Atostek ID 4.6 Installation Guide

for macOS

v1.0

Atostek

1. 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

3. INSTALLING THE SOFTWARE USING THE INSTALLER 6

3.1 Before installing 6

3.2 Installation 6

3.2.1 Editing program settings 8

4. INSTALLING THE SOFTWARE IN OTHER WAYS 13

4.1 Installation from the command line 13

4.1.1 Setting parameter LANGUAGE 13
4.1.2 Setting parameter NOTIFYUPDATE 13
4.1.3 Setting parameter NOTIFYCONNECTION 14
4.1.4 Setting parameter SHOWLOGIN 14
4.1.5 Setting parameter INSTALLVRKROOT 14
4.1.6 Setting parameter INSTALLSHORTCUT 14
4.1.7 Setting parameter DISABLEOLDTLS 14
4.1.8 Setting parameter WAITCARDTIMEOUT 14
4.1.9 Setting parameter REGISTERPROTOCOL 14
4.1.10 Setting parameter LOGINAUTORETRYCOUNT 15
4.1.11 Setting parameter USEINCLOSEDSYSTEM 15
4.1.12 Setting parameter LAUNCHCOMMANDLINE 15
4.1.13 Setting parameter ADDLAUNCH 16
4.1.14 Setting parameter KEEPOLDSETTINGS 16
4.1.15 Setting parameter SERVERPORT 16
4.1.16 Setting parameter SERVERRANDOMPORTS 16
4.1.17 Setting parameter PIN1BUFFERTIMEOUT 17
4.1.18 Setting parameter CONFIGUREBROWSER 17
4.1.19 Setting parameter SKIPCERTINSTALL 17
4.1.20 Setting parameter SERVERADDRESS 17
4.1.21 Setting parameter CARDCACHETYPE 17

4.2 Opening Atostek ID from the command line 18

5. INSTALLATION ON A TERMINAL (E.G. CITRIX AND REMOTE DESKTOP) 19

5.1 Configuring the erasmartcard.ehoito.fi interface 19

6. UNINSTALLING 19

7. ATOSTEK ID PKCS#11 MODULE INSTALLATION 20

8. GRANTING FULL DISK ACCESS ON MACOS 27 21

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. The Atostek ID application supports all versions of the macOS operating system 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 page https://downloads.ehoito.fi before installation.

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

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.

3. Installing the software using the installer

Atostek ID can be installed using a separate installation program via the installation program interface. The installation program will automatically open in the computer's language if the language is Finnish, Swedish, or English. Otherwise, the installation program will open in English. The language of the installation program can be forced when starting from the command line.

3.1 Before installing

Connect the card reader to the computer before installation if you have an external card reader. The operating system-level driver for the card reader is usually pre-installed in the operating system. If the card reader comes with a separate driver, it must be installed before installing the Atostek ID software. If the driver is not found or requires an update, you can download the necessary installation packages directly from the card reader manufacturer's own website. Atostek ID supports card readers that comply with PC/SC specifications.

Note! You do not need other card reader software to use the Atostek ID software. It is also not guaranteed that the Atostek ID software will work simultaneously with other card reader software, such as the previous card reader software from the Digital and Population Data Services Agency (Fujitsu's mPollux DigiSign Client).

3.2 Installation

To install Atostek ID using the software installer, follow the instructions below.

1. Before installation, download the Atostek ID installation program from the website of Digital and Population Data Services Agency https://dvv.fi/en/card-reader-software or from https://downloads.ehoito.fi.
2. Start the installer by double clicking it from the browser's *"Downloads"* menu situated at the top of the window (Figure 1). If the operating system warns about the installer, allow the installation of the software by selecting *"Allow"* (Figure 2).
3. The installation package opens by default in the language of the operating system. If the language of the operating system is not supported, the installation package opens in English.
4. Proceed to the installation by acknowledging the welcome message of the installation package. The first screen in the installation shows the main changes of the release. After reading the release notes, read the license agreement and accept it to continue with the software installation.
5. If you want, edit the program installation (Figure 4). Detailed instructions are in Chapter 3.2.1.
6. Complete the installation according to the instructions provided by the installer. During the installation, the password may be asked several times depending on the selected configurations. Give the password every time to guarantee a successful installation. The different password prompts are depicted in Figure 3. The leftmost prompt is required to authorize the installation. The middle prompt is presented every time a root certificate is about to be set. If the system already has all the root certificates installed, this prompt will not show. The rightmost prompt will be shown twice: it authorizes installing the root certificates for the Atostek ID SCS and erasmartcard.ehoito.fi interfaces.
7. Once the installation is complete, the Atostek ID application will start automatically. You can find more information about the usage and features of the application in the separate user guide.
8. After the installation, it may be necessary to restart the computer.

9. If you are using macOS 27, you must grant Atostek ID full disk access manually so that its modules can use the customized PIN dialog and the card cache, for example when authenticating with Suomi.fi. Detailed instructions are in Chapter 8.

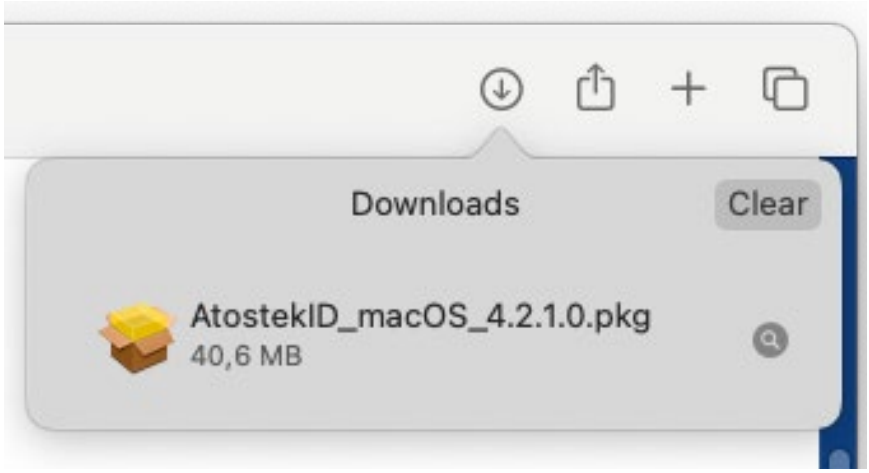


Figure 1. Starting the installer from the *"Downloads"* menu.

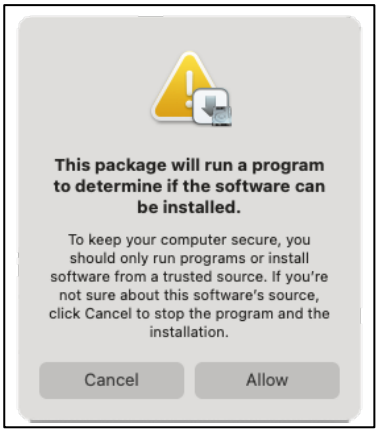


Figure 2. Allowing the installer to run.

