Atostek ID 4.6
User Guide

for macOS

v1.0

Atostek

Table of Contents

1. ATOSTEK ID SOFTWARE DESCRIPTION 4

2. BEFORE USE AND HOW TO START USING ATOSTEK ID 5

2.1. What is Atostek ID? 5

2.2. What do I need to use Atostek ID? 5
2.2.1. Installing Atostek ID 5
2.2.2. Uninstalling Atostek ID 7

2.3. Activating the smart card 7

3. DIGITAL AUTHENTICATION AND DIGITAL SIGNATURE 10

3.1. User authentication 10
3.1.1. mTLS authentication 11
3.1.2. Authentication via the SCS interface 11
3.1.3. Using Atostek ERA 11

3.2. Digital signature 12
3.2.1. Signing of PDF documents (Adobe Acrobat) 13
3.2.2. Signing via the SCS interface 13
3.2.3. Signing in the Atostek ERA system 13

4. FEATURES 14

4.1. Starting and shutting down 14

4.2. Application information and user guide 14

4.3. Changing PIN codes and unlocking locked codes 14

4.4. Readers and cards 16

4.5. Settings 17
4.5.1. Language 18
4.5.2. Notify when updates are available 18
4.5.3. Notify when only partial connection to browser is available 18
4.5.4. Disable SCS interface 18
4.5.5. Show “Log in to ERA” in pop-up menu 18
4.5.6. Start Atostek ID on boot 18
4.5.7. Enable MIFARE Chip Read and Write Features 19
4.5.8. Enable temporary card personalization 19
4.5.9. Allow logging 19
4.5.10. Turn on debug logging 19

4.5.11. Card cache type 19
4.5.12. Seconds to wait for reader and card to be inserted 20
4.5.13. Automatic login retries (0-5) 20
4.5.14. Minutes to store PIN1 in buffer (0-420) 20
4.5.15. Register erasmartcard:// -protocol 20
4.5.16. Timestamp server address 20
4.5.17. Custom login command 21
4.5.18. Custom launch commands 21
4.5.19. Set SCS certificate as trusted in Firefox 21
4.5.20. Open SCS server certificate download page 21
4.5.21. Settings file parameter CLEANCERTSTOREONCARDREMOVAL 22
4.5.22. Settings file parameter EXCLUDEDREADERS 22
4.5.23. Settings file parameter EXCLUDEDCARDTYPES 22
4.5.24. Settings file parameter ERRORLOGPATH 22
4.5.25. Settings file parameter ALLOWEDBROWSERLESSANDFORWARDDOMAINS 23
4.5.26. Settings file parameter ENABLECUSTOMDIALOG 23

4.6. Updating 23

4.7. Signing documents via the application 25

4.8. Email encryption and signing 26

4.9. Workstation login 26

4.10. MIFARE Chip Management 28

4.11. Logging and cache files 29
4.11.1. Logging and log files 29
4.11.2. Cache files 29

4.12. Error reporting 29

4.13. Diagnostics 31

5. FREQUENTLY ASKED QUESTIONS AND ERROR SITUATIONS 33

5.1. Frequently asked questions 33

5.2. Other problem situations 34
5.2.1. Atostek ID and TokenDriver 34
5.2.2. Importing the Card Issuer Certificates to Keychain Access 35

1. Atostek ID software description

Atostek Oy is a Finnish software company founded in 1999, specializing in healthcare and medical applications, industrial product development, and IT consulting for the public sector. Atostek's products include the Atostek ID card reader software and the Atostek ERA system.

Atostek ID will be offered as the official card reader software by the Digital and Population Data Services Agency starting in 2024. The software is intended for use with the certificate cards issued by the Digital and Population Data Services Agency. Using the software with cards, various operations such as digital authentication and digital signatures can be performed via multiple interfaces and modules. Additionally, the software supports certificate card activation, PIN handling, and viewing card information. Alongside the Atostek ID application, the software includes the Atostek ID Minidriver, Atostek ID TokenDriver, Atostek ID PKCS#11 modules, and the Atostek ID AD registration service. Furthermore, Atostek ID supports the issuance of backup cards by the Digital and Population Data Services Agency. In addition to the aforementioned functions, Atostek ID offers compatibility with the Atostek ERA system via the erasmartcard.ehoito.fi interface. Atostek ID was previously known as ERA SmartCard.

Installation packages and documentation for the Atostek ID software can be downloaded from both the website of the Digital and Population Data Services Agency and Atostek’s own driver download page. The Digital and Population Data Services Agency will generally announce software updates. Atostek will inform its contractual customers about updates according to specific agreements. In the event of errors or issues, individuals and organizations that have obtained software access through the Digital and Population Data Services Agency should primarily contact the support of the Digital and Population Data Services Agency (1st line support), which will forward requests to Atostek if necessary (2nd line support). Atostek's contractual customers should contact Atostek support directly in case of errors or issues, according to the terms of their agreement. The Digital and Population Data Services Agency and Atostek will inform about specific issues related to the software if necessary.

The Atostek ID software and its user guides have undergone accessibility evaluations in accordance with the WCAG 2.1 and 2.2 standards. The accessibility statement can be found on the website of the Digital and Population Data Services Agency alongside the driver downloads. The software undergoes security audits at regular intervals as agreed between Atostek and the Digital and Population Data Services Agency. The audit report will be made available on the website of the Digital and Population Data Services Agency alongside the driver downloads after the audit. Atostek ID is also part of the annual audit of the ERA system. The development of Atostek ID software is also guided by Atostek’s ISO 9001 certified quality system.

The functionality of the Atostek ID card reader software is not guaranteed if other similar card reader software is installed on the workstation.

For inquiries related to further development and additional features of the software, please contact Atostek directly (for Atostek's contractual customers) or the Digital and Population Data Services Agency.

2. Before use and how to start using Atostek ID

This chapter introduces the Atostek ID application. In addition, the requirements for using the application are explained and instructions are given on how to install the Atostek ID application on an macOS machine. The Atostek ID application supports all versions of macOS maintained by Apple.

2.1. What is Atostek ID?

Atostek ID is card reader software used with certificate cards issued by the Digital and Population Data Services Agency. These cards include professional, personnel and operator cards for social welfare and healthcare, organization cards, related backup cards, and citizen certificate cards (identity cards). The cards can be used for digital authentication and digital signatures in services and applications compatible with the software. In addition, the software supports certificate card activation, PIN handling, and viewing card information.

2.2. What do I need to use Atostek ID?

Atostek ID is compatible with the macOS operating system. Check the latest list of supported macOS versions from the website of Digital and Population Data Services Agency https://dvv.fi/en/card-reader-software or from Atostek's own driver download page https://downloads.ehoito.fi before installation.

Note! If you are using a Windows or Linux (Debian, Red Hat) operating system, see the user guide for that operating system.

Note! Separate installation instructions are available for the software, detailing each step of the installation process.

To use a certificate card with Atostek ID software, you will need a card reader and a card reader driver in addition to the program. The card reader driver is usually already included in the operating system. If the driver is not found or requires an update, you can download the necessary installation packages directly from the card reader manufacturer's website. Atostek ID supports card readers compliant with the PC/SC specifications.

Atostek ID supports web browsers Microsoft Edge, Mozilla Firefox, Apple Safari, and Google Chrome, specifically the versions currently supported by the browser vendors. Older versions of these browsers are not systematically tested. Atostek ID supports email applications Outlook, Apple Mail, and Thunderbird for encryption and signing. The software also supports Adobe Acrobat and PDF-XChange for signing PDF documents. Atostek ID is available in Finnish, Swedish, and English.

2.2.1. Installing Atostek ID

To install Atostek ID, follow instructions below:

1. Go to the page https://dvv.fi/en/card-reader-software or https://downloads.ehoito.fi.
2. Select the driver for the correct operating system and download it.
3. Follow the installation instructions. If necessary, consult the Atostek ID installation guide.

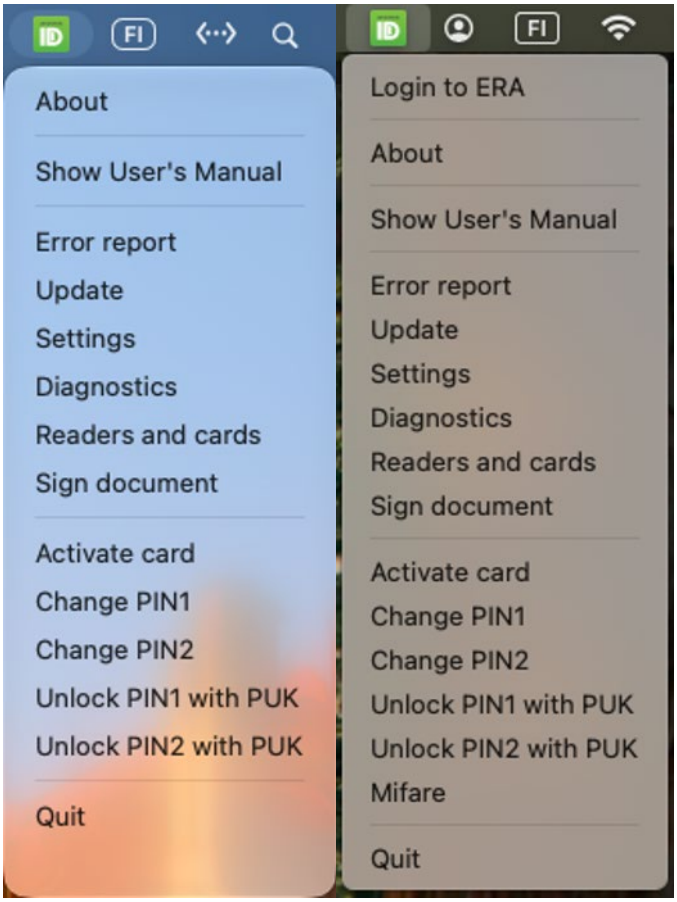


Figure 1. Atostek ID application.

After installation, the Atostek ID application can be found in the macOS menu bar. To view the application menu, right-click the Atostek ID icon (Figure 1). The program's logo is red if no card readers are connected. The logo is yellow if no cards are connected. The logo is green if a card is connected, and its information has been successfully read. The logo also indicates situations where reading the card information is in progress or the program is in an erroneous state.

