Atostek ID 4.5 Installation Guide

for Linux

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 and instructions are given on how to install the Atostek ID application on a Linux machine. The Atostek ID application supports all maintained versions of Debian and Red Hat distributions for the Linux operating system.

2.1. What is Atostek ID?

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

2.2. What do I need to use Atostek ID?

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

Note! If you are using a Windows or macOS operating system, see the user guide for that operating system.

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

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

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

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

3. Installing Atostek ID

Atostek ID can be installed on a Linux-system using the command line. A separate configuration file can be used to give installation parameters, such as installation language, to the installer.

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 from the command line

To install the Atostek ID app, follow the instructions below.

1. Download the Atostek ID installation package from the website of Digital and Population Data Services Agency https://dvv.fi/en/card-reader-software or from https://downloads.ehoito.fi. There is a *.deb* package (e.g. Debian, Ubuntu) and a *.rpm* package (e.g. Red Hat, Fedora).
2. Open a command line and go to the folder where you downloaded the installation package (e.g. *~/Downloads)*.
3. Ensure that you have root user privileges available (either via **su** or a user in the **sudo** group).
4. Install the application using the package manager of your choice, for example:
    a. On Debian-based distributions it is recommended to use *apt* package manager, which installs also required package dependencies. Installation can be started using command *sudo apt install ./atostekid_DEB_<version>.deb* where *<version>* should be replaced with the version of the package that is being installed. You can also use *dpkg* package manager in which case the dependencies need to be installed separately before installing Atostek ID. With *dpkg* the installation starts with command *sudo dpkg -I atostekid_DEB_<version>.deb* and it will warn about missing dependencies, if any.
    b. On Red Hat -based distributions it is recommended to use *dnf* package manager, which installs also required package dependencies. Installation can be started using command *sudo dnf install ./atostekid_RPM_<version>.rpm* where *<version>* should be replaced with the version of the package that is being installed. You can also use *rpm* package manager in which case the dependencies need to be installed separately before installing Atostek ID. With *rpm* the installation starts with command *sudo rpm -I atostekid_RPM_<version>.rpm* and it will warn about missing dependencies, if any.
5. Under normal circumstances, the application should now function as described in section 3.3.

After the installation is successful, the installation package starts and closes the application once so that it can create the SCS CA certificate and set it as trusted.

You can configure the installation by giving it parameters in a separate file. More information about the different parameters can be found after the example below. You can define the installation parameters by writing them into the file */tmp/AtostekIDConfig*, which is where the installer will look for them automatically. If the file cannot be found or parameters are missing in the file, default values will be used for the missing ones. For now, the Linux version of Atostek ID only supports the *LANGUAGE* parameter. Instructions for adjusting other settings after installation can be found in the Atostek ID user manual.

The configuration file can be for example as follows:

LANGUAGE=en
<empty line>

Installation parameters and their values are separated by an equals sign (=). Each parameter should be put on its own line. Notice that the file must have an empty line at its end.

3.2.1. Installation parameter LANGUAGE

The installation parameter LANGUAGE is used to configure the language for Atostek ID's installation. Currently supported languages are English ("en"), Finnish ("fi") and Swedish ("sv").

3.3. Setting up user-specific browser settings

The Atostek ID installer does not automatically modify browser settings for individual users. Each user needs to configure these settings themselves.

For this, the installer provides a script: */usr/bin/atostekid-setup-user-browser.sh*. When you run this script, it configures the browser settings required by Atostek ID in your user environment.

The script creates certificates for the Atostek ID SCS and erasmartcard.ehoito.fi interfaces and installs them as trusted certificates in your web browsers (Firefox, Chromium, Chrome).

3.4. Starting the program

After installing Atostek ID the application can be started by running the command *atostekid* on the command line. For more details about using Atostek ID, see the User Guide.

If there are problems during the installation or startup of the program, it is recommended to first see section 3.4 to ensure that your system contains all required dependencies for running Atostek ID.

3.5. About dependencies

By default, Atostek ID uses, and therefore requires, GNOME AppIndicator (*gnome-shell-extension-appindicator*) as the app indicator and PC/SC SmartCard Daemon (*pcscd*) for smart card readers. On Red Hat -based systems, *pcscd* is installed as part of the *pcsc-lite* package. If Atostek ID does not start or the application icon does not show up in the app indicator of your system, it may be necessary to install these packages.

