Atostek ID 4.5 Installation Guide

for Windows

v1.0

Atostek

Table of contents

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 Windows operating system (Windows and Windows Server) maintained by Microsoft.

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 Windows and Windows Server operating systems. Check the latest list of supported Windows 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 macOS 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 pressing the file name from the menu at the bottom or from the "*Downloads*" menu (Figure 1).
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. Chapter 4.2.1 gives instructions on how to open the installation package from the command line in a different language than the language of the operating system.
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. Detailed instructions are in chapter 3.2.1.
6. Complete the installation according to the instructions provided by the installer. 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.

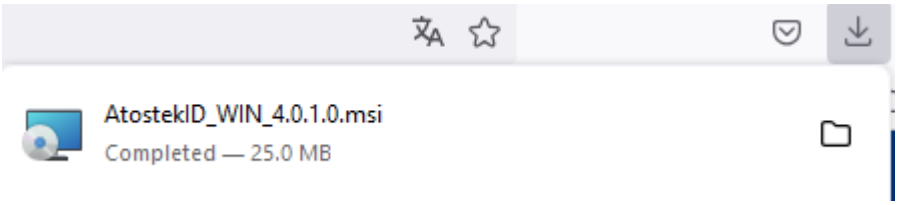

Figure 1. Starting the installer from the *"Downloads"* menu.

3.2.1 Editing program settings

After accepting the license agreement, the installer displays the *"Settings"* window, 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.

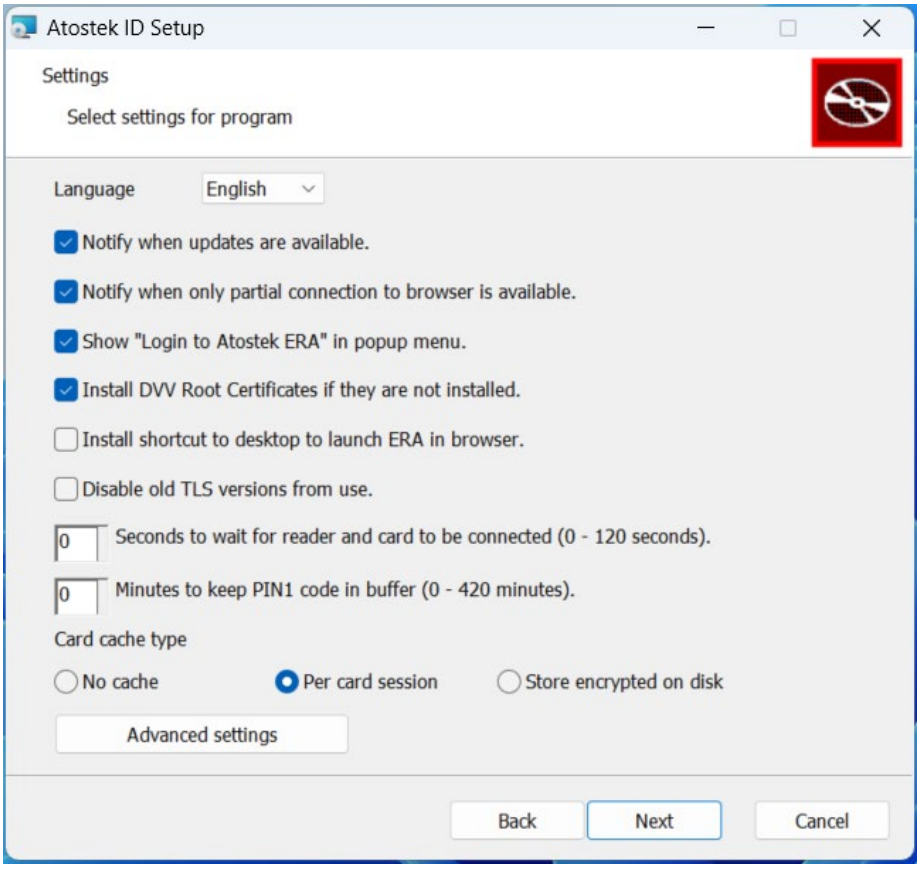

Figure 2. Selection of settings.

3.2.1.1. 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 *NOTIFYPARTIALCONNECTION.*

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

If you want the Atostek ID software to display an option in the Windows taskbar menu 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 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 in the Windows Certificate Store, 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 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 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. Seconds to wait for reader and card to be connected (0 – 120 seconds).

