AUSTRIACARD

ACDIS Minidriver
User Manual

Version: 1.0.0.0		AUSTRIACARD
Changed on:	11/04/2024 3:25 PM	Created on: 03/04/2024
Status:	FINAL	

Table of Content

1. GENERAL INFORMATION

1.1. COPYRIGHT

Austria Card Plastikkarten und Ausweissysteme GmbH is the sole owner of the information, knowledge and representations contained in this document. The documentation and the information, knowledge and representations contained within may not be provided to third parties, neither complete nor in part, directly nor indirectly, published nor otherwise dispersed. The assertion of all related rights, especially in the case of distribution of patents, is strictly reserved to Austria Card. The transfer of the documentation is no entitlement for a license or use.

© Copyright 2024 - All rights reserved Austria Card Ges.m.b.H, A-1232 Vienna.

1.2. DOCUMENT HISTORY

Version	Date	Author	Description
1.0.0.0	03/04/2024	AUSTRIACARD, Markus Punz	First release v1.0.0.0

1.3. MINIDRIVER HISTORY

Version	Date	Author	Description
1.1.0.0	03/04/2024	AUSTRIACARD	First release

1.4. DISCLAIMER OF LIABILITY

Austria Card guarantees for a period of twenty-four months from the time of delivery that the Software essentially corresponds to the program description in the accompanying written material with regard to its functionality.

Austria Card points out that the Software is qualified as a one-off service. Necessary updates can be obtained via the same channels through which the Software was obtained as long as the warranty applies.

Austria Card points out that according to the state of the art it is not possible to produce computer Software completely error-free.

If a defect occurs, the defect and its appearance must be described in such detail in a written notice of defect that a review of the defect (e.g. submission of error messages) is feasible and the exclusion of an operating error (e.g. specification of the work steps) is possible.

If the notice of defects proves to be justified, the licensee sets AUSTRIA CARD a reasonable deadline for subsequent performance. The licensee informs AUSTRIA CARD which type of supplementary performance - improvement of the delivered or delivery of a new, defect-free item - he wishes. However, AUSTRIA CARD is entitled to refuse the selected supplementary performance if this can only be carried out with disproportionate costs for it and if the other type of supplementary performance would not entail any significant disadvantages for the licensee. AUSTRIA CARD may also refuse subsequent performance altogether if it can only be carried out at disproportionate cost to it.

In order to carry out the supplementary performance, AUSTRIA CARD is entitled to two attempts for the same or directly related defect within the period set by the licensee. After the second failed attempt at subsequent performance, the licensee may withdraw from the contract or reduce the license fee. The right of withdrawal or reduction can already be exercised after the first unsuccessful attempt at subsequent performance, if a second attempt within the set period is not reasonable for the licensee. If subsequent performance has been refused under the conditions set out

above, the licensee is entitled to the right of reduction or withdrawal immediately.

If the licensee has made a claim against AUSTRIA CARD under warranty, and it turns out that either there is no defect or the asserted defect does not oblige AUSTRIA CARD to provide a warranty, the licensee must reimburse all expenses incurred by AUSTRIA CARD if he is grossly negligent or intentional responsible for the use of AUSTRIA CARD

A guarantee that the Software is suitable for the purposes of the licensee and cooperates with the licensee's existing Software is excluded.

Beyond this warranty, AUSTRIA CARD shall only be liable for a period of two years from delivery of the Software in the event of intent and gross negligence in accordance with the statutory provisions. In the event of slight negligence, AUSTRIA CARD shall only be liable if an essential contractual obligation is violated or if there is a case of delay or impossibility. In the event of liability arising from slight negligence, this liability shall be limited to such damages that are foreseeable or typical. Liability for the lack of the guaranteed quality, due to fraudulent intent, for personal injury and the General Data Protection Agreement remains unaffected.

In the event of a claim against AUSTRIA CARD under warranty or liability, contributory negligence on the part of the user must be taken into account appropriately, in particular in the case of insufficient error messages or insufficient data backup. Insufficient data backup exists in particular if the licensee has failed to take precautions against external influences, in particular against computer viruses and other phenomena that can endanger individual data or an entire database, by means of appropriate, state-of-the-art security measures.

Under no circumstances shall AUSTRIA CARD or its affiliates, partners, suppliers or licensors be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the Software and any third party content and services, whether or not the damages were foreseeable and whether or not company was advised of the possibility of such damages.

2. OVERVIEW

This document is the user manual for the AUSTRIACARD ACDIS Minidriver. This module is required to use ACDIS smartcards in Microsoft Windows environments.