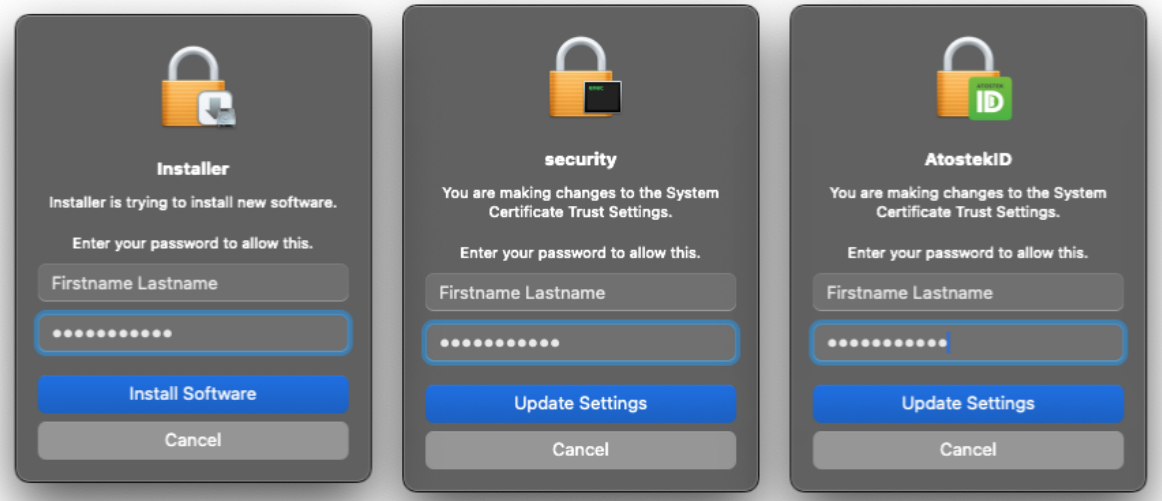
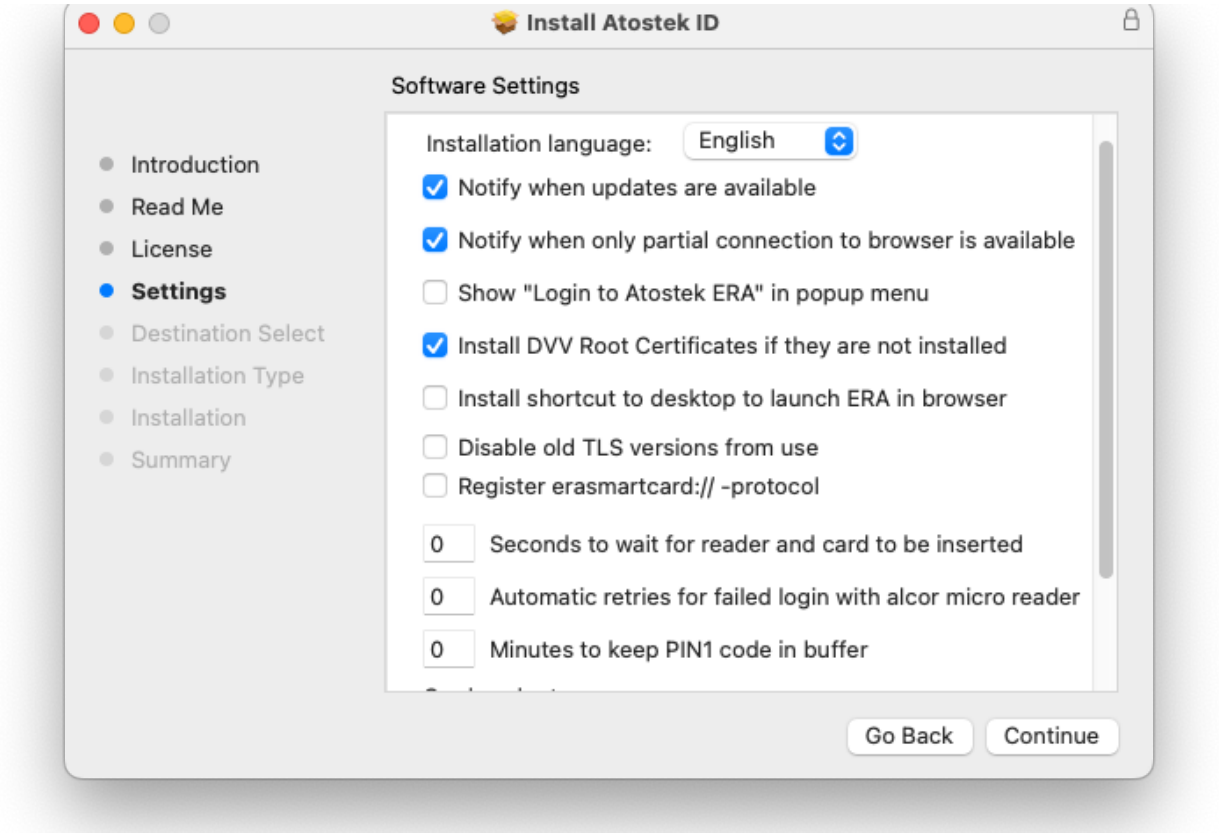


Figure 3. Password prompts while installing Atostek ID.

3.2.1 Editing program settings

After accepting the license agreement, the installer displays the *"Settings"* window (Figure 4), through which some settings of the Atostek ID software can be adjusted during the installation phase. More detailed descriptions of the settings can be found in the subchapters of this section.



3.2.1.1. Figure 4. Selection of settings.Language

You can select the language of the Atostek ID software from the options found in the drop-down menu. You can also change the language of the application later in the application settings. By default, the setting is the language of the installation package.

In command line installation, the name of the setting is *LANGUAGE.*

3.2.1.2. Notify when updates are available.

If you want the Atostek ID software to notify the user of available updates, select this feature. There is no reason to select the feature if the user does not have computer maintenance rights and thus the possibility to install updates. The setting is selected by default.

In command line installation, the name of the setting is *NOTIFYUPDATE.*

3.2.1.3. Notify when only partial connection to browser is available.

If you want the Atostek ID software to report an error situation if the default ports are not available, select this feature. There is no reason to select the feature when several users log into the same operating system, for example in a Citrix environment. The setting is selected by default. This setting concerns only the usage of the erasmartcard.ehoito.fi interface.

In command line installation, the name of the setting is *NOTIFYCONNECTION.*

3.2.1.4. Show the "Login to Atostek ERA" in popup menu.

If you want the Atostek ID software to display in its menu an option to start the ERA service in the default browser, select this feature. There is no reason to select the feature in environments where the default browser is not used to use Atostek's ERA service, for example because the version is too old. The setting is not selected by default.

In command line installation, the name of the setting is *SHOWLOGIN*.

3.2.1.5. Install DVV Root Certificates if they are not installed.

If you want the Atostek ID software to install the root and intermediate certificates of the Digital and Population Data Services Agency's cards for macOS's use, select this feature. Smart cards issued by the Digital and Population Data Services Agency use this certificate. The certificate is only installed if it has not been installed before. The setting is selected by default.

In command line installation, the name of the setting is *INSTALLVRKROOT*.

