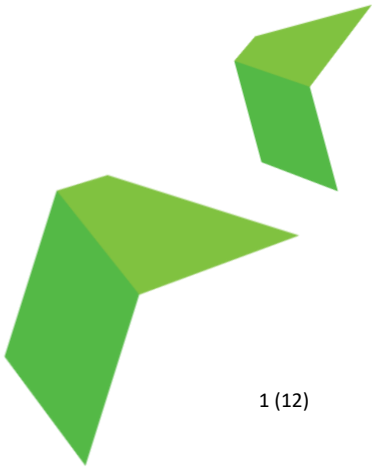
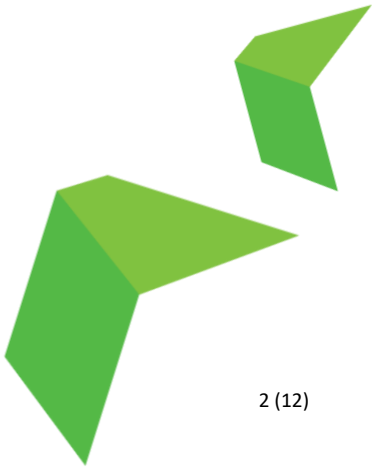
Atostek ID

Release Notes



Contents



1 Information about Atostek ID version numbers

Atostek ID releases are versioned using a four-number format. With each release, at least one of these digits is incremented to ensure the version number uniquely distinguishes it from previous releases. This numbering scheme reflects the significance of the changes in each release. Beta releases are specifically indicated by the term 'beta'.

The first number represents major updates, such as substantial modifications to application interfaces or the introduction of significant new features. The second number denotes intermediate changes, including new functionalities, enhancements to existing interfaces, or major fixes. The third digit is reserved for minor updates, such as small repairs or incremental improvements. Typically, the second and third digits undergo the most frequent changes between releases. The fourth digit is assigned to minor corrections arising from issues identified during acceptance testing.

2 General notes

This section provides an overview of each release of Atostek ID, highlighting the key new features and improvements in a user-friendly manner. For those interested in a deeper understanding of the updates, detailed technical descriptions are available in Chapter 2 (Technical notes).

2.1 Atostek ID 4.0.1.0

Release date: 4.10.2024

Summary: This is the second beta release before the first official release of Atostek ID as DVV's card reader software. Please note that we are still working on adding more features, which we plan to introduce later this year. You can find a list of the current features and any known issues below and with more details in Chapter 2. Atostek ID is built upon the previous ERA SmartCard software by Atostek Oy. If you have used ERA SmartCard in the past, it is important to note that Atostek ID has not completely absorbed all of ERA SmartCard's features yet. We aim to have a fully combined product by the end of the year.

Key features:

- Support for macOS 15 Sequoia
- Updated Atostek ID installation guide for Linux (Debian)
- Support for older citizen cards (Gemalto MultiApp)
- Fixes to *Readers and cards* view
- Fixes for organizational cards in *Diagnostics* view
- Activation is prompted when an inactive card is inserted into the reader
- Improvements to reader and card state indicators
- Full implementation of SCS interface version 1.2
- Atostek ID writes error messages to system log
- Atostek ID log file location can be changed
- Signed Atostek ID Minidriver for Windows use
    - mTLS authentication
    - Email encryption and signatures with Outlook
    - Windows logon with smart card
    - PDF signatures using Adobe and PDF xchange
- AD registration service for organizations (Windows logon)
- PKCS#11 module for Windows, macOS and Linux
- Atostek ID Toolkit