To install PC/SC SmartCard Daemon, get the package *pcscd* using your package manager, for example *sudo apt install pcscd*. The *systemd* services for *pcscd* must be running and their status can be checked using the commands *sudo systemctl status pcscd.service* and *sudo systemctl status pcscd.socket*. If they are not running, they can be activated using the commands *sudo systemctl start pcscd.service* and *sudo systemctl start pcscd.socket*.

To install GNOME AppIndicator, first get the package *gnome-shell-extension-appindicator* using your package manager, for example *sudo apt install gnome-shell-extension-appindicator*. The computer must be restarted after installing the package. The user must also activate the app indicator in their own environment, which can be done on the command line as follows:

- List GNOME extensions using the command *gnome-extensions list* and find from the command output the extension that contains the word *"appindicator"*. For example, on Ubuntu, the correct extension would be *ubuntu-appindicators@ubuntu.com*.
- Activate the extension using the command *gnome-extensions enable <extension name>*, for example on Ubuntu, the command would be *gnome-extensions enable ubuntu-appindicators@ubuntu.com*.

The package manager of your Linux distribution should normally install all required dependencies automatically when you install Atostek ID. However, if you run into problems when trying to install or run Atostek ID, make sure at least the following dependencies are installed:

- NSS certificate management tools
  - Debian: libnss3-tools (which usually also installs libnss3 and libnspr4)
  - Red Hat: nss-tools
- Qt 6 libraries
  - Debian: libqt6core6, libqt6gui6, libqt6network6, libqt6printsupport6, libqt6widgets6, libqt6xml6
  - Red Hat: qt6-qtbase-gui
- Most smart card readers need the CCID driver. This is usually installed automatically together with the pcscd package. It is especially useful to check this package is installed if you have problems with the smart card reader:
  - Debian: libccid
  - Red Hat: ccid

Missing dependencies can be installed using your system's package manager, such as *apt* (Debian) or *dnf* (Red Hat). For example, installing the package *libnss3-tools* on Ubuntu can be done using the command *sudo apt install libnss3-tools*.

3.6. Uninstalling Atostek ID

You can uninstall Atostek ID using the same package management tool you used to install it. If needed, refer to your package manager's documentation for detailed instructions.

Removing user-specific configuration and log files is the user's responsibility. These files are in ~/.local/shared/Atostek Oy/Atostek ID. User-specific settings are stored in *AtostekID.ini* and the application error log in *Error.log*.

4. Atostek ID PKCS#11-module

The Atostek ID package has Atostek ID PKCS#11-module bundled with it. The module can be used to interface with different software, but this may require additional setup. More information about the different modules and their usage can be found in the Atostek ID Integration Guide.

On Debian-based systems, the PKCS#11-module is installed to */usr/lib/Atostek-ID-PKCS11.so* and on Red Hat -based systems to */usr/lib64/Atostek-ID-PKCS11.so*.

4.1. Interfacing with p11-kit

Note! By default, the RHEL 8 distribution has all the dependencies required to use the Atostek ID PKCS #11 module preinstalled.

The different PKCS#11 modules on the system are managed by p11-kit. The following instructions make the bundled module visible to p11-kit.

1. Add a reference to the module in a location checked by p11-kit
   sudo install --directory --mode=755 /etc/pkcs11/modules
   a. Debian/Ubuntu: *echo "module: /usr/lib/Atostek-ID-PKCS11.so" | sudo tee /etc/pkcs11/modules/atostek-id.module > /dev/null*
   b. RedHat: *echo "module: /usr/lib64/Atostek-ID-PKCS11.so" | sudo tee /etc/pkcs11/modules/atostek-id.module > /dev/null*
   (Alternatively, the directory *~/.config/pkcs11/modules* can be used for local installation.)
2. Verify that p11-kit detects the module
   p11-kit list-modules
   a. The output can include information about other modules and logging but should contain the line "module: atostek-id". Additionally, if a reader is attached and a supported card is inserted, the command should show information about the tokens on the card.

4.2. Setting up the PKCS#11-module for browser-based mTLS-authentication (suomi.fi identification)

Setting up the Atostek ID PKCS#11-module for mTLS-authentication requires additional steps that depend on the browser. After the setup, mTLS can be tested with supported cards and readers in https://dvv.fineid.fi/en/authentication.

4.2.1. Firefox

Note! In the RHEL 8 distribution, the PKCS #11 module works in the Firefox browser without manual configuration.