Note! In some cases, you may receive the error "26352" during installation, which means that Atostek ID will not be installed on the device. In most cases, the error is caused by the fact that Atostek ID is not able to install the Digital and Population Data Services Agency's root and intermediate certificates on the device. Certificates cannot be installed on the device because they are already installed. Atostek ID's installer tries to detect if the root and intermediate certificates are already installed on the device, but in some rare cases these are not found and attempts are made to install the certificates again. In this situation, the installation is interrupted. If such a situation is reached during the installation, the installation of these root and intermediate certificates should be skipped during the installation phase of Atostek ID. Skipping the installation of the root and intermediate certificate is done either in the user interface or by changing the *INSTALLVRKROOT* parameter of the command line installation to *false*.

3.2.1.6. Install shortcut to desktop to launch ERA in browser.

If you want the Atostek ID software to install a shortcut on the user's desktop, select this feature. The shortcut opens the ERA service in the browser using the correct erasmartcard.ehoito.fi interface port. This enables several simultaneous users to operate on the same computer. The setting is not selected by default. There is no reason to select the feature if Atostek's ERA system is not used.

In command line installation, the name of the setting is *INSTALLSHORTCUT.*

3.2.1.7. Disable old TLS versions from use.

If you want the Atostek ID software to prevent the use of old TLS versions (TLS 1.0, TLS 1.1), select this feature. The setting is not selected by default.

In command line installation, the name of the setting is *DISABLEOLDTLS*.

3.2.1.8. Register erasmartcard:// protocol

The setting "Register erasmartcard:// protocol" can determine whether or not Atostek ID registers the erasmartcard:// protocol for itself. By default, this is not registered. This setting only concerns the use of the erasmartcard.ehoito.fi interface. The protocol can also be installed later via the Atostek ID application.

The protocol can be used, for example, on a web page with a link with the following form: *”Log in to the ERA system”*. The link also works without the HTTPS specification, for example with the following form: *”Kirjaudu ERA-järjestelmään”.* The string *“{PORT}”* is automatically replaced by the erasmartcard.ehoito.fi interface port that Atostek ID is using. This way, the Atostek ID application can be used in a multi-user system. Some browsers or their versions will not work if the two slashes after the colon are added to the protocol. Some browsers or their versions will in turn work also with the slashes.

When *“{PORT}”* is used in Atostek ID , the address is opened with the default browser. Alternatively, the *“{PORT_WITH_CUSTOM_COMMAND}”* embedding can be used with the protocol. This embedding opens the address with the browser specified in the CUSTOMCOMMAND parameter.

In command line installation, the name of the setting is *REGISTERPROTOCOL*.

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

If the card reader or card is not connected when the login is started, the user is shown a dialog asking to connect the card or reader. The dialog remains open for the set number of seconds or closes earlier if the reader or card is connected. After connecting, logging in continues normally. If the reader or card is not connected, the dialog closes after waiting and the login continues normally, i.e. Atostek ID returns an error code related to the absence of a card reader or card. The reader and card can be waited for a maximum of 120 seconds. A waiting time value of 0 means that there is no waiting for the reader or the card at all. This setting only concerns the use of the erasmartcard.ehoito.fi interface.

In command line installation, the name of the setting is *WAITCARDTIMEOUT*.

3.2.1.10. Automatic retries for failed login with Alcor Micro reader

With this setting, you can define how many times Atostek ID will automatically try to log in again in case the login fails due to an issue with the Alcor Micro reader. By default, the number of the setting is 0, which means that login failure is reported and a retry is asked separately a maximum of three times. When the setting is in effect, failed logins caused by Alcor Micro readers are not reported, but retries are performed automatically by the given value. The minimum allowed value of the setting is 0 and the maximum is 5. This setting concerns only the use of the erasmartcard.ehoito.fi interface.

In command line installation, the name of the setting is LOGINAUTORETRYCOUNT.

3.2.1.11. Minutes to keep PIN1 code in buffer

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.

3.2.1.12. 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. Installing the software in other ways

In addition to the graphical interface installation, the installation can also be done, for example, from the command line. This chapter introduces the command line installation of the application. It also explains how to change the language of the graphical interface installation and how to start the application with different parameters from the command line.

4.1 Installation from the command line

To install the program from the command line, follow these instructions:

1. Move the installation package to the desired folder.
2. Start a new Terminal window.
3. Navigate in the command prompt to the folder where the installation package is.
4. Run the command *sudo installer -pkg AtostekID_macOS_<version number>.pkg -target /*. This will perform the installation without the graphical interface with the default settings.

When installing from the command line, configuration parameters can also be provided. You can read a more detailed description of the installation parameters after the example. The configuration parameters are provided in a file named *AtostekIDConfig* with no extension. The file is placed in the */tmp* folder, where the installer program will search for it automatically. If the file does not exist or some parameters have not been provided in the file, the default values will be used in installation.

An example of the configuration parameters in the file:

LANGUAGE=fi

NOTIFYUPDATE=true
SHOWLOGIN=true
WAITCARDTIMEOUT=0

LOGINAUTORETRYCOUNT=0
<empty row>

Installation parameters and their values are separated by an equals sign. Each installation parameter must be on its own line. Note that there must be one empty line at the end of the file!

4.1.1 Setting parameter LANGUAGE

The LANGUAGE parameter specifies the language of the Atostek ID application. Currently supported languages for Atostek ID are English (*"en"*), Finnish (*"fi"*), and Swedish (*"sv"*).

4.1.2 Setting parameter NOTIFYUPDATE

The NOTIFYUPDATE parameter selects whether the user is notified about application updates. With the value *"true"*, notifications are enabled, and with the value *"false"*, notifications are disabled.

4.1.3 Setting parameter NOTIFYCONNECTION

The NOTIFYCONNECTION parameter selects whether the user is notified about partial connections to the erasmartcard.ehoito.fi interface, which occurs when the default ports are not in use. With the value *"true"*, partial connection notifications are enabled, and with the value *"false"*, they are disabled. This setting only concerns the use of the erasmartcard.ehoito.fi interface.

4.1.4 Setting parameter SHOWLOGIN

The SHOWLOGIN parameter selects whether the *"Log in to the ERA system"* option is displayed in the application's menu. With the value *"true"*, the option is shown, and with the value *"false"*, it is not shown. This setting only concerns the use of the erasmartcard.ehoito.fi interface.

4.1.5 Setting parameter INSTALLVRKROOT

The INSTALLVRKROOT parameter selects whether the root and intermediate certificates for the Digital and Population Data Services Agency's cards are installed for macOS's use. With the value *"true"*, the installations are performed, and with the value *"false"*, they are not performed.

4.1.6 Setting parameter INSTALLSHORTCUT

The INSTALLSHORTCUT parameter selects whether a shortcut *"Log in to Atostek ERA system"* is installed on the user's desktop. With the value *"true"*, the installation is performed, and with the value *"false"*, it is not performed.

4.1.7 Setting parameter DISABLEOLDTLS

The DISABLEOLDTLS parameter selects whether the use of old TLS versions (TLS 1.0, TLS 1.1) is prevented. With the value *"true"*, the use is prevented, and with the value *"false"*, the use is not prevented.

4.1.8 Setting parameter WAITCARDTIMEOUT

The WAITCARDTIMEOUT parameter sets how long the card reader or card is waited for during login when using the erasmartcard.ehoito.fi interface if they are not connected when the login starts. The waiting time is given in seconds. The wait can be 0–120 seconds. This setting only concerns the use of the erasmartcard.ehoito.fi interface.