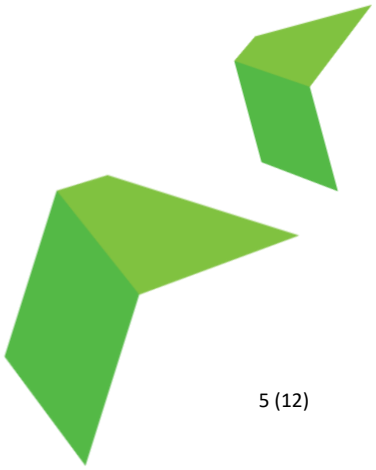
2.2 Atostek ID 4.0.0.0

Release date: 1.8.2024

Summary: This is the first beta release before the first official release of Atostek ID as DVV's card reader software. Please note that we are still working on adding more features, which we plan to introduce later this year. You can find a list of the current features and any known issues below and with more details in Chapter 2. Atostek ID is built upon the previous ERA SmartCard software by Atostek Oy. If you have used ERA SmartCard in the past, it is important to note that Atostek ID has not completely absorbed all of ERA SmartCard's features yet. We aim to have a fully combined product by the end of the year.

Key features:

- Atostek ID application for Windows, MacOS, Debian and Red Hat
    - For all the versions supported by the operating system vendor
- Supported languages: Finnish, Swedish, English
- Support for all DVV's currently used card types and card generations with RSA and ECC keys
    - Citizen Certificate, Organisation cards, Cards for social welfare and healthcare
- Card can be activated, and PIN codes changed/unlocked
- Support for all PC/SC suitable readers
- Support for multiple readers and cards at the same time
- Support for excluding readers and card types
- Card certificates are loaded to the certificate store (Windows)
- Information about cards and readers is shown in the application
- Card certificates can be opened and saved to computer
- Supported browsers: Microsoft Edge, Firefox, Safari, Google Chrome
- SCS interface version 1.1
- Partial implementation of PKCS#11 module
- Partial implementation of Windows Minidriver
- Support for automatic launch of application
- Support for updating application from application itself
- Logging and possibility to turn off logging
- Software diagnostics and support for testing PIN-codes and signing
- Installation manuals and user manuals



3 Technical notes

In this section, new features, fixes, and identified deficiencies are described from a more technical perspective. For instance, regarding more extensive interface descriptions, references can also be made to separate appendices at the end of this document.

3.1 Atostek ID 4.0.1.0

Release date: 4.10.2024

Features:

- Fixes for the HTTPS communication issues with the SCS interface that arose following the upgrade to macOS 15 Sequoia. Now, Mac users will need to enter their Keychain password to allow applications to access the HTTPS certificate stored in the login Keychain.

- The installation guide for Atostek ID on Linux has been updated, with specific enhancements for the Debian setup. The Atostek ID .deb package does not install all the necessary components automatically, so users will need to perform some steps manually. This update addresses the previously reported problems with the Debian installation of Atostek ID. We're planning to refine the installation package in the future to automate most of the setup process.

- Support for older citizen cards (Gemalto MultiApp cards)
    - Activation, PIN changing and unlocking, signature tests, signatures with SCS interface, *Readers and cards* view

- Fixes for *Readers and cards* view and *Diagnostics* view
    - Empty readers are shown correctly in the view
    - NFC readers are shown correctly in the view
    - Fixed the issues related to fetching the version information from organization cards
    - Citizen card certificates are shown correctly

- Activation is prompted when an inactive card is inserted into the reader

- The application icon has been updated to display the status of the reader and card using various colors. Additionally, the icon now shows if the card reading process is active

- Full implementation of SCS interface version 1.2
    - Support for transactions communication mode
    - Support for *RSASSA-PSS* signature algorithm
    - Support for signature type *cms*
    - Support for signature type *cms-pades*

- Atostek ID now logs error-level messages to the system log on Windows, macOS, and Linux platforms

- The location of Atostek ID application's log file can be changed by modifying the .ini configuration file

- WHQL signed Atostek ID Minidriver
    - Support for SOTE and organizational cards (both RSA and ECC certificates)
        - mTLS authentication
        - Email encryption and signatures with Outlook
        - Windows logon with smart card