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*.

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

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

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

Note! The setting works with the Atostek ID external modules (Minidriver, PKCS#11) only if the setting *ENABLECUSTOMDIALOG* is true. Currently the parameter may not be set directly in the installer, but it can be stored in the registry, allowing centralized editing. Further instructions for using the parameter may be found in the user guide.

In command line installation, the name of the settings is *PIN1BUFFERTIMEOUT*.

3.2.1.10. 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.

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

3.2.1.11. Advanced setting: Register erasmartcard:// protocol

The "Advanced settings" button opens a window as shown in Figure 3, from which you can register special protocols of the program. 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*.

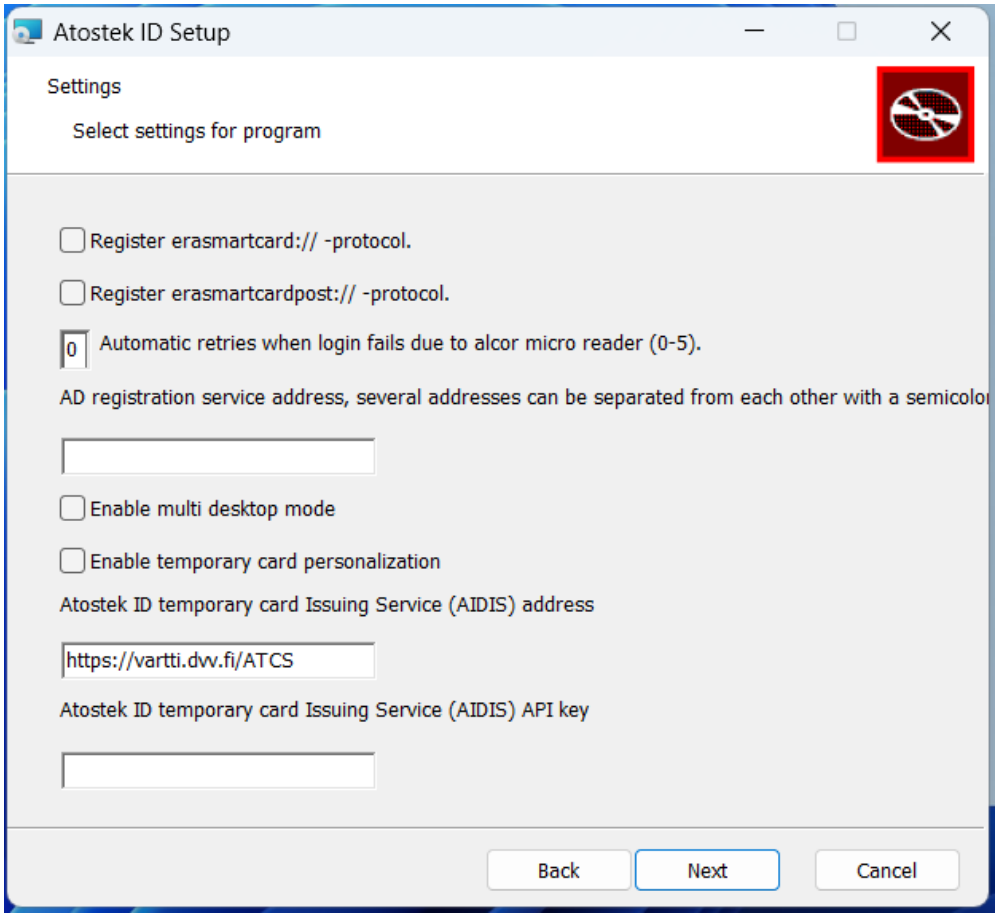

Figure 3. Settings defined in advanced settings.

3.2.1.12. Advanced setting: Register erasmartcardpost:// protocol

This setting can be used to install a special POST protocol. By default, this protocol is not installed. This setting concerns only the use of the erasmartcard.ehoito.fi interface. The protocol can also be installed afterwards through the Atostek ID application. See more detailed instructions for the use of the protocol in the Atostek ID integration guide.

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

3.2.1.13. Advanced setting: Automatic retries when login fails due to Alcor Micro reader (0 – 5)

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.

