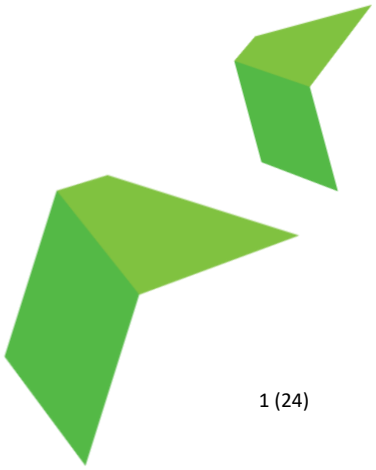
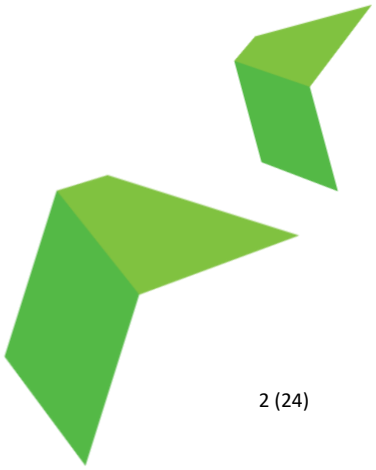
Atostek ID

Release Notes



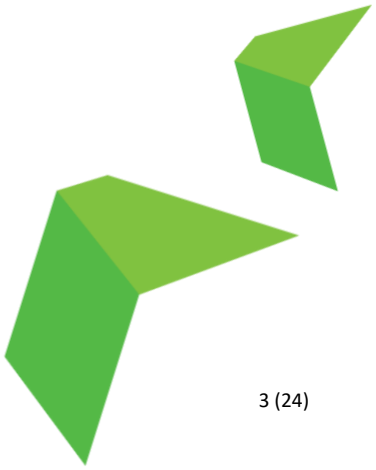
Contents



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 4.4.0.0

Release date: 19.9.2025

Package hashes:

- Windows (.msi): 08eafe3521b39d8a1ac57b344b6f1d57fa311a90aa5d9feeb0482225bc77fdb2
- macOS (.pkg): 1cc60b0a5920f908d53f54845b7e59d8b9bdcf4ee8190f7f44a242b40ac0b724
- Debian (.deb): 6dd0204f2af63963ae5cbaec9ecc85fc43cf430ace4de194e1055d071d43b326
- Red Hat (.rpm): 4834146bcb0b4d3b80351668c7eced31f0b5bc2620ec39ec9c1de86c97d5ade3

Summary: Atostek ID version 4.4.0.0 includes both new features and bug fixes. The new features address the needs and requests of users and organizations, while the bug fixes resolve the most urgent issues and improve the application's stability. This release also includes information security updates.

Key features:

- Desktop application
    - Support for using the Windows registry instead of a configuration file to manage application settings
    - Support for wildcards when setting ExcludedReaders
    - Support for macOS version 26
    - Fixed issues related to certificates being removed from the macOS keychain
    - SCS interface version 1.3 is now the default instead of version 1.2
    - Bug fixes
    - Information security improvements
    - Support for temporary card personalization for organizations
        - Note: Personalization of temporary cards with AID using the Vartti system is not yet in production. DVV will provide information about the production rollout later this year
- Minidriver module for Windows
    - Fixed crash issues with mTLS authentication (e.g., suomi.fi) when using newer Firefox versions on Windows
- AD registration service (for organizations)
    - Support for creating a database for pairings
    - Support for running ADRS as a Windows Service
    - Support for pairing with a registration number (available by request)
    - Bug fixes
- Updated user manuals and installation guides

2.2 Atostek ID 4.3.1.0

Release date: 13.6.2025

Package hashes:

- Windows (.msi): 925461a54a9c9e11de4d5975d95081dad6574886826d2e67e3f475ef889e73c1
- macOS (.pkg): 4530bfabd7305b6d5e13c86f9be71e191bcb21f611e376162b68448d76e73454
- Debian (.deb): ddc6566efe71f8d4ff1ab5bab15af96f97b0d30ec5a43bca56c562f945de1c30
- Red Hat (.rpm): 33c189212bd19b975889909b67fcf8e693fa59715bcc3c167a5e0416681c4f57

Summary: Atostek ID 4.3.1.0 release contains both the support for Thales v5.1 citizen cards and further improvements based on customers' feedback after the release of version 4.3.0.0. Card operations have been optimized and refactored resulting in improved performance and stability especially in long time use. Information security fixes are also included in this release.