If you receive error messages from the Atostek ID application immediately after installation, please check that you do not have another smart card reader software installed at the same time. The earlier card reader software from the Digital and Population Data Services Agency may interfere with the operation of the Atostek ID software if both are used simultaneously.

The application is then fully ready for use.

2.2.2. Uninstalling Atostek ID

When you install Atostek ID, a separate uninstaller application is also installed. To remove Atostek ID, locate and open *Uninstall Atostek ID.app* in your Applications folder, then enter your password when prompted.

2.3. Activating the smart card

Activate the smart card according to the following instructions:

1. Connect the card reader to the computer and insert the smart card into the reader.
2. If the card has not been activated before, the application will show the activation window automatically. The card only needs to be activated once. If the activation window is not shown, select *"Activate card"* from the application menu.
3. In the window that opens (Figure 2), enter the activation code number (PUK) stated in the code letter delivered with the card.
4. Set the PIN for the authentication certificate (PIN1) and the PIN for the signing certificate (PIN2). The window will specify the maximum and minimum lengths of the PINs. After this, you may click *OK*. The success or failure of the activation will be indicated in a separate window.

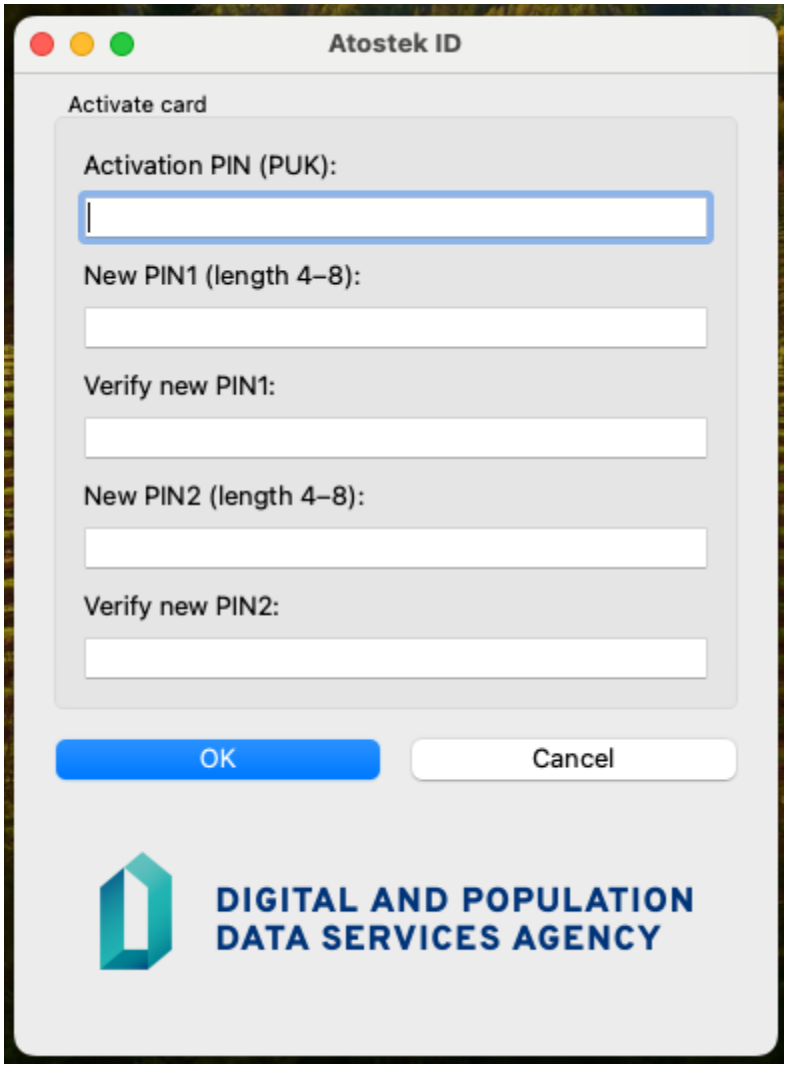


Figure 2. Activating the smart card

Note that both the PIN1 and PIN2 must be set to activate the smart card. The minimum and maximum lengths of the card's PINs vary depending on the card type and card generation, so the required lengths may differ for your various cards. You need to activate the smart card only once. If you have activated the smart card on another device, you do not need to activate the card again.

Note also that the smart card cannot be activated using an NFC reader, since to establish a secure NFC connection between the card and the reader, the PIN1 code of the smart card must be entered.

Note! Entering the activation code number incorrectly five times in a row will lock the activation code number. After this, the card can no longer be activated or locked PIN codes unlocked. Previously set PIN codes and their associated signatures will still work, even if the activation code number is later locked. The activation PIN cannot be unlocked; obtaining a functioning activation code number requires ordering a new card. The program shows a warning each time the activation PIN is entered incorrectly and displays the number of remaining attempts before the PIN is locked.

Note! Newer citizen certificate cards use a new 7-digit activation PIN for card activation. The activation PIN is different to the separate 8-digit unblocking PIN (PUK) which can be used to activate the card if the activation PIN is locked. **Please be aware which PIN Atostek ID is asking while activating the card.** The unblocking PIN can also be used to open the PIN1 and PIN2 codes if they have been locked after too many failed attempts. You can obtain the unblocking PIN via your local authorities. Please refer to the Digital and Populational Data Service Agency’s website for the latest information.

3. Digital authentication and digital signature

This chapter describes how you can use the Atostek ID application to perform authentication to a compatible service using your smart card. In addition, this chapter explains how to create a digital signature using the Atostek ID application. Please also refer to the user instructions for the service or application you are using for authentication or performing a signature, if necessary.

This chapter provides a more detailed description of some of the most common use cases related to authentication and signing. Not all possible services are described in this guide, and not all the use cases described here apply to all users. This chapter focuses solely on the functionality of authentication and signing. The next chapter will provide a more detailed overview of the software's other functionalities.

3.1. User authentication

The Atostek ID application can be used to authenticate the user when logging into a compatible service. To authenticate the user, the PIN1 code of the smart card must be entered.

To perform the authentication, insert the smart card into the reader, check that the Atostek ID application is running (Figure 1) and start logging into the compatible service. The service provider provides more detailed instructions for logging in. The service calls the Atostek ID application, after which Atostek ID requests the PIN1 code from the user (Figure 3). When prompted for the PIN, you may also see the standard macOS PIN window (without the Atostek and Digital and Population Data Services Agency logos). The PIN windows differ slightly depending on which interface is used for the authentication. If the certificate card is about to expire within two months, Atostek ID will inform you of this during authentication.

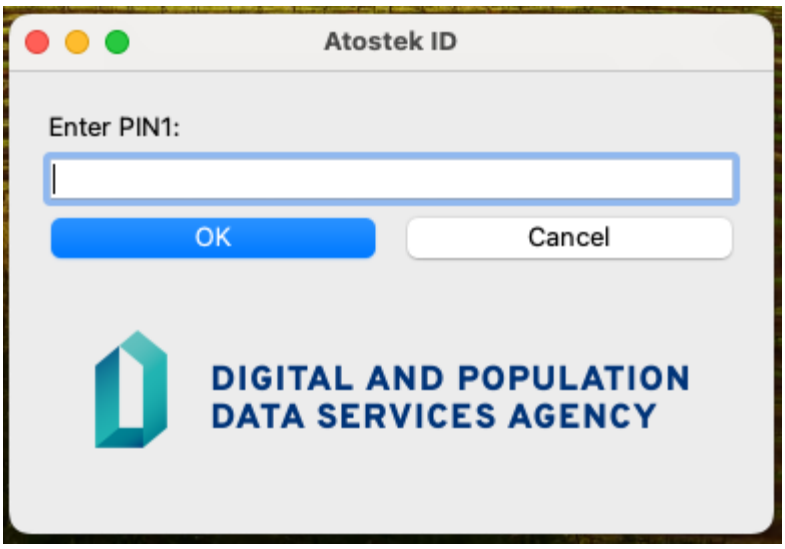


Figure 3. Authenticating the user using PIN1 code. During authentication, the standard macOS PIN window may also be shown.

3.1.1. mTLS authentication

Authentication can be performed using the card's authentication certificate via mTLS (mutual TLS) in the browser. In this case, the Atostek ID Minidriver module is utilized, which automatically installs with the installation of the macOS version of Atostek ID. More details about the Atostek ID Minidriver module can be found in the Atostek ID software integration guide.

This type of authentication is used, for example, in public administration service portals (**suomi.fi authentication**). To authenticate with the service, connect the card reader to your computer, insert the card into the reader, and begin authentication in the browser. You will be prompted for the card's authentication certificate PIN, or the card's PIN1 code. After this, the authentication will be complete, and you will be directed to the service. In case of issues, first refer to chapter 5 of this guide, where solutions to common problems are described.

3.1.2. Authentication via the SCS interface

Authentication can also be performed, for example, by utilizing the SCS interface (Signature Creation Service) of the Atostek ID application. SCS is an HTTPS interface defined by the Digital and Population Data Services Agency, specifically used for web services during authentication. The SCS interface is utilized by, for example, many patient information systems.

The use of the SCS interface is not particularly visible to the user when using the application. To authenticate, you need to connect the card reader to your computer and the card to the reader. After this, you can start the authentication process with the system. At this point, Atostek ID will ask you to select the certificate to be used for authentication. Once the certificate is selected, you will be prompted to enter the corresponding PIN code. After this, the authentication will be complete, and you will be directed to the service.

3.1.3. Using Atostek ERA

Please note that this use case is intended only for social and healthcare users who are registered to use the ERA system. If your organization has not instructed you to use Atostek's ERA system or if you are a citizen user (using an identity card), this use case does not apply to you. In such cases, you can skip this section of the instructions. You are not required to log in to the ERA system unless you have been specifically instructed to do so.

You can log in to Atostek's ERA service using the Atostek ID application. Navigate to the ERA system login page with your browser or select *"Log in to ERA"* (Figure 1) from the application menu to open the login page in your default browser. Note that this option is only visible if the option "*Show 'Log in to ERA' in pop-up menu"* has been enabled in the settings or during installation. This option can also be used to log into ERA when the default ports cannot be opened, because the feature opens the login page with the port information of the Atostek ID application. Such a situation can occur, for example, when several users are logged on to the same computer.