3.2.1.14. Advanced setting: AD Registration service address

With this setting, you can define URLs for the Atostek ID AD Registration Service (ADRS) installed by your organization. More details about ADRS can be found from the separate ADRS installation guide. For this parameter, you can define as many URLS as you have ADRS installed. Each URL is separated with the semicolon character ";". The HTTP scheme of the URL must be defined for each URL separately. In addition, the port must be included in the address if present, and the address must not end with a slash. Configured URLs are used in the same order that they appear in configuration so that if connection fails to the first service, the second one is used, and so on. An example of the configuration value: *"https://adrs1.com:12345;https://adrs2.com:23456;http://adrs3.fi"*

The property name of the setting in the settings file is ADRSURL.

This setting is stored in the Windows registry path *"HKLM/Software/Atostek/AtostekID"*.

3.2.1.15. Advanced setting: Enable multi-desktop mode

With this setting, you can specify whether the SCS interface provided by Atostek ID should be configured for a multi-user environment where Virtual Loopback IP is not in use. By default, this setting is disabled, in which case the SCS interface will open to its default port 53952 as specified in the specification. If Virtual Loopback IP is not used in your environment, such as in AVD environments, enabling this setting makes it possible to use the SCS interface there as well. For this functionality, a separate commercial proxy is required to route SCS interface requests to the correct users. Please contact Atostek ID support if your organization requires this proxy.

The property name of the setting in the settings file is *MULTIDESKTOPMODE*.

3.2.1.16. Advanced setting: Enable temporary card personalization

With this setting, you can enable the personalization of temporary cards in Atostek ID. This feature is primarily needed by staff at registration points. Regular users do not need to select this setting to use the temporary card issued to them. By default, the setting is disabled, and the option for temporary card personalization will not appear in the Atostek ID application menu. Detailed instructions for the personalization process for temporary cards are provided by the Vartti system.

The property name of the setting in the settings file is *REPLACEMENTCARDSERVICEENABLED*.

3.2.1.17. Advanced setting: Atostek ID temporary card Issuing Service (AIDIS) address

With this setting, you can specify the address where the Atostek ID temporary card Issuing Service (AIDIS) is located. Atostek ID will connect to the AIDIS instance running at this address during temporary card personalization. The default value *https://vartti.dvv.fi/ATCS* is the production address and typically does not need to be modified in regular use.

The property name of the setting in the settings file is *AIDISURL*.

3.2.1.18. Atostek ID temporary card Issuing Service (AIDIS) API key

With this setting, you can define the API key for the AIDIS interface, which enables communication between Atostek ID and AIDIS. If the field is left empty, an API key compatible with the production version will be used as the AIDIS API key. Any unencrypted API key you enter will be encrypted and the encrypted key will be saved in the Atostek ID configuration file.The property name of the setting in the settings file is *ENCRYPTEDAIDISAPIKEY.*

If the value is empty in the settings file or in the Windows registry, then Atostek ID will default to an internal value that is compatible with production release.

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 Changing the language of the installation

The graphical interface installation opens by default in the operating system's language or in English if the language is not among the supported languages. You can open the installation package in Finnish from the command line with the following command: *msiexec /i AtostekID_WIN_4.3.0.0.msi TRANSFORMS=":1035"*. The Swedish installation package can be opened with the parameter value 1053. However, do not use the TRANSFORMS parameter with a non-interactive (i.e., silent) installation.

Always select the language for the Atostek ID application using the LANGUAGE parameter.

4.2 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 command prompt with admin rights.
3. Navigate in the command prompt to the folder where the installation package is.
4. Run the command: *msiexec /quiet /i AtostekID_WIN_<version number>.msi*. This will perform the installation without the graphical interface with the default settings. Please note that name of the installer package in the command must match with the actual installer package that you want to install.

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. If you cannot find a particular setting in the description, it may be other than an installation parameter. Please refer to Subchapter 4.5 of the user manual of the corresponding operating system and Atostek ID version for additional descriptions of other parameters supported by Atostek ID. Example installation command for Atostek 4.4.0.0 that includes configuration parameters:

msiexec /quiet /i AtostekID_WIN_4.3.0.0.msi LANGUAGE="fi" NOTIFYUPDATE="true" SHOWLOGIN="true" NOTIFYPARTIALCONNECTION="true" INSTALLVRKROOT="true" INSTALLSHORTCUT="false" REGISTERPROTOCOL="false" WAITCARDTIMEOUT="0" LOGINAUTORETRYCOUNT="0" LAUNCHCOMMANDLINE="IkM6XFByb2dyYW0gRmlsZXMgKHg4NilcTW96aWxsYSBGaXJlZm94XGZpcmVmb3guZXhlIiB7VVJMfQ==" ADDLAUNCH="ZWRlbW8qS2lyamF1ZHUgZURlbW9sbGUqKmh0dHBzOi8vZWRlbW8uYXRvc3Rlay5jb20vVXNlci9Qb3J0U2VsZWN0TG9naW4ve1BPUlR9fG5ldHRpcmVzZXB0aSpLaXJqYXVkdSBOZXR0aVJlc2VwdGlpbiBGaXJlZm94aWxsYSoiQzovUHJvZ3JhbSBGaWxlcyAoeDg2KS9Nb3ppbGxhIEZpcmVmb3gvZmlyZWZveC5leGUiIHtVUkx9Kmh0dHBzOi8vZWRlbW8uYXRvc3Rlay5jb20vVXNlci9Qb3J0U2VsZWN0TG9naW4ve1BPUlR9"

4.2.1 Settings 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"*).

4.2.2 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.

4.2.3 Setting parameter NOTIFYPARTIALCONNECTION

The NOTIFYPARTIALCONNECTION 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.

4.2.4 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.

4.2.5 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 in the Windows certificate store. With the value *"true"*, the installations are performed, and with the value *"false"*, they are not performed.

4.2.6 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.

4.2.7 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.

4.2.8 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.

4.2.9 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 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: *"AtostekID.exe -installERASmartCardProtocol"*. To uninstall the protocol, open the application from the command line with the command: *"AtostekID.exe -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.

4.2.10 Setting parameter REGISTERPOSTPROTOCOL

This setting allows the installation of a special POST protocol. 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. For detailed instructions on using the protocol, refer to the Atostek ID software integration guide.

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: *"AtostekID.exe -installERASmartCardPostProtocol"*. To uninstall the protocol, open the application from the command line with the command: *"AtostekID.exe uninstallERASmartCardPostProtocol"*. 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.

4.2.11 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.

4.2.12 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.

4.2.13 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 can be, for example: *"C:\Program Files (x 86)\Mozilla Firefox\firefox.exe" {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, so the line above becomes the following: *"IkM6XFByb2dyYW0gRmlsZXMgKHg4NilcTW96aWxsYSBGaXJlZm94XGZpcmVmb3guZXhlIiB7VVJMfQ==".*

4.2.14 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_Address2"*. 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* "C:/Program Files (x86)/Mozilla Firefox/firefox.exe" {URL}*https://era.ehoito.fi/User/PortSelectLogin/{PORT}"*

As the entire parameter should be entered coded in base64 format, the example above becomes approximately the following:
"ZWRlbW8qS2lyamF1ZHUgZURlbW9sbGUqKmh0dHBzOi8vZWRlbW8uYXRvc3Rlay5jb20vVXNlci9Qb3J0U2VsZWN0TG9naW4ve1BPUlR9fG5ldHRpcmVzZXB0aSpLaXJqYXVkdSBOZXR0aVJlc2VwdGlpbiBGaXJlZm94
WxsYSoiQzovUHJvZ3JhbSBGaWxlcyAoeDg2KS9Nb3ppbGxhIEZpcmVmb3gvZmlyZWZveC5leGUiIHtVUkx9Kmh0dHBzOi8vZWRlbW8uYXRvc3Rlay5jb20vVXNlci9Qb3J0U2VsZWN0TG9naW4ve1BPUlR9"

4.2.15 Setting parameter ALLOWEDBROWSERLESSANDFORWARDDOMAINS

The ALLOWEDBROWSERLESSANDFORWARDDOMAINS parameter is used to define the domains that Atostek ID is allowed to send requests to during browserless login/signing and message forwarding. The value should contain the allowed domains separated bya comma. The default value is "era.ehoito.fi, edemo.atostek.com".

4.2.16 Setting parameter FORCEINSTALLMINIDRIVER

The FORCEINSTALLMINIDRIVER parameter can be used to install the bundled Atostek ID minidriver to the system without discovering smartcards. With the default value *"true"*, the installer also forcibly makes the driver available to the system without going through the Windows Plug and Play process. With the value *"false"*, the minidriver installation is only handled by the Plug and Play service when a supported card is discovered.

4.2.17 Setting parameter KEEPOLDSETTINGS

The KEEPOLDSETTINGS parameter ensures that the installation of Atostek ID does not overwrite existing global settings. For example, this parameter can be used during an update to preserve the global settings specified in the previous installation. By default, this parameter is disabled.