2.1. SUPPORTED OPERATING SYSTEMS

- Microsoft Windows 10 22H2 – 32 Bit
- Microsoft Windows 10 22H2 – 64 Bit
- Microsoft Windows 11 22H2 – 64 Bit
- Microsoft Windows 11 23H2 – 64 Bit

3. MINIDRIVER INSTALLATION

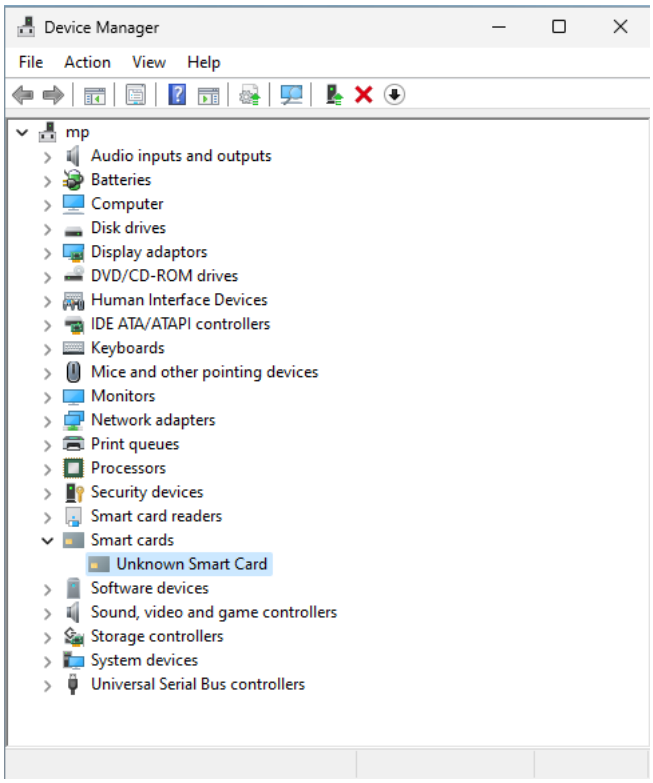
Installation can be done in 2 ways:

- Manually
- Automatically

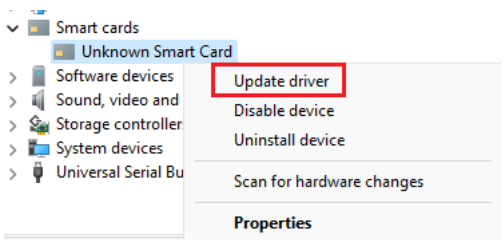
3.1. MANUAL INSTALLATION

Prerequisite: Please connect a card reader and insert an ACDIS smart card.

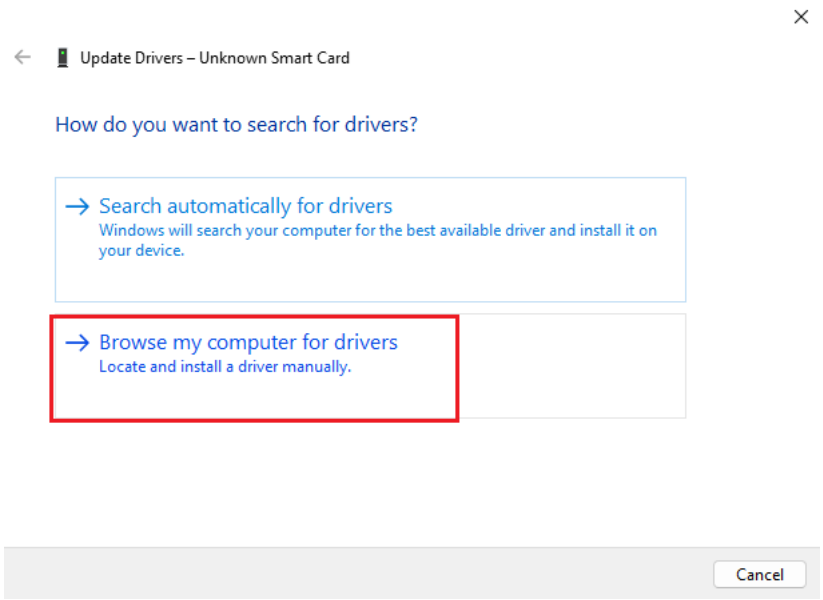
The smart card is initially displayed in the device manager as “Unknown Smart Card”:



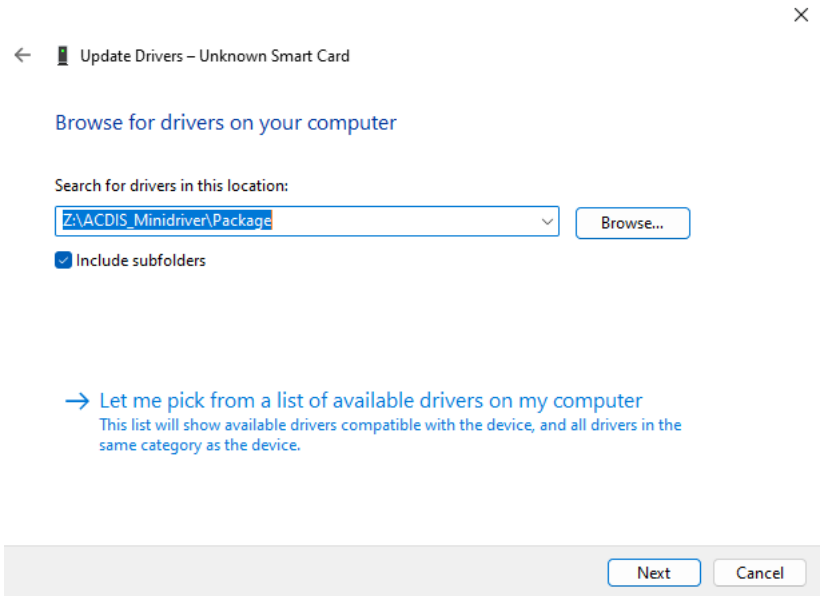
Please select the entry “Update driver” in the context menu:



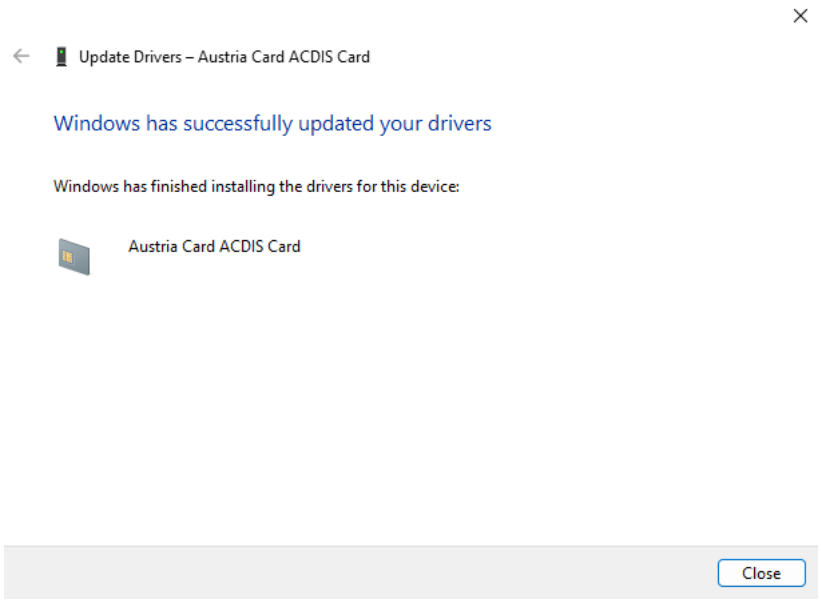
Then select “Browse my computer for drivers”:



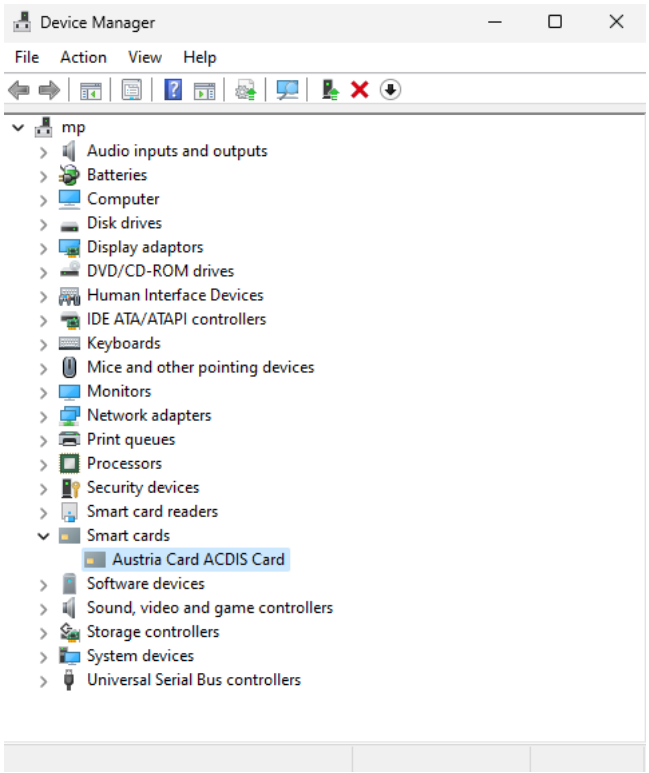
Then select the directory in which the driver files are located and click on “Next”:



Finally, the following window will be displayed, indicating that the Minidriver has been installed correctly:



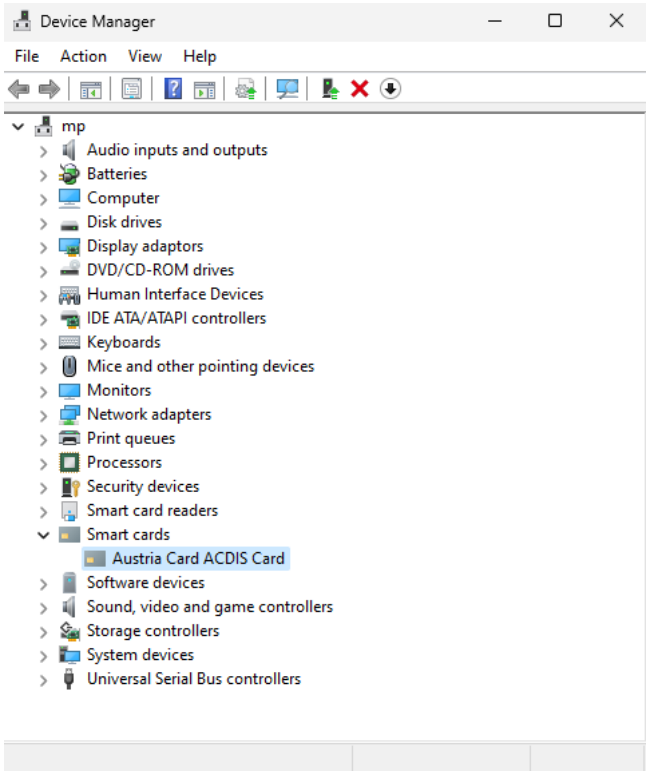
An “Austria Card ACDIS Card” is now displayed in the device manager:



3.2. AUTOMATIC INSTALLATION

"Automatic" means installation via Windows Update. This means that the Minidriver is automatically installed by Windows as soon as a card reader is connected and an ACDIS smart card is inserted.

After installation, an "Austria Card ACDIS Card" must be displayed in the device manager under "Smart cards":



Note:

In corporate environments, certain Windows updates may be delayed or not rolled out at all. In this case, the automatic installation may not work. The installation must be done manually.

4. MINIDRIVER UPDATES

All that was described under 3 also applies to updates of the Minidriver. These can be installed manually at any time or automatically via Windows Update.

5. MINIDRIVER-MODE

The Minidriver can run in 2 different modes:

- Generic-Mode
- SSCD-Mode

As you know, an ACDIS smart card contains a generic application and optionally one or more SSCD applications.

However, the Minidriver concept does not allow multiple applications (- specifically the Generic application and the SSCD application) to be used at the same time. This means you can use the Minidriver either in Generic mode - i.e. with the Generic application or in SSCD mode with the SSCD applications.

This mode can be changed in the PKCS#11 Manager. For details, please refer to the PKCS#11 Manager user manual.

5.1. GENERIC-MODE

In generic mode, any RSA/ECC keys can be created on the ACDIS smart card. Importing certificates and PKCS#12 keys is also supported. The key can be protected with one of the PINs ROLE_USER, PIN#3-PIN#6. This allows users to personalize an ACDIS smart card according to their specific requirements - for example as an employee card, etc.

The Microsoft environment, especially the Microsoft CA for creating your own certificates, is optimally supported.

5.2. SSCD-MODE

SSCD keys serve as a qualified signature and are generated during the manufacturing process. A qualified signature certificate is then applied to the card. This can be done either via the PKCS#11 Manager application or via another software application.

The Minidriver in SSCD mode cannot make any changes to the ACDIS smart card. It only makes the SSCD keys available for usage in the Windows environment - i.e. for creating qualified signatures (- for example via Acrobat Reader).

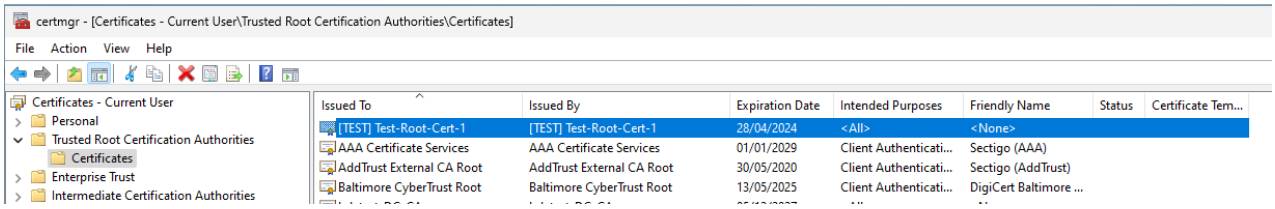
An ACDIS smart card can provide a maximum of 6 signature keys at the same time. The Minidriver architecture doesn't allow anything more, as each of these SSCD keys has its own signature PIN and the number of PINs is limited. Which SSCD keys are made available can be selected via the PKCS#11 manager. Please refer to the PKCS#11 Manager user manual for details.

