

ACDIS macOS-CTK User Manual

Version: 1.0.0.0

AUSTRIACARD 

Changed on: 10/07/2024 9:47 AM

Created on: 10/07/2024

Status: FINAL

Table of Content

1.	GENERAL INFORMATION	1
1.1.	COPYRIGHT	1
1.2.	DOCUMENT HISTORY	1
1.3.	MACOS-CTK HISTORY	1
1.4.	DISCLAIMER OF LIABILITY	2
2.	OVERVIEW	4
2.1.	SUPPORTED OPERATING SYSTEMS	4
3.	ACDIS CTK INSTALLATION	5
3.1.1.	Install Homebrew	5
3.1.2.	Install PKCS#11 Library via Homebrew	5
3.1.3.	Uninstall ACDIS CTK.....	6
3.2.	ALL OPERATING SYSTEMS.....	6
4.	UPDATES	7
4.1.	MANUALLY TRIGGERED UPDATES	7
4.2.	CONFIGURE AUTOMATIC UPDATES	7
4.3.	ISSUES AFTER UPDATES.....	8
5.	REGISTRATION OF THE CTK EXTENSION FOR THE LOGGED-IN USER	9
6.	ACDIS CTK – IN USE	12
6.1.	ADOBE ACROBAT	12
6.2.	APPLE MAIL	13
6.3.	SAFARI UND GOOGLE-CHROME	14
7.	KNOWN ISSUES	15
7.1.	AFTER AN UPDATE THE SIGNATURE DOES NOT WORK.....	15
7.2.	ERROR DELETING ACDISTOKENAPP.....	15
8.	TROUBLESHOOTING.....	16

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	10.07.2024	AUSTRIACARD, Markus Punz	First release v1.0.0.0

1.3. MACOS-CTK HISTORY

Version	Date	Author	Description
1.0.0.0	10.07.2024	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 macOS-CTK (CryptoTokenKit). This module is required to use ACDIS smart cards in macOS environments.

2.1. SUPPORTED OPERATING SYSTEMS

- macOS Monterey (Version 12)
- macOS Ventura (Version 13)
- macOS Sonoma (Version 14)

3. ACDIS CTK INSTALLATION

The installation is carried out under macOS using the “Homebrew” package manager. To do this, Homebrew must first be installed if it is not already installed. Skip this step if Homebrew is already installed.

3.1.1. Install Homebrew

For Intel-Mac and Apple-Silicon please execute:

- `/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"`

Please also do the following on Apple-Silicon (ARM) – must be omitted on Intel-Mac:

- `(echo; echo 'eval "$(/opt/homebrew/bin/brew shellenv)"') >> ~/.zprofile`
- `eval "$(/opt/homebrew/bin/brew shellenv)"`

3.1.2. Install PKCS#11 Library via Homebrew

Please execute:

- `brew tap austriacard/acdisctk`
- `brew install --cask acdisctk`

Note:

- On Intel-Mac the above commands install the CryptoTokenKit in the directory `/usr/local/Caskroom/acdisctk/<<Version>>/`
- On Apple-Silicon the CryptoTokenKit is installed in the directory `/opt/homebrew/Caskroom/acdisctk/<<Version>>/`
- A program icon to the CryptoTokenKit (= “ACDISTokenApp”) is created in the Applications folder of your Mac.

3.1.3. Uninstall ACDIS CTK

- `brew uninstall --cask acdisctl`
- `brew untap austriacard/acdisctl`

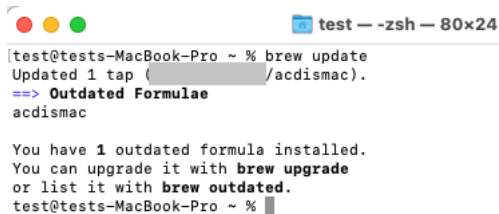
3.2. ALL OPERATING SYSTEMS

Please install the card reader driver recommended by the manufacturer for your device.

