it, valid 10 years, named after the current user and usable for client authentication, server authentication, smart card logon and EFS. Windows asks for the PIN of the card:

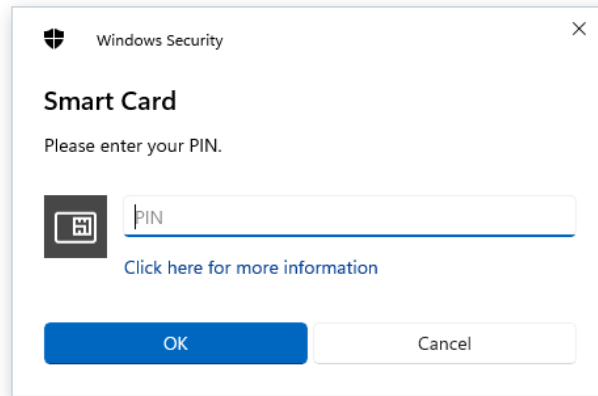


Figure 14 – PIN prompt displayed by Windows

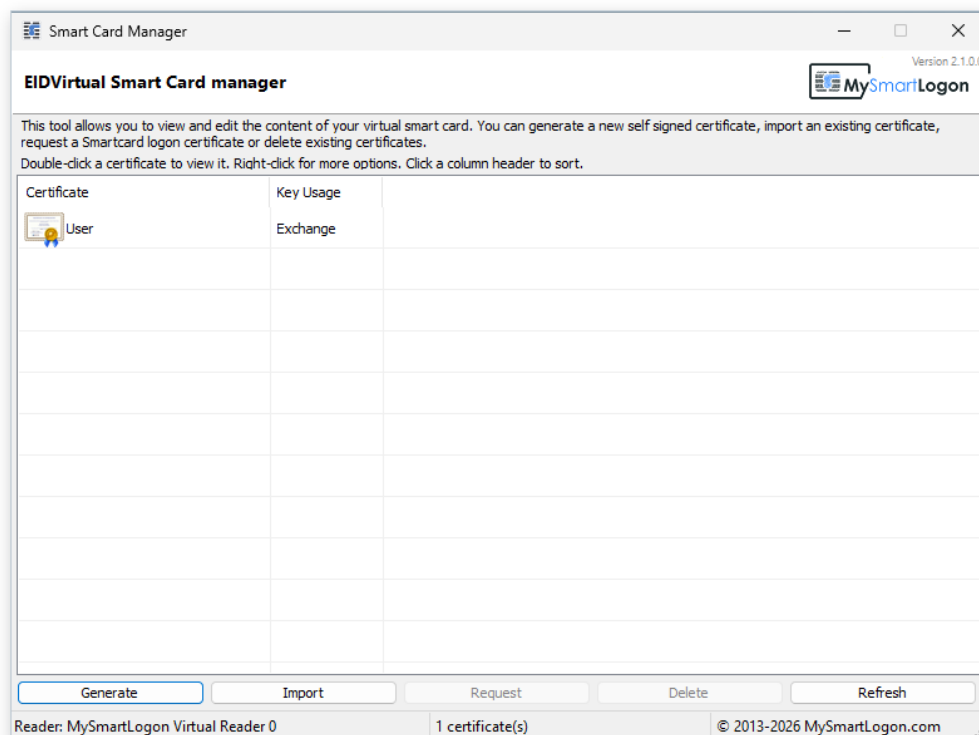


Figure 15 – The card after the generation of a certificate

A self-signed certificate is useful for tests, for EFS and for EIDAuthenticate, which accepts certificates that do not come from a PKI. For Active Directory smart card logon, use **Request**.

5.3 Import

Import writes a certificate and its private key from a **.pfx** / **.p12** file (PKCS#12) on the card.