4.2.18 Setting parameter SERVERPORT

The SERVERPORT parameter allows you to specify the default ports used by Atostek ID for the erasmartcard.ehoito.fi interface. The ports should be separated by commas. The default value of the parameter is "44304,52984,64007".

The property name of the setting in the settings file is HTTPSERVERPORT.

4.2.19 Setting parameter SERVERRANDOMPORTS

The SERVERRANDOMPORTS parameter allows you to define the range of ports from which Atostek ID will randomly select a port for the erasmartcard.ehoito.fi interface, if the default ports specified by the HttpServerPort parameter are already in use. The lower and upper bounds of the range are separated by a hyphen. The default value of the parameter is “49152-65535”.

The property name of the setting in the settings file is HTTPSERVERRANDOMPORTS.

4.2.20 Setting parameter PIN1BUFFERTIMEOUT

The PIN1BUFFERTIMEOUT parameter allows you to specify the number of minutes that Atostek ID will store the PIN1 code of a card in its buffer. While the PIN1 code is buffered, the user will not be prompted for it each time. The default value of the parameter is “0”, in which case the PIN1 code is always requested whenever the corresponding private key is needed. The maximum value is 420 minutes (7 hours).

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 (Minidriver, PKCS#11) only if the setting *ENABLECUSTOMDIALOG* is true. Currently the parameter may not be set directly in the installer, but it can be stored in the registry, allowing centralized editing. Further instructions for using the parameter may be found in the user guide.

4.2.21 Setting parameter CONFIGUREBROWSER

The CONFIGUREBROWSER parameter allows you to specify whether the CA certificates for the SCS and erasmartcard.ehoito.fi interfaces, generated during installation, are added as trusted authorities in the Firefox browser. The default value of the parameter is “true”. If the value is set to “false”, the CA certificates must be manually added to Firefox’s certificate store for the SCS and erasmartcard.ehoito.fi interfaces to function with that browser.

4.2.22 Setting parameter SKIPCERTINSTALL

The SKIPCERTINSTALL parameter allows you to choose whether to skip generating the server certificates required by the SCS and erasmartcard.ehoito.fi interfaces during installation. The default value of the parameter is “false”, in which case the certificates are generated during installation. Without these certificates, the aforementioned interfaces cannot be used.

4.2.23 Setting parameter SERVERADDRESS

The SERVERADDRESS parameter allows you to specify the address to which Atostek ID will send error reports. The default value of this parameter is “https://aid.ehoito.fi/”.

4.2.24 Setting parameter MULTIDESKTOPMODE

The MULTIDESKTOPMODE parameter allows you to specify whether the SCS interface provided by Atostek ID should be configured for a multi-user environment where Virtual Loopback IP is not in use. By default, this setting is disabled, in which case the SCS interface will open to its default port 53952 as specified in the specification. If Virtual Loopback IP is not used in your environment, such as in AVD environments, enabling this setting makes it possible to use the SCS interface there as well. For this functionality, a separate commercial proxy is required to route SCS interface requests to the correct users. Please contact Atostek ID support if your organization requires this proxy.

The property name of the setting in the settings file is MULTIDESKTOPMODE.

4.2.25 Setting parameter ADRSURL

The ADRSURL parameter allows you to define URLs for the Atostek ID AD Registration Service (ADRS) installed by your organization. More details about ADRS can be found from the separate ADRS installation guide. For this parameter, you can define as many URLS as you have ADRS installed. Each URL is separated with the semicolon character ";". The HTTP scheme of the URL must be defined for each URL separately. In addition, the port must be included in the address if present, and the address must not end with a slash. Configured URLs are used in the same order that they appear in configuration so that if connection fails to the first service, the second one is used, and so on. An example of the configuration value: "https://adrs1.com:12345;https://adrs2.com:23456;http://adrs3.fi"

This setting is stored in the Windows registry path "HKLM/Software/Atostek/AtostekID".

4.2.26 Setting parameter EXCLUDEDREADERS

The EXCLUDEDREADERS parameter allows you to specify which card readers Atostek ID will ignore. By default, the parameter is empty, so Atostek ID will detect all card readers connected to the computer. The value of the parameter is a string listing the readers (Reader1, Reader2, Reader3) that should be disabled. Atostek ID will not recognize cards inserted 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. Wildcards * (matches one or more characters) and ? (matches a single character) are supported. For example, the value EXCLUDEDREADERS="ACS*" will hide all readers whose name begins with "ACS".