Successful authentication to the ERA system requires that you have been configured in the system beforehand. When authenticating, the card reader must be connected to the computer and the card must be in the reader. Once the authentication process has started, Atostek ID will prompt you for the card's PIN1 code. If authentication is successful, you will be directed to the service.

The ERA system uses the erasmartcard.ehoito.fi interface of the Atostek ID application. You can test the functionality of the interface by opening the application menu and selecting "*Diagnostics*", then "*Open Atostek ID test site".* This will open the interface test page in your default browser, displaying "*Test page loaded OK.*"

3.2. Digital signature

With Atostek ID, the user can use the signing certificate of their certificate card to create a digital signature for a compatible service. During signing, the user must enter the PIN2 of their card.

To create the digital signature, insert the card into the card reader, connect the reader into the computer, and check that the Atostek ID program is running (Figure 1). If necessary, check the instructions of the service or application on how the digital signature is performed in the service or application in question. During signing the service or application calls the Atostek ID application, after which Atostek ID requests the PIN2 code from the user (Figure 4). When prompted for the PIN, you may also see the standard macOS PIN window (without the Atostek and Digital and Population Data Services Agency logos). The PIN windows differ slightly depending on which interface is used for the authentication.

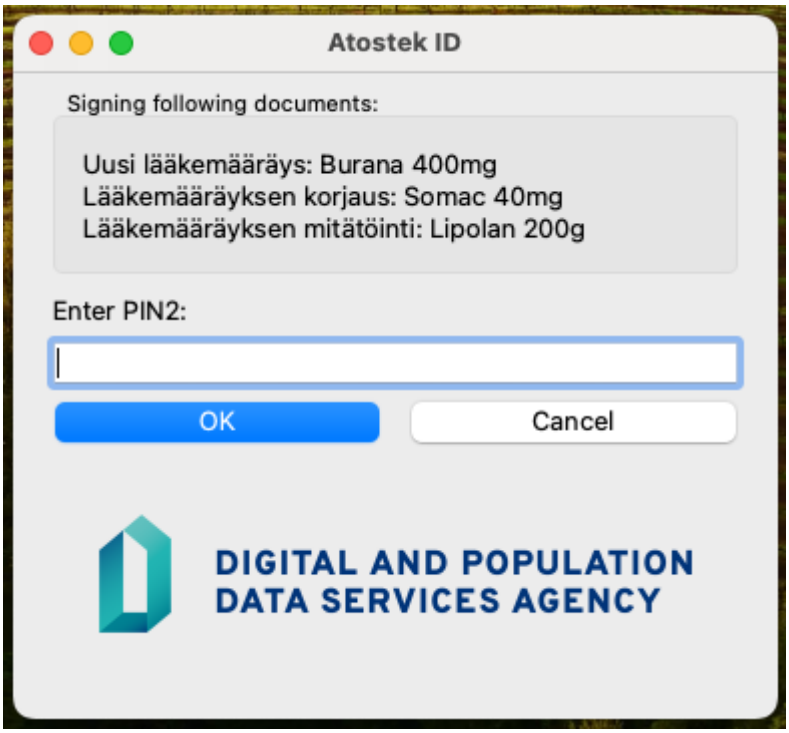


Figure 4. Electronic signature with PIN2 code. During signing, the standard macOS PIN window may also be shown.

3.2.1. Signing of PDF documents (Adobe Acrobat)

A PDF document can be signed using the Adobe Acrobat application. In this case, the Atostek ID Minidriver module is utilized. The module is automatically installed with the installation of the macOS version of Atostek ID. More details about the Atostek ID Minidriver module can be found in the Atostek ID software integration guide.

When signing with Adobe, select the document to be signed and choose to use the certificate from the tools menu. You can select digital signing from the menu that opens, at which point you will need to draw your signature in the desired location on the document using your mouse. After that, you will be prompted to select the certificate to be used. Once you have selected the certificate, you must enter the PIN code for the certificate in the window that opens. After this, the card will perform the signing, which will be attached to the document.

3.2.2. Signing via the SCS interface

Signing can also be performed, for example, by utilizing the SCS interface (Signature Creation Service) of the Atostek ID application. SCS is an HTTPS interface defined by the Digital and Population Data Services Agency, specifically used in web services during signing. The SCS interface is utilized by, for example, many patient information systems.

The use of the SCS interface is not particularly visible to the user when using the application. For signing, you need to connect the card reader to your computer and the card to the reader. After this, you can start the signing process. At this point, Atostek ID will ask you to select the certificate to be used for signing. Once the certificate is selected, you will be prompted to enter the corresponding PIN code. After this, the signing is complete, and the signature will be passed from the application to the service that requested it.

3.2.3. Signing in the Atostek ERA system

Please note that this use case is intended only for social and healthcare users who are registered to use the ERA system. If your organization has not instructed you to use Atostek's ERA system or if you are a citizen user (using an identity card), this use case does not apply to you. In such cases, you can skip this section of the instructions. You are not required to log in to the ERA system unless you have been specifically instructed to do so.

You can perform a signing operation, such as the signing of a prescription, in Atostek's ERA service using the Atostek ID application once you have authenticated yourself in the system. When signing, the card reader must be connected to the computer and the card must be in the reader. Once the signing process has started, Atostek ID will prompt you for the card's PIN2 code. After this, the card will perform the signature and pass it to the ERA system.

The ERA system uses the erasmartcard.ehoito.fi interface of the Atostek ID application. You can test the functionality of the interface by opening the application menu and selecting "*Diagnostics*", then "*Open Atostek ID test site".* This will open the interface test page in your default browser, displaying "*Test page loaded OK.*"

4. Features

This chapter introduces the main features of the Atostek ID application. They include, for example, changing and opening access (PIN) codes. In addition, the settings related to the application are presented with instructions on how to change them.

4.1. Starting and shutting down

The Atostek ID application starts automatically after you have installed the application and logged into the operating system. You can turn off automatic starting in the application's settings.

When you wish to close the application, select *"Quit"* from the application menu. This will completely shut down the Atostek ID application. There is usually no need for this, and after this you can no longer log in to the services or create signatures through, for example, the SCS interface or the erasmartcard.ehoito.fi interface until the program is restarted. The program can be found in the start menu under the name *"Atostek ID"* and can be restarted from there if necessary.

4.2. Application information and user guide

Information about the Atostek ID application, such as the version number and the ports used by HTTPS servers, can be found in the application's About view. This can be accessed by selecting *"About"* from the application's menu. The version number is displayed at the top of the window. Open and closed ports, as well as certificate-related information, pertain to the erasmartcard.ehoito.fi interface. Additionally, the view indicates whether a connection can be established to port 53952 of the SCS interface. A connection cannot be made if another application is reserving the port. This can occur, for example, if DigiSign card reader software is installed and running on the computer, as it opens its corresponding service on that port. Issues with the SCS interface port will also be indicated in the Atostek ID application's logo as a triangle with an exclamation mark.

The user guide can be accessed through the application by selecting *"Show User's Manual"* from the menu. The user guide opens in the application's language (Finnish, Swedish, or English). Software user guides, installation instructions, and other documentation can also be downloaded from both the Digital and Population Data Services Agency's card reader software page and Atostek's own driver page.

4.3. Changing PIN codes and unlocking locked codes

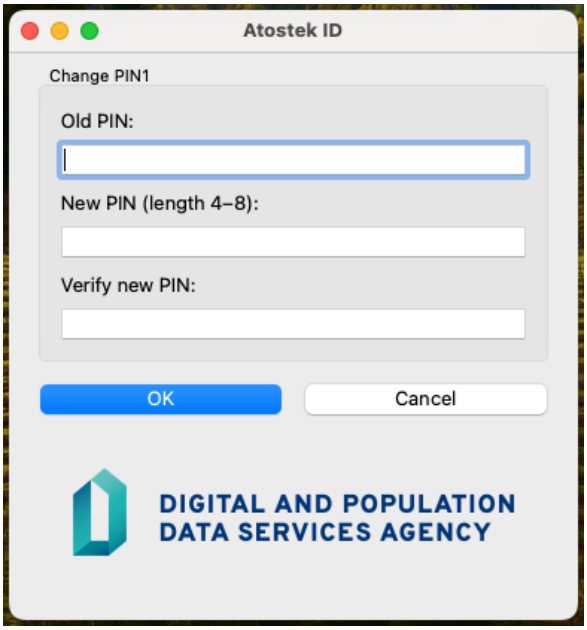
You can change PIN codes by selecting *"Change PIN1"* or *"Change PIN2"* from the application menu and entering the current PIN code and the new PIN code twice (Figure 5).

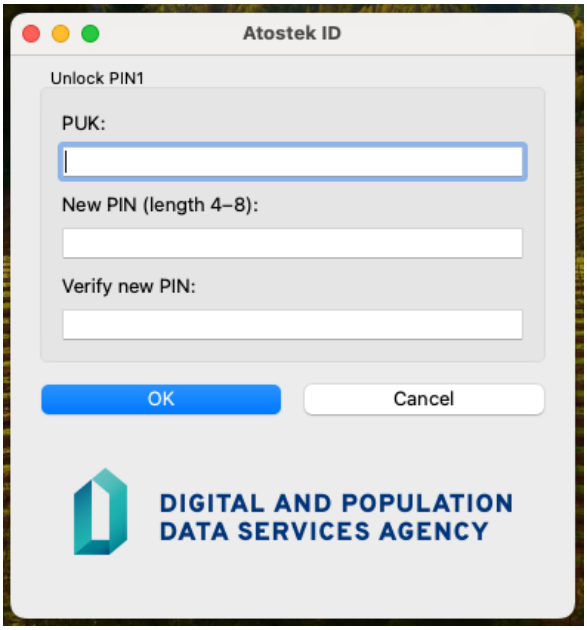
You can open locked PIN codes by selecting *"Open PIN1 code with PUK code"* or *"Open PIN2 code with PUK code"* from the application menu and entering the PUK code and the new PIN code twice (Figure 6). The PUK code is provided with the certificate card.