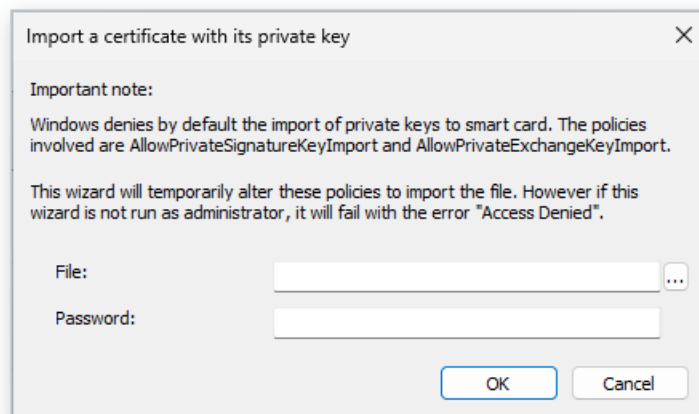


Figure 16 – Import of a PKCS#12 file

NOTE

Windows refuses by default to import a private key into a smart card (policies `AllowPrivateSignatureKeyImport` and `AllowPrivateExchangeKeyImport`). The manager enables them for the duration of the import and restores them afterwards, which requires administrator rights: start the manager with **Run as administrator**, or use `EIDVirtualCmd import` from an elevated prompt.

5.4 Request

Request enrolls a certificate from the Active Directory certification authority, with the **Smartcard Logon** template, and a 2048-bit key generated on the card. The button is available only when the user belongs to a domain.

- An enterprise certification authority must publish the **Smartcard Logon** template, and the user must have the right to enroll for it. A duplicated template is not used by this button.
- For smart card logon, every domain controller also needs a valid domain controller certificate (**Kerberos Authentication** or **Domain Controller Authentication**).

5.5 View, delete and refresh

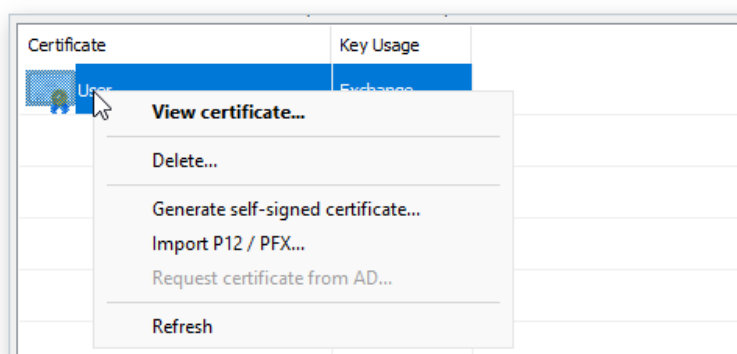


Figure 17 – Context menu of a certificate

- **View certificate** (or a double-click) opens the Windows certificate dialog.
- **Delete** removes the selected certificates and their private keys, after confirmation. This cannot be undone.

- **Refresh** reads the card again, after a change made by another program.

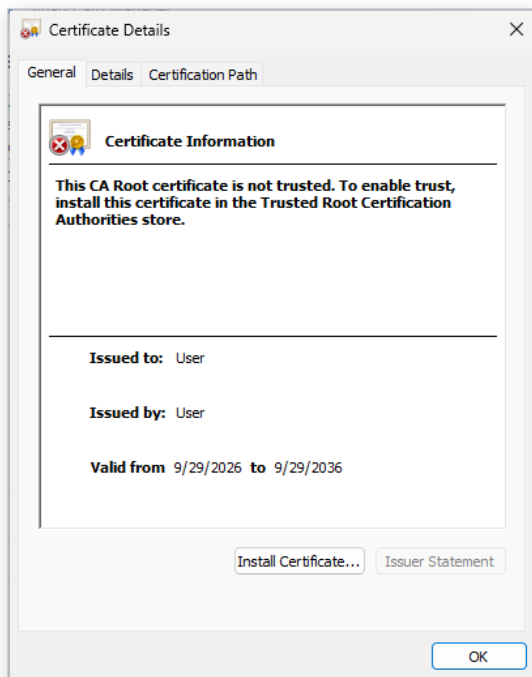


Figure 18 – Certificate displayed by Windows

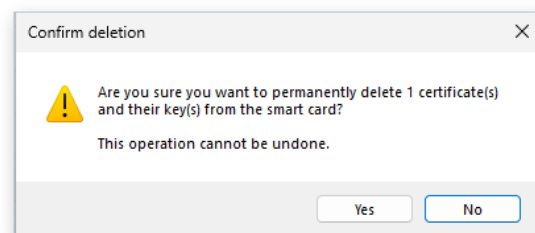


Figure 19 – Confirmation of a deletion

6 Using the virtual smart card

6.1 In Windows and in applications

The card behaves as a physical GIDS card. Its certificates are propagated to the personal store of the user while the card is inserted (Windows certificate propagation service), which makes them visible to browsers, Outlook, Office and the other applications. The PIN is asked by Windows, in the same dialog as for any card.

