ProID

Installing the ProID+ software for macOS

Installation guide

Submitted by MONET+,a.s.
Za Dvorem 505, Zlín - Štípa

Prepared by: 16/06/2021
Version number: 1.1.

1 AUTHORSHIP STATEMENT

2 TABLE OF CONTENTS

3 INTRODUCTION

To use the electronic functions in the macOS environment the ProID+ software must be installed on the PC.

The current package revision installation support for ProID+, ProID+Q, ProID+QSeal and ProID+NG cards.

This document describes how *ProID+* is to be installed on computers with the macOS operating system.

The software is installed using a PKG installation package that serves as a graphical installation guide.

4 INSTALLED SW

The ProID+ software package contains complete support for electronic functions for macOS. After a successful installation, Mac users will have all the software applications available for ProID cards that the macOS offers.

The installed ProID+ package includes several separate software applications that work with a ProID chip card. This concerns:

- The chip drivers (PKCS#11, CryptoTokenKit, TokenD) of the ProID+, ProID+NG, ProID+Q and ProID+QSeal cards for working with certificates and creating electronic signatures.
- The CardManProID.app (hereinafter referred to as ProID Card Manager), for managing certificates and card access codes.

In the following sub-chapters, the characteristics of the individual installed applications are briefly described.

4.1 PROID CARD ADMINISTRATOR

The ProID Card Administrator is an application for managing user certificates and access codes for ProID cards.

The user can, for example, use the ProID Card Administrator to:

- View the list of cryptographic keys on the chip.
- View information about the certificates on the chip.
- Import or delete a certificate.
- Set, unblock or change any of the access codes (PUK, PIN,...).
- Diagnose problems with the reader, chip, certificates, ...

4.2 CHIP DRIVERS

In order to work with electronic certificates, it is necessary to install the cryptographic drivers on the operating system.

The ProID card drivers will allow applications to work with the certificates stored in the card chip. The drivers, certificates (and keys) can be used for:

- electronic signature (documents, emails, etc.);
- signing in (e.g. to a website).

However, the drivers are also used to **manage certificates** on the chip:

- Reading the information on saved certificates.
- Creating or registering new certificates and cryptographic keys.
- Deleting unnecessary certificates and keys.

Another important function of the drivers is to work **with access codes**:

- displaying the window for entering the code;
- checking the code values against the chip;

- change the code value;
- blocking the code after repeated incorrect entry;
- etc.

The drivers comply with the recognised technical standards for the integration of chip cards into macOS operating systems:

- The **CryptoTokenKit -** the driver is designed to work with certificates in native macOS applications (e.g.: Mail, Safari, etc.).
- The **tokenD** - an older version of the driver, used by native macOS applications (e.g.: Spanner, Mail, Safari, etc.). This driver can be installed on the older version of the macOS (up to version 10.15).
- **PKCS#11** - driver for applications that do not rely on the macOS functions, but implement their cryptography (e.g.Firefox, Thunderbird, etc.).

5 BEFORE STARTING THE INSTALLATION

The installation of ProID + software must be carried out in the following steps:

- Download the installation package
  - see section 5.2
- Start the installation package
  - as the Operating System admin
  - see section 6.1
- Perform all the installation steps
  - the user's graphical installation guide provides continuous instruction
  - see section 6

5.1 COMPUTER STATUS BEFORE INSTALLATION START

The operating system does not need to be specifically modified to perform the installation. The proID + software installation guide will take care of everything that's necessary.

An internet connection is not necessary for the proID + installation itself. An Internet connection is only required to download the installation package.

To install the ProID + software, it is not necessary to have a reader and reader drivers installed on the Mac. The card reader can be installed only after the *ProID*+ software is installed. However, it is recommended that the **reader is installed before installing the *ProID*+ software**.

The installation of the *ProID*+ software must be run under a user account that has the **admin rights for the operating system**. If the user does not have the specified permissions, they should contact the Operating System Administrator and ask them to perform the installation.

Before starting the installation, it is recommended to save the work in progress and stop running applications. The installation wizard requires a restart of the operating system after completing the installation.

5.2 DOWNLOAD THE INSTALLATION PACKAGE

Installing the *ProID* application is done using the installation package. The **installation file is stored in the form of a disc image (DMG) and must be downloaded from the Internet**, from the ProID card support website. .

In the disc image itself (DMG), a graphical installation package is stored in the PKG format, which will guide the user through the installation process itself.

When downloading the installation package, the user should note to which directory the download file is saved - so that the installation program can be run from this directory.

Both the *initial* installation and *ProID* + software *upgrades* can be performed using the installation package. Users that have an older version installed can download the current version and start the installation - an upgrade to the latest version will be made.

5.3 VERIFYING THE ORIGIN OF THE INSTALLATION PACKAGE

Before installing the software, the user should always verify that the software comes from a reliable source and that no one has manipulated the contents of the package. Installation of untrusted or modified software creates the risk of a computer virus or other harmful software getting inside the Mac.

The ProID+ installation package is electronically signed using the Monet+,a.s. certificate. The macOS operating system automatically checks the electronic signature of the installation package before installation. If the installation package is not signed with a trustworthy certificate (or an appropriate key), the operating system will not allow the installation to be carried out.

After verifying the electronic signature of the installation package, the user can trust that they are using the original ProID+ package that does not contain harmful software.

More on verifying the integrity and origin of the installation package in chapter 11

6 START-UP AND INSTALLATION EXECUTION

The installation of the *ProID+* driver software is performed using a **graphical installation guide** stored on the downloaded disc image.
The graphical installation guide controls the installation progress and is designed to simplify the work of a normal user as much as possible.

6.1 STARTING THE INSTALLATION

The installation is started by running the installation program downloaded from the ProID support website.
The user downloads the disc image in DMG format and starts the installation program stored in the *ProID+.pkg* file.

6.2 MOUNTING THE DISC IMAGE

When the disk DMG is run, the image is automatically mounted. The operating system will then automatically display its contents.

Figure1: Mounting the disc image

The user must select the *ProID +.pkg* installation file and run it.