4. UPDATES

4.1. MANUALLY TRIGGERED UPDATES

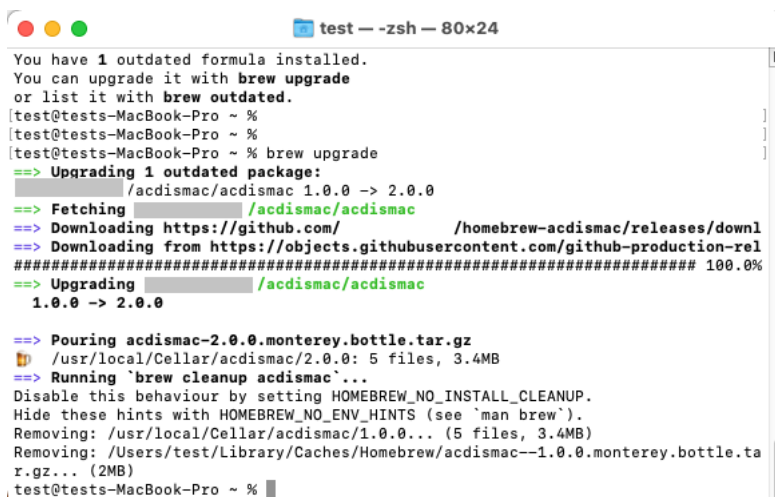
Mac users can run the “brew update” function on the command line. This checks whether there is a new version:



```
test -- zsh -- 80x24
[test@tests-MacBook-Pro ~ % brew update
Updated 1 tap ( /acdismac).
==> Outdated Formulae
acdismac

You have 1 outdated formula installed.
You can upgrade it with brew upgrade
or list it with brew outdated.
[test@tests-MacBook-Pro ~ % ]
```

If a new version is found, it can be installed with "brew upgrade":



```
test -- zsh -- 80x24
You have 1 outdated formula installed.
You can upgrade it with brew upgrade
or list it with brew outdated.
[test@tests-MacBook-Pro ~ % ]
[test@tests-MacBook-Pro ~ % ]
[test@tests-MacBook-Pro ~ % brew upgrade
==> Upgrading 1 outdated package:
 /acdismac/acdismac 1.0.0 -> 2.0.0
==> Fetching /acdismac/acdismac
==> Downloading https://github.com/ /homebrew-acdismac/releases/downl
==> Downloading from https://objects.githubusercontent.com/github-production-rel
##### 100.0%
==> Upgrading /acdismac/acdismac
1.0.0 -> 2.0.0

==> Pouring acdismac-2.0.0.monterey.bottle.tar.gz
 /usr/local/Cellar/acdismac/2.0.0: 5 files, 3.4MB
==> Running `brew cleanup acdismac`...
Disable this behaviour by setting HOMEBREW_NO_INSTALL_CLEANUP.
Hide these hints with HOMEBREW_NO_ENV_HINTS (see `man brew`).
Removing: /usr/local/Cellar/acdismac/1.0.0... (5 files, 3.4MB)
Removing: /Users/test/Library/Caches/Homebrew/acdismac--1.0.0.monterey.bottle.ta
r.gz... (2MB)
[test@tests-MacBook-Pro ~ % ]
```

4.2. CONFIGURE AUTOMATIC UPDATES

The Homebrew package manager can be configured to install upgrades automatically. To do this, please run the following in a terminal window:

```
brew tap homebrew/autoupdate
mkdir -p $HOME/Library/LaunchAgents
```

If you want to check for updates every 24h (= default)

```
brew autoupdate start --upgrade
```

Alternatively: If you want to check for updates every hour (= 3.600 seconds)