Scenario	What is needed
Active Directory smart card logon	A certificate enrolled with Request (or any smart card logon template).
Standalone computer logon	EIDAuthenticate, and any certificate of the card associated with the local account.
TLS client authentication	A certificate with the Client Authentication usage, trusted by the server.
Email (S/MIME) and document signature	A certificate issued for the email address or the signer.
EFS	A certificate with the Encrypting File System usage, selected in the EFS settings.

6.2 Changing the PIN

The PIN is changed with the Windows tools, as for any smart card:

- 1 Press **Ctrl+Alt+Del** and choose **Change a password**.
- 2 Click **Sign-in options**, then the smart card icon.
- 3 Type the current PIN, the new PIN and its confirmation, then press **Enter**.

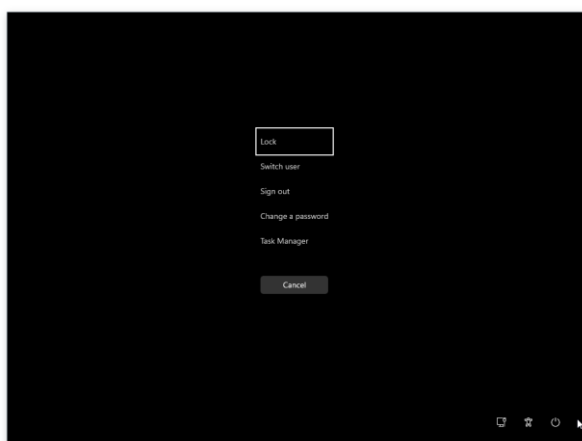


Figure 20 – Ctrl+Alt+Del screen

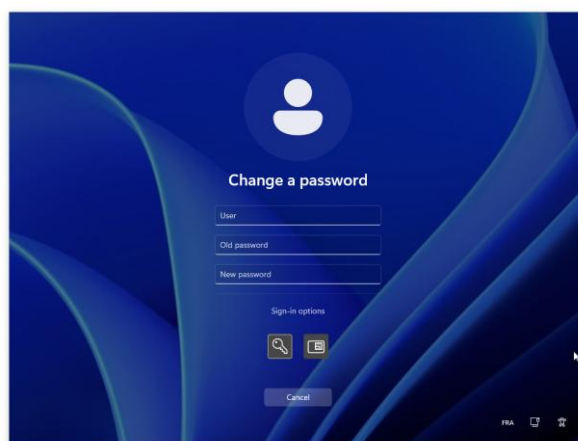


Figure 21 – Sign-in options: password or smart card

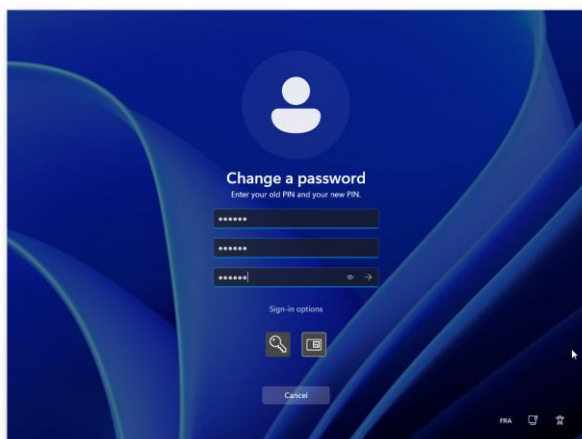


Figure 22 – Current PIN, new PIN and confirmation

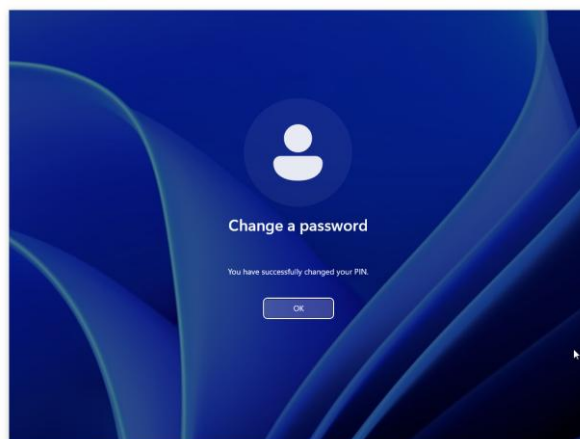


Figure 23 – PIN changed

The new PIN must have 4 to 16 digits.