6.3 WELCOME WINDOW

As the next step, the *ProID+* software installation wizard window appears:

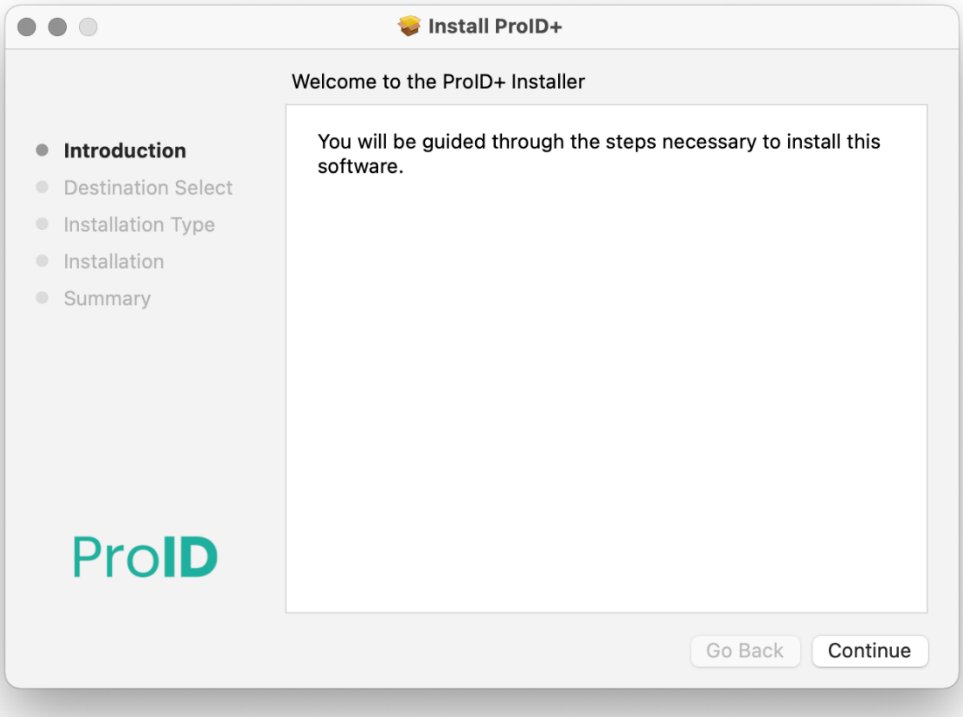

Figure2: The ProID+ installation wizard welcome window

To continue the installation process, it is necessary to press the *Go* button.

6.4 INSTALLATION TYPE

The next window displays the following installation options:

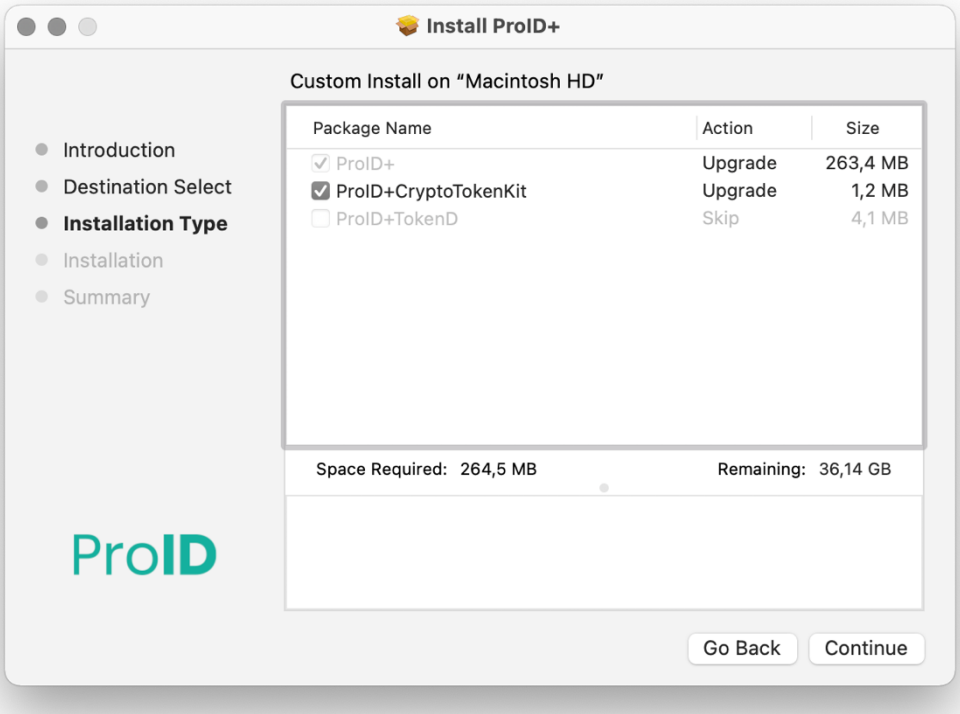

Figure3: The installation options window

In this window, it is possible to change the commonly installed CryptoTokenKit driver to the tokenD driver.

» The CryptoTokenKit driver can be installed on macOS 10.13.5 or higher operating systems.

» The tokenD driver can be installed on macOS 10.15 or older operating systems.

It is always possible to install only one driver type. More information about the ProID card drivers is described in section 8.1.

To continue the installation process, it is necessary to press the *Continue* button.

6.5 INSTALLATION PROGRESS

In the next step, the user will start the installation using the *Install* button:

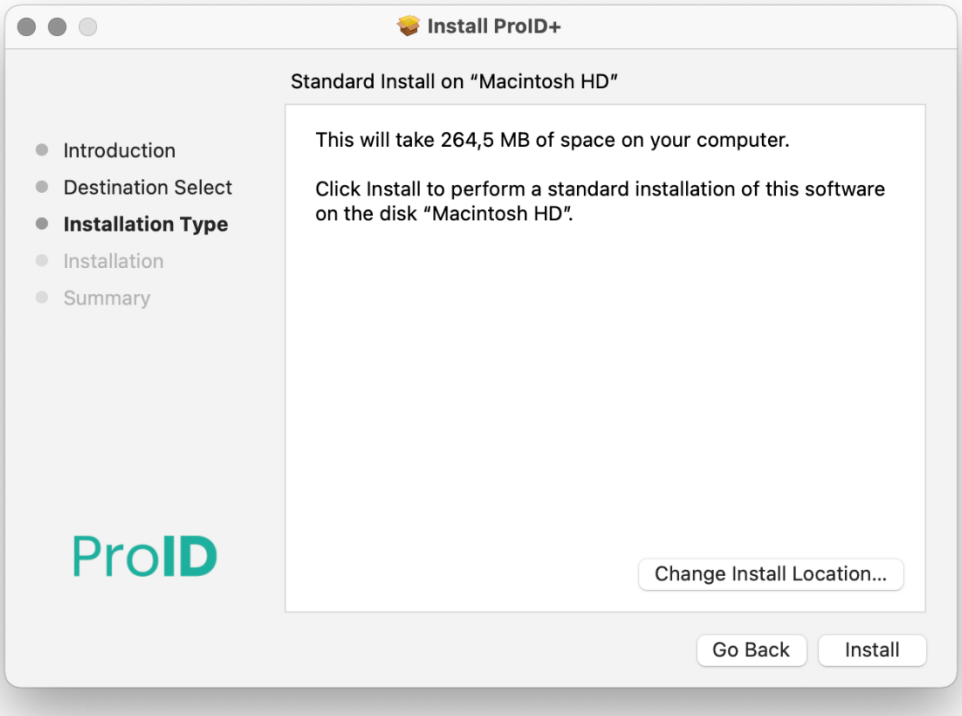

Figure5: Window to start the installation process

Warning: The installation program must be run under a user account with **admin rights for the operating system**. If the installation is run under a user account that does not have admin rights, the installation wizard displays the operating system window to increase (change) the user's rights. An unprivileged user can enter the name and password of the administrator account in this window to authorize the subsequent installation process. When the installation is completed, ProID+ will be available to all PC users.