4.1.9 Setting parameter REGISTERPROTOCOL

The REGISTERPROTOCOL parameter can be used to determine whether Atostek ID registers the erasmartcard:// protocol for itself. With the value *"true"*, the installation is performed, and with the value *"false"*, the installation is not performed. By default, this protocol is not registered. This setting only concerns the use of the erasmartcard.ehoito.fi interface.

The protocol can be used on a web page with a link like: *"Log in to the ERA system"*. The link also works without the HTTPS specification, for example, in the following form: *"Log in to the ERA system"*. The string *"{PORT}"* is automatically replaced with the port used by Atostek ID for the erasmartcard.ehoito.fi interface. This way, the Atostek ID application can be used in a multi-user system. Some browsers or their versions do not work if the slashes after the colon are added to the protocol. Some browsers or their versions also work with slashes.

When the *"{PORT}"* embedding is used in the Atostek ID application, the address is opened with the default browser. Alternatively, the *"{PORT_WITH_CUSTOM_COMMAND}"* embedding can be used with the protocol, which opens the address with the browser specified in the CUSTOMCOMMAND parameter.

The protocol can also be registered and unregistered after installation by opening the Atostek ID application from the command line with a special registration and unregistration command. To install the protocol, open the application from the command line with the command: *"open ./ AtostekID.app --args "-installERASmartCardProtocol""*. To uninstall the protocol, open the application from the command line with the command: *"open ./ AtostekID.app --args "-uninstallERASmartCardProtocol""*. The command line must be run as an admin user to register or unregister the protocol. The protocol can also be registered after installation through the Atostek ID settings. This is described in more detail in the application user guide.

4.1.10 Setting parameter LOGINAUTORETRYCOUNT

The LOGINAUTORETRYCOUNT parameter defines the number of automatic login retries when a login fails due to an issue with the Alcor Micro reader. The minimum allowed value is 0 and the maximum is 5. This setting concerns only the use of the erasmartcard.ehoito.fi interface.

4.1.11 Setting parameter USEINCLOSEDSYSTEM

The USEINCLOSEDSYSTEM parameter can configure Atostek ID for closed environments. In these environments, Atostek ID does not attempt to fetch the certificate for the erasmartcard.ehoito.fi interface from the ERA system but instead uses an internal certificate for the erasmartcard.ehoito.fi interface. In such cases, Atostek ID must be regularly updated to ensure the certificate within the application does not expire.

4.1.12 Setting parameter LAUNCHCOMMANDLINE

In the LAUNCHCOMMANDLINE parameter, the path to start the browser from the desktop icon or from the "*Log in to Atostek ERA system*" button can be entered. This can be used when you want to launch something other than the default browser. The path is of the form *"<path to browser binary>" {URL}.*

Atostek ID automatically replaces the *"{URL}"* text with the correct port and address of the ERA service. The parameter should be entered base64 coded.

4.1.13 Setting parameter ADDLAUNCH

The ADDLAUNCH parameter can contain multiple addresses that are to be opened in the browser from the Atostek ID menu. The parameters are separated by * and must be entered in the order mentioned below. Several addresses can be entered, and they are separated by a vertical line, i.e. the | sign. For example:
*"Identifier*Title*Browser_Path*Website_Address|Identifier2*Title2*Browser_Path2*Website_Address 2"*. The identifier is internal to the function. The title is the text displayed in the context menu. The browser path tells which browser is opened from the menu. An empty path opens the default browser. A *"{URL}"* string can be used in the browser path parameter, which Atostek ID replaces with the website address. The website address indicates the address of the ERA service. The *"{PORT}"* string can be used in the website address, which Atostek ID replaces with the correct port of the erasmartcard.ehoito.fi interface.

For example, if two shortcuts are desired for the menu, one to open Atostek's Edemo in the default browser and another to open Atostek's ERA service in Firefox, you can put the following command in the *ADDLAUNCH* parameter: *"edemo*Login to eDemo**https://edemo.atostek.com/User/PortSelectLogin/{PORT}|ERA*Login to ERA with Firefox* "<path to Fireox's binary>" {URL}*https://era.ehoito.fi/User/PortSelectLogin/{PORT}"*

As the entire parameter should be entered coded in base64 format.

4.1.14 Setting parameter KEEPOLDSETTINGS

With this parameter as "*true*", the Atostek ID installation will not overwrite old global settings. For instance, it may be used to make sure the previously configured setting values stay in force when updating the installation. The setting is off by default.

4.1.15 Setting parameter SERVERPORT

With this parameter one may configure the default port numbers for the erasmartcard.ehoito.fi interface used by Atostek ID. The port numbers should be separated by commas. The default value is "*44304,52984,64007"*.

The corresponding parameter in the configuration file is named *HTTPSERVERPORT*.

4.1.16 Setting parameter SERVERRANDOMPORTS

When the HTTPSERVERPORT numbers are already reserved for other uses, Atostek ID will pick a random port to access the erasmartcard.ehoito.fi interface. This parameter may be used to define the port range from which the pick is made. The value should be composed of the lower and upper limits of the range separated by a dash. The default value is "*49152-65535"*.

The corresponding parameter in the configuration file is named *HTTPSERVERRANDOMPORTS*.

4.1.17 Setting parameter PIN1BUFFERTIMEOUT

The PIN1BUFFERTIMEOUT 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.

4.1.18 Setting parameter CONFIGUREBROWSER

During the installation, new issuer certificates may be generated for the server certificates of the SCS and erasmartcard.ehoito.fi interfaces. This parameter determines whether the issuer certificates will be added to the Firefox trusted certificate list. The default value is "*true*". If the value is "*false*", the issuer certificates must be manually added to the Firefox certificate store before the SCS and erasmartcard.ehoito.fi interfaces may be used on the browser.

4.1.19 Setting parameter SKIPCERTINSTALL

This parameter determines whether generating the server certificates for the SCS and erasmartcard.ehoito.fi interfaces will be skipped. Given the default value "*false*", those certificates will be generated during installation. The interfaces cannot be used without the certificates.

4.1.20 Setting parameter SERVERADDRESS

Atostek ID sends its error reports to the address defined by this parameter. The default value is "*https://aid.ehoito.fi*".

4.1.21 Setting parameter CARDCACHETYPE

The CARDCACHETYPE setting allows you to specify whether Atostek ID stores card file data in its cache. There are three options for caching: "NONE", "SESSION" and "DISK". With option "NONE" 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 "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 "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.

4.2 Opening Atostek ID from the command line

The Atostek ID application can be opened using the *"launch"* parameter from the command line or from a shortcut. The parameter can be used with a command of the form *"open ./ AtostekID.app --args "-launch default""*. In this command, the default value opens the ERA service in the browser set in the LAUNCHCOMMANDLINE parameter during installation. If the LAUNCHCOMMANDLINE parameter has not been set, ERA will be opened in the default browser. In addition to the *"default"* value, any value of the ADDLAUNCH parameter defined in installation may be used. For example, Atostek's Edemo service would work as follows: *"open ./ AtostekID.app --args "-launch edemo""*.

In place of the default value or a service defined in the ADDLAUNCH parameter, a directly launchable URL can also be used. In the address, the keyword *"{PORT}"* is automatically replaced with the port used by Atostek ID, for example in the command *"open ./ AtostekID.app --args "-launch https://era.ehoito.fi/User/PortSelectLogin {PORT}""*. The default browser defined in the system is used for accessing the page.