6.3 Blocked PIN

After **3** wrong PINs in a row, the card is blocked: the PIN can no longer be verified, even the right one. The counter is reset by every correct PIN.

- A blocked card can be unblocked with its **admin key** by a management tool that performs the smart card challenge / response authentication (the admin key never travels in clear).
- EIDVirtual does not ship an unblock tool. Without the admin key, initialize the card again with the wizard: its content is lost.

6.4 Moving, copying and backing up a card

- A card cannot be moved to another device: `EIDVirtual2.bin` is encrypted with the identity of the device, and a copy on another key is ignored by the reader.
- A copy of the file on the **same** device (a backup) can be restored, including an older one: the PIN attempt counter is part of the file.
- Keep a backup of the private keys that matter - a PFX kept offline, or the key archival of your certification authority - rather than of the card file.

7 Command-line administration

NEW IN 2.1

EIDVirtualCmd.exe is new in 2.1. It is installed in C:\Program Files\EID Virtual Smart Card, which is not on the PATH: call it with its full path or from that folder. Messages and options are in English.

7.1 EIDVirtualCmd.exe

Command	Effect
<code>format --drive X: [--pin p] [--admin-key h] [--serial h]</code>	Initialize a card on the volume <code>x:</code> - the same operation as the wizard. PIN default <code>0000</code> , admin key default all zeros, serial generated at random.
<code>import --pfx file [--password p] [--pin p] [--reader r]</code>	Import a PKCS#12 file on the card. Requires an elevated prompt (private key import policy, see 5.3). The PIN is passed on the command line, without prompt.
<code>eject</code>	Remove the card from the reader. The volume is then free, for instance to be backed up.
<code>swallow [--drive X:]</code>	Insert the card of <code>x:</code> in the reader, without unplugging the device. Without <code>--drive</code> , the first volume holding a valid card is used.
<code>nonremovable [on off status]</code>	Show or change the <code>AllowNonRemovable</code> setting (section 2.2). <code>on</code> and <code>off</code> require an elevated prompt.

The exit code is 0 on success and non-zero on failure, so that the commands can be chained in scripts.

```
C:\Program Files\EID Virtual Smart Card>EIDVirtualCmd nonremovable status
AllowNonRemovable = on (any disk that reports an identity)

C:\Program Files\EID Virtual Smart Card>EIDVirtualCmd eject
Ejecting the card...
Card ejected.

C:\Program Files\EID Virtual Smart Card>EIDVirtualCmd swallow --drive E:
Swallowing the card from E:...
Card taken by the reader.
```

Figure 24 – Checking the device policy, ejecting and re-inserting the card

UNATTENDED PROVISIONING OF A CARD (ELEVATED PROMPT)

```
cd "C:\Program Files\EID Virtual Smart Card"
EIDVirtualCmd format --drive F: --pin 482915 --admin-key
7E3A91C04BD25F68A0137C9E52D4B86F1A09E3C7D5B2486F
EIDVirtualCmd import --pfx C:\Deploy\user.pfx --password "PfxPassword" --pin 482915
```

WARNING

Command lines are recorded in the history of the console, in process auditing (event 4688) and by endpoint protection products. Do not use real PINs, admin keys or PFX passwords in shared scripts; change the PIN of a card provisioned this way before handing it over.

8 Troubleshooting

8.1 Common problems

Symptom	Probable cause	Solution
The drive does not appear in the wizard	The device is a fixed disk, the volume is read-only, or the device reports no identity.	Use a USB key or a removable card, or allow fixed disks with <code>EIDVirtualCmd nonremovable on</code> .
"Insert Smart Card" although the device is plugged in	The volume holds no card, the card file was copied from another device, or it is damaged.	Check with <code>certutil</code> (8.2) and the trace (8.4); initialize a card with the wizard.
The card disappears after a while	The device went to sleep or was removed without being ejected.	Plug it in again; use <code>EIDVirtualCmd swallow</code> to re-insert the card.
"The Smart Card Resource Manager is not running"	The Smart Card service is stopped or disabled.	Set the Smart Card service to Automatic and start it.
Import fails with "Access Denied"	The manager was not started as administrator.	Run it as administrator, or use <code>EIDVirtualCmd import</code> from an elevated prompt.
The PIN is refused although it is right	The card is blocked (3 wrong PINs).	See 6.3.