4.2.27 Setting parameter REPLACEMENTCARDSERVICEENABLED

The REPLACEMENTCARDSERVICEENABLED parameter allows you to enable the personalization of temporary cards in Atostek ID. This feature is primarily needed by staff at registration points. Regular users do not need to select this setting to use the temporary card issued to them. By default, the setting is disabled, and the option for temporary card personalization will not appear in the Atostek ID application menu. Detailed instructions for the personalization process for temporary cards are provided by the Vartti system.

4.2.28 Setting parameter AIDISURL

The AIDISURL parameter allows you to specify the address where the Atostek ID temporary card Issuing Service (AIDIS) is located. Atostek ID will connect to the AIDIS instance running at this address during temporary card personalization. The default value https://vartti.dvv.fi/ATCS is the production address and typically does not need to be modified in regular use.

4.2.29 Setting parameter AIDISAPIKEY

The AIDISAPIKEY parameter allows you to specify the API key for the Atostek ID temporary card Issuing Service (AIDIS) interface, which enables the communication between Atostek ID and AIDIS. If the field is left empty, an API key compatible with the production version will be used as the AIDIS API key. Any unencrypted API key you enter will be encrypted and the encrypted key will be saved in the Atostek ID configuration file.

If after installation the value of ENCRYPTEDAIDISAPIKEY is empty in the settings file or Windows registry, then Atostek ID will use a default key that is compatible with the release version.

4.2.30 Setting parameter DISABLEMDINSTALLATION

The DISABLEMDINSTALLATION parameter allows you to enable or disable the installation of the minidriver. The minidriver installation is enabled by default, meaning the installer installs the mindriver during the installation process. If the parameter is false, then the minidriver will not be installed. The parameter will not affect removing the prior minidrivers during updating or uninstalling. This parameter is only used during installation, so Atostek ID will not use it afterwards. Disabling the minidriver installation can be useful if, for example, another minidriver by a different vendor is already in use and you want to prevent installing Atostek ID's minidriver at the same time. Use this parameter only if you know that you do not need it, or you already have an alternative driver you wish to use with your card.

This parameter overrules the value in the parameter FORCEINSTALLMINIDRIVER. The minidriver will not be installed even if FORCEINSTALLMINIDRIVER was true, if the parameter DISABLEMDINSTALLATION is true.

4.2.31 Setting parameter DISABLESCSINTERFACE

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

4.2.32 Setting parameter CARDCACHETYPE

The CARDCACHETYPE parameter 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 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.

4.2.33 Setting parameter CONFIGUREREGISTRY

This parameter controls whether the application’s settings are saved in the Windows Registry. If set to “true”, the settings specified during installation will be stored in the registry. In addition, any settings not yet present in the registry will be assigned default values. When this parameter is set to its default value, “false”, no settings are saved to the registry and any existing settings are deleted. The settings are also removed when the application is uninstalled.

The registry path is Computer\HKEY_LOCAL_MACHINE\SOFTWARE\AtostekOy\AtostekID\AppConfig.

The CONFIGFILE and LANGUAGE parameters are not saved in the registry.

Note that the parameters in the registry override any parameters in the config file. Furthermore, changes between the registry and the config file are not synchronized after installation. More information about the registry parameters can be found in Subchapter 4.5.2.

4.2.34 Setting parameter CONFIGFILE

The CONFIGFILE installation parameter is intended for recording other configuration parameters in a file instead of the command line. In this case, only the path to the configuration parameter file is given on the command line during installation. The configuration parameters should be defined in a file with an .ini extension, starting with the *[General]* label. The parameter names are separated from the values by an equals sign without spaces. Each parameter should be on its own line. Below is a list-style example of what the file might look like. Each element in the list corresponds to a line in the file. Parameters not defined in the file will get the default value during installation.