The card can also be activated through the *"Activate card"* option in the menu. The application prompts the user to activate the card when a non-activated card is inserted into the reader, which means the user does not need to trigger the activation themselves through the menu.

Note! While processing PIN codes, the certificate card must be present in the reader. Both PIN1 and PIN2 codes must be opened for the card to be activated. Activating the card will also open both PINs.

Note! Entering the activation code number incorrectly five times in a row will lock the activation code number. After this, the card can no longer be activated or locked PIN codes unlocked. Previously set PIN codes and their associated signatures will still work, even if the activation code number is later locked. The activation PIN cannot be unlocked; obtaining a functioning activation code number requires ordering a new card. The program shows a warning each time the activation PIN is entered incorrectly and displays the number of remaining attempts before the PIN is locked.





Figures 5 and 6. Changing and unlocking the PIN1 code.

4.4. Readers and cards

Connected card readers and cards can be viewed by selecting *"Readers and Cards"* from the application's menu. In the window that opens (Figure 7), the card readers connected to the computer are listed vertically on the left side. For NFC readers, two different readers will appear in the listing if the reader has both an NFC and a standard USB reader (contact reader) separately. You can select a reader as active by clicking its name in the left-side list of the window.

Once a reader is selected, information about the card connected to the card reader is displayed on the right side of the window, including the name details and expiration date. The window also shows the certificate chain of the card presented in a tree-like structure, from the root certificate through intermediate certificates to the user's certificates. Related to the user's certificates, both the public part of the certificate and the corresponding private key are displayed. The public parts of the certificates can be opened or saved by right-clicking the certificate in the view. This will open an additional menu with the options *"Open"*, *"Save As..."*, "*Validity check*" and "*Verify Certificate Chain*". By selecting "*Validity check*", one can check the certificate's expiration date and revocation lists (CRL, OCSP). "Verify Certificate Chain" will verify the chain of trust of the certificate. If the certificate isn't trusted due to certificate authorities' certificates being absent from the certificate store, they may be added to the store with the user's explicit permission. Adding certificates to the store may require administrator's privileges, in which case they will be requested from the user. Note that the verification of the chain of trust is only supported on Windows and macOS.

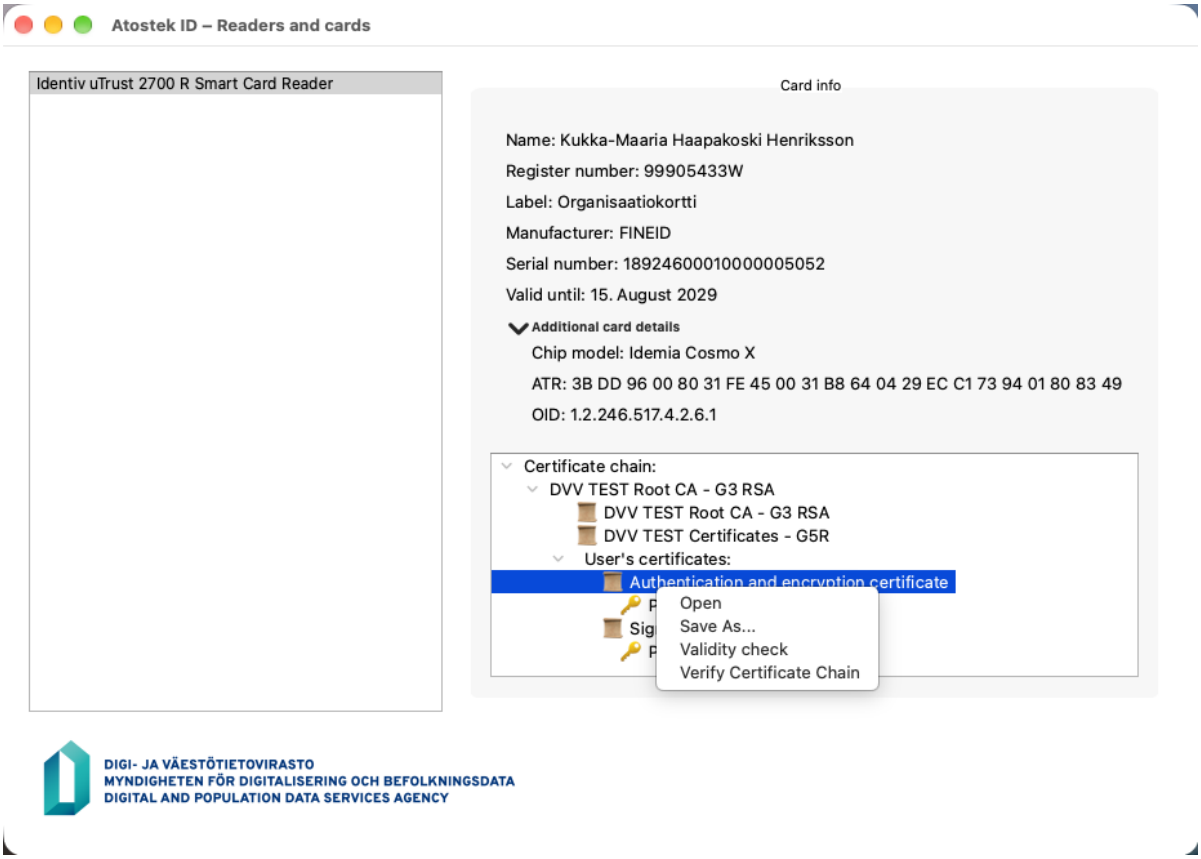


Figure 7. Readers and cards view

When using the NFC reader, the user is prompted for the card's PIN1 code when the card is brought to the reader. The PIN is used to establish a secure NFC connection. If the card is removed from the NFC reader, the user has 10 seconds to bring the card back before the PIN1 code must be entered again to re-establish the connection.

The Atostek ID TokenDriver saves the user's certificates to the macOS keychain if the card in the reader is paired with the user of the macOS device.

4.5. Settings

You can edit the application settings by selecting *"Settings"* from the application menu. With the settings (Figure 8) you can, for example, change the application language and modify the displayed notifications and commands related to the program. Please note that the changes will only take effect after saving. The settings are detailed in their own subsections.

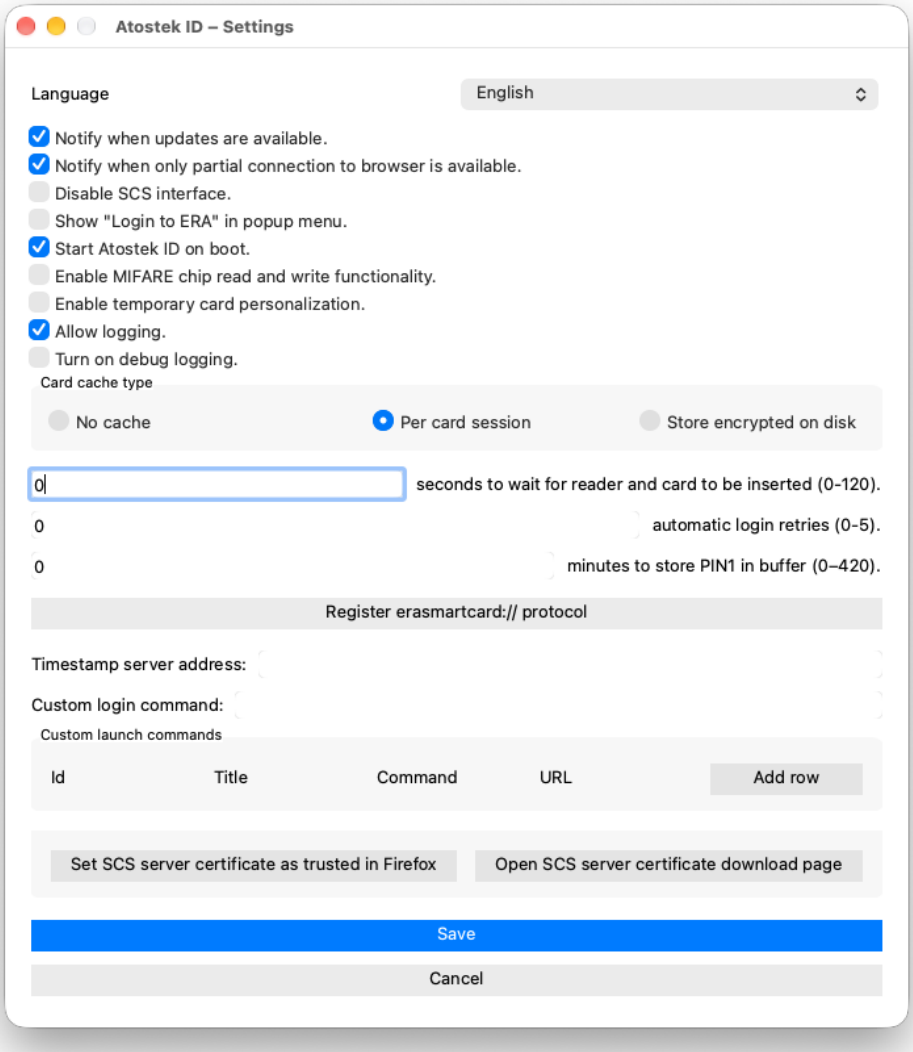


Figure 8. Application settings.

4.5.1. Language

The "**Language**" setting allows you to change the language of the Atostek ID application. The languages supported at the moment are Finnish, Swedish, and English.

4.5.2. Notify when updates are available

The "**Notify when updates are available**" setting can be used to enable Atostek ID notifications of new available versions. When enabled, Atostek ID will send a separate notification that a new version is available for download and installation.

4.5.3. Notify when only partial connection to browser is available

The "**Notify when only partial connection to browser is available**" setting can be used to enable Atostek ID notifications about a partial connection when the application's erasmartcard.ehoito.fi interface cannot connect to default ports and the system being used must be opened using Atostek ID launch commands. This setting concerns only the usage of the erasmartcard.ehoito.fi interface.