Key features:

- Desktop application
  - Support for Thales MultiApp v5.1 citizen cards
  - Fixed odd side effects of long time use on Windows
  - Switched to a self-generated and signed HTTPS certificate for erasmartcard.ehoito.fi interface
- Minidriver module for Windows
  - Support for Thales MultiApp v5.1 citizen cards
  - Added support for forced installation for customer environments
- TokenDriver module for macOS
  - Support for Thales MultiApp v5.1 citizen cards
- PKCS#11 module for Windows, macOS, and Linux
  - Support for Thales MultiApp v5.1 citizen cards
  - Enhanced support for concurrency throughout the module and optimized commands

2.3 Atostek ID 4.3.0.0

Release date: 11.4.2025

Package hashes:

- Windows (.msi): 7003a231123dfabc4f6029f9b056a9ddb209d4840fac88471142b68aea7c872a
- macOS (.pkg): c276f8c76b2557e73ca53f5cff46f5104d3deecab5d2ee235cf0d482f546414a
- Debian (.deb): fc753b03e171b39e28bd9f85a43d0986409dbad6d72801cd1d63762a6f444f73
- Red Hat (.rpm): f1659579e9209d2d840deccc90b1899069ac77a9af16552aa6e52836ad3e3b81

Summary: Atostek ID 4.3.0.0 release contains the most important fixes and improvements to the application based on customers' feedback after the release of version 4.2.1.0. Major issues with Minidriver and PKCS#11 modules have been fixed in version 4.3.0.0. The focus has been in making workstation login and mTLS authentication more stable. In addition, the usability of Atostek ID has been improved. Version 4.3.0.0 has gone through a third-party information security audit, and no major information security threats were found.

Key features:

- Desktop application
  - Produced a universal binary from the software suite for the macOS platform
  - Updated the root certificates from DVV that are installed during setup
  - Made security fixes to /ForwardMessage request in the erasmartcard.ehoito.fi interface
  - Corrected the CMS-PAdES signature in the SCS interface
  - Made corrections to the event monitoring of /Login request in the erasmartcard.ehoito.fi interface
  - Forced focus to always be on the PIN code entry field in PIN query windows
  - Forced Atostek ID dialogs to always be on top
  - Fixed activation errors with Atostek test cards

    - Corrected errors in activation when using multiple cards simultaneously
    - Updated software user guides and installation instructions where guidance was missing
    - Support for Microsoft AVD environments (SCS interface)
- Minidriver module for Windows
    - Fixed the 32-bit driver version to install automatically with the rest of the installation
    - Disabled the customized PIN query window during Windows workstation login
    - Added necessary dependencies to install directly with the rest of the installation
    - Added version information for the driver
- TokenDriver module for macOS
    - Improvements to workstation login
- PKCS#11 module for Windows, macOS, and Linux
    - Enhanced support for concurrency throughout the module and optimized commands
    - Implemented C_DeriveKey function for ECC cards
    - Reviewed parameter values and made corrections as needed
    - Fixes to Cosmo X cards' mTLS authentication

2.4 Atostek ID 4.2.1.0

Release date: 14.2.2025

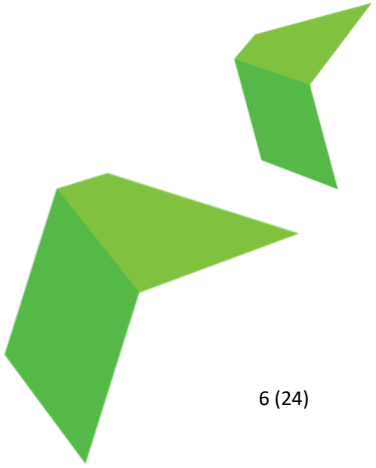
Package hashes:

- Windows (.msi): d99478c77cdbcb1372d9eed0fbf6d49ab2f23341704307d880e6f7223ce34381
- macOS (.pkg): 7bd20e71e8406c797592a4f979951e86581e06e5426c7db835964d5d0e5c5c86
- Debian (.deb): d9d80be53478f002bb704be16528c353da4aabba5d06c7d7982510cbb0cf3f90
- Red Hat (.rpm): d1dc858d1bb963fed3b894e15ad1c9a939d444e67c691a9f1fc6ae93ba034042

Summary: This is the second official release of Atostek ID as DVV's card reader software. It contains several fixes and improvements to the application. Atostek ID is built upon the previous ERA SmartCard software by Atostek Oy. This version of Atostek ID includes all the features of ERA SmartCard. This means that all users of ERA SmartCard on Windows and macOS should transition to using Atostek ID from this point forward. We are scheduled to release one final version of ERA SmartCard for Windows and macOS (version 3.1.0.0) before the end of March 2025. This release is intended to be the last update for ERA SmartCard. Its built-in certificate will remain valid until March 2026.