Please specify the desired update-interval in seconds

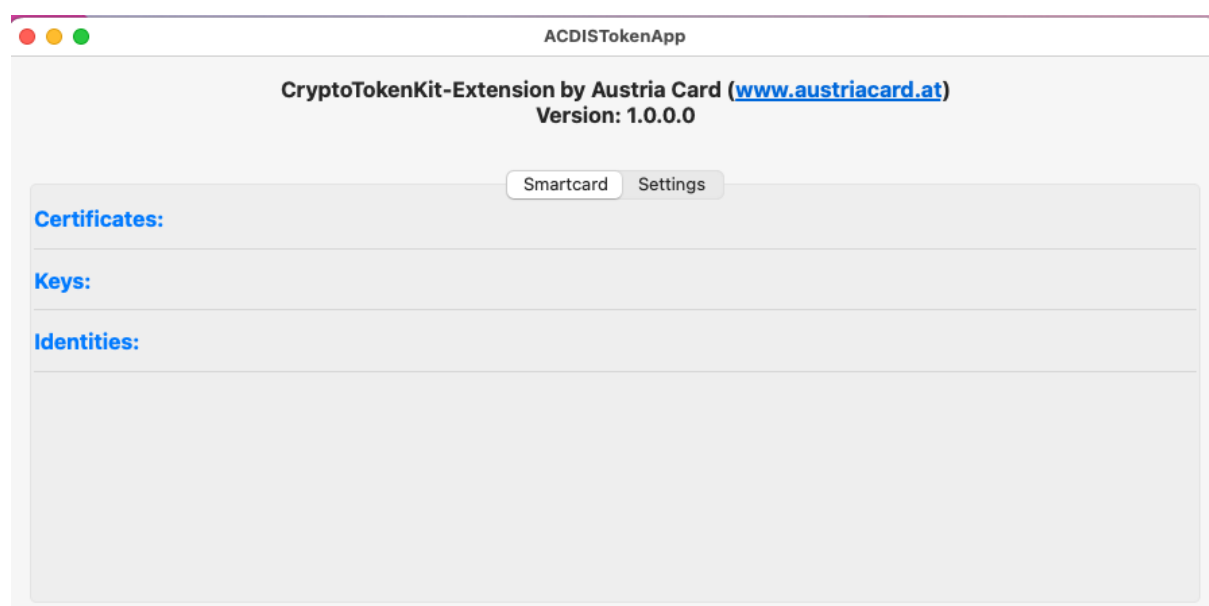
```
brew autoupdate start 3600 --upgrade
```

To stop automatic updates you can do the following:

```
brew autoupdate stop
```

4.3. ISSUES AFTER UPDATES

If an ACDIS smart card is inserted and there are certificates on it, they sometimes do not appear in the “ACDISTokenApp”. A blank window will be displayed:

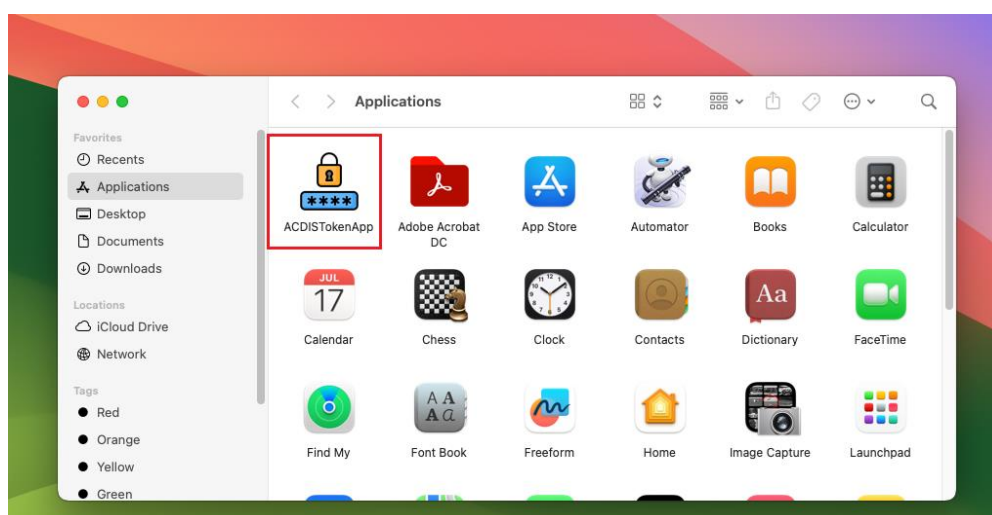


In this case, please restart macOS.