8.2 Checking the card with certutil

`certutil -scinfo` is the reference diagnostic of Windows for smart cards. Open a command prompt and type:

COMMAND PROMPT
`certutil -scinfo -silent`

A healthy EIDVirtual card is reported as **SCARD_STATE_PRESENT**, with the ATR `3B 8C 01 4D 79 53 6D 61 72 74 4C 6F 67 6F 6E A5` ("MySmartLogon"), the card name **Identity Device (Microsoft Generic Profile)** and the provider **Microsoft Base Smart Card Crypto Provider**. Each certificate is then analyzed.

```
The Microsoft Smart Card Resource Manager is running.
Current reader/card status:
Readers: 1
  0: MySmartLogon Virtual Reader 0
--- Reader: MySmartLogon Virtual Reader 0
--- Status: SCARD_STATE_PRESENT | SCARD_STATE_UNPOWERED
--- Status: The card is available for use.
--- Card: Identity Device (Microsoft Generic Profile)
--- ATR:
      3b 8c 01 4d 79 53 6d 61 72 74 4c 6f 67 6f 6e a5 ;..MySmartLogon.

=====
Analyzing card in reader: MySmartLogon Virtual Reader 0
-----
===== Certificate 0 =====
--- Reader: MySmartLogon Virtual Reader 0
--- Card: Identity Device (Microsoft Generic Profile)
Provider = Microsoft Base Smart Card Crypto Provider
Key Container = 345f5e8e-7b4f-4335-854c-f81ef0623309 [Default Container]

No AT_SIGNATURE key for reader: MySmartLogon Virtual Reader 0
Serial Number: 6a3ffaf3e55877824d8970836787c666
Issuer: CN=User
NotBefore: 9/29/2026 1:43 PM
NotAfter: 9/29/2036 1:43 PM
Subject: CN=User
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): b9541929e2f203f8b2bcdd0f1c631e18376f7f8c
```

Figure 25 – A healthy card holding one certificate

SCARD_STATE_EMPTY means that the reader is present but holds no card: no device with a valid card is plugged in, the card was ejected, or its file could not be decrypted.

```
C:\Program Files\EID Virtual Smart Card>certutil -scinfo -silent | more
The Microsoft Smart Card Resource Manager is running.
Current reader/card status:
Readers: 1
  0: MySmartLogon Virtual Reader 0
--- Reader: MySmartLogon Virtual Reader 0
--- Status: SCARD_STATE_EMPTY
--- Status: No card.
--- Card:

=====
Analyzing card in reader: MySmartLogon Virtual Reader 0
-----

Done.
```

Figure 26 – The reader without a card

When the Smart Card service is stopped, certutil cannot list any reader:

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

Figure 27 – The Smart Card service is not running

8.3 Checking the driver

In Device Manager, the reader appears under **Smart card readers** and the inserted card under **Smart cards**. The **Driver** tab shows the version of the driver - the version of the product - and its signer.