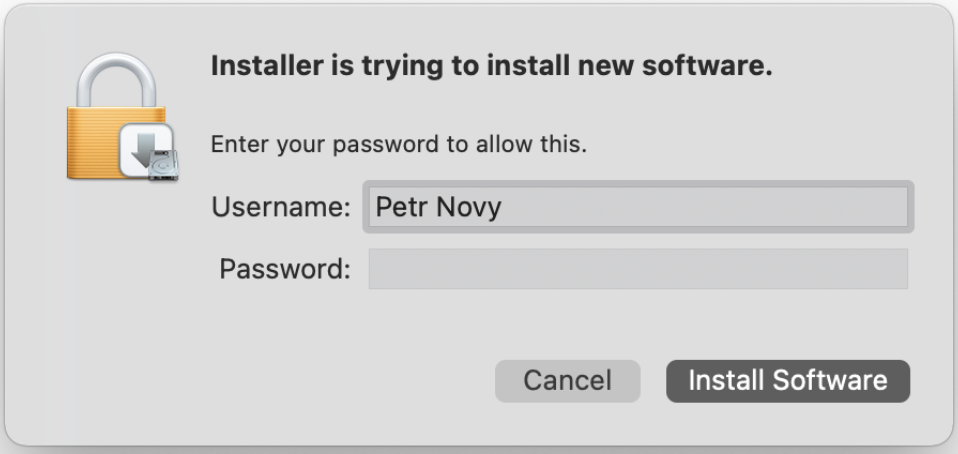

Figure6: Rights elevation window, to approve the installation by the admin account

When started, the files and configurations of the operating system are installed. The installation process takes place automatically; it is necessary to wait for the completion of the process:

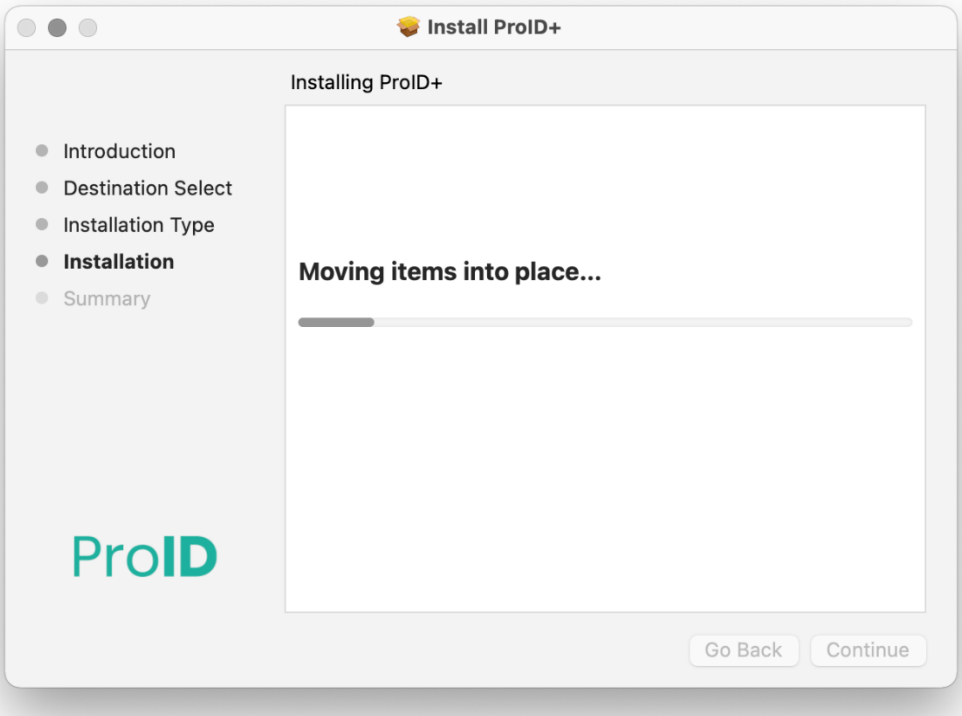

Figure7: The ProID+ software installation progress

The installation package automatically executes all the necessary steps:

» It installs the application and configuration files.

- It performs the application registration.
- It installs the app in the *Applications* (*/Applications*) folder.

During the installation, the installation wizard may require a PC admin permission, in which case permission must be granted. In this step, the installation wizard registers the ProID card drivers (CryptoTokenKit interface or tokenD).

Figure8: The ProID+ software installation progress - admin permission

6.6 COMPLETION OF INSTALLATION

When the installation is complete, the installation guide displays information about the result:

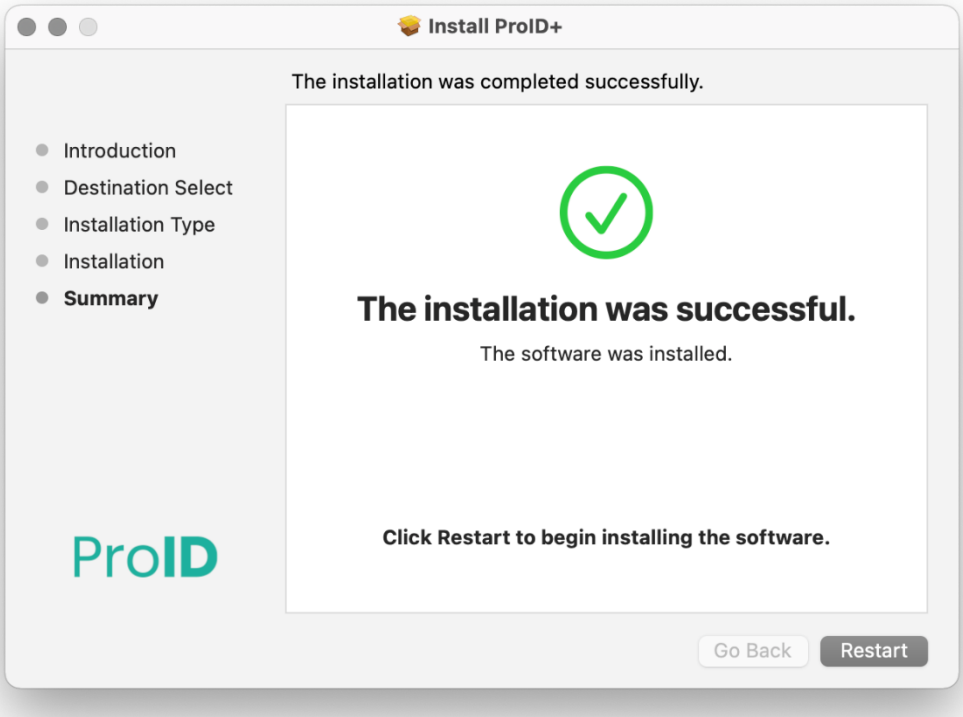

Figure9: The ProID+ software installation completion window

To successfully complete the installation, the operating system must now be restarted.