Key features:

- Support for DVV's new Idemia Cosmo X cards (SOTE and organization cards)
- Added ability to check card's validity manually (*Readers and cards* view)
- Added support for different document signing types (*Sign document* view)
- Compatibility with signatures from DigiDoc software
- Added ability to read and write card's Mifare tag using NFC-connection
- Fixes required by the security audit
- Fixes to PDF signing with Adobe Acrobat software
- Fixed application crashing when no readers were connected
- Fixes to modules (Minidriver, TokenDriver, PKCS)
- SCS certificates are now generated under ProgramData folder
- Increased the time limit for the card activation dialog
- Improvements to PIN-dialogs
- Improvements to wordings
- Atostek ID Toolkit for macOS and Linux
- Bug fixes



2.5 Atostek ID 4.1.1.0

Release date: 20.11.2024

Summary: This is 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 included all of ERA SmartCard's features yet. We aim to have a fully combined product by the end of the year.

Key features:

- All the features from the previous test and beta releases (AID versions 4.0.0.0 and 4.0.1.0)
- Fixes for known issues
- Compatibility with NFC readers for citizen cards in the Atostek ID application
- Support for SCS version 1.3
- Enhanced logging capabilities and the automatic launch feature of the Atostek ID application
- Ability to sign PDF documents within the Atostek ID application (PAdES)
- Option to set a timestamp server address for PDF signatures
- Updated installation and user guides
- Updates to old dependencies within the Atostek ID application
- Atostek ID TokenDriver for macOS use
- Improvements to Atostek ID PKCS11 module

2.6 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

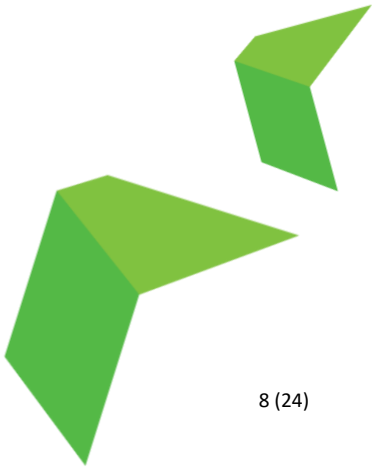
2.7 Atostek ID 4.0.0.0

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 4.4.0.0

Release date: 19.9.2025

Features:

- Desktop application
  - Support for using the Windows registry instead of a configuration file to manage application settings
    - Use the CONFIGUREREGISTRY setting during command line installation. See the installation guide and user manual for details.
  - Added support for wildcards in the ExcludedReaders setting. ExcludedReaders can now also be set as an installation parameter in command line installation. See the installation guide and user manual for more information.
  - Support for macOS version 26
  - Fixed issues related to certificates being removed from the macOS keychain
    - Now, installing or uninstalling Atostek ID only removes Atostek ID certificates from the keychain, without affecting other certificates.
  - SCS interface version 1.3 is now the default instead of version 1.2
  - Versions 1.1 and 1.2 are still supported but need to be specified explicitly in requests.
  - Bug fixes
    - Fixed app crashes after long sleep periods or after frequently changing cards in readers.
    - Fixed an issue where multiple AID instances appeared when using erasmartcard protocols before card has been read to cache.
    - The {PORT} placeholder is now case-insensitive when used with erasmartcard protocols or custom commands.
    - The AllowedBrowserlessAndForwardDomains setting is now supported as a command line installation parameter in Windows. See the installation guide and user manual for more details.
    - Fixed the erasmartcard protocol on macOS.
    - Fixed a problem where the application could crash randomly during certificate validity checks (OCSP/CRL).
  - Information security improvements
  - Support for temporary card personalization for organizations
    - Note: Personalization of temporary cards with AID using the Vartti system is not yet in production. DVV will provide information about the production rollout later this year. Instructions for using Atostek ID for temporary card personalization will also be delivered later this year.
- Minidriver module for Windows
  - Fixed crash issues with mTLS authentication (e.g., suomi.fi) when using newer Firefox versions on Windows
- AD registration service (for organizations)
  - Support for creating a database for pairings. See ADRS user guide for more information.