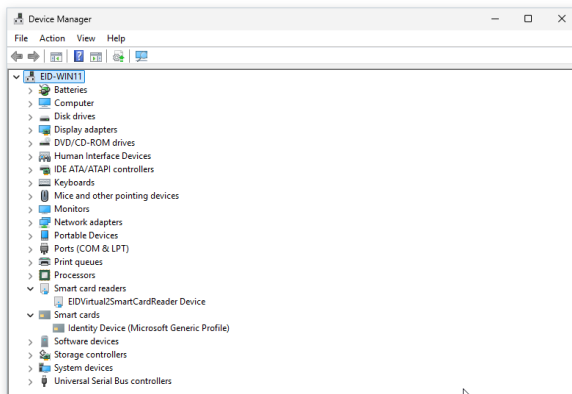


Figure 28 – The reader and the inserted card

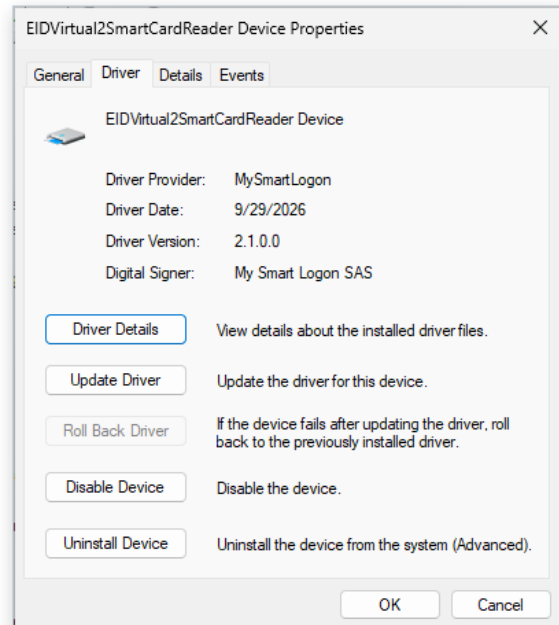


Figure 29 – Driver 2.1.0.0 signed by My Smart Logon SAS

8.4 Collecting traces with EIDVirtual Tracing

EIDVirtualTrace.exe, in C:\Program Files\EID Virtual Smart Card, records the debug trace of the reader, the wizard and the manager. It is the first thing support will ask for. Start it from an elevated prompt.

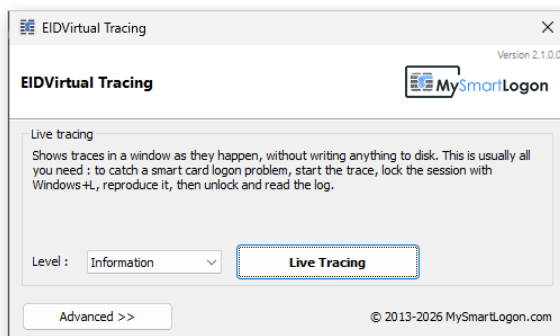


Figure 30 – Live tracing

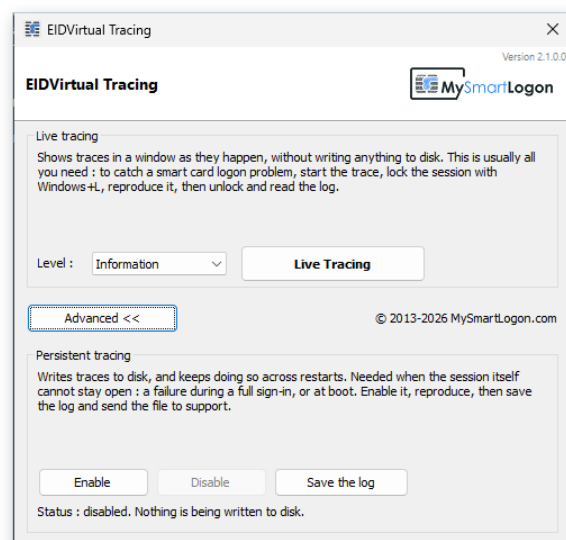


Figure 31 – Advanced: persistent tracing

8.4.1 Live tracing

Choose the level and click **Live Tracing**: traces are displayed as they happen, without writing anything to disk. Reproduce the problem, then **Copy** or **Save** the log. **Find** filters the lines, errors are displayed in red and counted in the status bar. To capture a logon problem, start the trace, lock the session with Windows+L, reproduce the problem, then unlock.