The ProID Card Administrator executable is available in the usual Application (/Applications) folder after installation:

» CardManProID.app.

The installation wizard window can be closed to restart the Mac using the *Restart* button.

7 READERS

The *ProID+* software communicates with the chip card via a chip card reader. It is not possible to use electronic functions without a chip card reader. Therefore, the user must:

» get a suitable card reader,

» connect the reader to the Mac,

» and possibly install the drivers for the reader.

7.1 READER SELECTION

A reader that is in accordance with the CCID standard and cooperates with the PC/SC subsystem of the operating system must be acquired and connected to the macOS operating system computer.

The *ProID+* software can cooperate:

» both with common readers (with no integrated keyboard);

» as well as with readers that have their own keyboard, or even display.

7.2 READER DRIVER

A card reader, like any device connected to a PC, must have an appropriate driver installed in the operating system. If the correct driver is not installed, the operating system cannot communicate with the reader and the reader will not work.

Warning: **Reader drivers are not included in the *ProID+* installation package.** The reader commissioning (including the possible installation of drivers) must be carried out separately - outside the installation of the *ProID+* software.

Some readers (Plug&Play) *do not require* drivers to be installed, or the operating system will find and install the necessary drivers. It is necessary to install the driver separately for other readers. The installation of drivers requires admin rights - the drivers can only be installed by a user with admin rights for the operating system.

The retailer or supplier of the reader should inform the user if it is necessary to install a driver (in the given operating system). If an installation is required, the retailer or supplier should provide an installation package with reader drivers. The user must then ensure that the drivers are installed.

7.2.1 Verifying the functionality of the reader driver

In the macOS operating system, the functionality of the readers is dependent on the *PC/SC Lite* service. This service is a standard part of the operating system.

The functionality of the reader can be verified, for example, with the *pcsctest* command run from the command line. The program lists all the connected readers and prompts the user to select the reader to be tested. The user is then prompted to enter the card in the desired reader. The first part of the test will take place and the user is prompted to select the tested reader again. Upon completion of the test, the application displays the resulting status. The user should see the ATR Cards (*Current Reader ATR Value*) during the test and the reader name *(Current Reader Name*).

```
MUSCLE PC/SC Lite Test Program

Testing SCardEstablishContext    : Command successful.
Testing SCardGetStatusChange
Please insert a working reader   : Command successful.
Testing SCardListReaders         : Command successful.
Reader 01: Gemalto PC Twin Reader
Enter the reader number          : 1
Waiting for card insertion
                                 : Command successful.
Testing SCardConnect             : Command successful.
Testing SCardStatus              : Command successful.
Current Reader Name              : Gemalto PC Twin Reader
Current Reader State             : 0x54
Current Reader Protocol          : 0x0
Current Reader ATR Size          : 19 (0x13)
Current Reader ATR Value         : 3B 7E 94 00 00 80 25 D2 03 10 01 00 56 00 00 00 02 02 00
Testing SCardDisconnect          : Command successful.
Testing SCardReleaseContext      : Command successful.
Testing SCardEstablishContext    : Command successful.
Testing SCardGetStatusChange
Please insert a working reader   : Command successful.
Testing SCardListReaders         : Command successful.
Reader 01: Gemalto PC Twin Reader
Enter the reader number          : 1
Waiting for card insertion
                                 : Command successful.
Testing SCardConnect             : Command successful.
Testing SCardStatus              : Command successful.
Current Reader Name              : Gemalto PC Twin Reader
Current Reader State             : 0x54
Current Reader Protocol          : 0x0
Current Reader ATR Size          : 19 (0x13)
Current Reader ATR Value         : 3B 7E 94 00 00 80 25 D2 03 10 01 00 56 00 00 00 02 02 00
Testing SCardDisconnect          : Command successful.
Testing SCardReleaseContext      : Command successful.

PC/SC Test Completed Successfully !
```

Figure 10: Verifying the functionality of the reader using pcsctest

After successful completion of the test, the following information should be listed: *PC/SC Test Completed Sucessfully!*

7.3 CONNECTING THE READER

The reader must be connected to the PC via a connector for the given reader type. The most common readers are supplied with a USB cable. These must be connected to a free USB port on the Mac. USB readers are powered directly via the Mac USB port and can be used immediately after the drivers have been installed.

It is not advisable to extend the USB cable to the reader using extension USB cables due to a drop in the power supply.

8 INTEGRATION OF INSTALLED SOFTWARE

In order to work with **electronic certificates**, it is necessary to **integrate the ProID card drivers** into the operating system or in the applications used. The drivers are part of the installation - they need to be connected to the applications. The procedure for integrating drivers into the operating system and applications is described in the following sub-chapters.

8.1 PROID CARD DRIVER TYPES

The proID+ installation also includes chip drivers. For work with certificates. Drivers are installed:

- The **CryptoTokenKit -** the driver is designed to work with certificates in native macOS applications (e.g.: Mail, Safari, etc.).
- The **tokenD** - an older version of the driver, used by native macOS applications (e.g.: Spanner, Mail, Safari, etc.). This driver can be installed on the older version of the macOS (up to version 10.15).
- **PKCS#11** - driver for applications that do not rely on the macOS functions, but implement their cryptography (e.g.Firefox, Thunderbird, etc.).

8.1.1 CryptoTokenKit

The CryptoTokenKit driver can be used for three basic operations (depending on the type of certificate):

- Login/Authorization (Safari, LoginWindow, PKINIT, SSH, Screensaver)
- Signature (Mail)
- Encoder (Mail, Keychain Access)

Login (Authorization)

The operating system supports verification by means of chip cards, incl. login with a certificate to the website using Safari.
macOS also supports verification using the Kerberos protocol.