Note! In Ubuntu distributions, the default version of Firefox is packaged using the snap system. The snap versions have interoperability problems with PKCS#11-modules due to strict confinement. The setup for Atostek ID PKCS#11-module has been tested with the version of Firefox installed through a .deb package according to Mozilla's instructions: https://support.mozilla.org/en-US/kb/install-firefox-linux#w_install-firefox-deb-package-for-debian-based-distributions. The version can be checked by making sure that the output of *sudo apt install firefox* does not contain references to snap. We recommend to first uninstall the snap version to avoid having multiple installations of the browser and then following Mozilla's instructions.

The use of the Atostek ID PKCS#11-module can be enabled in Firefox through p11-kit proxy on a per-user basis. The proxy can be loaded in the Firefox user interface as follows:

1. Connect the Atostek ID PKCS#11-module to p11-kit according to section 4.1
2. In Firefox settings, go to section "Privacy & Security" and select "Security Devices" (see Figure 1)
3. Select "Load", input the module name *p11-kit-proxy* and module filename *p11-kit-proxy.so* and select "OK" (see Figure 2)
4. If loading the proxy is successful, it should appear in the "Security Modules and Devices" list on the left (see Figure 3). If a reader is connected and a supported card inserted, the tokens on the card should also appear in the list, and their information can be viewed. If loading the proxy fails, ensure that you are not using the snap version of Firefox.