4.5.4. Disable SCS interface

The "**Disable SCS interface**" setting can be used to enable or disable the software's SCS interface. The interface is enabled by default, meaning the application starts it and its associated CA certificate download service upon startup. This HTTPS interface requires a port as specified in the specifications (https://dvv.fi/en/fineid-specifications). The port may already be reserved by another card reader software if it implements the same interface. This setting can be used to disable the SCS interface, freeing the port for another application, if the interface is not needed via Atostek ID. Disabling the interface means that Atostek ID will not start the interface at all. Therefore, there will be no warning, for example, if another program is using the ports required by the interface. Please note that disabling the interface without any additional measures will prevent performing authentication and signatures in systems that utilize the interface via Atostek ID. Therefore, only disable the interface if you are certain that you do not need it for your use case. Also see the MULTIDESKTOPMODE setting.

4.5.5. Show "Log in to ERA" in pop-up menu

The **"Show 'Log in to ERA' in pop-up menu**" setting can be used to display or hide the ERA login link in the application menu. Please note that the use of the ERA system applies only to social and healthcare users who are configured to use the ERA system. The setting is off by default, and the login link is thus not available in the application menu.

4.5.6. Start Atostek ID on boot

The **"Start Atostek ID on boot"** setting can be used to enable or disable the automatic starting of the application. Changing the setting requires admin privileges, which are requested from the user after saving the settings. The application will close while the setting is changed and automatically start up again afterwards.

4.5.7. Enable MIFARE Chip Read and Write Features

The **"Enable MIFARE chip read and write functionality"** setting will display an option "*Mifare"* in the application menu, which opens a separate management view for the MIFARE chip. Please refer to the MIFARE chip reading and writing instructions before attempting any reading or writing. You will need an NFC reader for handling the chip.

4.5.8. Enable temporary card personalization

The "Enable temporary card personalization" setting will display an option *"Temporary card"* in the application menu, which opens a separate dialog for temporary card personalization. This dialog is only used by employees at registration points, and other users do not need it to use their personalized temporary card. Other settings meant for registration points such as *AIDISURL* are already suitable for temporary card personalization by default. However, these settings can be changed if necessary. For more information on the personalization of temporary cards, please see the instructions of the Vartti system.

If the system has been configured with a timeout value for smart card connections, one should make sure it is large enough. During personalization, the card may take a long time to generate new keys, and the connection should not be interrupted at that time. A minimum timeout value of 2 minutes is recommended to ensure successful personalization.

4.5.9. Allow logging

With the **"Allow logging"** setting, the logging done by the application can be disabled. Disabling logging does not remove prior logs, but prevents the logging of new entries.

4.5.10. Turn on debug logging

The "**Turn on debug logging**" setting allows you to choose whether DEBUG level log messages are logged in the error log or only INFO, WARNING and ERROR level log messages.

4.5.11. Card cache type

The "**Card cache type**" setting allows you to specify whether Atostek ID stores card file data in its cache. There are three options for caching: "No cache", "Per card session" and "Store encrypted on disk". With option "No cache" Atostek ID does not store any files read from the card in its separate cache. Instead, the file contents are read from the card every time they are needed. The option "Per card session" is selected by default, and the file contents are stored in the cache for as long as the card remains in the reader. The values are cleared from cache when the card is removed from the reader or Atostek ID is closed. With the option "Store encrypted on disk" the cache is stored encrypted in the user's local directory. The card cache remains intact even though the card is removed from the reader or Atostek ID is closed. If the setting is changed from this value, the cache stored on disk is removed.

Using the card cache improves the performance of Atostek ID as it reduces the relatively slow communication with the card. The biggest increase in performance in long-term use is attained when the card cache is stored encrypted on disk.

4.5.12. Seconds to wait for reader and card to be inserted

The "**Seconds to wait for reader and card to be inserted**" setting allows you to specify the number of seconds during which an unconnected reader or card should be connected after login has started via the erasmartcard.ehoito.fi interface. When the value is set to 0, login fails immediately if the reader or card is missing. The maximum value for the setting is 120 seconds. This setting concerns only the usage of the erasmartcard.ehoito.fi interface.

4.5.13. Automatic login retries (0-5)

The "**Automatic login retries (0-5)"** setting allows you to define how many times the login is automatically retried if the login fails due to the Alcor Micro reader when the erasmartcard.ehoito.fi interface is in use. When the value is set to 0, each retry attempt is asked separately (however, no more than three times in total). This setting concerns only the usage of the erasmartcard.ehoito.fi interface.

4.5.14. Minutes to store PIN1 in buffer (0-420)

The "**Minutes to store PIN1 in buffer (0-420)**" setting allows you to define how long Atostek ID keeps the PIN1 in its buffer. The value is given in minutes in the range 0-420, i.e., the maximum time that the PIN1 code can be kept in buffer is seven (7) hours. The default value is 0 minutes, resulting in prompting the user for PIN1 every time it is needed. When the PIN1 code is in buffer, the user is not prompted for it. Instead, the value in the buffer is used. The PIN1 code is erased from the buffer when the set time limit is exceeded, the card is removed from the reader, the card receives a wrong PIN1 code, the PIN1 code is changed or Atostek ID is closed. The time limit starts from the moment the given PIN1 code is successfully verified on the card.

Note! Storing the PIN1 code in buffer is a deliberate decision made by the user or organization. The buffering time should be set to as low as possible with the use case in mind. The information security aspects of storing the PIN1 code in buffer must also be taken into account when making the decision.

Note! The setting works with the Atostek ID external modules (TokenDriver, PKCS#11) only if the setting *ENABLECUSTOMDIALOG* is true.

4.5.15. Register erasmartcard:// -protocol

The **"Register erasmartcard:// protocol"** button allows you to register the **erasmartcard://** -protocol for the Atostek ID application. More information can be found in the installation guide. Changing the setting requires admin privileges, which are requested from the user after saving the settings. The application will close during the change of the setting and then automatically start up again. This setting concerns only the usage of the erasmartcard.ehoito.fi interface.

4.5.16. Timestamp server address

In the **"Timestamp server address"** field, you can define the timestamp service used to retrieve timestamps for higher-level signatures (e.g., signing a PDF document through the application at PAdES standard levels B-T, B-LT, B-LTA). The timestamp service address is specified wholly, e.g., https://timestampservice.fi/ts. Please note that the example timestamp service provided is not a real service. Use your organization's recommended timestamp service.

4.5.17. Custom login command

The "**Custom login command"** field can be used to define a browser that you want to open instead of the default browser when a launch command without a separately defined command is executed. The browser is defined as: *"<Path to browser .exe file> {URL}",* for example *"/Applications/Google Chrome.app/Contents/MacOS/Google Chrome" {URL}.*

4.5.18. Custom launch commands

The "**Custom launch commands**" section can be used to add new launch links to the Atostek ID menu that can be used to open a system that utilizes Atostek ID and convey the port information of the application. This is especially important in Citrix and RDP environments.

In the launch command attributes, the identifier of the command (Id) is the value with which the launch command can be used, for example, in a command line launch.

In the launch command attributes, the title field is used to define the text that displays in the application menu.

In the launch command attributes, the command field is used to define the browser that you want to open with the command. The format is the same as in the custom login command.

In the launch command attributes, the URL field contains the target URL. The port of Atostek ID can be entered using {PORT} embedding. At launch, Atostek ID replaces the {PORT} text with the actual port where Atostek ID is connected to.

Example of a launch command:

- "Id": edemo
- "Title": Login to edemo service
- "Command": "/Applications/Google Chrome.app/Contents/MacOS/Google Chrome" {URL}
- "URL": https://edemo.atostek.com/

4.5.19. Set SCS certificate as trusted in Firefox

The **"Set SCS server certificate as trusted in Firefox"** button allows you to add the self-generated CA certificate of the SCS interface as trusted in Firefox. This setting concerns only the usage of the SCS interface.

4.5.20. Open SCS server certificate download page

The **"Open SCS server certificate download page"** button allows you to open the SCS interface page where you can download the CA certificate. The page also contains instructions on how to manually set the certificate as trusted in Firefox. This setting concerns only the usage of the SCS interface.

4.5.21. Settings file parameter CLEANCERTSTOREONCARDREMOVAL

You may use the setting parameter *"CLEANCERTSTOREONCARDREMOVAL"* directly in the application's settings file (*"/Users/<username>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). The default value *"true"* in the setting clears the certificates of the user's card from Windows' certificate store when the card is removed from the reader. The value *"false"*, in turn, preserves the certificates in the store. Please note that the settings file must be saved, and Atostek ID must be restarted after changes for the settings to take effect.

4.5.22. Settings file parameter EXCLUDEDREADERS

You may use the setting parameter *"EXCLUDEDREADERS"* directly in the application's settings file (*"/Users/<username>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). Give the setting a string-form list of readers (Reader1, Reader2, Reader3) that you want to remove from use. Atostek ID will then ignore the cards in these readers. If the reader name in the "Readers and cards" view ends with extra numbers, exclude them when configuring the setting. For example, if the reader name in the view is "Windows Hello for Business 0", use the string "Windows Hello for Business" in the setting. The setting supports wildcard characters * (matches one or more characters) and ? (matches a single character). For example, the value ExcludedReaders=ACS* will hide all readers whose name begins with the string "ACS". Please note that the settings file must be saved, and Atostek ID must be restarted after changes for the settings to take effect.

4.5.23. Settings file parameter EXCLUDEDCARDTYPES

You may use the setting parameter *"EXCLUDEDCARDTYPES"* directly in the application's settings file (*"/Users/<username>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). Give the setting a string-form list of card types that you want to reject. The allowed types are ORGANISATION CARD, PROFESSIONAL CARD, PERSONNEL CARD, IDENTITY CARD, OPERATOR CARD and FINEID (temporary cards). The values are case-insensitive. Please note that the settings file must be saved, and Atostek ID must be restarted after changes for the settings to take effect.

4.5.24. Settings file parameter ERRORLOGPATH

You may use the setting parameter *"ERRORLOGPATH"* directly in the application's settings file (*"/Users/<username>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). Give the setting the path to which the application's error log should be written. The path can be for example *"ErrorLogPath=/var/log/atostekid/AID.log"* If the path is erroneous or it does not exist, the application will continue to write the logs to the default location. Please note that the settings file must be saved, and Atostek ID must be restarted after changes for the settings to take effect.