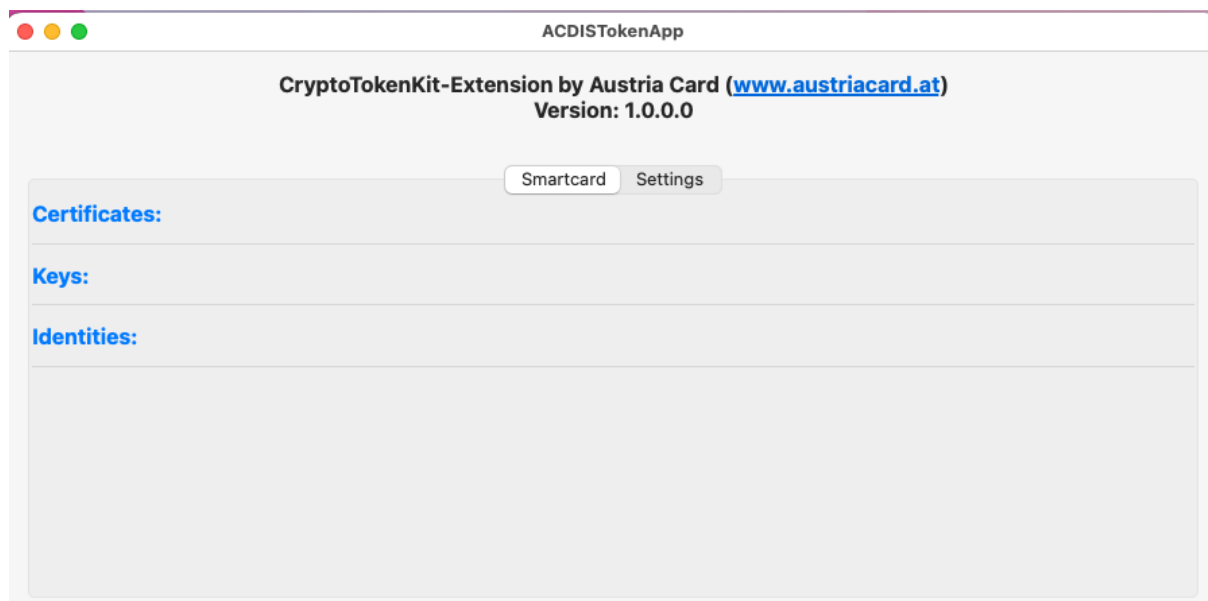
5. REGISTRATION OF THE CTK EXTENSION FOR THE LOGGED-IN USER

To use ACDIS CTK, it must be configured for the first time.

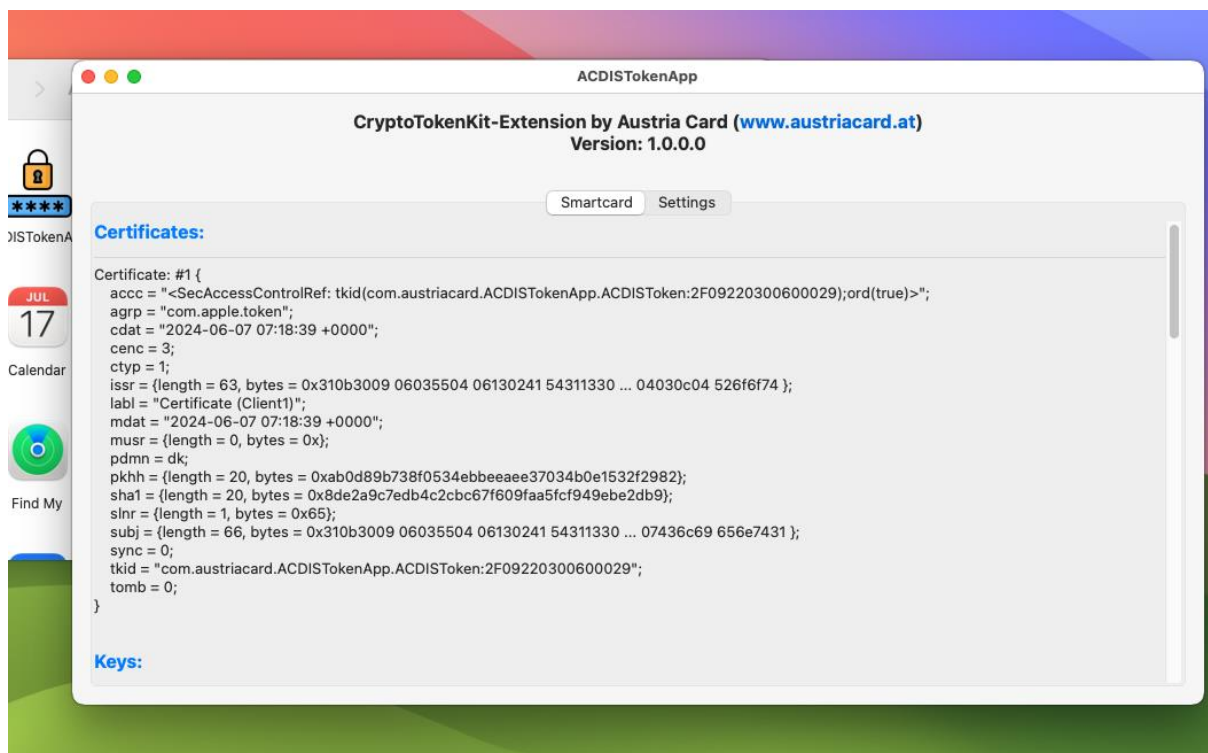
- a) Please plug in the Mobility Card Reader
- b) The CTK extension is displayed as „ACDISTokenApp“ in the Applications folder:



- c) Please run „ACDISTokenApp“
- d) This shows the following window:



- e) Now insert the ACDIS smart card or, if it is already inserted, remove it and insert it again.
- f) If you now close the ACDISTokenApp window and reopen it, the Certificates of the smart card must be displayed:



You can then close the ACDISTokenApp (Quit) or let it continue running. This is not relevant.