When launching from the command line, the parameters *"launchWithCustomCommand"*, *"reset",* and *"resetToGlobalSettings"* may also be used. The "*launchWithCustomCommand"* parameter works like the "*launch"* parameter, but the URL is opened using the browser set in the LAUNCHCOMMANDLINE parameter. If the browser is not set, the default browser is opened. The *"reset"* parameter, in turn, resets the settings of Atostek ID, and the *"resetToGlobalSettings"* parameter resets the user settings to match the global configuration file. During reinstallation, this parameter allows you to reset the settings to match the latest installation. In addition to these parameters, the "version" parameter shows the version number of Atostek ID.

5. Installation on a terminal (e.g. Citrix and Remote Desktop)

When using Atostek ID with a browser, Atostek ID must be installed on the same computer where the browser to be used is installed. For the SCS interface by the Digital and Population Data Services Agency, the Virtual Loopback IP solution can be used in Citrix to enable opening the Atostek ID SCS server to the same port in all users. As for the erasmartcard.ehoito.fi interface, there are multiple different valid solutions for declaring the port information if the Citrix Virtual Loopback IP solution cannot be used.

5.1 Configuring the erasmartcard.ehoito.fi interface

The first user gets access to the default ports of the Atostek ID program. If the three default ports used by Atostek ID are occupied, a new port will be randomly drawn. In environments where a random port must be used, the port must be declared to the client system with the login command.

The port can be determined through one of the following methods:

- If the client system is a desktop application, it can request the port from the Atostek ID application using the *"Named pipe"* command supported by the operating system. The name of the named pipe is of the form *"eRASmartCard_USERDOMAIN_USERNAME"*, where the username and username depend on where Atostek ID is used and who is using it. The message *"GetPort"* should be sent to the pipe and the response will be, for example, *"OK:44304"* or *"ERROR:1000"*.
- If the client system is browser-based, Atostek ID can be configured to open it using the launch function from Atostek ID's menu (the parameter ADDLAUNCH). The startup command can also be made into a shortcut.
- The erasmartcard:// protocol can also be registered for use in Atostek ID. The protocol can be used on the HTTP page, for example, by creating the link *" Log in to the utilizing system"* . The character string "*{PORT}*" is automatically replaced by the port used by Atostek ID. If necessary, see the instructions for REGISTERPROTOCOL and REGISTERPOSTPROTOCOL.
- Atostek ID can also complete the port information in the command line launch just like in the protocol registration. In this case, the client system can be opened from the desktop using the command line launch and port embedding.

6. Uninstalling

Atostek ID may be uninstalled using the application *"/Applications/Uninstall Atostek ID.app*". Running this will uninstall the software and remove both configuration files "*AtostekIDDefaults.ini*" and "*AtostekID.ini*", which are described in detail in the Atostek ID user guide. The uninstalling application asks for password as administrator privileges are needed to complete the uninstallation.

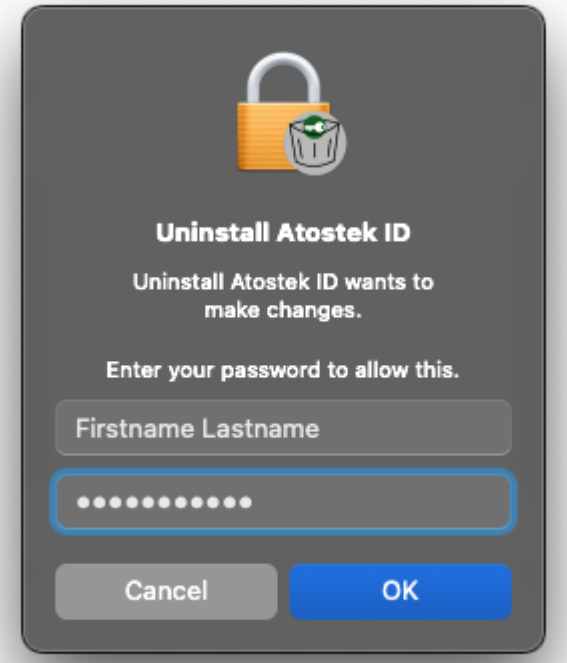


Figure 5. The password prompt while uninstalling

7. Atostek ID PKCS#11 Module Installation

The Atostek ID installation package provides the PKCS#11 module. More detailed information about module can be found in the Atostek ID integration guide. There is no need to separately install the module or a use case-specific TokenDriver module in Adobe for signing, in browsers for authentication (suomi.fi), in the operating system for workstation login, or in the Apple Mail email application for encryption and signing.

8. Granting full disk access on macOS 27

If you are using macOS 27, you must grant Atostek ID full disk access manually so that its modules can use the customized PIN dialog and the card cache, for example when authenticating with Suomi.fi. If the permission is not granted, the user sees the macOS system's own PIN dialog instead of the Atostek ID PIN dialog in certain use cases. Likewise, in those same cases the cache (the CARDCACHETYPE setting) is not used to speed up reading the card data, and all data is read directly from the card again every time.

Illustrated instructions for granting Atostek ID full disk access are given below.

Start by opening System Settings. You can open System Settings by, for example, clicking the Apple logo in the top left corner of the screen and selecting ”System Settings…” from the menu that opens. See Figure 6.

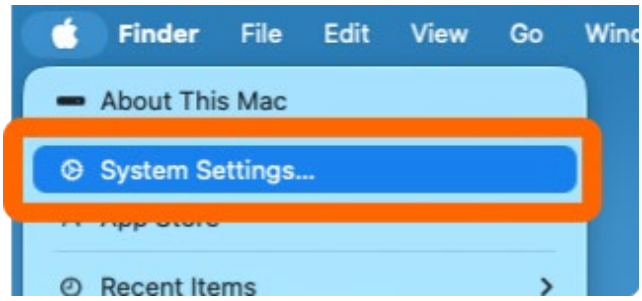


Figure 6. Opening System Settings

The instructions continue on the next page.