- [General]
- LANGUAGE=fi
- DISABLEOLDTLS=false
- INSTALLSHORTCUT=true
- INSTALLVRKROOT=true

- NOTIFYPARTIALCONNECTION=false
- NOTIFYUPDATE=true
- REGISTERPOSTPROTOCOL=true
- REGISTERPROTOCOL=true
- SHOWLOGIN=true
- USEINCLOSEDSYSTEM=false
- WAITCARDTIMEOUT=0
- LOGINAUTORETRYCOUNT=0
- LAUNCHCOMMANDLINE=IkM6XBFyb2dyYW0gRmlsZXMgKHg4NilcTW96aWxsYSBGaXJlZm94XGZpcmVmb3guZXhlIiB7VVJMfQ==
- ADDLAUNCH=ZWRlbW8qS2lyamF1ZHUgZURlbW9sbGUqKmh0dHBzOi8vZWRlbW8uYXRvc3Rlay5jb20vVXNlci9Qb3J0U2VsZWN0TG9naW4ve1BPUlR9fG5ldHRpcmVzZXB0aSpLaXJqYXVkdSBOZXR0aVJlc2VwdGlpbiBGaXJlZm94aWxsYSoiQzovUHJvZ3JhbSBGaWxlcyAoeDg2KS9Nb3ppbGxhIEZpcmVmb3gvZmlyZWZveC5leGUiIHtVUkx9Kmh0dHBzOi8vZWRlbW8uYXRvc3Rlay5jb20vVXNlci9Qb3J0U2VsZWN0TG9naW4ve1BPUlR9

When using the CONFIGFILE parameter on the command line, a command like the following is executed: "*msiexec /quiet /i AtostekID.msi CONFIGFILE="C:\Users\<username>\Documents\setup.ini""*. In other words, the CONFIGFILE parameter provides the path to the created configuration file with an .ini extension, and other installation parameters are NOT given on the command line but in the file instead. **ALTERNATIVELY**, you can perform a command line installation without using a configuration file by adding the desired parameters one by one to the command being executed. The parameter names and purposes remain the same regardless of whether they are specified in the configuration file or on the command line.

Any parameters found in the registry override those in the configuration file.

4.3 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 *"AtostekID.exe -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: *"AtostekID.exe -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 *"AtostekID.exe –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.

4.4 Installation as a Group Policy Object

To install the Atostek ID software via Microsoft Active Directory as a Group Policy Object, follow these instructions:

1. If necessary, modify the properties using the Orca software meant for editing MSI installation packages. Editable properties can be found in the Property table. INSTALLSHORTCUT or LAUNCHCOMMANDLINE may not necessarily be found in the Property table, but if you need to edit them, you can add them yourself.
2. Move the installation package to a shared folder that can be accessed by all the computers you want to install the software on.
3. Open "*Administrative Tools*" and this after "*Group Policy Management*".
4. Add a new GPO (Group Policy Object) to the domain. You can give it whichever name you want. The name can be, for example, "AtostekIDInstall".
5. Select the GPO you just added and then open the context menu with the right mouse button. After that, select "*Edit*" from the context menu.
6. In the editing view, open the following selections from the tree view on the left in order: "*Computer Configuration*", "*Policies*", "*Software Settings*", "*Software Installations"*. After that, open the context menu with the right mouse button and select *"New Package"*. Select the Atostek ID installation package and "*Assigned Deployment Method*". Close the edit view.
7. Select the GPO you just added. The object's information opens on the right side of the view.
8. Select the tab "*Scope*", and from the lower *"Security Filtering"* view, select the computers you want to install on. Link the object to the domain in the upper *"Links"* view.
9. Finally, select the upper level "*Group Policy Objects"* folder from the tree view on the left side and check that the GPO you just added is in "*Enabled*" mode.

4.5 Windows Registry Changes

The installation of Atostek ID modifies the Windows registry. This section summarizes the registry changes made during installation. Efforts will be made in the future to refactor and clarify the branches used. Relevant parties will be informed in advance of significant changes wherever possible. The release notes also document changes made to the registry. Always refer to the installation guide for the relevant operating system and version for information on registry settings for versions newer than 4.4.1.0.

4.5.1 Register Branches

The following sub-sections describe the entries made in each registry branch. Note that some branches are only created if the corresponding installation parameter is set to a value other than its default.

4.5.1.1. HKLM\SOFTWARE\CLASSES\eRASmartCard

This branch is created if the REGISTERPROTOCOL parameter is set to “true” during installation. The branch is also created if the erasmartcard protocol is registered later in the Atostek ID settings interface.

4.5.1.2. HKLM\SOFTWARE\CLASSES\eRASmartCardPost

This branch is created if the REGISTERPOSTPROTOCOL parameter is set to “true” during installation. The branch is also created if the erasmartcardpost protocol is registered later in the Atostek ID settings interface.