Digital signature and encoding in the Mail application

In the Mail application, the user can send messages that are digitally signed and encoded. The e-mail address of the sender must be the same as the e-mail stated on the certificate.

Data protection Keychains

Passwords in the keychain can be protected using the keys stored with certificates on the ProID cards. The ProID cards can be used to secure the use of Keychain passwords. Passwords from the Keychain can be used after entering the ProID card in the reader and entering the PIN.

8.1.2 PKCS#11

Applications that **do not use the operating system interfaces** do not **communicate directly with PKCS#11**. In order for these applications to work with certificates on ProID cards, the user must configure the correct PKCS#11 (sometimes called Cryptoki)libraries. The configuration method of the library is different for each application, the user should find the correct way in the application's technical documentation.

For each type of ProID card, a different PKCS#11 library is specified:

- ProID+ card
  - Location of PKCS#11 libraries /usr/local/lib/ProIDPlus/libproidcm11.dylib
- ProID+Q card

- Location of PKCS#11 libraries /usr/local/lib/ProIDPlus/libproidqcm11.dylib

- ProID+NG card
  - Location of PKCS#11 libraries /usr/local/lib/ProIDPlus/libproidngcm11.dylib

The procedure for the configuration of the PKCS#11 driver for Firefox and other applications is described in chapters 8.3 and 8.4.

8.1.3 TokenD

An older version of the driver. In later versions of macOS, the *TokenD* is replaced by the *CryptoTokenKit* driver.

There is no need to configure applications that use drivers via tokenD. The operating system itself ensures that these applications can work with the ProID card.

The certificates from the ProID cards can be viewed using the TokenD in the *Keychain Access* application.

8.2 CRYPTOTOKENKIT DRIVER INTEGRATION

The macOS operating system since version 10.14 no longer supports the tokenD interface. The ProID+ software responds to changing supported card drivers in macOS. In later versions, therefore, ProID+ installs the CryptoTokenKit driver. Using the CryptoTokenKit interface, certificates from ProID cards can be used in native applications such as Mail, Safari, etc...

From the user's perspective, a transition to CryptoTokenKit means new options, but also some limitations:

- With the cryptographic key from the Keychain (*Keychain Access*) data can be encoded. After encoding, it is possible to approve the safe use of the Keychain data by the ProID card - e.g., to sign in to the operating system. More about the protection of the Keychain in chapter 8.2.1.
  For the activation of the Keychain protection, it is necessary to match the ProID card with the operating system - see section 8.2.2.

- The user cannot choose which certificate to be used in native applications, e.g., for an electronic email signature.
  (The original tokenD driver enables the selection of the certificate in the key.)

- You cannot view the list of certificates stored on the chip card in the keychain. (The key card offered this option for the older tokenD driver.)
  The contents of the ProID card chip can be viewed using the *ProID Card Administrator* application, see also section 4.1. For technical display of the chip content, the terminal command can also be used:
  SPSmartCardsDataType system_profiler:
  `$ system_profiler SPSmartCardsDataType`

8.2.1 Data protection Keys using ProID cards

A user that has a *commercial* certificate stored in the ProID card can use the tab to secure the Keychain data. The commercial certificate key can encode the passwords in the key. The ProID tab can then be used to approve the use of Keychain passwords. The ProID tab can then be used by the user, e.g., to log on to the operating system or to the Safari website. The user must confirm using the ProID card for signing in by entering a PIN.

Technically, the data in the key is encoded with the public key of the selected certificate. Before using data from the Keychain, a private key (protected in a chip) must be used to decipher the data. The user must approve the operation with a private key using a PIN.

If the operating system finds that a suitable certificate with a key is stored in the ProID chip card, it automatically offers the possibility to use the Keychain data protection key. When the card is entered into the

reader, the card pairing process is started. During pairing, the key to protect the Keychain data is selected. The pairing process is described in the ProID Card Pairing section.

8.2.2 Pairing ProID Cards

When an unmatched card is entered into the reader, the operating system automatically starts the pairing process:

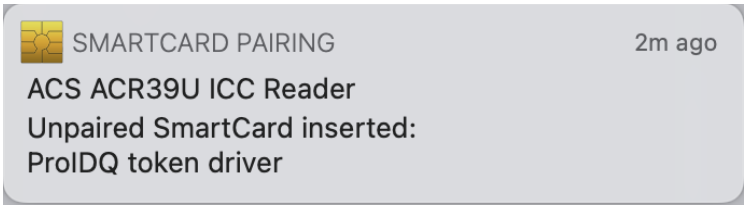

Figure12: Window to Pair a User Account Card

In the *ID card* list, the user selects the certificate key identifier that he/she wishes to pair with their user account. The pairing is confirmed by using the *Pair* button:

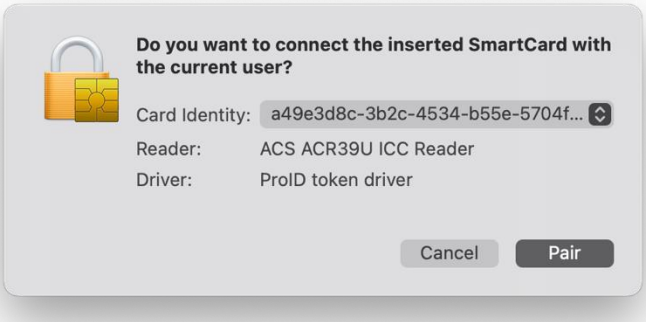

Figure13: Confirming the pairing of a card with a user account

Click on *Pair* to match the selected certificate to the user account. The user is prompted to enter a password for the user account:

Figure14: Enter Pair Approval Password

After entering the password, the user is prompted to enter the ProID card PIN value:

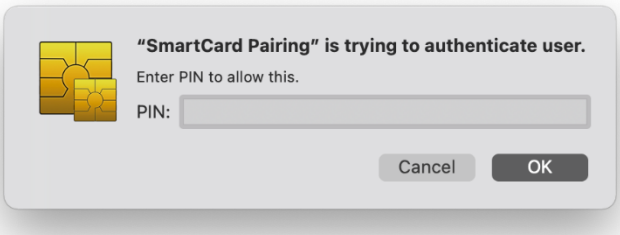

Figure154: Confirming the pairing of the ProID card with the user account

After entering a valid PIN value, the user is once again prompted to enter a password for the user account:

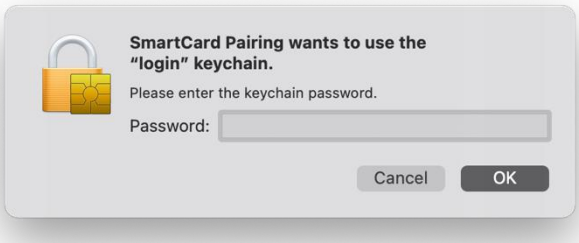

Figure16: Enter Pair Approval Password

The pairing of the certificate on the ProID card is completed with this step. The pairing does not verify the validity of the certificate and is valid until it is cancelled by the user.