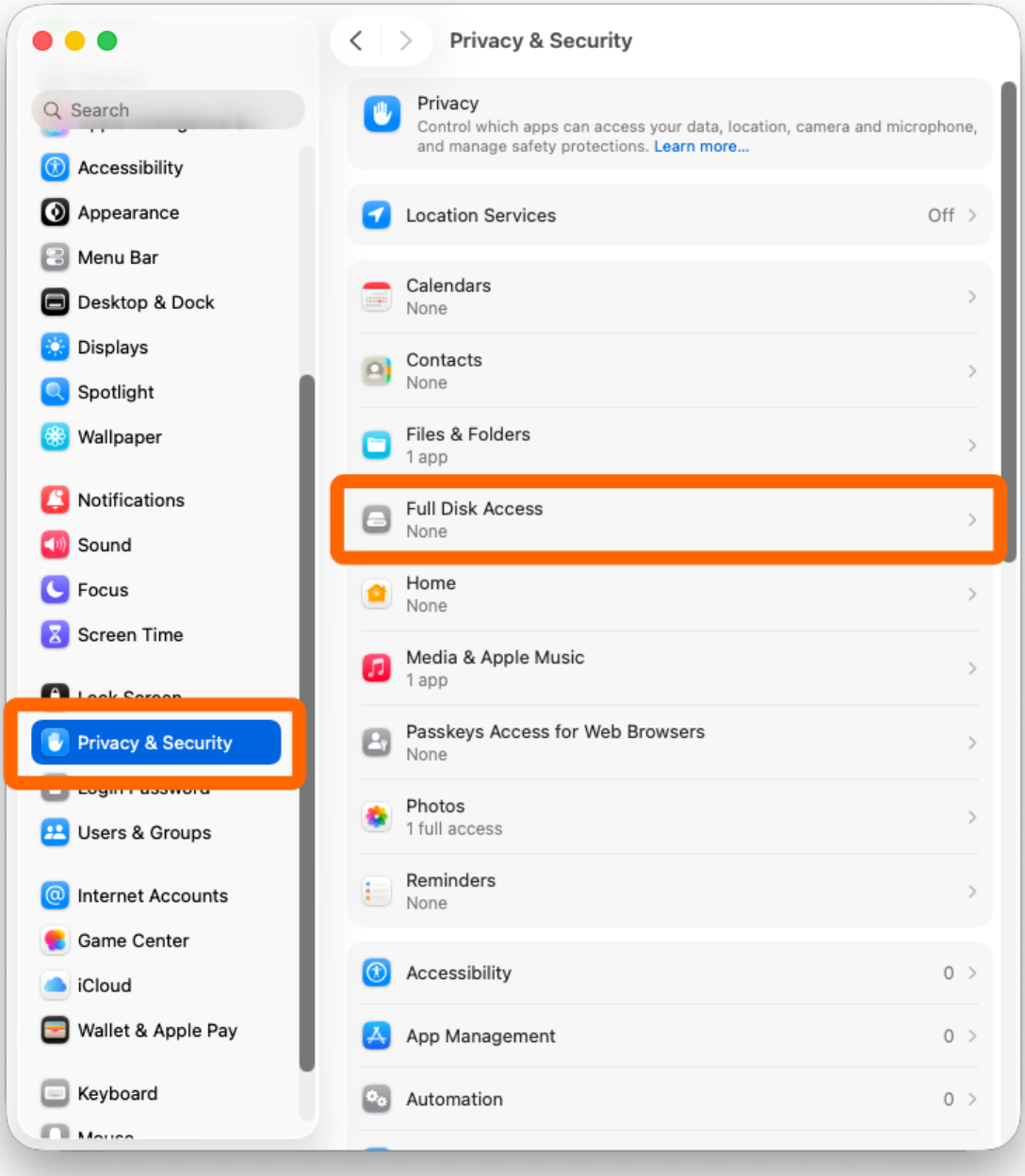
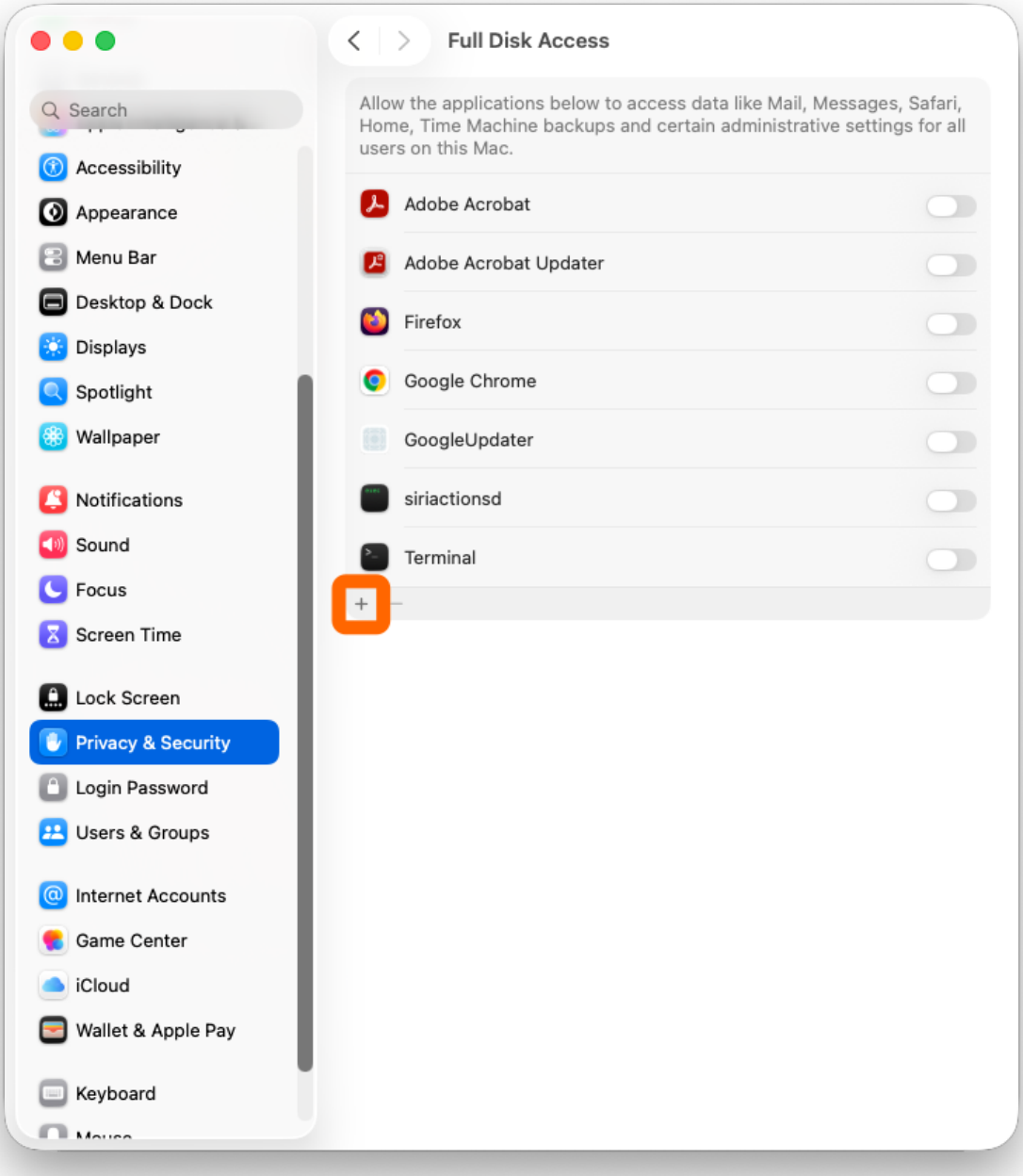


Figure 7. Navigating in System Settings

Once the System Settings window has opened, select ”Privacy & Security” in the menu bar on the left, and then ”Full Disk Access” in the view that opens.



Kuva 8. Adding full disk access for a new application

Click the small plus button in the bottom left corner of the ”Full Disk Access” section to grant full disk access to an application that is not yet on the list.

