DIGITAL AND
POPULATION DATA
SERVICES AGENCY

Atostek ID 4.4 User Guide

for Linux

v2.0

Atostek

Sisällysluettelo

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 electronic identification and electronic signatures can be performed through 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 through 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 a Linux machine. The Atostek ID application supports all maintained versions of Debian and Red Hat distributions for the Linux operating system.

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 electronic identification and electronic 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 maintained versions of Debian and Red Hat distributions for the Linux operating system. Check the latest list of supported Linux versions from the website of Digital and Population Data Services Agency https://dvv.fi/en/card-reader-software or from the page https://downloads.ehoito.fi before installation.

Note! If you are using a Windows or macOS 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.

Note! A separate integration guide is also available for the software, intended specifically for system developers and the IT departments of organizations.

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 the 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.

See the Atostek ID program startup instructions in Subsection 3.1.

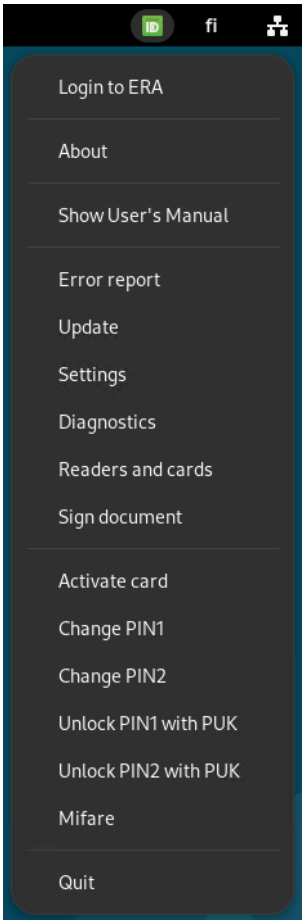


Figure 1. Atostek ID application.

After installation, the Atostek ID application can be found in the operating system's indicator area. To view the program menu, right-click on the green 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.

2.3. 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.

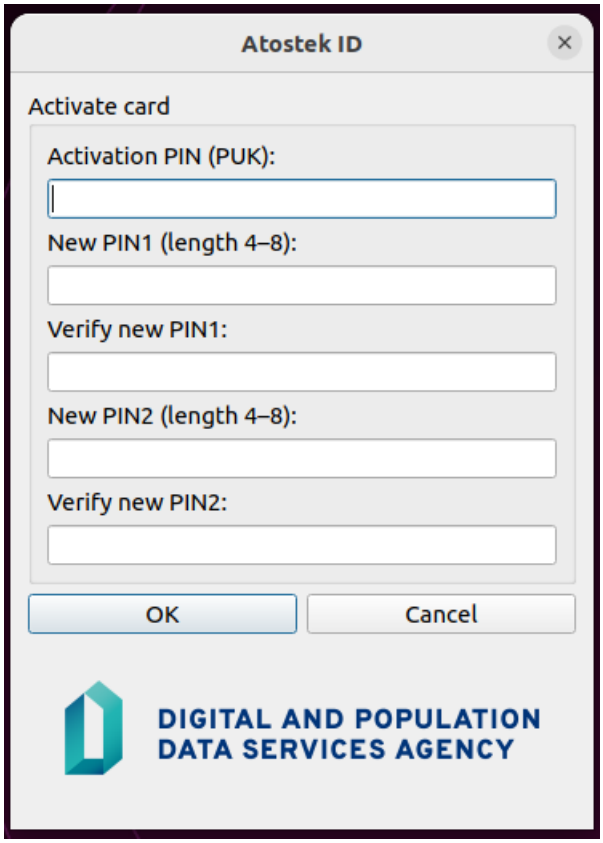


Figure 2. Activating the smart card.

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 an electronic 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. Digital 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 certificate 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 operating system 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 smart card is about to expire within two months, Atostek ID will inform you of this during authentication.

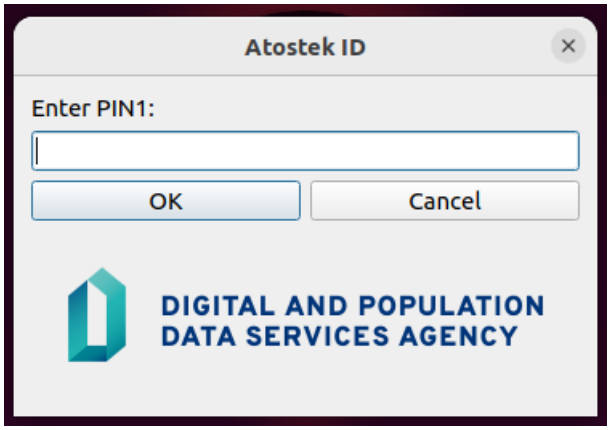


Figure 3. Authenticating the user using PIN1 code. During authentication, the standard operating system PIN window may also be shown.