        - PDF signatures using Adobe and PDF xchange
    - Atostek ID Minidriver is installed automatically during Atostek ID Windows installation
    - More information in Minidriver – Atostek ID

PKCS#11 – Atostek ID

- AD registration service for organizations (Windows logon)
    - Administrator tools
    - Receives calls from Atostek ID Minidriver to pair card with user's altSecurityIdentities attribute in AD
        - Note: There is separate Atostek ID Minidriver for this (no WHQL signature, signed version will be available in the next release)

- PKCS#11 module for Windows, macOS and Linux
    - Fixes to the module to ensure it can be installed on various applications, such as Adobe and Firefox.
    - Enhanced support for additional interface functions (More information in PKCS#11 – Atostek ID)
    - Note: PKCS#11 modules are not yet installed automatically during Atostek ID installation. Load them separately from DVV's site.

- Atostek ID Toolkit

- Atostek ID integration guide for SCS, PKCS, Minidriver and Toolkit integration

Deficiencies:

- The application still has some dependencies on outdated libraries (this will be fixed in the next release)
- It is not yet possible to configure app settings during installation on Debian and Red Hat systems
- There is not yet support for DVV's new card generation (Idemia Cosmo X) as the test cards are not yet available
- It is not yet possible to manually check the certificate's validity (OCSP and CRL requests)
- Card certificates are not yet loaded to operating system's certificate store on MacOS, Debian or Red Hat
- Atostek ID application does not yet support citizen cards with NFC readers
- PKCS#11 module
    - Only SOTE RSA cards are supported
    - During the installation of Atostek ID, modules are not saved to the device by default. You must download them separately from the DVV website
    - There is not a 32-bit version for Windows available yet
    - Some of the main ways to use the software haven't been officially tested, even though many interface functions are already in place.
    - NFC readers are not yet supported
    - Only part of the necessary functions is implemented. More detailed information in PKCS#11 – Atostek ID
- Windows Minidriver and AD registration service
    - To test the card pairing to AD user you must use Atostek ID Minidriver with test signature as the pairing feature is not yet in the WHQL signed Atostek ID Minidriver (that is installed automatically during Atostek ID Windows installation). Please load this Minidriver separately from DVV's site to test the pairing functionality.
    - There is not a 32-bit version available yet
    - NFC readers are not yet supported
    - Citizen cards are not yet supported
- mTLS authentication with card is not yet supported with macOS, Debian or Red Hat
- The app is not automatically launched on Debian or Red Hat
- There is not yet a 32-bit version available for Atostek ID Windows use
- User manuals and installation guides will be improved

Planned features and improvements for the next releases:

- No dependencies on outdated libraries
- App settings can be configured during installation on Debian and Red Hat systems
- Support for checking certificate validity manually (OCSP and CRL requests)
- Card certificates are loaded into operating system's certificate store on MacOS, Debian and Red Hat
- Atostek ID application supports NFC readers with citizen cards
- SCS interface version 1.3
- Implementations for the remaining necessary functions for the PKCS#11 module.
    - Support for organizational and citizen cards
    - Automatic installation during Atostek ID installation
    - 32-bit version
    - NFC readers
    - Implementation for remaining functions and official testing of the main use cases
- Implementations for the remaining necessary Minidriver functions and features
    - Citizen cards
    - 32-bit version
    - NFC readers
    - AD registering in WHQL signed package
- MacOS Token Driver
- Customized PIN code dialogs for Minidriver, TokenDriver and PKCS usage instead of operating system's default dialogs
- Improvements to app launch
- Improvements to settings dialog
- PDF signing with a card using the Atostek ID application
- Mifare operations (reading and writing)

3.2 Atostek ID 4.0.0.0

Release date: 1.8.2024

Features:

- The application's name has been changed to Atostek ID in the user interface as well as in installation packages, files, and file locations. However, the previous name (ERA SmartCard) still appears, for example, in custom protocols such as erasmartcard:// and erasmartcardpost://.