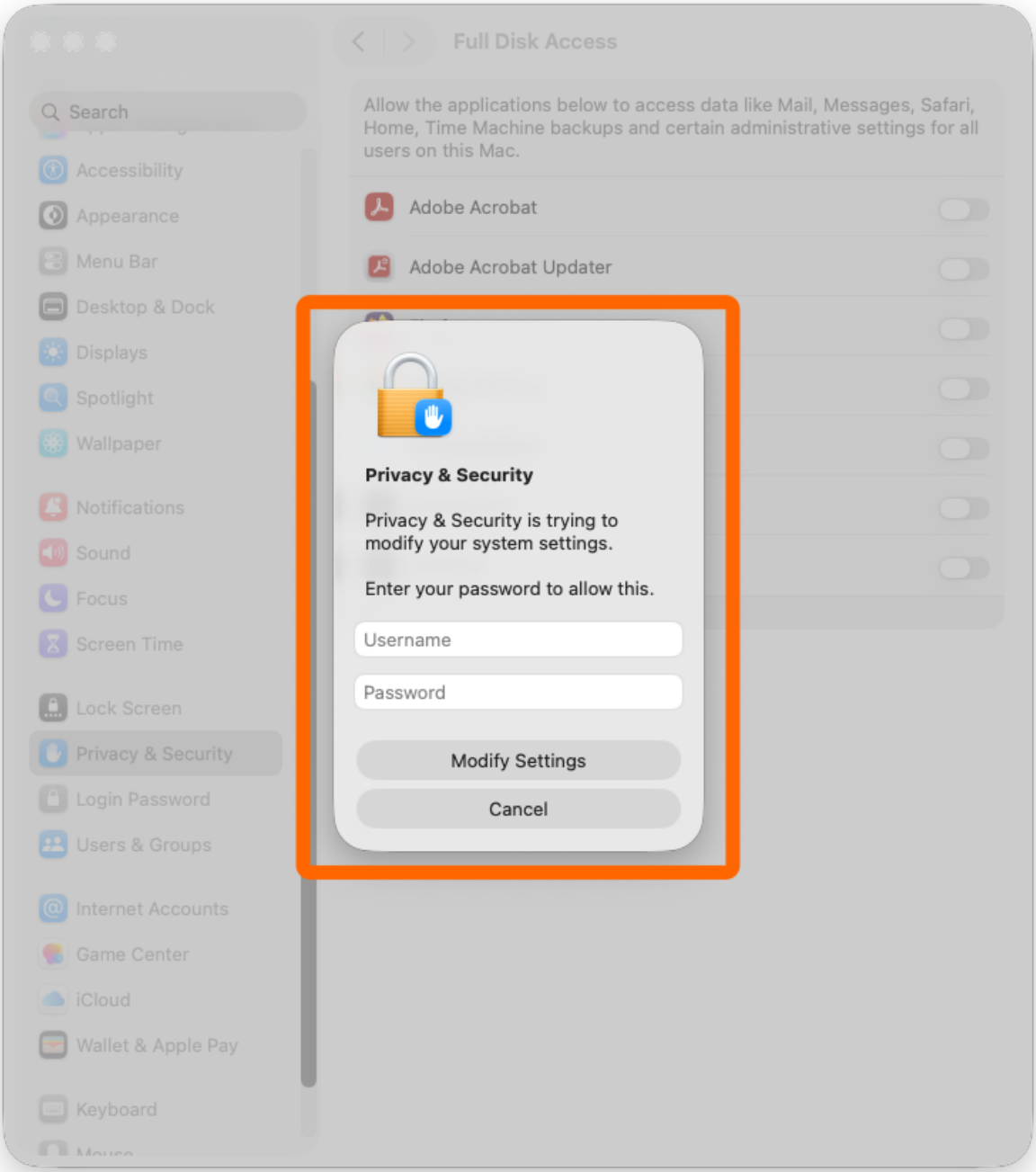


Figure 9. Password prompt for changing system settings

Changing full disk access permissions requires authentication. Enter your user name and password in the prompt that appears on the screen.

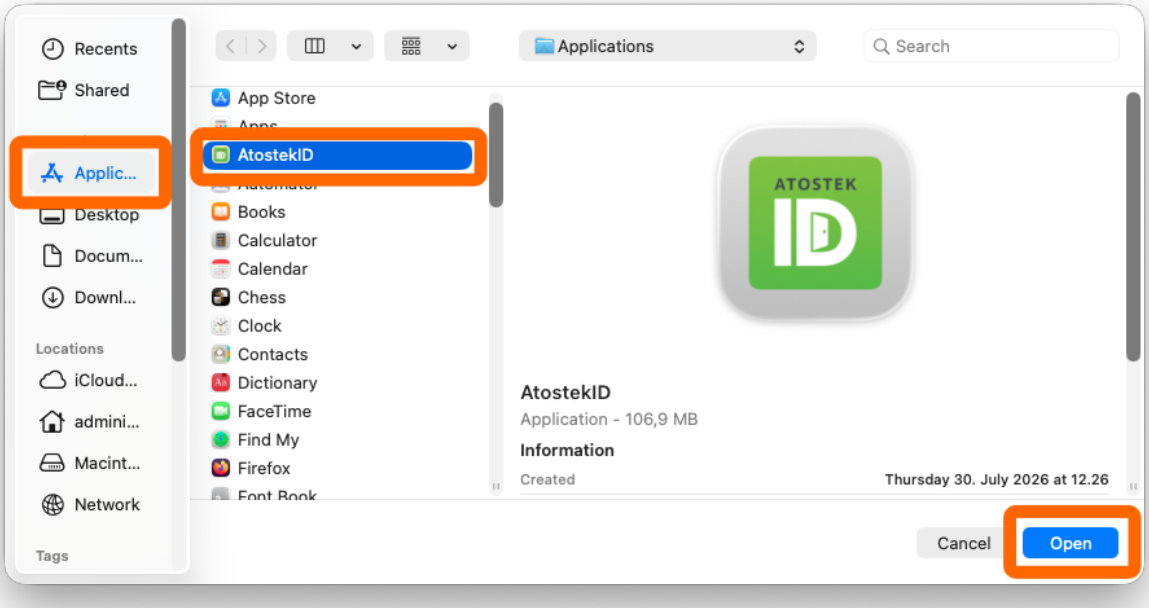


Figure 10. Selecting Atostek ID in the file browser

Once the password prompt has been answered successfully, a file browser opens on the screen. Select ”Applications” in the left-hand column of the file browser, then find ”AtostekID” and click it. Finally, click ”Open” in the bottom right corner of the file browser dialog.