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 PKCS#11 module is utilized, which automatically installs with the Atostek ID Linux versions' installation. More details about the Atostek ID PKCS#11 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"* 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"* is enabled from the settings. 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 an electronic signature for a compatible service. During signing, the user must enter the PIN2 of their card.

To create the electronic 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 electronic 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 Linux 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.

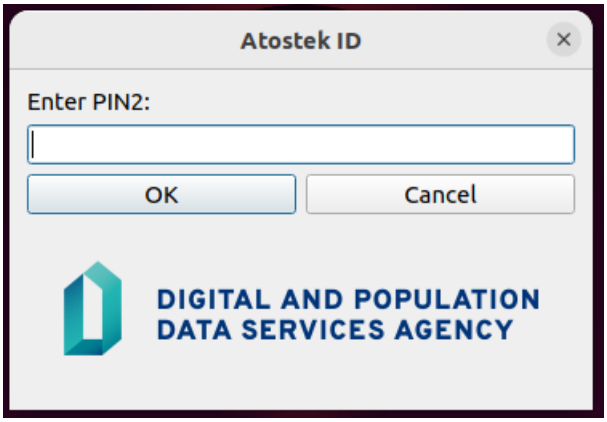


Figure 4. Digital signature with PIN2 code. During signing, the standard operating system PIN window may also be shown.

3.2.1. 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.

3.2.2. 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 program does not start automatically. It needs to be launched from the command line by typing its name:

```
$ atostekid
```

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.

4.3. Changing PIN codes and unlocking locked codes

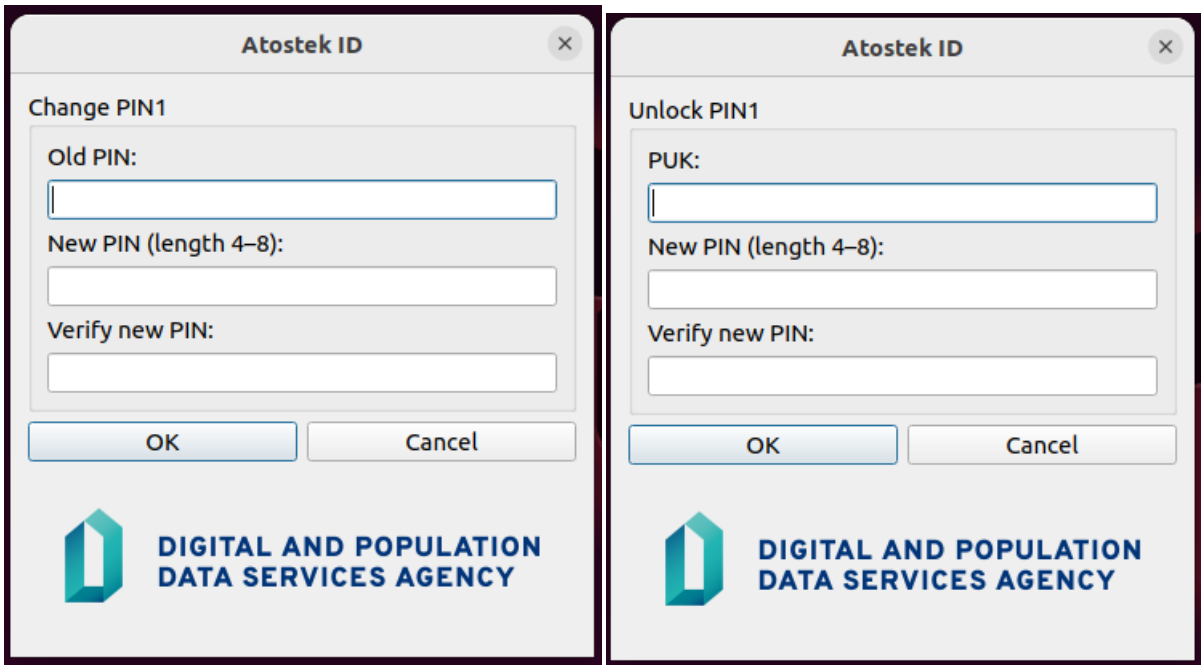
You can change PIN codes by selecting *"Change PIN1"* or *"Change PIN2"* from the application menu and entering the current PIN code and the new PIN code twice (Figure 5).

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, also known as the activation code number, 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"* and *"Save As..."*. Additionally, the validity of certificates can be checked by selecting "*Validity check*". This checks the certificate's expiration date and revocation lists (CRL, OCSP).