4.5.1.3. HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

This branch enables Atostek ID to start automatically when Windows launches. Atostek ID writes the location of its binary here under the key “Atostek ID”.

4.5.1.4. HKLM\SOFTWARE\Atostek\AtostekID

The value of the ADRSURL installation parameter is stored in this branch as a REG_SZ value. Atostek ID uses the address specified here to connect to its AD registration service.

4.5.1.5. HKLM\SOFTWARE\AtostekOy\AtostekID\AppConfig

This branch is created if the CONFIGUREREGISTRY installation parameter is set to “true”. The parameters stored in this branch override values set in the Atostek ID configuration file.

4.5.1.6. HKLM\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards

Atostek ID’s minidriver installs registry values here as specified in its .inf file, enabling operation in 64-bit environments.

4.5.1.7. HKLM\ SOFTWARE\WOW6432Node\Microsoft\Cryptography\Calais\SmartCards

Atostek ID’s minidriver installs registry values here as specified in its .inf file to ensure compatibility with 32-bit applications in 64-bit environments.

4.5.1.8. HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\Atostek ID

The keys “EventMessageFile” and “TypesSupported” are specified in this branch. These values enable Atostek ID logging in the Windows Event Log.

4.5.1.9. HKCU\Software\Atostek\AtostekID

This branch is used to store REG_DWORD values under the keys “defaultsettingsini” and “installed”. These values mainly ensure backward compatibility and should no longer be used for integration purposes. In addition, if the INSTALLSHORTCUT installation parameter is set to “true”, the key “installedDTSC” is also added here. Its integer value of 1 indicates that a shortcut for the default launch command has been created.

4.5.1.10. HKCU\Software\Atostek Oy\Atostek ID\Certificates

A REG_SZ key named “WHQLCertificate” is stored in this branch. Its value is empty, and the WHQL certificate is saved to the installation directory of Atostek ID.

4.5.2 Settings Registered in the Registry

If the CONFIGUREREGISTRY parameter is set to “true” during installation, the Atostek ID configuration settings are saved under the registry branch “Computer\HKEY_LOCAL_MACHINE\SOFTWARE\AtostekOy\AtostekID\AppConfig”. The data type for settings in the registry is REG_SZ, and the settings are stored in the same format as in the Atostek ID configuration file. The values stored in the registry are listed below. The default value for each parameter is shown in parentheses, and an empty set of quotation marks (“”) indicates a blank value. For parameter descriptions, see the installation or user manual for the relevant version.

- ADRSURL (“”)
- AIDISURL (””)
- ALLOWEDBROWSERLESSANDFORWARDDOMAINS (”era.ehoito.fi, edemo.atostek.com”)
- ALLOWLOGGING (”true”)
- CARDCACHETYPE (“SESSION”)
- CLEANCERTSTOREONCARDREMOVAL (”true”)
- COMMAND (””)
- DEBUGLOG (”false”)
- DISABLEOLDTLS (”false”)
- DISABLESCSINTERFACE (“false”)
- ENABLECUSTOMDIALOG (”true”)
- EXCLUDEDCARDTYPES (””)
- EXCLUDEDREADERS (””)
- FORCEINSTALLMINIDRIVER (”true”)
- HTTPSERVERPORT (”44304,52984,64007”)
- HTTPSERVERRANDOMPORTS (”49152-65535”)
- INSTALLSHORTCUT (”false”)
- INSTALLVRKROOT (”true”)
- KEEPOLDSETTINGS (”false”)
- LAUNCHCOMMAND (””)
- LOGINAUTORETRYCOUNT (”0”)
- MIFARE (”false”)
- MULTIDESKTOPMODE (”false”)
- NOTIFYPARTIALCONNECTION (”true”)
- NOTIFYUPDATE (”true”)
- PIN1BUFFERTIMEOUT (”0”)
- REGISTERPOSTPROTOCOL (”false”)
- REGISTERPROTOCOL (”false”)
- REPLACEMENTCARDSERVICEENABLED (”false”)
- SERVERADDRESS (“https://aid.ehoito.fi/”)

- SHOWLOGIN (”true”)
- STARTONBOOT (”true”)
- TIMESTAMPSERVER (””)
- USEINCLOSEDSYSTEM (”false”)
- WAITCARDTIMEOUT (”0”)

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.

Using SCS in an Azure Virtual Desktop environment is possible under a separate contract.

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 sinking.

6. 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.