    - Support for running ADRS as a Windows Service. See ADRS user guide for more information.
    - Support for pairing with a registration number instead of SAN
        - This feature is available only by direct request and contract from Atostek
    - Fixed a bug in the ADRS_LDAB_BASE_OBJECT setting
- Updated user manuals and installation guides

3.2 Atostek ID 4.3.1.0

Release date: 13.6.2025

Features:

- Desktop application
    - Support for Thales MultiApp v5.1 citizen cards
    - Fixed odd side effects of long time use on Windows
        - The following were reported and could no longer be reproduced with version 4.3.1.0
            - Task manager freezes after approximately one hour of use
            - Upon logging out, Windows warns that other users might lose progress
            - Disturbances with Skype
    - Switched to a self-generated and signed HTTPS certificate for erasmartcard.ehoito.fi interface
        - Each installation generates its own self-signed HTTPS certificate for erasmartcard.ehoito.fi interface.
    - Improved caching so that PIN dialogs appear faster in login and sign
    - Fixed fetching a longer signature from the card
- Minidriver module for Windows
    - Support for Thales MultiApp v5.1 citizen cards
    - Added support for forced installation for customer environments
        - Even if the system does not recognize reader in Device Manager, Atostek ID minidriver is installed in the Windows registry and in needed locations.
    - Fixed APDU errors with certain readers
- TokenDriver module for macOS
    - Support for Thales MultiApp v5.1 citizen cards
- PKCS#11 module for Windows, macOS, and Linux
    - Support for Thales MultiApp v5.1 citizen cards
    - Enhanced support for concurrency throughout the module and optimized commands
    - Fixed faulty Windows 32-bit module in the previous release
    - Improved logging

Known deficiencies: See 6.3 Known deficiencies of the software

3.3 Atostek ID 4.3.0.0

Release date: 11.4.2025

Features:

- Desktop application
    - Produced a universal binary from the software suite for the macOS platform
        - macOS with ARM processors no longer need Rosetta to be compatible
    - Removed expired VRK Gov. Root CA from installation
        - thumbprint: faa7d9fb31b746f200a85e65797613d816e063b5

  - Fixed information security audit remarks in /ForwardMessage request in the erasmartcard.ehoito.fi interface
  - Corrected the CMS-PAdES signature in the SCS interface
    - SignerInfo's digestEncryptionAlgorithm corresponds now to RSA or ECC depending on the card in use
  - Made corrections to the event monitoring of /Login request in the erasmartcard.ehoito.fi interface
    - Implementation follows now the erasmartcard.ehoito.fi HTTP interface specification when NotificationsEnabled is used
  - Forced focus to always be on the PIN code entry field in PIN query windows
  - Forced Atostek ID dialogs to always be on top
  - Fixed activation errors with Atostek test cards
  - Corrected errors in activation when using multiple cards simultaneously
  - Updated software user guides and installation instructions where guidance was missing
  - Support for Microsoft AVD environments (SCS interface)
    - This requires a separate proxy component at the organizational level. You can contact Atostek if you are interested in arranging the use of Microsoft's AVD environment in terms of the SCS interface in your organization. This support is offered only through a separate agreement.
- Minidriver module for Windows
  - Fixed the 32-bit driver version to install automatically with the rest of the installation
    - Especially .NET projects utilizing Windows CryptoAPI seemed to use 32-bit minidriver
    - 64-bit driver is installed under C:\Windows\System32 folder and 32-bit driver under SysWOW64 folder
    - Registry keys for both drivers are written in Windows registry
      - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards (64-bit driver)
      - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Calais\SmartCards (32-bit driver)
  - Disabled the customized PIN query window during Windows workstation login
    - Using custom PIN query window during only those use cases where system would normally prompt a separate PIN query window
  - Added necessary dependencies to install directly with the rest of the installation
    - In previous versions, missing runtime libraries msvcp140.dll and vcruntime140.dll needed to be downloaded separately
  - Added version information for the driver
- TokenDriver module for macOS
  - Improvements to workstation login
    - Citizen cards (Gemalto and Thales)
    - ECC cards
- PKCS#11 module for Windows, macOS, and Linux
  - Enhanced support for concurrency throughout the module and optimized commands
  - Implemented C_DeriveKey function for ECC cards
  - Reviewed parameter values and made corrections as needed
    - REMOVABLE_DEVICE, HW_SLOT, WRITE_PROTECTED, LOGIN_REQUIRED, SECONDARY_AUTHENTICATION, C_GetTokenInfo SessionCount, C_GetTokenInfo utcTime ja SerialNumber
  - Fixes to Cosmo X cards' mTLS authentication