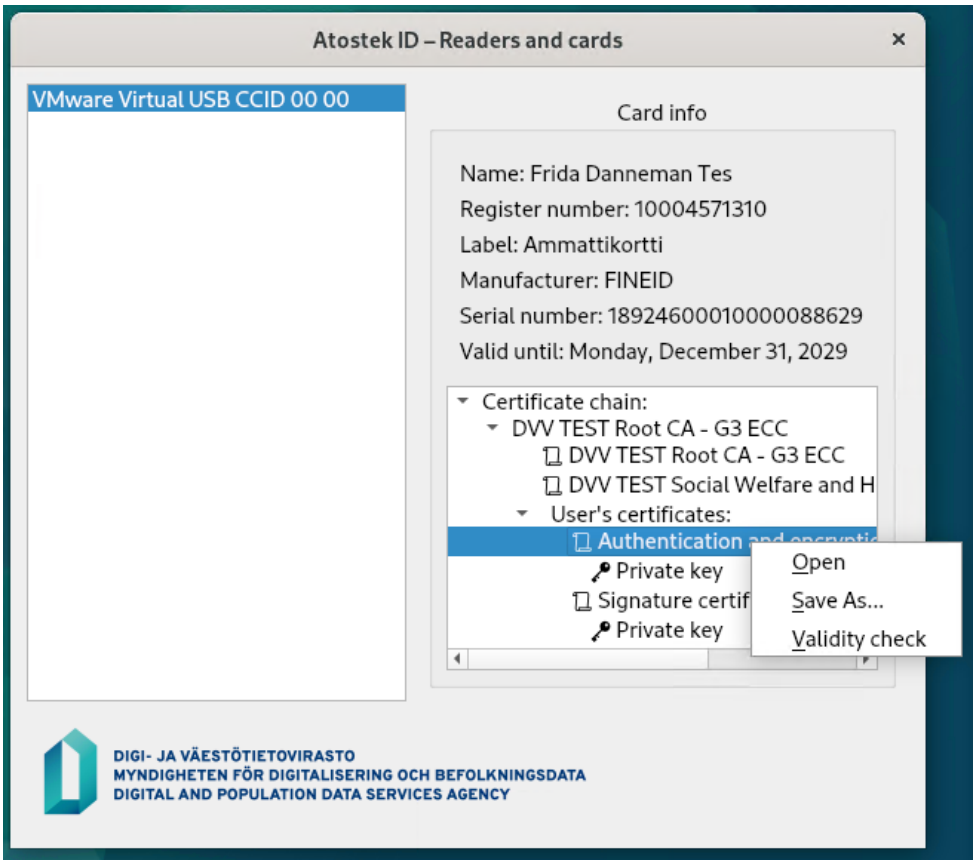


Figure 7. Readers and cards view.

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.

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 settings related to logging. Please note that the changes will only take effect after saving. The settings are detailed in their own subsections.

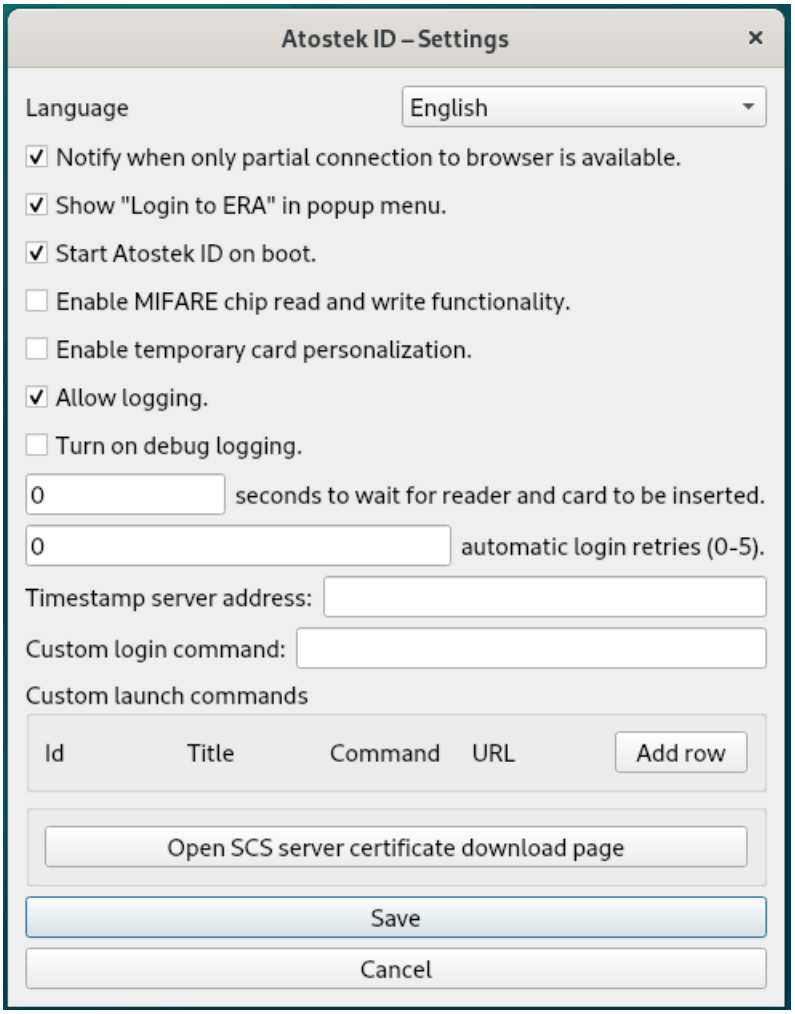


Figure 8. Application Settings.