The successful pairing of the certificate can be verified by the *sc_auth sheet* command that will be run in the terminal window. The command displays the identity of the paired certificate key (hash). If multiple certificates (from different chip cards) are paired, all of them are displayed.

Example of a list of paired certificates:

```
$ sc_auth list

Hash: 0B2BEA714EE562AAD60C33D5C7F82572AB26C2C7
```

If the user wants to cancel the pairing of the certificate, the *sc_auth unpair hash command can be used.* For example, it is advisable to cancel pairing when the paired certificate is expired and a new certificate needs to be paired.

```
$ sc_auth unpair 0B2BEA712EE563AAD60C33D5C7F82572AB26C2C7
```

8.2.3 More information on pairing ProID cards

By pairing the ProID card, there is no *obligation* to use the card with each access to the Keychain data. If the paired card is not entered in the reader, passwords from the Keychain will be used in the same way as when the user did not match the card at all. You can also always log in with a password to the operating system.

Pairing is only available when a *commercial* certificate with a key is stored on the chip. The *commercial* certificate keys can be used for encoder operations. If only the certificate for *electronic signature* is found on the chip, the pairing and data protection of the Keys are not offered. The signature certificate key cannot be used for encoding.

The user can refuse to pair the chip card. In this case, the operating system repeatedly calls for pairing each time an unpaired card is entered.

The operating system does not check the validity of a certificate whose key is protected by the Keychain data. The keychain's data protection operates even after the validity of the certificate has expired.

Only one certificate or key from the ProID card can be paired with the user account. If there are more usable certificates stored on the chip, the user must select when pairing which one is to be used to protect the Keychain data. After a successful pairing, the operating system no longer alerts about the pairing option.

The user has the option to turn off the pairing alert by using the *sc_auth pairing_ui -s disable* command:

```
$ sc_auth pairing_ui -s disable
```

This command permanently disables the pairing alert for all chip cards (not only for ProID cards).

Activation/deactivation of pairing can be verified by the command*sc_auth pairing*_ui -s status :

```
$ sc_auth pairing_ui -s status
```

Deactivated pairing can be re-activated with the *sc_auth pairing_ui -s enable:* command.

```
$ sc_auth pairing_ui -s enable
```

Keychain data can be encoded using several keys - from different chip cards. Before using data from the Keychain, the operating system will detect the entered card and use the available key to access the Keychain data.

8.3 INTEGRATION OF PKCS#11 INTO MOZILLA●

For illustration, this document displays the integration of the ProID card driver into the Mozilla Firefox application. It is probably the most popular and most commonly used application that uses PKCS#11's PKCS#11 interfaces.

The ProID card driver can be added to the application using the *Safety Device* menu in the *Options* menu *of the Safety and Safety Options menu.*

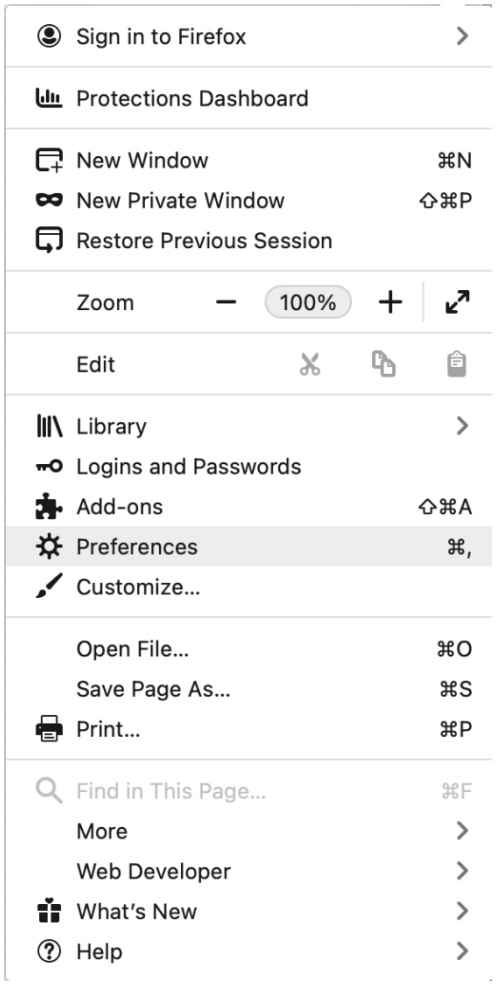

Figure17: Mozilla• application menu

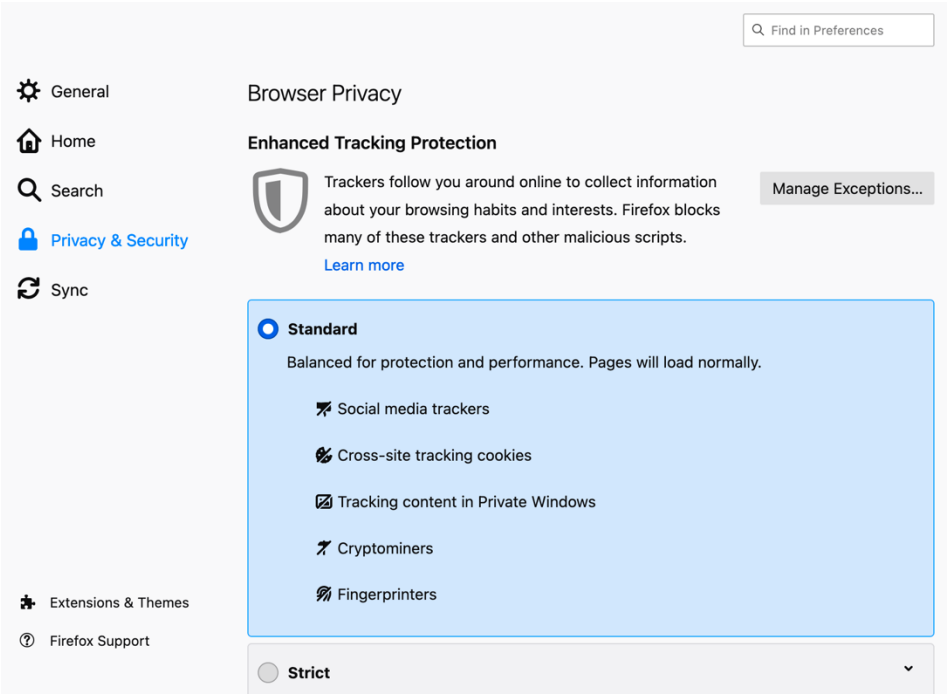

Figure18: The Mozilla Settings window

The *Safety Device* button must be pressed in the *Certificates* section.