6. CA CERTIFICATES

There can be CA certificates on an ACDIS smart card (whether in Generic mode or SSCD mode). CA certificates are typically the parent certificates of the respective signature certificates.

These CA certificates can be stored on the ACDIS smart card via the PKCS#11 manager. For details, please refer to the PKCS#11 Manager User Guide.

The ACDIS Minidriver recognizes CA certificates that are found on an ACDIS smart card and automatically copies them into the current user's Trusted Root certificate store. Here an example:



This is done automatically when an ACDIS smart card is inserted and is enabled by default in Windows.

Note:

There is the possibility of deactivating this feature using special Windows registry keys.

7. TROUBLESHOOTING

7.1. LOG-FILES

The Minidriver generates log files. There are 2 locations where these are created:

- C:\Windows\Temp (- System-wide Temp-Directory)
- C:\Users\<<current user>>\AppData\Local\Temp (- User-specific Temp-Directory)

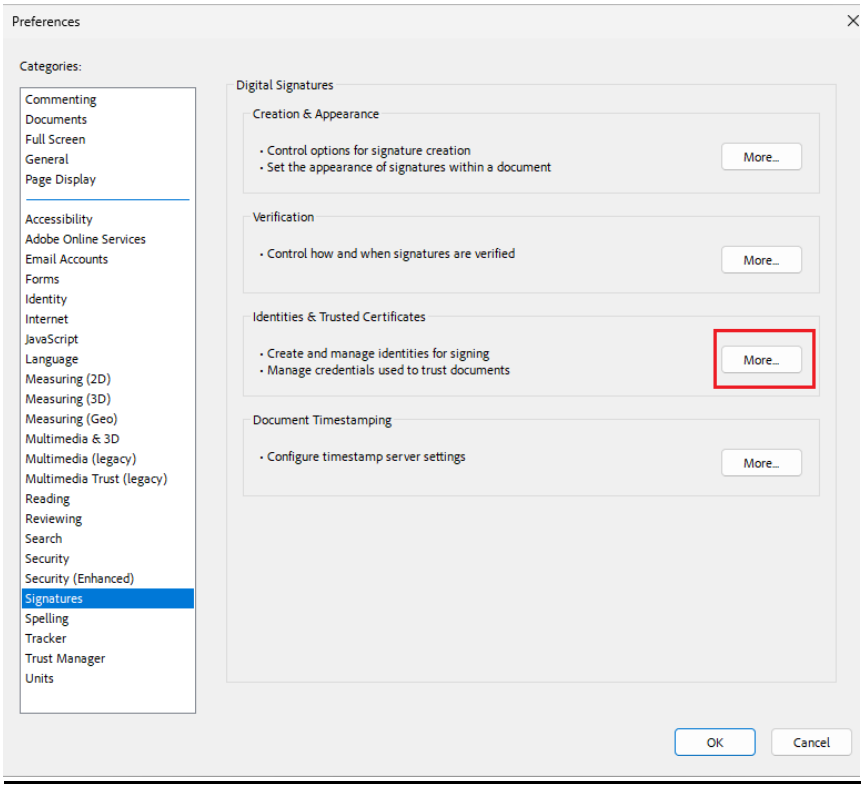
There is no active user (yet) during smart card logon. In this case, log statements are stored in the Windows Temp directory.
This also applies when an ACDIS smart card is inserted/removed - even if you are logged in to Windows. The insertion/removal of smart cards is processed by a Windows service that runs in the system context. These events are also logged in the Windows Temp directory.
All other Minidriver events that occur while logged in to Windows are logged in the current user's Temp directory.

The log files are so-called rolling files. This means that the log files are cyclically overwritten.
The file names are: acdismini_0.txt,acdismini_1.txt, etc.
The last digit of the file name corresponds to the ones digit of the current date.