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

The **"Show 'Log in to ERA' in pop-up menu**" setting can be used to hide or display 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.

4.5.5. 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.

4.5.6. 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.

4.5.7. 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.

4.5.8. 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.

4.5.9. 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.

4.5.10. 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.

4.5.11. 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.

4.5.12. 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.

4.5.13. 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 *"C:\Program Files\Google\Chrome\Application\chrome.exe " {URL}.*

4.5.14. 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": "C:\Program Files\Google\Chrome\Application\chrome.exe" {URL}
- "URL": https://edemo.atostek.com

4.5.15. 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.

4.5.16. Settings file parameter CLEANCERTSTOREONCARDREMOVAL

You may use the setting parameter *“CLEANCERTSTOREONCARDREMOVAL”* directly in the application’s settings file (*"/home/<user>/.local/share/Atostek Oy/Atostek ID/AtostekID.ini"*). The default value *“true”* in the setting clears the certificates of the user’s card from operating system’s 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.

4.5.17. Settings file parameter EXCLUDEDREADERS

You may use the setting parameter *"EXCLUDEDREADERS"* directly in the application's settings file (*"/home/<user>/.local/share/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.

4.5.18. Settings file parameter EXCLUDEDCARDTYPES

You may use the setting parameter *"EXCLUDEDCARDTYPES"* directly in the application's settings file (*"/home/<user>/.local/share/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 (organization cards), PROFESSIONAL (professional cards for social welfare and healthcare), PERSONNEL (personnel cards for social welfare and healthcare), IDENTITY (citizen certificates). Please note that the settings file must be saved, and Atostek ID must be restarted after changes for the settings to take effect.

4.5.19. Settings file parameter ERRORLOGPATH

You may use the setting parameter "ERRORLOGPATH" directly in the application's settings file (*"/home/<user>/.local/share/Atostek Oy/Atostek ID/AtostekID.ini"*). Give the setting the path to which the application's error log should be written. For example, the path can be *"ErrorLogPath=/home/<user>/log/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.

4.5.20. Settings file parameter ALLOWEDBROWSERLESSANDFORWARDDOMAINS

You may use the setting parameter *"ALLOWEDBROWSERLESSANDFORWARDDOMAINS"* directly in the application's settings (*"/home/<user>/.local/share/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.

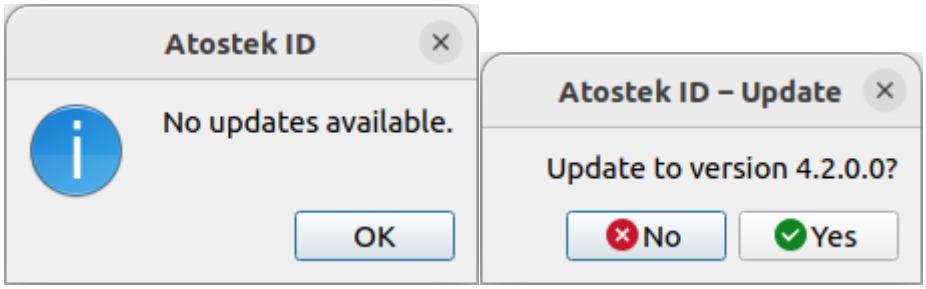
4.5.21. Settings file parameter ENABLECUSTOMDIALOG

You may use the setting parameter *"ENABLECUSTOMDIALOG"* directly in the application's settings file (*"/home/<user>/.local/share/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. 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.

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



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

4.7. Signing documents via the application

In addition to Adobe Acrobat and PDF-XChange applications, 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 11), select the signature type and browse your computer to find the document to be signed.

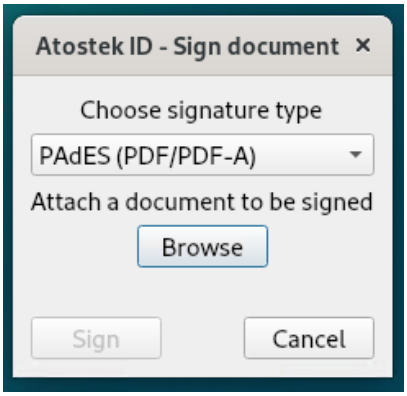


Figure 11. Document signing in the Atostek ID application.

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. Encrypting and signing emails

In several email applications, emails can be encrypted and signed using the certificates inside a smart card. On Linux, this utilizes Atostek ID PKCS#11 module, which is automatically installed during the installation of Atostek ID Linux versions. More detailed information about the Atostek ID PKCS#11 module can be found in the integration guide of the Atostek ID software. Please refer to the email application's own documentation for information on encrypting and signing emails.

The email application must be able to utilize the smart card before encrypting or signing emails. To send an encrypted email, you should have the recipient's public key linked to their contact.