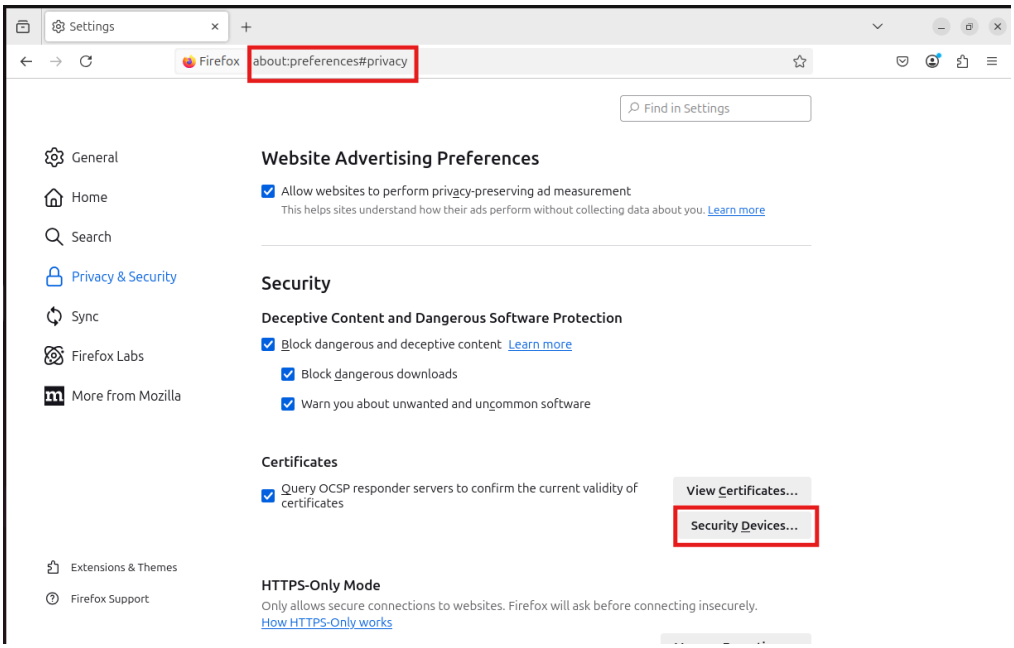

Figure 1: Security Devices under Firefox settings

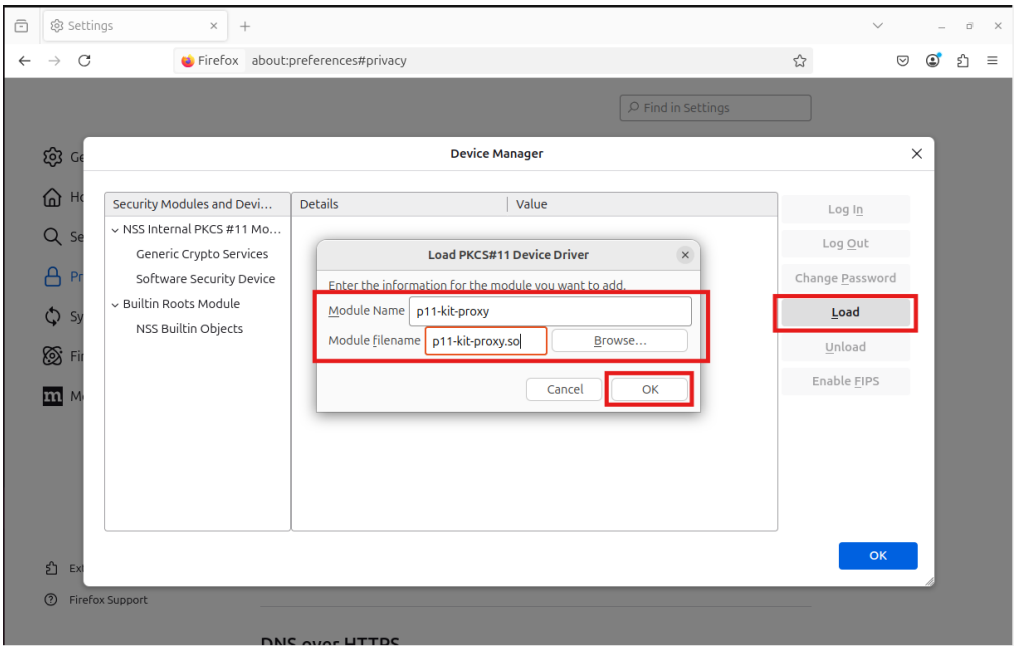

Figure 2: Loading the PKCS#11 module

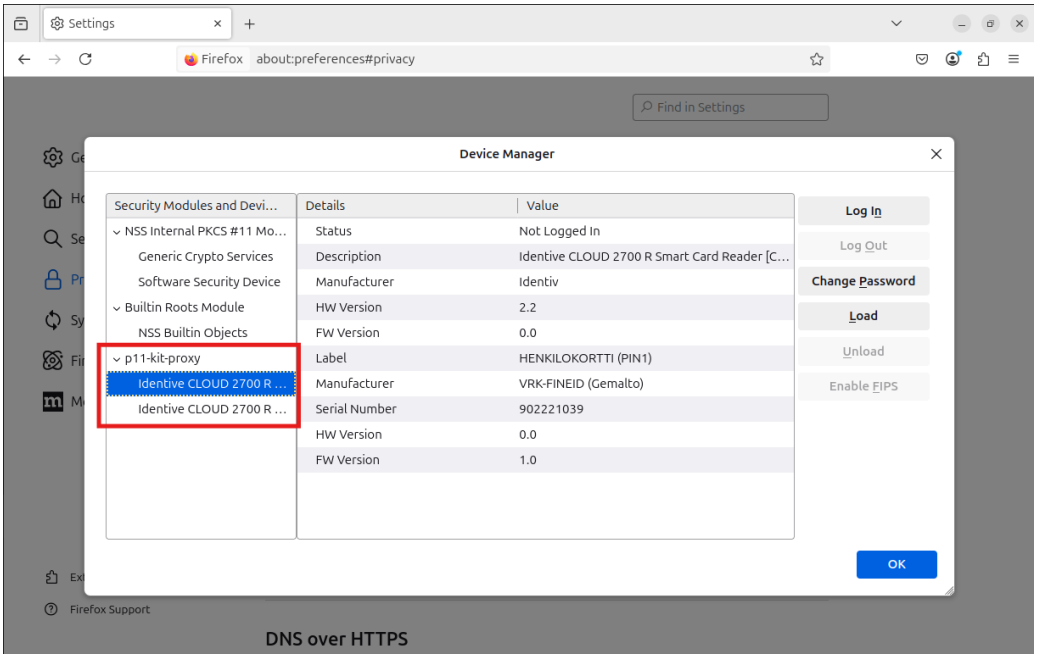

Figure 3: Firefox Device Manager

Alternatively, the p11-kit proxy can be loaded without the GUI by appending the lines *name=p11-kit-proxy* and *library=p11-kit-proxy.so* to *~/.mozilla/firefox/*.default-release/pkcs11.txt* after an empty line.

4.2.2. Chrome (and other NSS-compatible browsers)

Google Chrome and some other browsers use the Network Security Services (NSS) shared database to access PKCS #11 modules. Using Atostek ID PKCS #11 module with these browsers requires registering it to the NSS database of the current user.

The registration is done with the following command (the database path may vary by browser):

Debian/Ubuntu: *modutil -add "Atostek ID" -libfile /usr/lib/Atostek-ID-PKCS11.so -dbdir sql:$HOME/.pki/nssdb -mechanisms FRIENDLY*
RedHat: *modutil -add "Atostek ID" -libfile /usr/lib64/Atostek-ID-PKCS11.so -dbdir sql:$HOME/.pki/nssdb -mechanisms FRIENDLY*