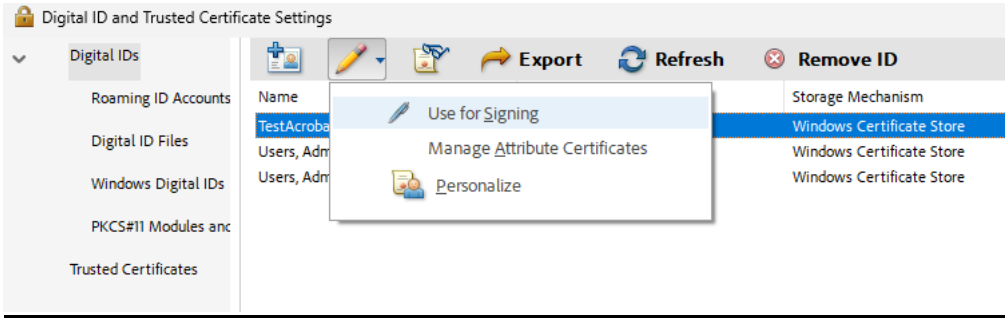
Example:
Let's assume that today is September 5th, 2023. The ones digit of the current day is therefore "5". So the Minidriver writes log statements to the file acdismini_5.txt.
Log statements of the respective day are appended to the file. However, if the file is older, it will be overwritten.
In total, this mechanism leads to a maximum of 10 log files: acdismini_0.txt - acdismini_9.txt

8. MINIDRIVER IN USE

8.1. ACROBAT READER

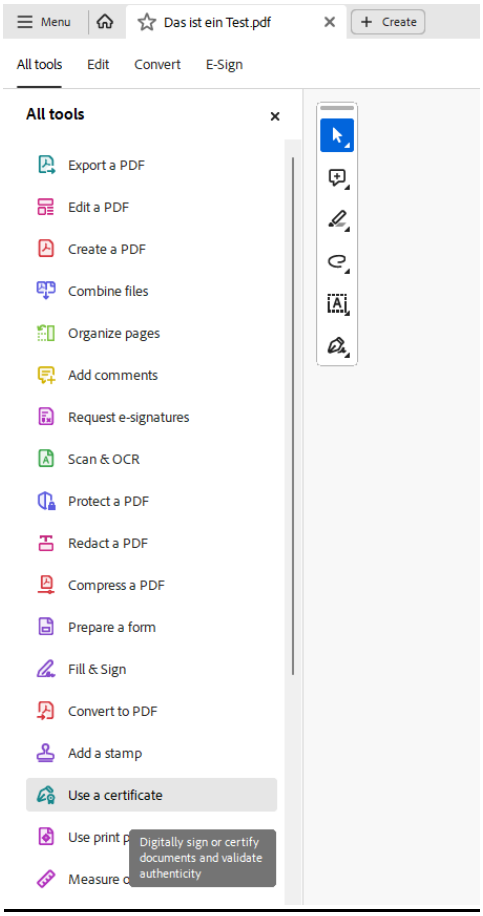


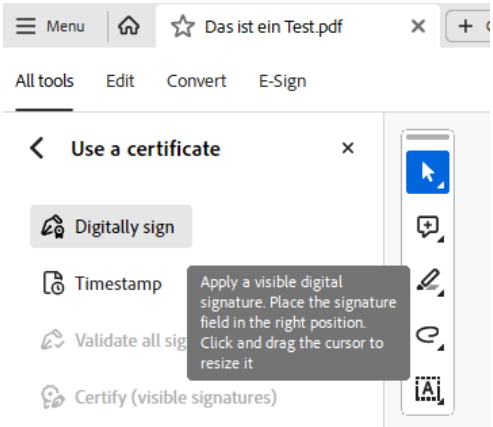
The certificates from the Windows Certificate Store must then appear here. You can check whether you can sign with it:



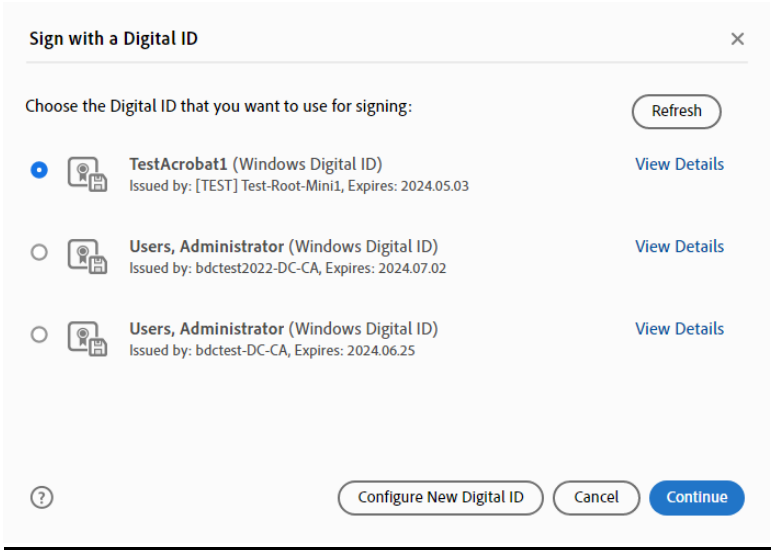
The “Use for signing” option must be displayed - then Acrobat can use the certificate.