4.9. Logging in to a workstation

Authentication to a Linux workstation can be performed using a smart card's authentication certificate. This process utilizes Atostek ID PKCS#11 module, which is automatically installed during the installation of Atostek ID Linux versions. More detailed information about the Atostek ID PKCS#11 module can be found in the integration guide of the Atostek ID software.

Once the Atostek ID PKCS#11 module is installed, a card reader with a smart card is connected to the machine, and the user's card information is paired with the Linux user, the user can log in to their workstation using their smart card. Authentication requires user to enter the PIN1 code.

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 12.

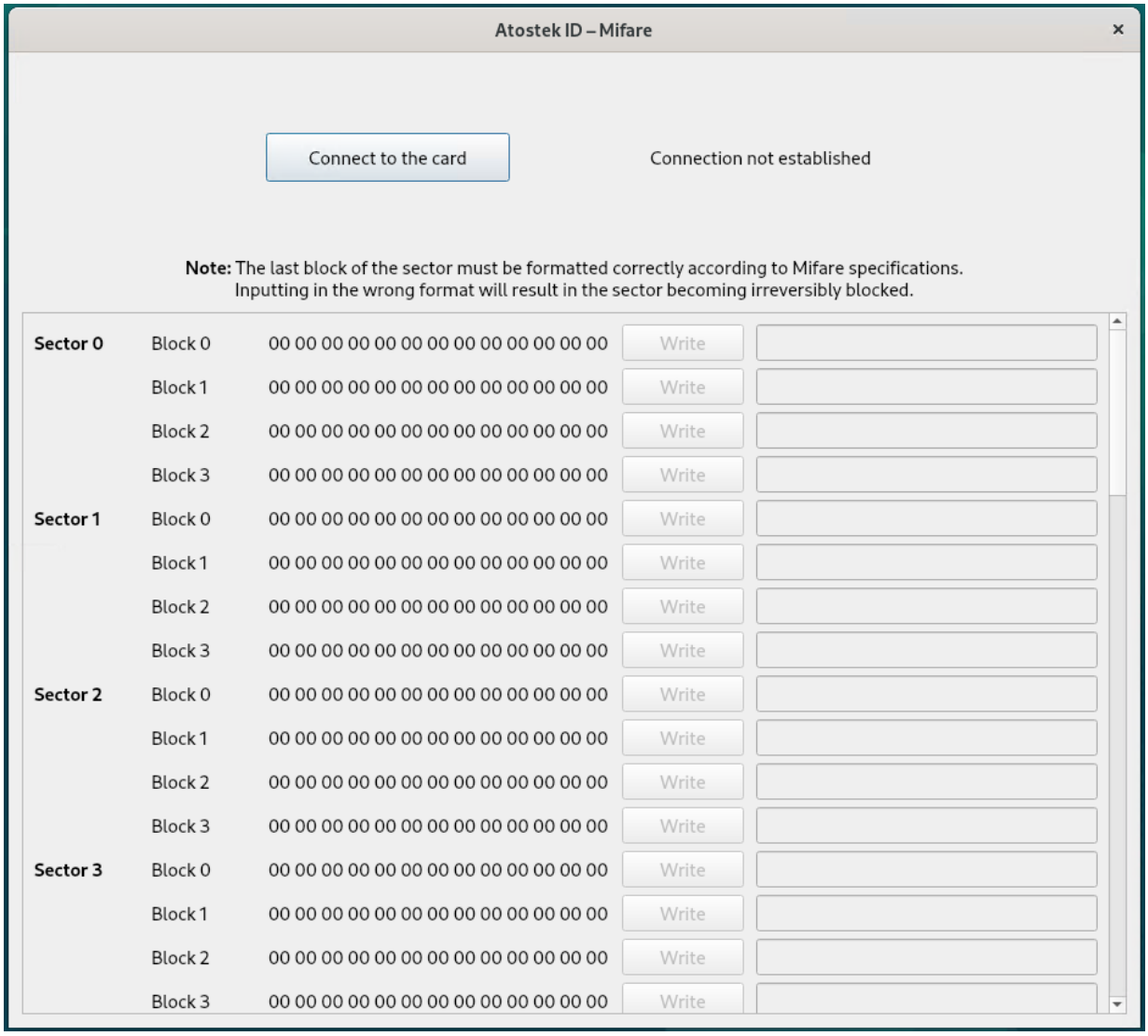


Figure 12. MIFARE chip management view.

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

Atostek ID logs messages about application activity and error situations into its own log file. The log file is by default located at the path *"/home/<user>/.local/share/Atostek Oy/Atostek ID/Error.log".* The log file can be accessed by selecting "Diagnostics" from the menu and then "Show Atostek ID log" from the window that appears. The location of the log file can be changed through the settings.

By default, logging is done for informational, warning, and error level notices. Debug-level logging can be enabled through the settings, which provides more detailed logging and produces more log data. Debug-level logging is particularly essential for troubleshooting error situations. Logging can also be completely turned off through the settings. This does not delete the previous log file; it simply stops new log messages from being recorded.