4.5.25. Settings file parameter ALLOWEDBROWSERLESSANDFORWARDDOMAINS

You may use the setting parameter *"ALLOWEDBROWSERLESSANDFORWARDDOMAINS"* directly in the application's settings file (*"/Users/<username>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). The *"ALLOWEDBROWSERLESSANDFORWARDDOMAINS"* parameter is used with the erasmartcard.ehoito.fi interface when performing browserless login, browserless signing, or /ForwardMessage requests to destinations other than Atostek ERA or Edemo systems. The systems era.ehoito.fi and edemo.atostek.com are automatically allowed external addresses for these requests. If you want to add additional allowed addresses for production or testing purposes, specify the allowed addresses in the parameter, e.g., *"AllowedBrowserlessAndForwardDomains=era.ehoito.fi, edemo.atostek.com, edemo5.atostek.com"*. Please note that the settings file must be saved, and Atostek ID must be restarted after changes for the settings to take effect.

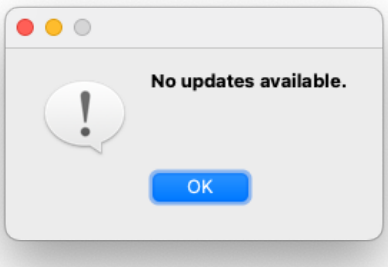
4.5.26. Settings file parameter ENABLECUSTOMDIALOG

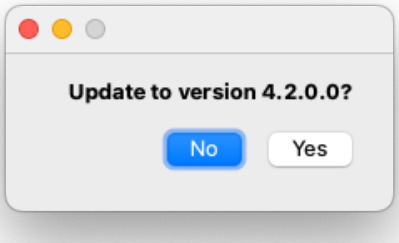
You may use the setting parameter *"ENABLECUSTOMDIALOG"* directly in the application's settings file (*"/Users/<user>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID.ini"*). With the default value *"true"*, the external modules of Atostek ID will display the Atostek ID custom PIN dialog when PIN code is prompted from the user. The only exceptions are those with restrictions on information security where the operating system handles PIN prompting, e.g., workspace login. If the setting is *"false"*, then the PIN dialog of the operating system will be used.

4.6. Updating

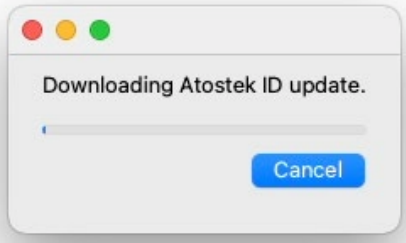
You can update Atostek ID by selecting "*Update*" from the application menu. Atostek ID first checks for updates and then displays the update status (Figures 9 and 10). If there are updates and you want to update the application to the latest version, select "*Yes*" in the window shown in Figure 10. The application will download and install the latest version (Figures 11 and 12).

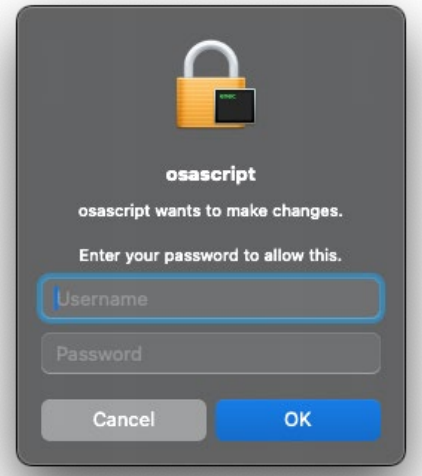
Note! Updating the application requires administrator rights, which are requested from the user automatically.





Figures 9 and 10. Status of updates when updates are not available and when updates are found.





Figures 11 and 12. Downloading and installing updates.

4.7. Signing documents via the application

In addition to Adobe Acrobat application, PDF and PDFA documents can also be signed directly via the Atostek ID application. The signature is compliant with the PAdES standard. The signature level (B-B, B-T, B-LT, B-LTA) is the highest possible the application can produce. This depends, for example, on whether the application has been configured with a timestamp service address via settings. In addition to the PAdES standard, the application also supports CAdES (B-B), JAdES (B-B), XAdES (B-B), and ASiC-E (B-B, B-T, B-LT) signature formats (detached signatures) for other document types.

To create a signature, open "*Sign Document*" from the application menu. Then, in the window that appears (see Figure 13), select the signature type and browse your computer to find the document to be signed.

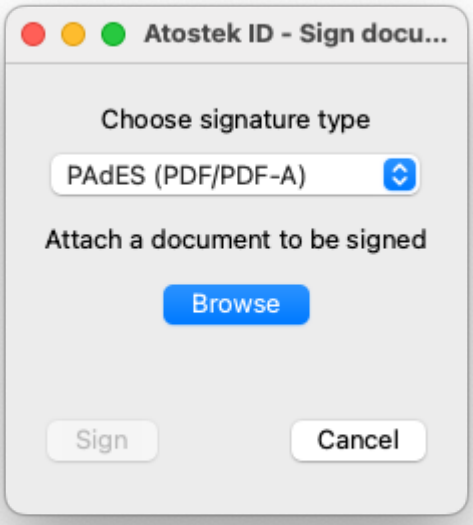


Figure 13. PDF document signing in the Atostek ID application.

When the signing process begins, the user is first prompted to select the certificate to be used for the signature. Once the certificate is chosen, the user is asked for the corresponding PIN code. After entering the code, the card performs the signing, and the signature is attached to a copy of the original document, with the text *"_signed"* added to the end of the file name. The application will then inform whether the signing was successful or not.

4.8. Email encryption and signing

Emails can be encrypted and signed in Apple Mail using the certificates from the certificate card. In this case, macOS utilizes the Atostek ID TokenDriver module, which is automatically installed with the macOS version of Atostek ID. More details about the Atostek ID TokenDriver module can be found in the integration guide for Atostek ID software. Please also refer to Apple Mail's own documentation on email encryption and signing if needed.

The certificate card must first be activated in the Apple Mail application. After this, you can use your card for encrypting and signing emails. To send an encrypted email to another person, you must have the recipient's public key attached to their contact information.

4.9. Workstation login

Authentication to the macOS workstation can be done using the authentication certificate from the certificate card. In this case, macOS utilizes the Atostek ID TokenDriver module, which is automatically installed with the macOS version of Atostek ID. More details about the Atostek ID TokenDriver module can be found in the integration guide for Atostek ID software.

Once the driver is installed, the card reader is connected to the machine, the card is in the reader, and the user's card data is paired with the macOS user, the user must log in to their workstation using the certificate card. In the macOS login screen, instead of a password, the user is prompted for a PIN code (see Figure 14). When logging in, the PIN1 code of the card must be entered.

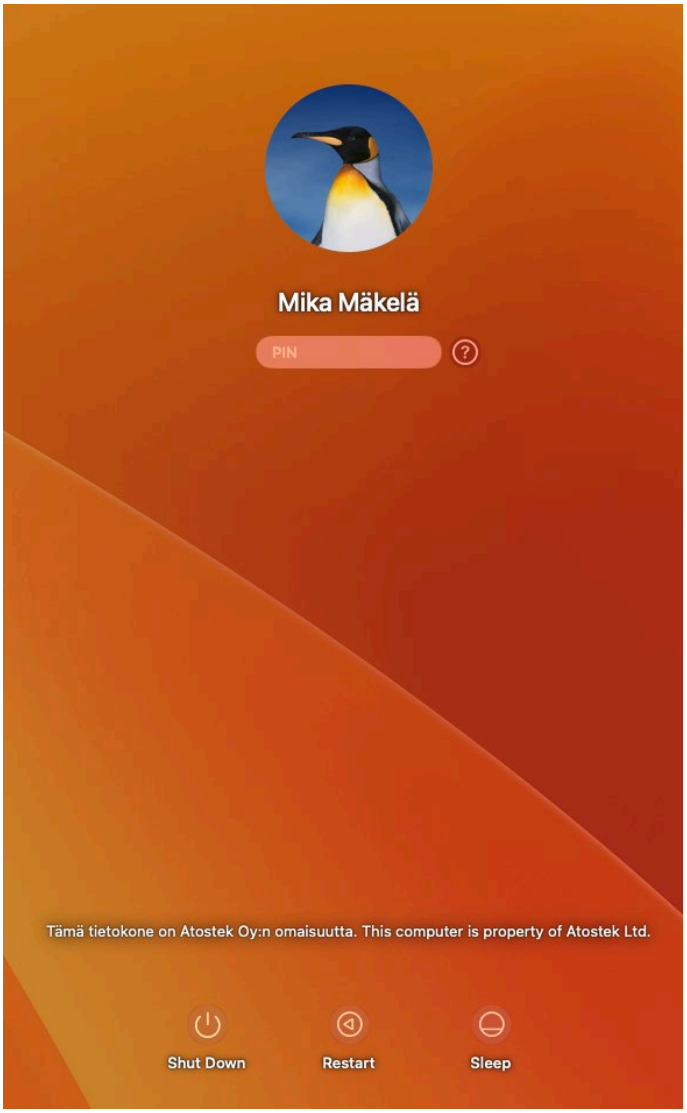


Figure 14. The workstation login view when the certificate card has been paired with the user.

4.10. MIFARE Chip Management

When you have selected the MIFARE option during installation or through settings, the Atostek ID application menu will display an option “Mifare” (Figure 1). Selecting this opens the MIFARE chip sector management view, as shown in Figure 15.