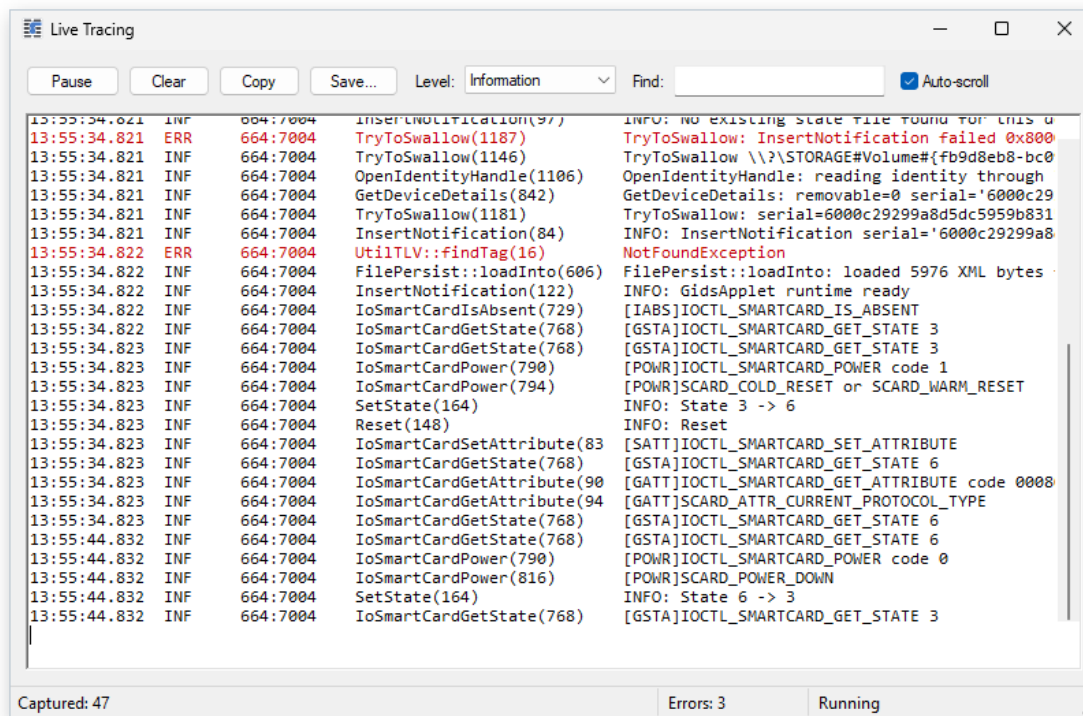


Figure 32 – Live tracing while a card is ejected and inserted again

8.4.2 Persistent tracing

When the problem prevents a session from staying open, click **Advanced >>**, then **Enable**: traces are written to %windir%\System32\LogFiles\WMI\EIDVirtual.etl, also across restarts. Reproduce the problem, click **Save the log** to produce a text file for support, then **Disable**.

NOTE

Traces never contain the PIN or the private keys, but they contain the identity of the devices (vendor, product, serial number) and the names of the certificates.

8.5 Capturing traces manually

On computers where the tool cannot be used, the same ETW providers can be recorded with the Windows tools:

ELEVATED COMMAND PROMPT

```
logman create trace EIDVirtualTrace -o C:\Temp\EIDVirtual.etl
logman update trace EIDVirtualTrace -p {7941FA8B-987B-4B0A-B164-5F4B5C069578} 0xFFFFFFFF 5
logman update trace EIDVirtualTrace -p {98EB9ED4-ACA8-47E7-A21D-45A4313B4FC4} 0xFFFFFFFF 5
logman update trace EIDVirtualTrace -p {1952FB1B-888D-48E1-A301-ABA8250E480D} 0xFFFFFFFF 5
logman start EIDVirtualTrace
REM ... reproduce the problem ...
logman stop EIDVirtualTrace
logman delete EIDVirtualTrace
```

The three providers are the reader driver, the configuration wizard and the manager. Send the .etl file to support.

8.6 Troubleshooting the installation

VERBOSE INSTALLATION LOG

```
msiexec /i EIDVirtualSetup.msi /l*v install.log
```

The custom actions of the setup (publisher certificate, driver package, device creation, Smart Card service) write their diagnostics in this log.

9 Appendix - reference

9.1 Files

Location	Content
C:\Program Files\EID Virtual Smart Card\EIDVirtualWizard.exe	Configuration wizard
C:\Program Files\EID Virtual Smart Card\EIDVirtualManager.exe	Smart Card manager
C:\Program Files\EID Virtual Smart Card\EIDVirtualCmd.exe	Command-line tool
C:\Program Files\EID Virtual Smart Card\EIDVirtualTrace.exe	Tracing tool
C:\Program Files\EID Virtual Smart Card\EIDVirtualSmartCardReader2\	Driver package (INF, catalog, DLL) - UMDF 2
C:\Program Files\EID Virtual Smart Card\EIDVirtualSmartCardReader1\	Driver package - UMDF 1 compatibility driver (older Windows only)
X:\EIDVirtual2.bin	The card, at the root of the removable volume

9.2 Registry

Value	Meaning
HKLM\SOFTWARE\MySmartLogon\EIDVirtual\AllowNonRemovable	DWORD. Absent or 0: only removable devices can carry a card. 1: any disk that reports an identity. Set with EIDVirtualCmd nonremovable.
HKLM\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EIDVirtual	Persistent tracing session, created and removed by EIDVirtual Tracing.