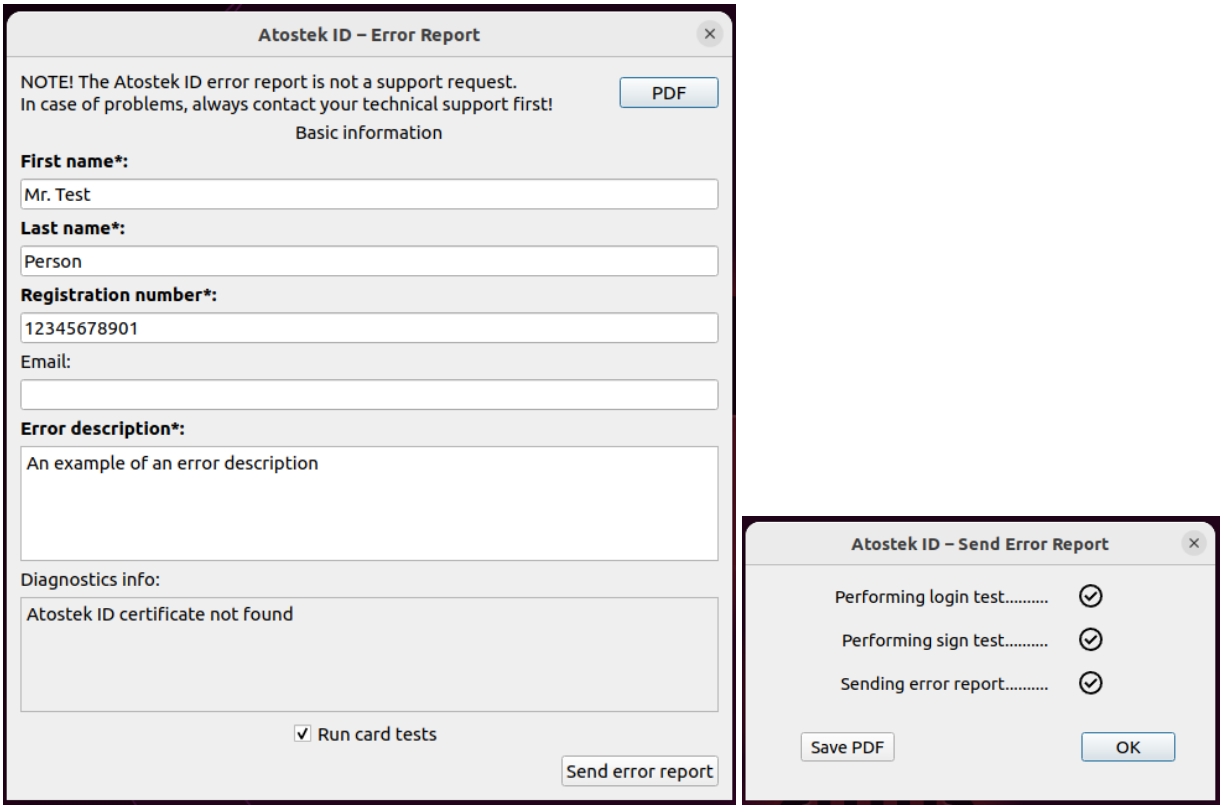
Atostek ID also logs error-level messages to the operating system's log (Syslog).

The Atostek ID PKCS#11 module's log file is located at the path *"/home/<user>/.local/share/Atostek Oy/Atostek ID/PKCS11.log".*

4.12. Error reporting

The Atostek ID application menu includes an option "Error Report," which allows you to send an error report to Atostek's AIDERA service. However, the error 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 using this function. There is a limited number of error reports that can be sent per day.

An error report is created by providing sufficient contact information and writing a description of the error (Figure 13). If the card reader and card are connected, the card information is automatically filled in.



Figures 13 and 14. Error report and sending it.

Fields marked with an asterisk and in bold are mandatory. The error report can be sent using the "Send Error Report" button found at the bottom right. Please note that the button cannot be pressed if any of the mandatory fields are missing.

If you wish, you can also save a PDF file of the error report to your own computer using the "PDF" button located at the top right. The checkbox "Run certificate card tests" found at the bottom of the view allows you to choose whether to run card tests when sending the error report.

Upon sending the error report, a window will open where you can monitor the progress of the submission (Figure 14). The status of the card tests only appears in the error report submission window if you have chosen to run the card tests from the window shown in Figure 13. If the error report is successfully sent, the error report window (Figure 13) will close automatically. From the error report submission window (Figure 14), you can still save the error report as a PDF file using the "Save PDF" button.