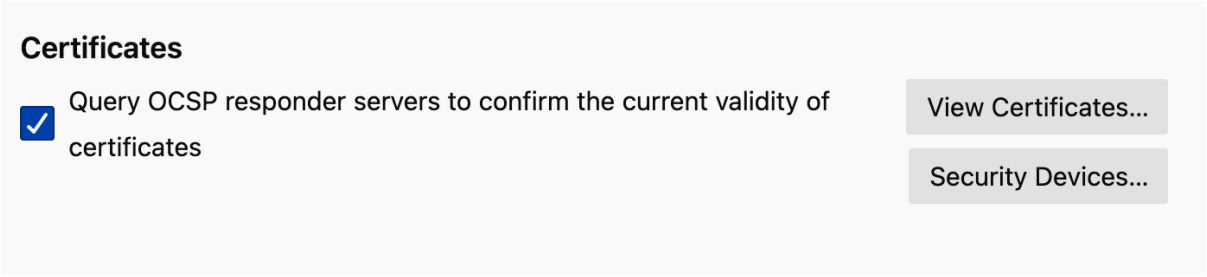

Figure19: Security settings in Mozilla●

The *Safety Device Manager* window appears. Use this window to add a new safety device: a chip card. The addition is done by pressing the *Populate* button. The window for finding the chip card driver is displayed:

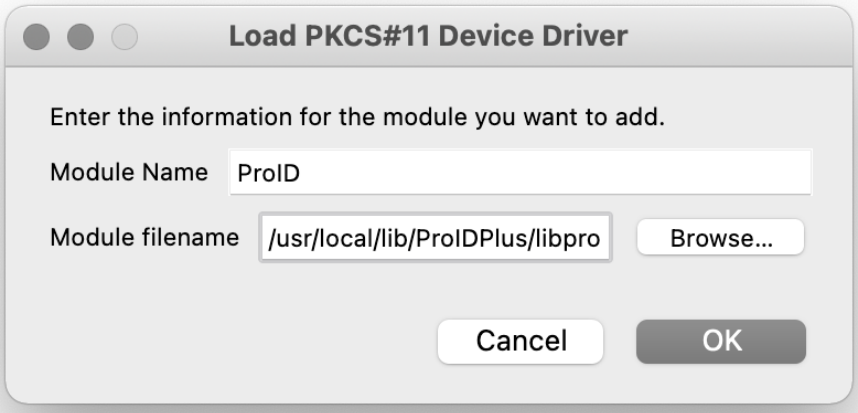

Figure20: Adding the chip card driver to Mozilla●

In the *New Driver PKCS#11 of the unit*, it is necessary to:

- Set the module name - arbitrary, e.g., ProID or ProIDQ.
- Indicate the path to the libproidproxyp11.dylib module
- Usually /usr/local/lib/ProIDPlus/libproidproxyp11.dylib
- Save the settings with the OK button.

Pressing the *OK* button will attempt to load the specified driver module. Once the module has been successfully loaded, the Applications will display information on the connected chip card reader or information on the entered chip card:

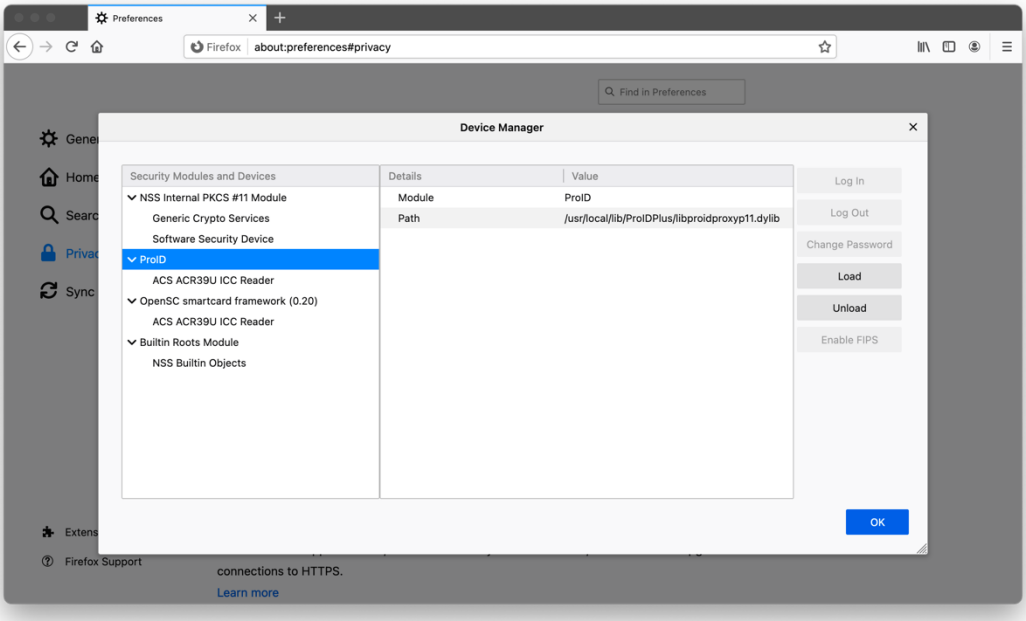

Figure215: Mozilla● window with a list of safety modules

Unsuccessful loading of the library is indicated by an error message: *Failed to add the module.* If the module fails to be added, the user should make sure that the correct path was indicated when added and that the libproidproxyp *11.dylib file is really present in the target path.*

8.4 PKCS#11 INTEGRATION INTO OTHER APPLICATIONS

If the user is using other applications with the PKCS#11 interface, the use of the chip card must be configured in the manner specified in the application documentation. The configuration is usually done by entering the path to the *libproidproxyp 11.dylib* chip card library in the configuration part.

9 INSTALLING A NEWER VERSION

If a newer version of *ProID+* is available, an upgrade should be made on the user's computer. The new version can correct errors and offer enhanced functionality or control.

The user can check the availability of a new ProID+ package on the ProID website.

The *ProID+* software update runs in a similar way to the initial installation:

- the installation package must be downloaded from the website,
- run it,
- follow the instructions in the installation guide.

The installation procedure is described in section 6

Warning: Just like the initial installations, the update of the ProID+ application must be run under a user account with **admin rights** for the operating system. If the installation is run under a user account that does not have admin rights, the installation wizard displays the login window to raise the user rights for the operating system during installation. An unprivileged user can enter the name and password of the administrator account in this window to authorize the subsequent installation process.