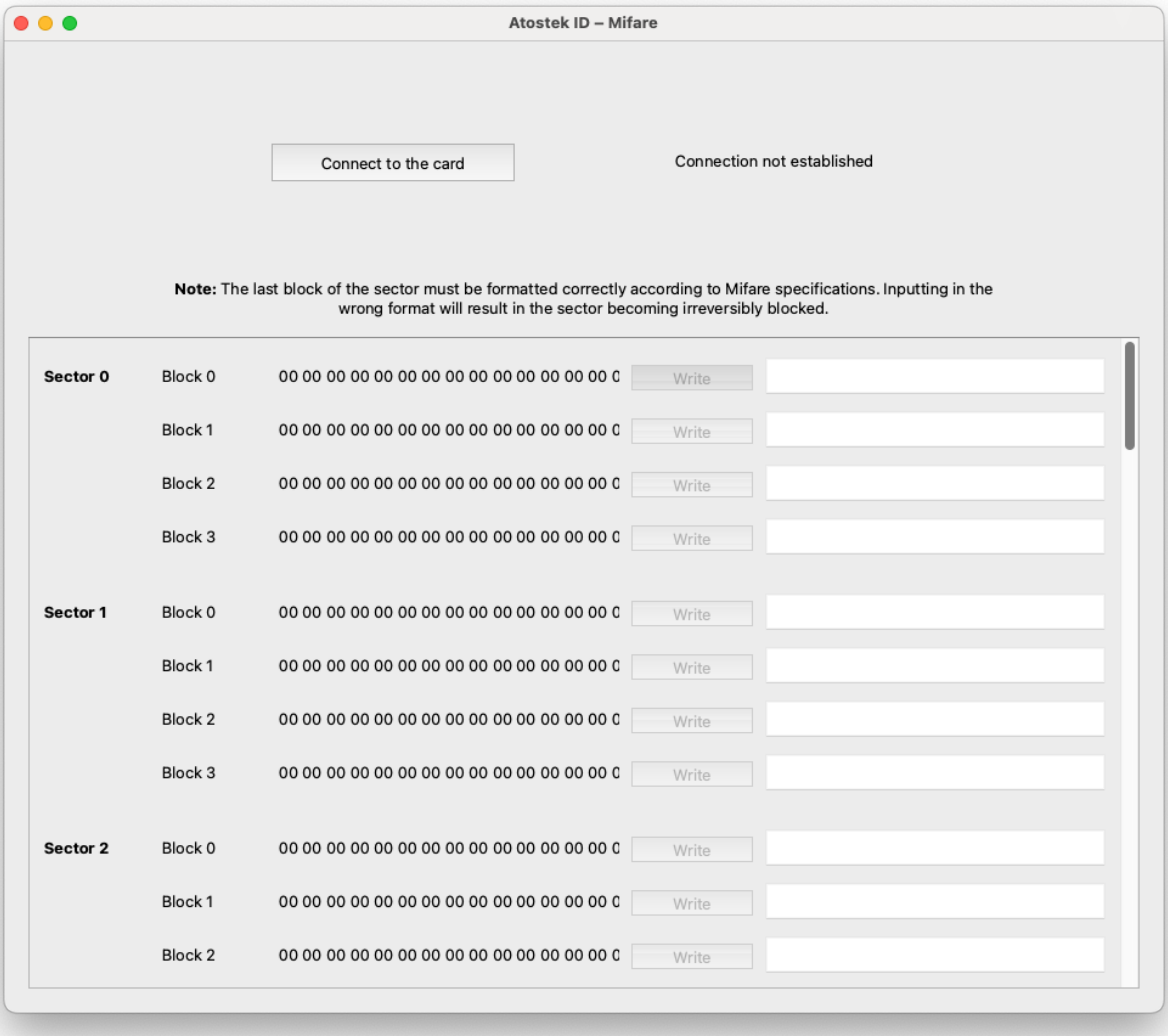


Figure 15. MIFARE chip management view.

To read and write to the MIFARE chip, you need an NFC reader. Connect the reader to the computer, place the card in the reader, and enter the card's PIN1 when prompted to establish a secure connection. After that, press the "Connect to the card" button in the Mifare view. The view will indicate whether the connection is successful or not. The sixteen sectors of the MIFARE chip and the contents of their four blocks are automatically displayed in the view.

It is also possible to write to the chip's blocks in this view. **Please do not write anything to the MIFARE chip unless you are absolutely sure of what you are writing, and that writing is necessary! Writing is not required in normal use cases or for the application to function correctly. If needed, contact your organization's IT support**. Incorrect writing can lead to permanent locking of a sector (especially if writing occurs to the last block of a sector). Before writing, please review NXP's MIFARE Classic EV1 documentation. One relatively safe way to test writing is to write all bytes in sector 2, block 1 to 0xFF (i.e., input FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF). Values can be restored by writing all bytes back to their original values (usually input 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00).

4.11. Logging and cache files

4.11.1. Logging and log files

Atostek ID logs messages about the application's operation and error situations in its own log file. By default, the log file can be found at the path *"/Users/<user>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID/Error.log".* The log file can be opened by selecting *"Diagnostics"* from the menu and then *"Show Atostek ID log"* in the window that appears. The location of the log file can be changed through the settings.

By default, logging captures informational, warning, and error-level messages. You can enable debug-level logging through the settings, which provides more detailed logging and generates more log entries. Debug-level logging is particularly essential for troubleshooting error situations. You can also disable logging completely through the settings. In this case, the previous log file will not be deleted, but no new log messages will be recorded.

Atostek ID also logs error-level messages to the operating system's log (System Log).

The main log file of the Atostek ID PKCS#11 module can be found at "*/Users/<user>/Library/Application Support/Atostek Oy/Atostek ID/PKCS11.log*". However, when run by TokenDriver, the module logs to "/Users/<*user*>/Library/Containers/com.atostekid.AtostekIDToken/Data/Library/Logs/PKCS11.log".

The Atostek ID TokenDriver module's log can be viewed using the command shown in section 5.2.1 of this document.

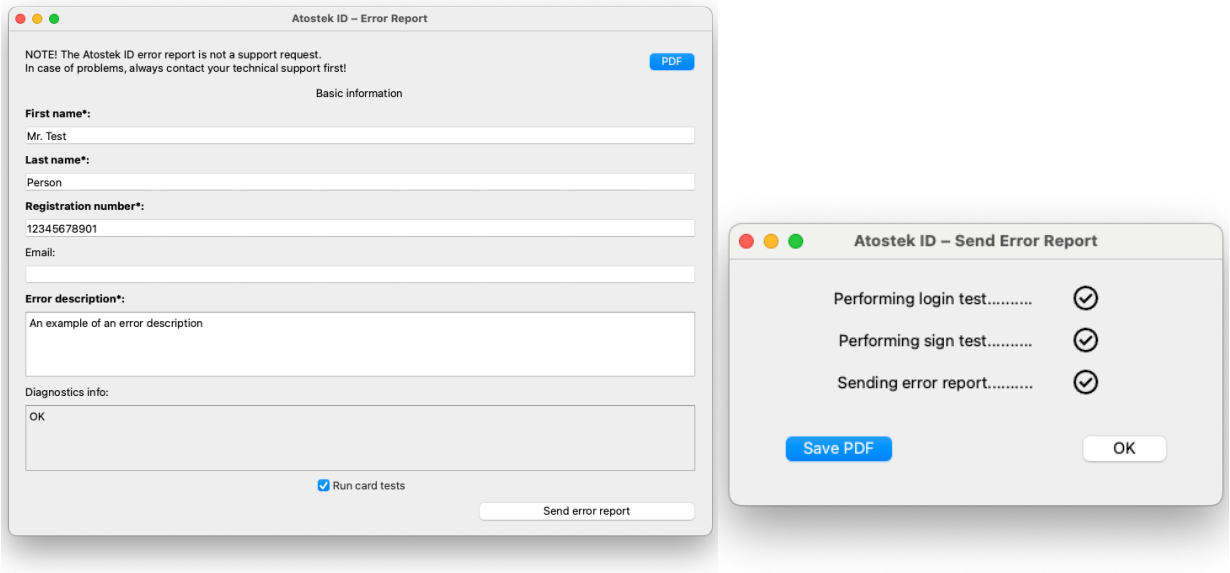
4.11.2. Cache files

If "Store encrypted on disk" has been selected as the card cache type, the cache will be stored in the file "*/Users/<user>/Library/Application Support/Atostek Oy/Atostek ID/AtostekID/cache.json*". The cache file is cleared automatically when another card cache type is selected. To clear the cache, you may indeed switch the cache type setting, or alternatively, delete the cache file manually.

4.12. Error reporting

In the application menu, you can find the option "*Error report*", which you can use to send an error report to Atostek's AIDERA service. However, a bug report itself is not a support request. If you encounter a problem, always contact your technical support first. If necessary, you will be asked to send an error report through this functionality. Only a limited number of error reports may be sent per day.

An error report is created by providing sufficient contact information and writing a description of the error (Figure 16). If the reader and the card are connected, the card information is filled in automatically.



Figures 16 and 17. Error report and sending it.

Mandatory fields are in bold and marked with an asterisk. You can send an error report by clicking the "*Send error report*" button on the bottom right. Please note that the button cannot be pressed if one of the mandatory fields is missing.

If you wish, you can also save a PDF file from the error report to your computer using the "*PDF*" button on the top right. With the check box "*Run card tests"* at the bottom, you can choose whether to run card tests when sending an error report.

After sending the error report, a window opens where you can monitor sending progress (Figure 17). The window for sending an error report shows the status of the card tests only if you have selected the card tests to be run in the window in Figure 16. If the error report is sent successfully, the error report window (Figure 16) closes automatically. From the error report sending window (Figure 17), you can also save the error report as a PDF file by clicking the "*Save PDF*" button.

4.13. Diagnostics

You can open the diagnostics view of Atostek ID (Figure 18) from the application menu with "*Diagnostics*". When the view opens, tests are run, which takes a few seconds. The test results contain information about, among other things, the version of the Atostek ID application, connected readers and supported browsers.