- Atostek ID application for Windows, MacOS, Debian and Red Hat
    - For all the versions supported by the operating system vendor
    - Windows: SCS-interface can be used in Citrix environment with Virtual Loopback IP
    - MacOS: Both Intel and ARM Macs are supported
    - Windows and MacOS: Both UI installation and quiet installation from terminal are supported
    - Debian and Red Hat: Installation from terminal is supported

- Supported languages: Finnish, Swedish, English
    - Installer packages automatically use the language of the operating system (or English if selected language is not supported by packages)
    - Language can be changed during installation (Windows, MacOS) or from settings after installation

- Suppport for all DVV's currently used card types and generations with RSA and ECC keys
    - Citizen Certificate, Organisation cards, Cards for social welfare and healthcare

- Card can be activated, and PIN codes changed/unlocked

- Support for all PC/SC suitable readers
    - Reader drivers are usually already installed to operation system. If reader driver cannot be found, please download and install the needed driver from the reader manufacturer's website.

- Support for multiple readers and cards at the same time

- Support for excluding readers and card types
    - Readers can be excluded by adding the name of the reader to application's configuration file. See user manual for more information.
    - Card types can be excluded by adding the name of the card type to application's configuration file. See user manual for more information. Card type names are supported in every supported language (fi, en, sv).
    - When excluded the reader or card is not shown in dialogs or given as an option to be used in card operations.

- Card certificates are loaded to the certificate store when the card is inserted to the reader and deleted when the card is removed from the reader

- Information about cards and readers is shown in separate view

- Card certificates can be opened and saved to computer from *Readers and cards* dialog

- Supported browsers for mTLS and SCS use: Microsoft Edge, Firefox, Safari, Google Chrome

- SCS interface version 1.1
    - The SCS interface cannot be used simultaneously with DigiSign's SCS interface as they use the same port
    - SCS CA certificate is generated and set trusted during installation.

- Partial implementation of PKCS#11 module
    - More information in PKCS#11 – Atostek ID

- Partial implementation of Windows Minidriver
    - More information in Minidriver – Atostek ID

- Support for automatic launch of application

- Support for updating application from application itself

- Logging and possibility to turn off logging

    - Default logging levels are INFO, WARNING and ERROR. Debug logging can be allowed from settings
    - Logging can be completely disabled from settings

- Software diagnostics and support for testing PIN-codes and signing
    - Authentication and signing can be tested with SHA-1, SHA-256 and SHA-512 algorithms

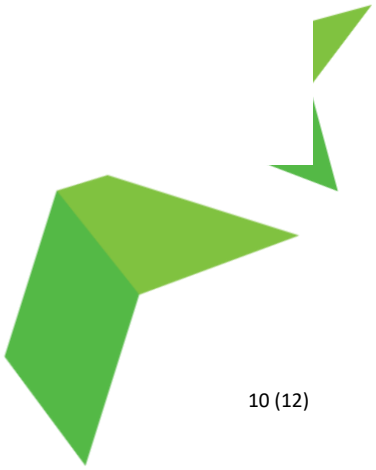
- Installation manuals and user manuals

Deficiencies:

- The application still has some dependencies on outdated libraries
- It is not yet possible to configure app settings during installation on Debian and Red Hat systems
- There is not yet support for DVV's new card generation (Idemia Cosmo X) as the test cards are not yet available
- It is not yet possible to manually check the certificate's validity (OCSP and CRL requests)
- The application does not yet automatically prompt user with card activation if non-activated card is inserted to reader
- Card certificates are not yet loaded to operating system's certificate store on MacOS, Debian or Red Hat
- The *Readers and cards* dialog does not yet show citizen certificates completely correctly
- SCS version 1.2
    - Transactions communication is not yet supported
    - Signature algorithm RSASA-PSS is not yet supported
    - Signature types cms and cms-pades are not yet supported
- PKCS#11 module
    - Only available for Windows at this point
    - Only part of the necessary functions is implemented. More detailed information in PKCS#11 – Atostek ID
- Windows Minidriver and AD registration service
    - Minidriver does not yet have WHQL signature
    - AD registration service is not yet published
    - Only part of the necessary functions is implemented. More detailed information in Minidriver – Atostek ID
- mTLS authentication with card is not yet supported
- The app is not automatically launched on Debian or Red Hat