4.13. Diagnostics

You can open the diagnostic view (Figure 15) of the Atostek ID application from the "Diagnostics" section of the menu. When the view opens, general tests are run, which takes a few seconds. The test results include information about the version of the Atostek ID application, connected readers, and supported browsers

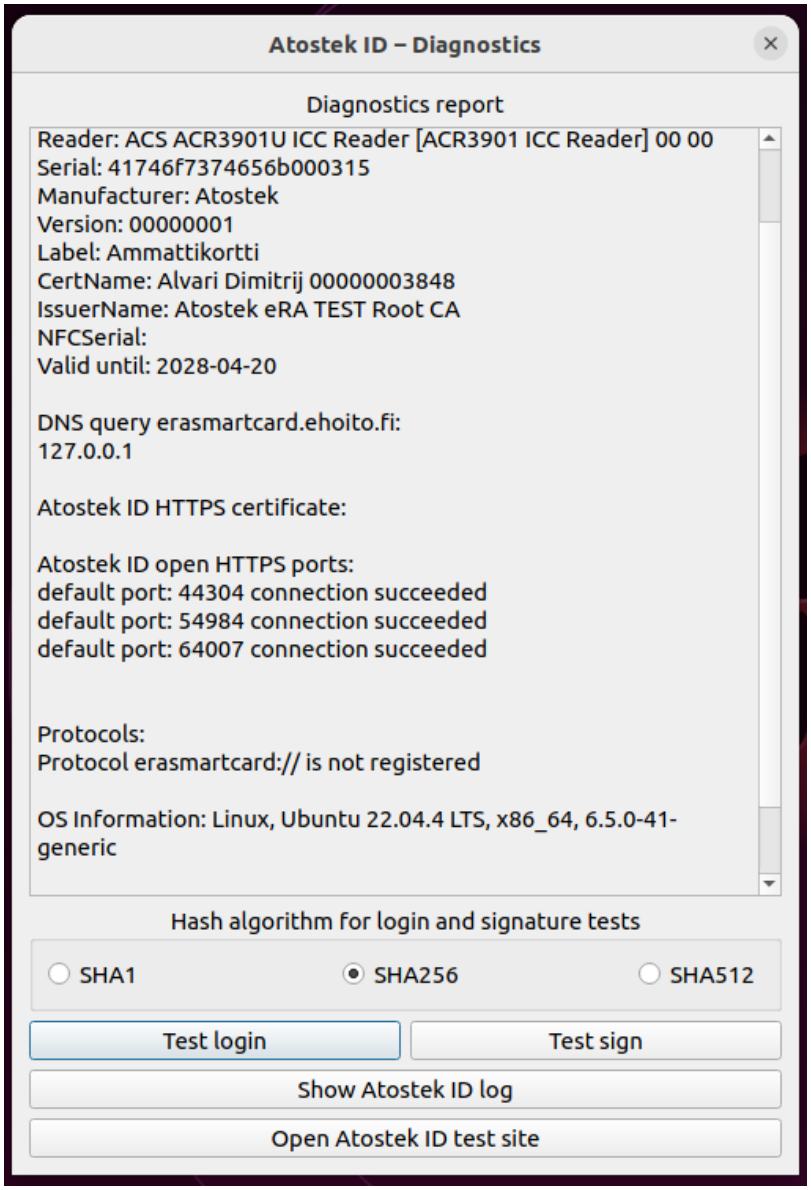


Figure 15. Atostek ID diagnostics view.

In the diagnostic view, you can also test login (authentication) and signature while the card is connected. You can select the hash algorithm to be used using the radio buttons. The results of the login and signature tests are saved in the "Diagnostics report" view.

You can display the application log using the "Show Atostek ID log" button. The log opens in a separate window.

By clicking on the "Open Atostek ID test page" button, you can try whether the Atostek ID application's erasmartcard.ehoito.fi interface is working correctly. If the button does not open an otherwise blank webpage with the text "Test page loaded OK", something is wrong. For example, if the certificates required by the Atostek ID application are not trusted in the certificate store, the test page will not open correctly.

5. Frequently Asked Questions and error situations

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

- Atostek ID cannot start the SCS interface HTTPS server on port 53952 because the port is not available.
- An operation cannot be performed because the card is not in the reader.
- An operation fails (such as authentication or signature) due to incorrect requests or card issues.

In addition, Atostek ID logs messages related to error situations and shows in its logo if something is amiss.

5.1. Frequently asked questions

Q: The application shows a warning "Failed to open SCS server on port 53952!" or "Failed to open SCS CA server on port 53953!".

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.

Q: I cannot read the information on the card.

A: Is the card inserted into the reader correctly? Please note that the card's contact surface (metal square) must touch the reader's contact points to establish a connection (except for NFC readers). You can also try to lightly clean the contact surface as any dirt can impede reading. Is the card reader properly connected to the device? Can you try another USB port? Is the card reader's driver installed and up to date, given that the card reader vendor provides a driver? Drivers from card reader manufacturers are usually pre-installed on the operating system. However, they may also be missing or need an update. Driver packages can generally be downloaded from the card reader manufacturer's own websites.

Q: The application says that the PIN code is locked.

A: The PIN code has then been entered incorrectly too many times in a row. You can unlock the PIN code with the PUK code, also known as the activation code number, via the application's menu.