To actually sign, open a PDF document and go to “All tools” in the tab. Then select “Use a certificate” here:



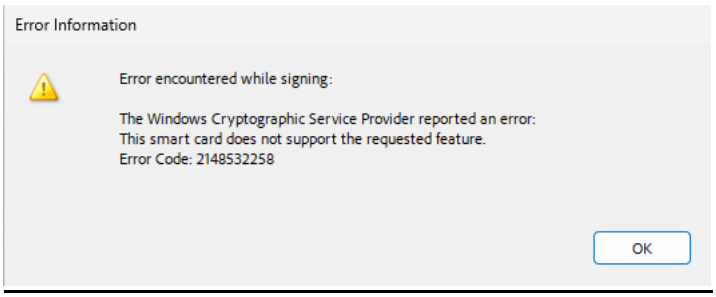


You then have to select the certificate and enter the PIN:



Note: If using an RSA-SSCD Key maybe the following errors occur:

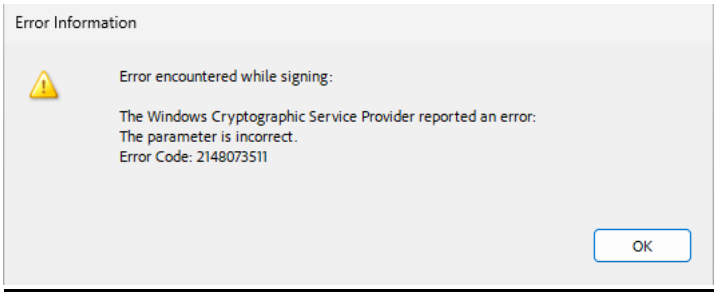
1)
The smart card does not support the requested feature
Error Code: 2148532258



Reason:
RSA-SSCD Keys only support RSA-PSS padding. This must be explicitly enabled in the Adobe Registry settings – see 0 There are no known problems with ECC-SSCD keys. No special settings are necessary here.

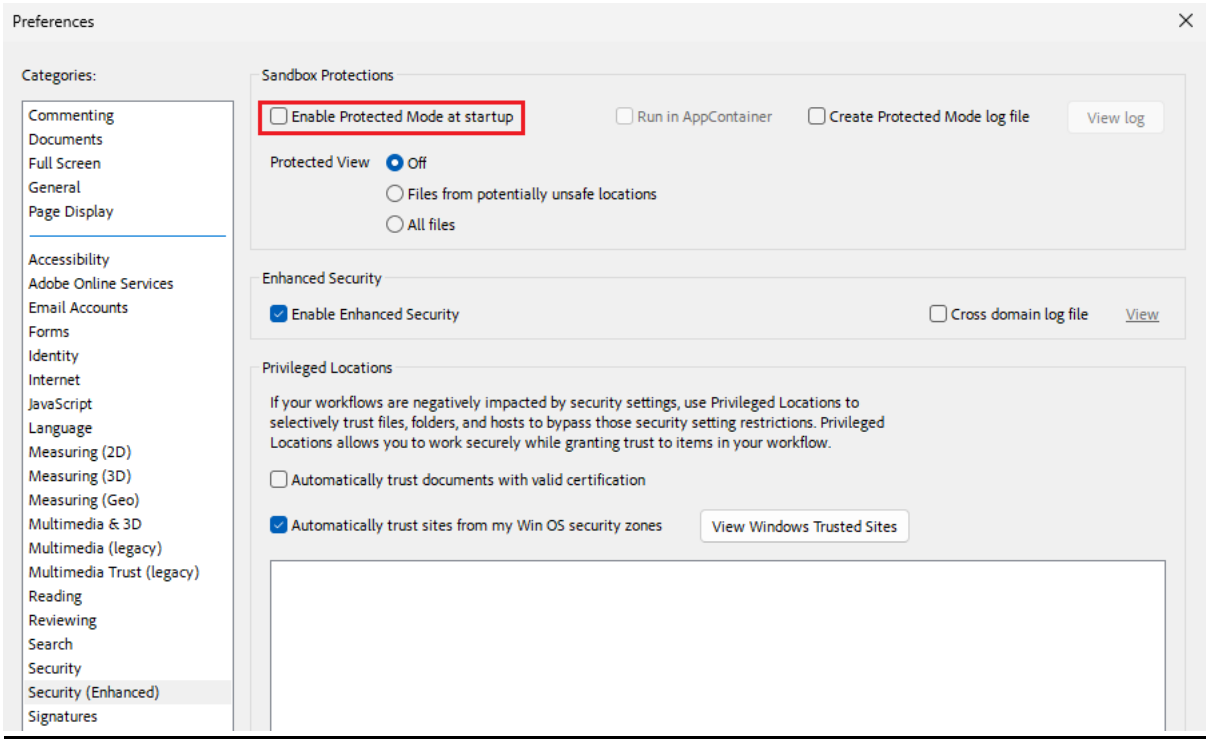
RSA-PSS Padding in Acrobat-Reader.