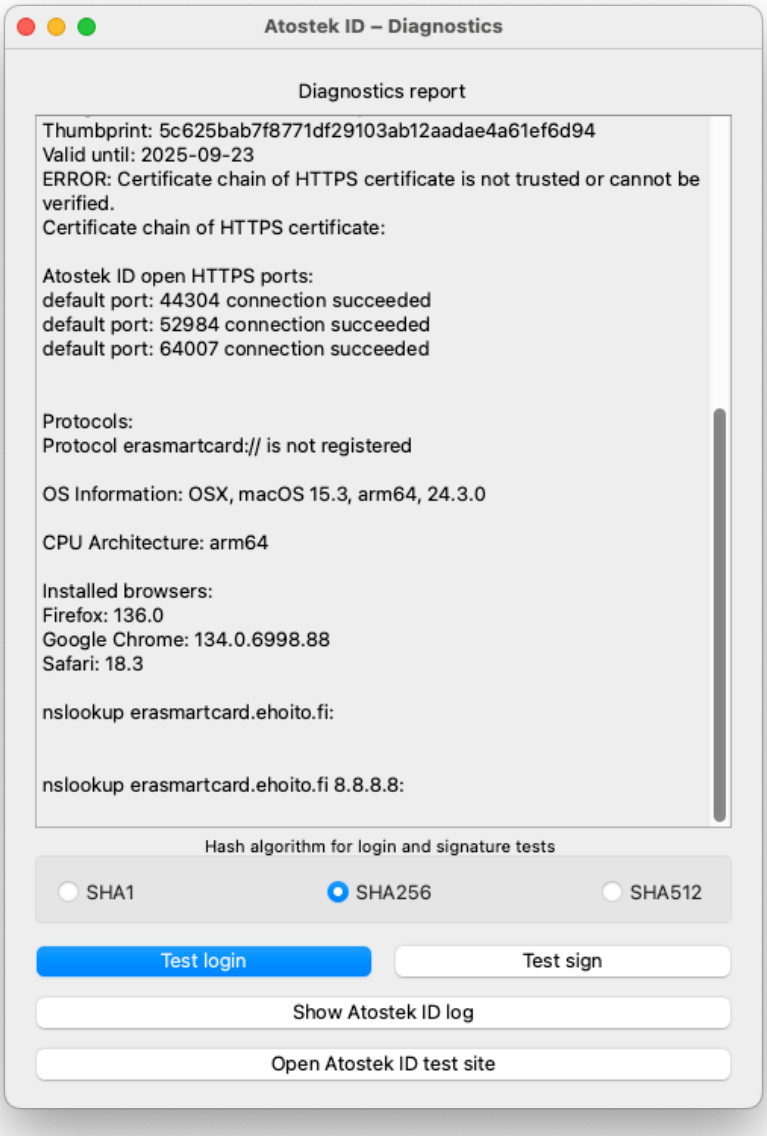


Figure 18. Diagnostics view.

In the diagnostics view, you can also test login and signature when the card is connected. You can select the hashing algorithm to be used using the radio buttons. The results of the login and signature test are saved in the "*Diagnostics report*" view.

You can view the error log of the Atostek ID application by clicking the *"Show Atostek ID log"* button. The error log opens in a separate window.

From the button "*Open Atostek ID test site*" you can test whether the Atostek ID application works correctly. If the button does not open a white website with the text "*Test page loaded OK*", something is wrong. For example, if the certificates required by the Atostek ID are not set to trusted, the test page does not open correctly.

5. Frequently asked questions and error situations

Atostek ID displays separate error windows when error situations occur. These include scenarios where:

- Atostek ID cannot start the HTTPS server for the SCS interface on port 53952 because the port is not available.
- The operation cannot be performed because the card is not in the reader.
- The operation fails (for example, authentication or signing) due to invalid requests or card issues.

In addition, Atostek ID logs messages related to error situations and indicates with its logo if something is wrong.

5.1. Frequently asked questions

Q: The application shows a warning "Starting SCS Server in port 53952 failed!" or "Staring SCS CA Server in port 53953 failed!".

A: This error typically occurs when the specified ports are not available, meaning another program is occupying them. Ensure that you do not have another card reader software installed or running that reserves these ports. These warnings only prevent the use of the application's SCS interface and do not necessarily block other functionalities in your use cases. If closing and removing the other card reader software does not help, you can check via the command prompt which program is using the ports Atostek ID requires (using the lsof command). If possible, contact your organization's IT support. If you do not need the SCS interface at all in your use case and releasing the port is not possible, then you can fully disable the interface from the settings. This way the application does not start the interface, preventing any related warnings.

Q: Reading the card's information is not successful.
A: Is the card in the reader the right side up? Please note that the card's contact surface (the metallic square) must connect with the reader's contact surfaces for a connection to be established (readers other than NFC). You can also try gently wiping the contact surface, as any dirt can make reading difficult. Is the card reader properly connected to the device? Can you try another USB port? The card reader should be visible in addition to the application's views in Windows Device Manager (under Smart card readers). Is the card reader's own driver installed and up to date given that the card reader vendor provides a driver? Driver packages from card reader manufacturers are typically pre-installed with the operating system. However, they may also be missing or require an update. Driver packages can usually be downloaded from the card reader manufacturer's website.

Q: The application says that the PIN code is locked.
A: This means the PIN code has been entered incorrectly too many times in a row. You can unlock the PIN code using the PUK code, also known as the activation code number, through the application menu.

Q: What is the PUK code?

A: The PUK code, or activation code number, is the code that was sent to you in a separate letter when you ordered your card. The activation code number is used to activate the card and unlock locked PIN1 and PIN2 codes.

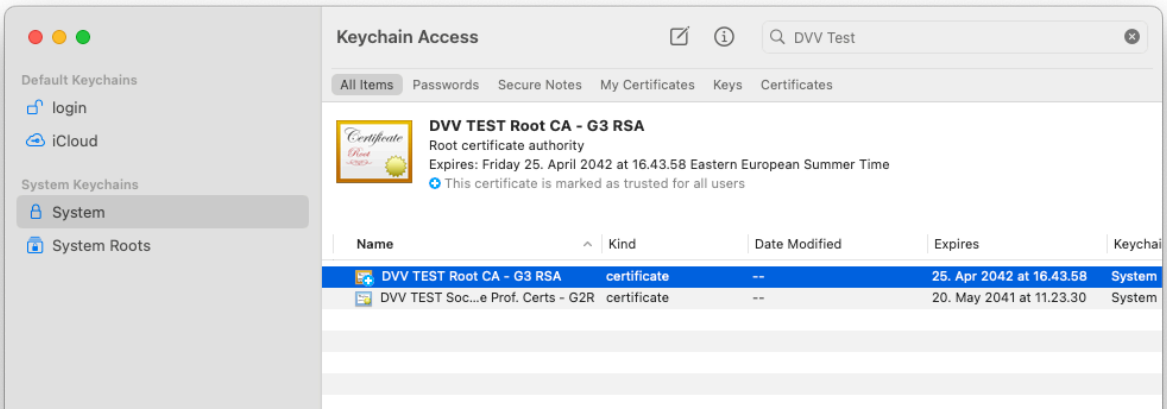
Q: Authentication or signing in the browser fails.
A: The specifics of this issue depend on which interface is being used. If mTLS authentication is involved (e.g., suomi.fi), please check that the Atostek ID TokenDriver is installed correctly. If the issue is authentication or signing via the SCS or erasmartcard.ehoito.fi interface, you can check if you can access the interface's test page (https://localhost:53952/ or https://erasmartcard.ehoito.fi:44304/). The browser usually indicates if access is denied due to DNS issues or untrusted certificates. For DNS issues, please contact your organization's IT department. Certificates can be manually installed as trusted in the browser or operating system's certificate store. You can also check the application's *"About"* view to see if the default ports required by the interfaces are in use by the application.

5.2. Other problem situations

5.2.1. Atostek ID and TokenDriver

The Atostek ID TokenDriver module is used, for example, in mTLS authentication (suomi.fi), signing documents with Adobe software, encrypting and signing emails with the Apple Mail application, and logging into a workstation with a certificate card. The module installs automatically into the system during the installation. However, problems may occur during the installation or with the module itself. Please check the following sections if you encounter any issues.

When using Safari or Firefox for mTLS authentication, you must set the card's root and intermediate certificates as trusted in the Keychain certificate store. Atostek ID will try to set them during installation, but if it has not succeeded, certificates can be added to the Keychain from the Readers and Cards view by right-clicking them and selecting "Open" from the menu that appears.



Picture 19. Card's root and intermediate certificate in keychain.

The installation of the TokenDriver module can be checked with the command *"pluginkit -vv -m -p com.apple.ctk-tokens"*. Entries in the TokenDriver module's log, such as mentions of error situations, can be monitored with the command *"log stream --predicate '(subsystem == "com.apple.CryptoTokenKit") || (process == "AtostekIDToken")'"*.

After the installation, it is advisable to log out or restart the entire computer to ensure that the new TokenDriver is registered for use.

The command "sc_auth list" can be used to check the valid pairings between users and cards. The command "sc_auth unpair <username>" can be used to remove a valid pairing from a selected user. A pairing must be valid for the card to be used for workstation login.

If all the previous steps work and your use case still fails in the browser, try clearing the browser cache or using an incognito window to ensure that cached data does not interfere with the card's usage.

5.2.2. Importing the Card Issuer Certificates to Keychain Access

If something goes wrong during the Atostek ID installation and the root and intermediate certificates for the cards are not added as trusted to Keychain, you can add them manually using one of the following methods:

Option 1: When the card is in the reader, open the "Readers and cards" dialog and right-click on one of the certificates. From the menu that appears, select "Verify Certificate Chain". If the certificate chain is not yet trusted, the application will offer the option to set it as trusted. Select OK and enter the password as many times as prompted. This adds the root and intermediate certificates of the card in the reader to the Keychain and sets the root certificate as trusted, if this is not already the case.

Option 2: Uninstall Atostek ID and try reinstalling it. Ensure that the " Install DVV Root Certificates if they are not installed" option is enabled in the installer, and enter your password each time the installer prompts you.

Option 3: You can also add the root and intermediate certificates from the card currently in the reader by following the steps described in section 5.2.1.

Option 4: When Atostek ID is installed, a file called "*DVV VRK certificates.mobileconfig*" is placed in the "*/Library/Atostek ID*" directory. This file allows you to add the root and intermediate certificates to your user's Keychain. To find the file, open a new Finder window, choose "Go to Folder…" from the "Go" menu in the menu bar, type "*/Library/Atostek ID*" into the text field, and press Enter. The folder will open, and you should see "*DVV-and-VRK-certificates.mobileconfig*" listed among the other files. Double-click the file. A pop-up will appear, letting you know that the profile has been added and that you need to review it in System Settings to complete the installation. Open System Settings and select "Profile Downloaded" near the top of the left sidebar. Then double-click the "Atostek ID – DVV & VRK CA" profile, which will display a warning triangle with the message "Profile is not installed. Double-click to review." Click "Install" in each of the subsequent dialog boxes that ask you to confirm the installation of this profile.

Option 5: Download the root and intermediate certificates directly from the DVV website at https://dvv.fi/en/ca-certificates and install them into Keychain.