Note:

Every time after inserting the ACDIS smart card, the operating system shows a pairing notification on the desktop:



Smart card pairing is not supported. This notification can be ignored.

If desired, smart card pairing can be disabled. Then this notification will no longer be displayed. To do this, run the following command in the terminal:

```
sudo defaults write /Library/Preferences/com.apple.security.smartcard  
UserPairing -bool false
```

6. ACDIS CTK – IN USE

The ACDIS CTK extension provides read-only functions for reading the smart card and using cryptographic functions (signature/encryption). Functions for writing, especially for generating keys and applying certificates are not available via CTK.

To do this, please use the ACDIS PKCS#11 Manager or the ACDIS PKCS#11 library.

6.1. **ADOBE ACROBAT**

The support of smart cards via the CTK extension is very unusually implemented by Adobe. Acrobat derives the signature algorithm to be used (RSA-PKCS#1v1.5 or ECDSA) from the signature algorithm with which the signature certificate is signed.

This means that if the signature certificate was signed with ECDSA by the respective certification authority, then ECDSA is also requested to sign the document. If the signature certificate is signed with RSA-PKCS#1 then RSA-PKCS#1 is requested for the signature of the document.

Note:

The RSA-PSS algorithm is currently not supported by Acrobat via CTK.

Summary:

- For simple signatures (= Generic-Application), Acrobat supports ECC signatures if the signature certificate is signed with ECDSA.
- For simple signatures (= Generic-Application), Acrobat also supports RSA-PKCS#1v1.5 if the signature certificate is signed with RSA-PKCS-#1v1.5.
- For qualified signatures (= SSCD-Application), Acrobat supports ECC signatures if the qualified signature certificate is signed with ECDSA.
- **RSA-PSS is not supported** - neither Generic nor SSCD. Here Acrobat displays an error.

Note:

If the signature certificate and signature key algorithms do not fit together, Acrobat displays an error. For example, if it is an ECC signature key and the associated signature certificate is signed with RSA. In this case, Acrobat requests RSA as the signature algorithm, which is not possible with an ECC key.

Furthermore:

The SHA-1 hash algorithm is deprecated for signature certificates. The certificate must be signed at least using SHA-256.

If the certificate is signed with SHA-1, Acrobat lets you select the certificate for signing, but then an error occurs.

6.2. APPLE MAIL

Signature algorithms:

- For simple signatures (= Generic-Application), Apple Mail supports RSA and ECC keys
- For qualified signatures (= SSCD-Application), Apple Mail supports ECC signatures.
- RSA-PSS is not supported - neither Generic nor SSCD.

Furthermore:

The signature certificate must have the extension enhanced key usage "Secure Email" set. Furthermore, the common name must contain the sender's email address. Only then signature creation will be offered by Apple Mail.

To encrypt emails, you have to import the encryption certificates into the macOS Keychain and then right-click under “Certificates” and select “New Certificate Preference”. Here you have to enter the email address to which the certificate should be assigned. If you subsequently send an email to this address, you can select the encryption option.

6.3. SAFARI UND GOOGLE-CHROME

Algorithms:

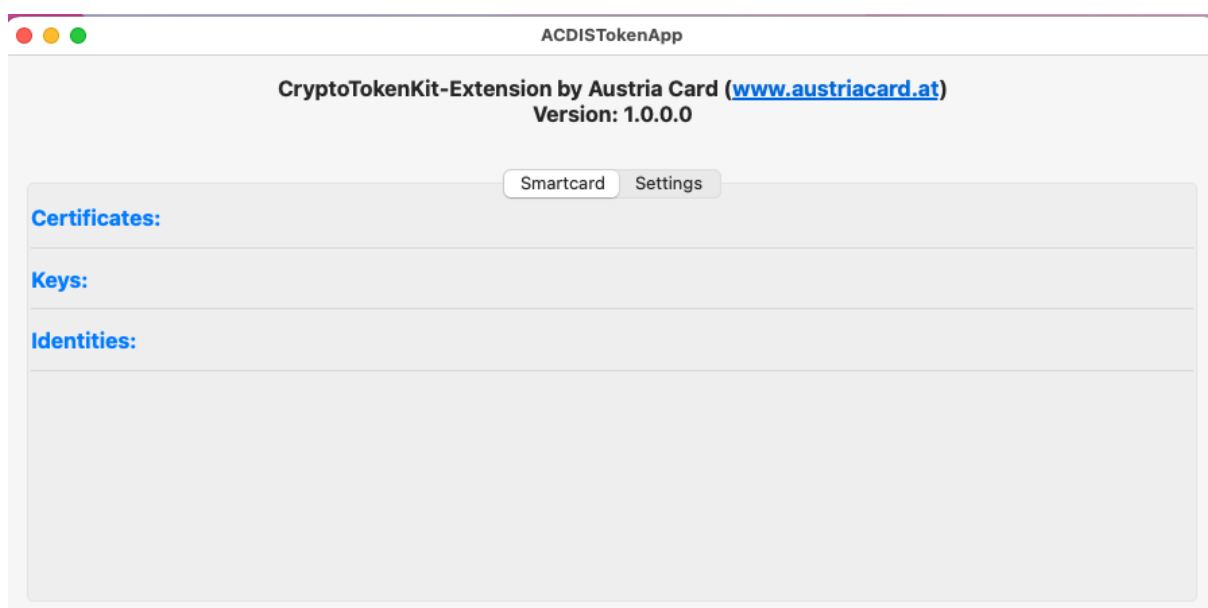
- RSA-PSS: Standard with TLS 1.3
- RSA-PKCS#1
- ECC

If the web server requires client authentication, a selection dialog will be displayed in the browser window in which the desired certificate must be selected. If no certificate selection window appears, then no suitable certificate is available for client authentication. Only if at least 1 certificate comes into question a selection window will be displayed. You will then be asked to enter your PIN.

7. KNOWN ISSUES

7.1. AFTER AN UPDATE THE SIGNATURE DOES NOT WORK

If an ACDIS smart card is inserted and there are certificates on it, they sometimes do not appear in the “ACDISTokenApp”. A blank window will be displayed:



In this case, please restart macOS.

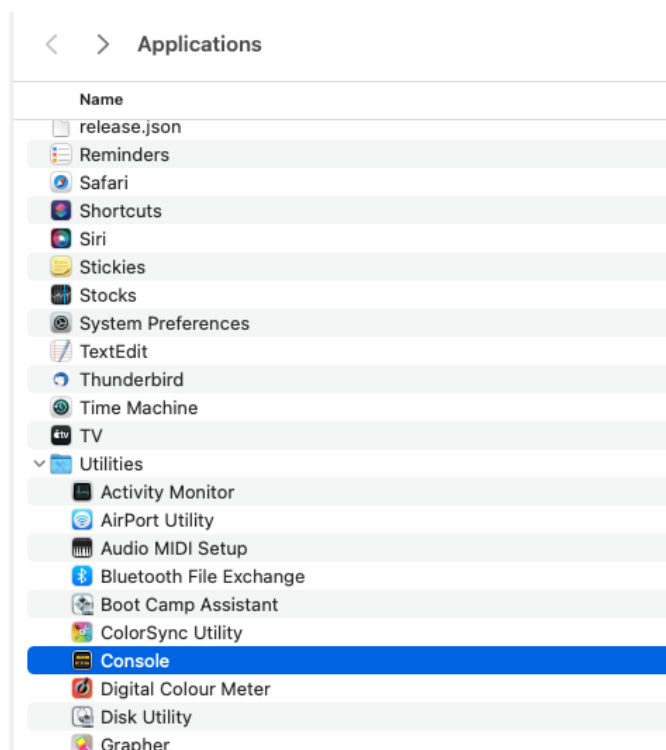
7.2. ERROR DELETING ACDISTOKENAPP

If you delete the “ACDISTokenApp”, an error may occur that it is “in-use”. You have to unplug the card reader and wait a few seconds - then you can delete the app.

8. TROUBLESHOOTING

In the event of an error, a log file can be generated via the Console.App.

Start Applications – Utilities – Console:



Filter for “ACDIS” and click <ENTER>.

Click on “Start”.