2)
The parameter is incorrect
Error Code: 2148073511



Reason:

If RSA-PSS padding is enabled as described under 0 then Acrobat Reader has an error in connection with the Acrobat “Protected-mode”. By default, Acrobat Reader DC runs in the so-called “Protected Mode”. This prevents Adobe's own registry settings for RSA-PSS from being read correctly. This leads to the above error.
In order to be able to sign using RSA-PSS keys, the protected mode must be disabled:



There are no known problems with ECC-SSCD keys. No special settings are necessary here.

8.1.1. RSA-PSS Padding in Acrobat-Reader

In conjunction with Minidriver, Acrobat Reader supports RSA-PSS, which is mandatory for SSCD. However, this must be configured in Acrobat Reader.

To do this, please close Acrobat Reader and create the following registration key:

HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\Security\cPubSec\cRSAPSSSigning\bEnableRSAPSSSigning
Typ: REG_DWORD
Value: 1

Then restart Acrobat Reader.

Details can be found at the following link from Adobe:
https://helpx.adobe.com/ee/acrobat/using/whats-new-dc-2017.html#RsaPss

Note:

In addition, the protected mode must be deactivated (as described above). Otherwise Acrobat Reader cannot interpret these registry keys correctly.

8.1.2. Minidriver vs. PKCS#11 in Acrobat Reader

There is the following to note:

If the PKCS#11 library and the Minidriver are configured in parallel in Acrobat Reader and you create a signature via Minidriver, you will see an invalid signature.
If you then click on the signature details then a PKCS#11 error is displayed.
This is a bug in Acrobat Reader. Although signing is done via Minidriver, Acrobat does something on the PKCS#11 module.
However, the signature is not invalid. This means that if you close the document and reopen it, the signature verification works.

We therefore recommend signing in Acrobat Reader exclusively via ACDIS Minidriver. The ACDIS PKCS#11 library should not be configured to avoid the error described above.

8.2. CODESIGNING VIA SIGNTOOL

signtool.exe sign /v /s MY /sha1 "<<SHA-1 fingerprint of certificate>>" /fd SHA256 /tr "<<URL to timestamping-Server>>" /td SHA256 <<File to sign>>

Example:

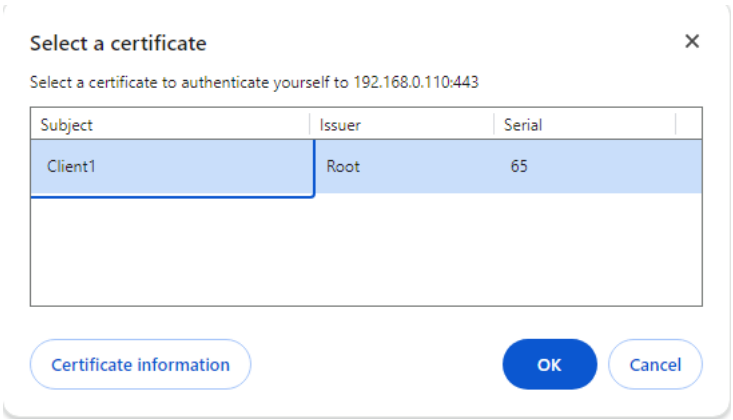
signtool.exe sign /v /s MY /sha1 "d0ace3bc30f63292384c0965db72298c5944dbf5" /fd SHA256 /tr "http://timestamp.digicert.com" /td SHA256 "acdis-pkcs11-64.dll"

Note:

The CodeSigning certificate must be valid and have the Enhanced KeyUsage “Code Signing” set. Otherwise signtool returns an error.

8.3. CHROME / EDGE UND WINDOWS

Chome on Windows supports Minidriver. This means that if there are certificates on the ACDIS smart card that are suitable for SSL client authentication and the respective website requires client authentication, then these will be made available by Minidriver:



Exactly the same applies to the Edge browser.

When you click “OK”, client authentication is carried out.