Planned features and improvements for the next release:

- No dependencies on outdated libraries
- App settings can be configured during installation on Debian and Red Hat systems
- Support for checking certificate validity manually (OCSP and CRL requests)
- The user is prompted to activate the card upon insertion into the reader if it has not been activated already
- Improvements to *Readers and cards* view in the application
- Improvements to icons to indicate the app state
- Card certificates are loaded intoto operating system's certificate store on MacOS, Debian and Red Hat
- SCS interface (version 1.2) fully implemented
- Implementations for the remaining necessary Minidriver functions and a separate AD registration service for Windows AD login using the card. WHQL signature for Atostek ID Minidriver.
- Implementations for the remaining necessary functions for the PKCS#11 module.
- MacOS Token Driver
- Customized PIN code dialogs for Minidriver, TokenDriver and PKCS usage instead of operating system's default dialogs
- Improvements to logging and app launch
- Improvements to settings dialog
- PDF signing with a card using the Atostek ID application
- Toolkit for integrations (SCS interface)
- Mifare operations (reading and writing)

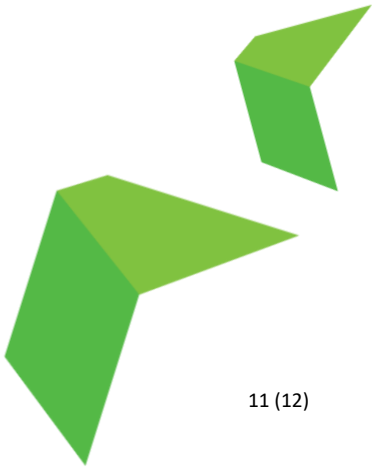


4 Appendix

4.1 PKCS#11 – Atostek ID

Note that some the functions of the PKCS#11 interface are not applicable to FINEID cards. The following functions are already implemented in the most recent release:

- Initialize
- Finalize
- GetInfo
- GetFunctionList
- GetInterfaceList
- GetInterface
- FindObjectsInit
- FindObjects
- FindObjectsFinal
- GetAttributeValue (partially)
- SetAttributeValue (partially)
- GetFunctionStatus
- CancelFunction
- OpenSession
- CloseSession
- CloseAllSessions
- GetSessionsInfo
- Login (PIN2 slot not implemented)
- Logout
- SignInit
- Sign
- SignUpdate
- SignFinal
- VerifyInit
- Verify
- VerifyUpdate
- VerifyFinal
- GetSlotList
- GetSlotInfo
- GetTokenInfo
- WaitForSlotEvent
- GetMechanismList
- GetMechanismInfo
- EncryptInit
- Encrypt
- EncryptUpdate
- EncryptFinal
- DecryptInit
- Decrypt
- DecryptUpdate
- DecryptFinal



4.2 Minidriver – Atostek ID

Note that some of the functions of the Windows Minidriver are not applicable to FINEID cards. The following functions are already implemented in the most recent release:

- CardAcquireContext
- CardDeleteContext
- CardAuthenticatePin
- CardDeauthenticate
- CardAuthenticateEx
- CardReadFile
- CardGetfileInfo
- CardEnumFiles
- CardQueryFreeSpace
- CardQueryCapabilities
- CardGetContainerProperty
- CardGetProperty
- CardGetContainerInfo
- CardRSADecrypt
- CardConstructDHAgreement
- CardDeriveKey
- CardDestroyDHAgreement
- CardSignData
- CardQueryKeySizs