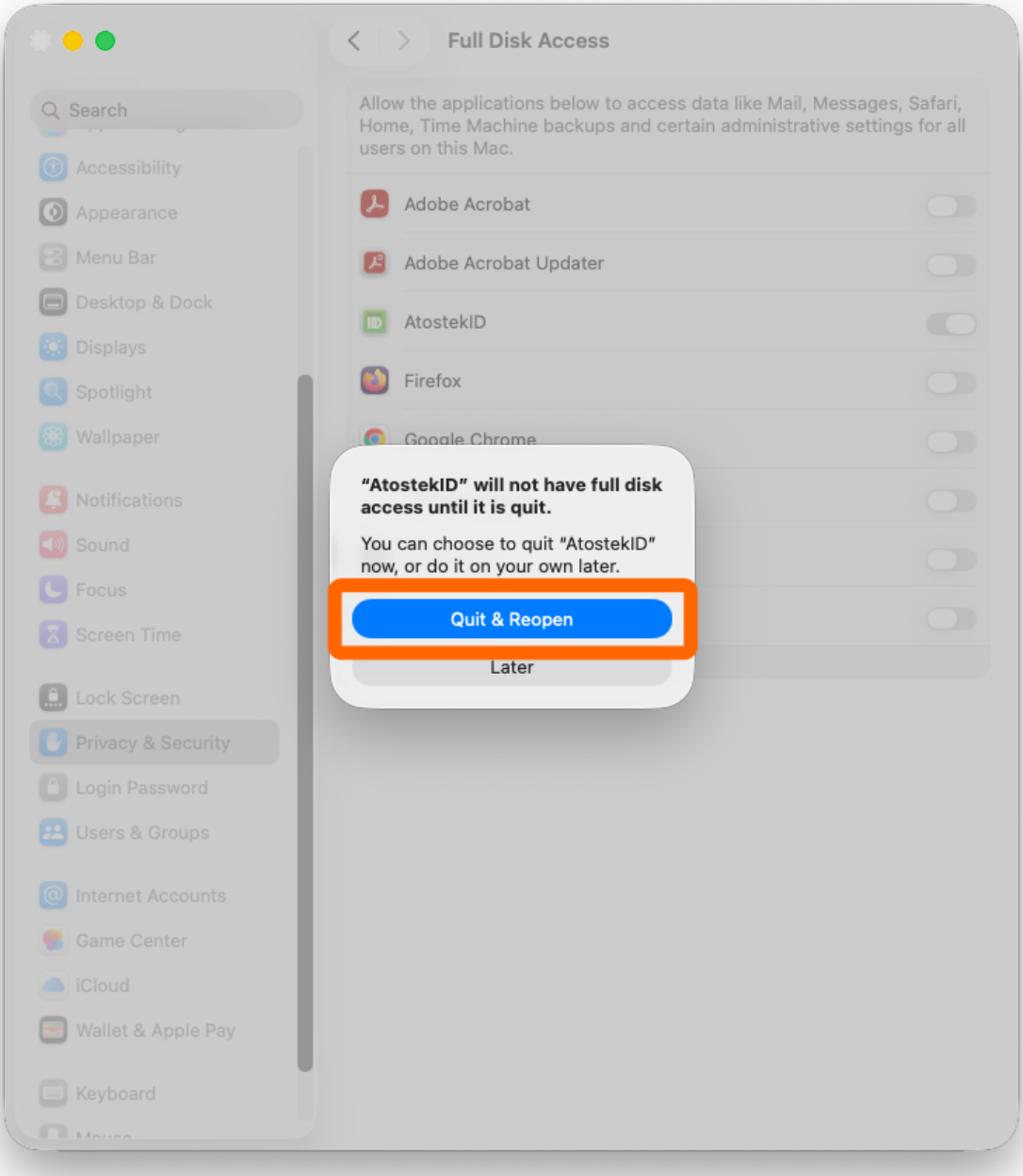


Figure 11. Restarting the Atostek ID application after changing permissions

If Atostek ID is running when its full disk access permissions are changed, the Atostek ID desktop application must be restarted for the new permissions to take effect. Select ”Quit & Reopen” in the dialog that appears in the System Settings window.

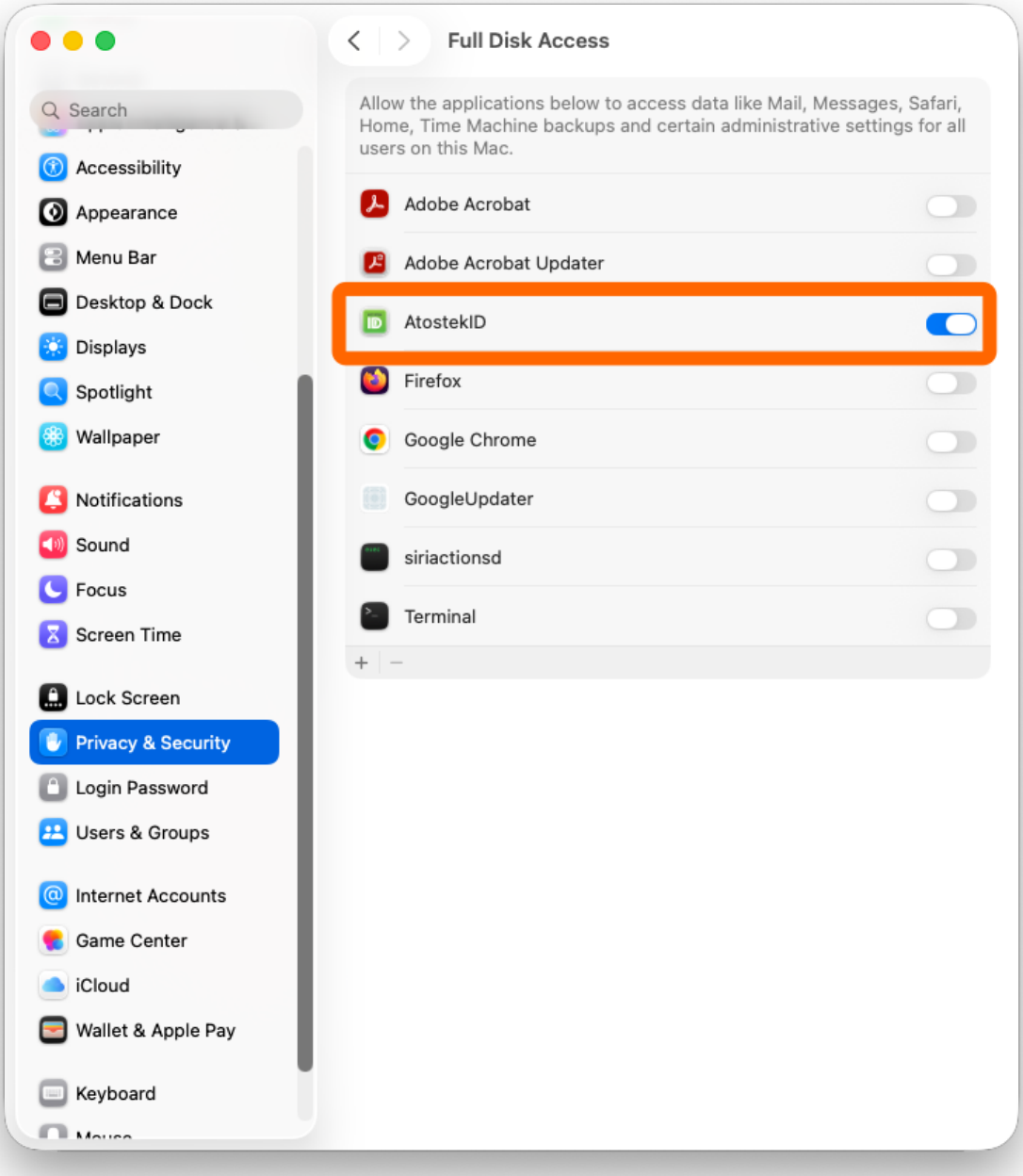


Figure 12. The view after the permissions have been added successfully

Once the permissions have been added successfully, Atostek ID appears in the list in the ”Full Disk Access” section of System Settings, with the toggle next to it switched on.