Q: What is the PUK code?

A: The PUK code or activation code number is a 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 to unlock locked PIN1 and PIN2 codes.

Q: Authentication or signature does not work in the browser.

A: The exact clarification of this problem depends on the interface being used. If it is mTLS authentication (e.g., suomi.fi), please ensure that the Atostek ID PKCS#11 module is installed correctly. If the issue is authentication or signature through 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 there is a problem accessing the page due to DNS issues or untrusted certificates. For DNS issues, contact your organization's IT department. Certificates can be manually installed as trusted in the browser's or operating system's certificate store. You can also check from the application's "About" menu view if the default ports required by the interfaces are in use by the application.

5.2. Other problems

5.2.1. The Atostek ID PKCS11 module

The Atostek ID PKCS11 module is used for example in mTLS authentication (suomi.fi), document signing, email encryption and signing with Thunderbird, and logging into a workstation with a certificate card. The module is automatically installed along with Atostek ID. More information about installing and setting up the module can be found in the installation and integration guides. The following points may help with diagnosing potential problems.

Make sure that the p11-kit platform, which manages the PKCS11-modules on the system, sees the Atostek ID PKCS11 module using the command "*p11-kit list-modules*". If the module is not listed under the name atostek-id, ensure that the file "*/etc/pkcs11/modules/atostek-id.module*" contains a reference to its path according to the instructions in the integration guide, and that the module has been installed in the location the path points to. If the module has been installed correctly and a card is in a connected reader, the command "*p11-kit list-modules*" should also list the tokens on the card.

Note! When using mTLS authentication for the first time, your browser may prompt for the PIN code multiple times. This is normal behaviour due to how browsers handle certificates. Please enter your PIN for each prompt.

5.2.2. PCSC interface is not on

Atostek ID uses the PC/SC Smart Card Daemon (pcscd) software to communicate with the card. Therefore, the systemd services pcscd.service and pcscd.socket for PCSCD must be running for Atostek ID to interact with the card. You can check the status of these services with the commands *sudo systemctl status pcscd.service* and *sudo systemctl status pcscd.socket*. If the services are not running, you can activate them with the commands *sudo systemctl start pcscd.service* and *sudo systemctl start pcscd.socket*. For more detailed instructions, please consult the installation guide for the respective version and operating system.

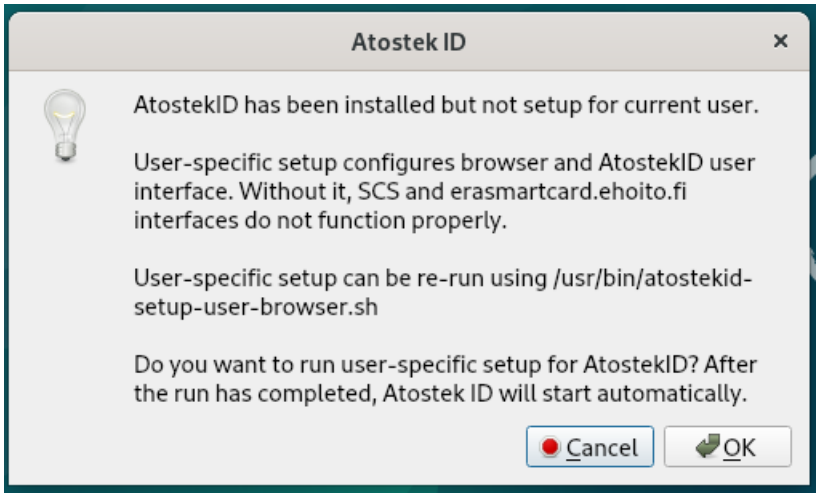
5.2.3. Atostek ID warns about a missing taskbar

Atostek ID uses the GNOME AppIndicator for the application to be visible in the taskbar. If a suitable taskbar is not available in the operating system, Atostek ID will inform the user of this with a separate warning upon startup. This issue can be resolved by installing the package *gnome-shell-extension-appindicator* using the package manager with administrator privileges. For more detailed instructions, please consult the installation guide for the corresponding version and operating system.

5.2.4. A secure connection to SCS or erasmartcard.ehoito.fi interface cannot be established

The installation of Atostek ID requires user-specific setup that cannot be performed automatically by the installation package. Therefore, the user must complete the installation by running the script */usr/bin/atostekid-setup-user-browser.sh*, which is included with the installation package, with user privileges. This script configures the SCS and erasmartcard.ehoito.fi server certificates generated by Atostek ID as trusted in the web browsers in use. For more detailed instructions, please consult the installation guide for the respective version and operating system.

Atostek ID attempts to detect whether the installation finalization script has been executed. If the script has not been executed, Atostek ID will, upon startup, offer the possibility to run it as shown in Figure 16.



When the prompt in Figure 16 is accepted, Atostek ID will run the finalization script, which may take several seconds to complete. After the script has been executed, Atostek ID will restart automatically, and the application will then be ready for use.