The *ProID+* software update is done in the same way as initial installations - see the section Running and installing.

On macOS operating systems, automatic uninstallation of applications isn't usually offered. The user has the option to remove ProID+ by moving the application directories from the *Applications* folder (*/Applications*) to the bin. These are the concerned applications or respectively the application directories:

10 UNINSTALLATION

On macOS operating systems, automatic uninstallation of applications isn't usually offered. The user has the option to remove ProID+ by moving the application directories from the *Applications* folder (*/Applications*) to the bin. These are the concerned applications or respectively the application directories:

Application	Application directory
ProID Card Administrator	/Applications/CardManProID.app
CryptoTokenKit	/Applications/CryptoTokenKit_ProID/ProIDNGTokenApp.app /Applications/CryptoTokenKit_ProID/ProIDTokenApp.app /Applications/CryptoTokenKit_ProID/ProIDQSealTokenApp.app /Applications/CryptoTokenKit_ProID/ProIDQTokenApp.app

ProID+ uses a number of other files that are installed in the system directory to run and are not normally available to ordinary users. These are user configuration files, operational records and system components.

Unlike application directories, which can be deleted in a normal way, these directories and files must use rights elevation using the *suda* command. A list of all installed directories and files is shown below:

Directories:

- /usr/local/lib/ProIDPlus/
- /opt/ProIDCM/
- ~/.config/ProID/
- ~/.ProIDCM_logs/

Files:

- /usr/local/etc/crplus/proidcm.cfg
- /usr/local/etc/crplus/proidcm.tokend.cfg
- /usr/local/etc/crplus/proidngcm.cfg
- /usr/local/etc/crplus/proidngcm.tokend.cfg
- /usr/local/etc/crplus/proidqcm.cfg
- /usr/local/etc/crplus/proidqcm.tokend.cfg
- /usr/local/etc/crplus/proidqscm.cfg
- /usr/local/etc/crplus/proidqscm.tokend.cfg
- /usr/local/etc/crplus/proidproxy.cfg
- /Library/Security/tokend/proidcm.tokend
- /Library/Security/tokend/proidqcm.tokend
- /Library/Security/tokend/proidqscm.tokend

If the user deletes the list of files and directories, the user will remove the ProID+ software. The *ProID* software can be reinstalled on the PC at any time.

Reader drivers are not included in the *ProID*+ installation package. Uninstalling the reader must be carried out separately according to the manufacturer's instructions.

11 VERIFYING THE INTEGRITY AND ORIGIN OF THE INSTALLATION PACKAGE

Before installing the software, the user should always verify that the software comes from a reliable source and that no one has manipulated the contents of the package. Installation of untrusted or modified software creates the risk of a computer virus or other harmful software getting inside the Mac.
For ProID+, both integrity and origin can be verified in two ways:

- **By verifying the electronic signature of the installation package**.
  The verification of the electronic signature is done by the macOS operating system before the installation **automatically**. If the installation package is not signed with a trustworthy certificate (or an appropriate key), the operating system displays a warning and does not allow the installation to be carried out.
- By downloading the installation package exclusively from the ProID software support website and comparing the installation package's hash.

After verifying the electronic signature, or the hash of the installation package, the user can trust using an original ProID+ package that does not contain any harmful software.

11.1 VERIFICATION OF THE ELECTRONIC SIGNATURE OF THE INSTALLATION PACKAGE

The proID+ installation package for macOS is always signed using a certificate intended for the electronic signing of the macOS installation packages *(Developer ID Installer certificate*). The certificate is issued from the certification authority of the company, which trusts the macOS operating system - it is able to verify the reliability of the certificate. The holder of the signature certificate is Monet+,a.s.
In addition to the electronic signature, the ProID installation package also undergoes a safety check - the so-called *notarization* process. Notarization is carried out by Apple. Notarized modules are recognized by the operating system as a 'known developer'. If the installed modules were not reported, then the Gatekeeper of the operating system would refuse to install them.

Before starting the installation, the operating system automatically checks whether the application originates from a known developer and that the package signature is created using a trustworthy certificate. **If the origin or signature is not reliable, the operating system will display a warning:** *The application "ProID+.pkg" cannot be opened because it originates from an unidentified developer*. **In such a case, the user should not continue the installation.** They should download the current version of the installation package and start the installation again.

Before installing ProID+, the user can verify the trustworthiness of the signature using the *pkgutil --check-signature* command.

```
pkgutil --check-signature /Volumes/ProID/ProID+.pkg
Package "ProID+.pkg":
   Status: signed by a developer certificate issued by Apple for distribution
   Signed with a trusted timestamp on: 2021-01-13 09:45:22 +0000
   Certificate Chain:
    1. Developer ID Installer: Monet, a.s. (A8X9UKGE74)
       Expires: 2025-09-25 14:25:11 +0000
       SHA256 Fingerprint:
           B0 AD 82 A4 89 CE BA C5 13 8D 2A 08 8E 27 7B 57 7F 10 25 DC 1F F8
           5A 0E B9 1C AF 93 91 8F F5 7A
       ------------------------------------------------------------------------
    2. Developer ID Certification Authority
       Expires: 2027-02-01 22:12:15 +0000
       SHA256 Fingerprint:
           7A FC 9D 01 A6 2F 03 A2 DE 96 37 93 6D 4A FE 68 09 0D 2D E1 8D 03
           F2 9C 88 CF B0 B1 BA 63 58 7F
       ------------------------------------------------------------------------
    3. Apple Root CA
       Expires: 2035-02-09 21:40:36 +0000
       SHA256 Fingerprint:
           B0 B1 73 0E CB C7 FF 45 05 14 2C 49 F1 29 5E 6E DA 6B CA ED 7E 2C
           68 C5 BE 91 B5 A1 10 01 F0 24
```

Figure6: List of the pkgu program when verifying the signature of the installation package

If the electronic signature of the installation package is verified like so, the installation package originates from a reliable source and can be used for installing the ProID+ software without worries.

11.2 COMPARISON OF INSTALLATION PACKAGE HASH

On the macOS operating system, the file hash value can be calculated using the *openssl* program. For calculating the SHA-256 hash, it is possible to specify in the command line: *openssl dgst -sha256 <path_k_inst_file>*
where *<path_k_inst_file> is* the path to the file with the *ProID.dmg* installation package.

Example of SHA-256 hash calculation:
In the directory with the installation package file, you can enter the following in the command line:
openssl dgst -sha256 ProID.dmg
The value of the hash is reported as:
Sha256(ProID.dmg)= 8f2be5f316b806352e0feb2691abc40fd1aea87596f652b442a70cc651df5499