Known deficiencies: See 6.3 Known deficiencies of the software

3.4 Atostek ID 4.2.1.0

Release date: 14.2.2025

Features:

- Fixes for macOS and Linux use cases, especially PKCS and mTLS features that were missing from the previous release
    - macOS
        - mTLS authentication when using Thales citizen cards
        - mTLS authentication when using Safari and Firefox browsers
        - Log in to workstation with Thales citizen cards
        - Signing and mail encryption/decryption with Thales citizen cards in Apple Mail
    - Linux
        - mTLS authentication with any of the supported card types when using Chrome or Firefox browsers
        - Log in to workstation with Thales citizen cards
        - Signing and mail encryption/decryption with Thales citizen cards in Thunderbird
- Support for Idemia Cosmo X cards (SOTE and organization cards)
    - Support for each module: Atostek ID application, Atostek ID Minidriver, Atostek ID TokenDriver and Atostek ID PKCS modules (Windows, macOS, Debian, Red Hat)
    - Support for both RSA and ECC cards
- Added ability to check card's validity date from the card's certificate and certificate revocation status from OCSP and CRL lists (*Readers and cards* view)
- Added support for ASiC-E, CAdES (ASiC-E), XadES and JAdES signatures (*Sign document* view)
    - Signature form: detached signatures
- Compatibility with ASiC-E DigiDoc signatures made using Estonian ID-software
- Added ability to read and write card's Mifare tag using NFC-connection
    - This feature is enabled from application's *Settings* view
    - It is possible to read all the 16 sections of the Mifare tag. It is possible to write to any of the 16 sections of the tag that allow writing.
- Fixes required by the security audit. These fixes are under audit during February 2025. Audit report will be available after that.
- Smaller fixes to PDF signing with Adobe Acrobat
- Fixed application crashing on some systems when there was no reader connected when the application was started (libstdc++-6 error)
- Fixed application crashing when Atostek ID is missing permission to write to the log file
- Fixed C_GetSlotList (PKCS) to also return the readers that do not have cards and to react correctly when card is inserted to reader or removed from the reader
- SCS certificates are now generated under C:\ProgramData on Windows to avoid problems with Users folder (C:\Users\<user> \AppData\Local\Atostek Oy\Atostek ID). This problem occurred for example on Windows 11 Pro 22H2 (Finnish installation).
- Improvements to PIN-dialogs:
    - Add scrollbar so that the data to be signed does not widen the PIN dialog too much
    - Show the data to be signed in a more reasonable way so that there are no confusing binary characters, but instead the data is either plain text or base64 encoded
    - Increase the time limit for the card activation dialog
- Improvements to wordings
    - Change card certificate expiration date announcement to be in past tense if the card has already expired
    - Change forward slashes to backslashes in file paths on Windows when signing documents
- Atostek ID Toolkit for macOS and Linux as a dynamic .NET library (requires .NET to run)
- Support for SCS interface in AVD environments (requires separate proxy component)
- Customized pin dialog (Atostek ID pin dialog) for modules (Minidriver, TokenDriver, PKCS)

Known deficiencies: See 6.3 Known deficiencies of the software

3.5 Atostek ID 4.1.1.0

Release date: 20.11.2024

Features:

- Removed dependencies to outdated components.
- Support for setting application language in Linux command line installation.
- Support for NFC with citizen cards.
- Support for PDF signing with a card using the Atostek ID application and for configuring a timestamp service.
- SCS interface version 1.3 (version 1.2 still the default version).
- MacOS TokenDriver for mTLS, PDF signing and macOS login.
- Improvements to user guides and installation guides.
- Atostek ID Minidriver
    - 32-bit version available for Windows
- PKCS#11 module for Windows, macOS and Linux
    - Fixes and improvements
    - Support for all card types
    - 32-bit version available for Windows

Deficiencies:

- 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)
- PKCS#11 module
    - Newer citizen cards are not yet fully supported (Thales). Finding objects, verifying PIN codes and signing is supported. mTLS authentication (suomi.fi), macOS login or Apple Mail encryption are not yet supported).
    - mTLS authentication (suomi.fi) does not yet work on Linux
    - NFC readers are not yet supported
- Windows Minidriver and AD registration service
    - NFC readers are not yet supported
- There is not yet a 32-bit version available for Atostek ID Windows use

Planned features and improvements for the next releases:

- Support for checking certificate validity manually (OCSP and CRL requests)
- Implementations for the remaining necessary functions for the PKCS#11 module.
- Support for NFC readers for PKCS and Minidriver modules
- Customized PIN code dialogs for Minidriver, TokenDriver and PKCS usage instead of operating system's default dialogs
- Improvements to settings dialog
- Improvements to Linux installations
- Mifare operations (reading and writing)
- Support for CAdES, JAdES, XAdES and ASiC-E signatures

3.6 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
- 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)

3.7 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

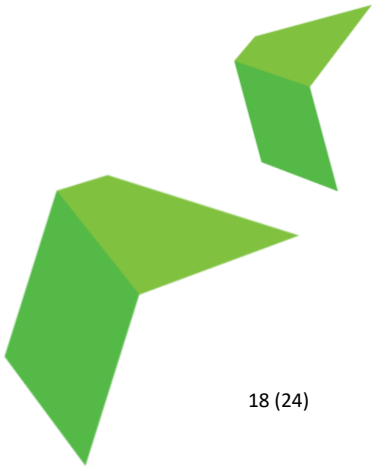
Deficiencies:

- 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 About testing

Each Atostek ID version undergoes thorough testing, both manual and automated, prior to its release. We ensure compatibility with various operating systems (Windows, macOS, Debian, and Red Hat). We also check that the software communicates effectively with different types of readers and cards. Additionally, we conduct regression testing on modules and interfaces to confirm that key features are functioning correctly. Our automated tests are comprehensive, utilizing physical cards and readers to verify card functionalities and employing virtualized cards to test the functionalities of the application's user interface. All new features are also comprehensively tested before release.

Any critical or major issues will be fixed before making a release. Despite our efforts, some issues may persist, these are detailed in section 6.3. Should you come across any bugs, we encourage you to reach out to us or the Digital and Population Data Services Agency. 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 also conducts its own acceptance testing for each new version before it is made available on their website.

We update this section with each new release to provide the latest information on our testing practices. Our testing tools and methods are subject to regular reviews and enhancements to continually refine our testing process.

Readers used for testing

- Identiv utrust 2700
- Identiv uTrust 4700
- Identiv uTrus 4701
- ACS ACR3901U
- ACS ACR38U
- Alcorlink Alcor Micro
- Lenovo SmartCard Wired Keyboard

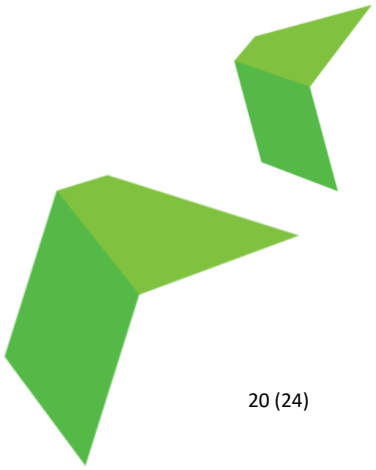
Card types used for testing

- Oberthur IAS-ECC
- Idemia Ideal Citiz 2.17i ID.me
- Idemia Cosmo X
- Gemalto MultiApp v.3.0
- Gemalto MultiApp v.4.2
- Thales MultiApp v.5.0
- Thales MultiApp v.5.1

Operating systems used for testing

- Windows 11 24H2
- Windows 11 23H2
- Windows 11 22H2
- Windows 10 22H2
- Windows Server 2022
- Windows Server 2019
- macOS Tahoe 26 (preview version)
- macOS Sequoia 15.6

- macOS 14 Sonoma 14.2
- macOS Monterey 12.7.6
- Debian 12
- Ubuntu 24.04
- Red Hat RHEL 9



5 Application dependencies

The Atostek ID application utilises various third-party components and dependencies to deliver its intended features. These dependencies are included with the installation of Atostek ID. We consistently monitor and update these components to ensure optimal performance and security. Below is a list of the third-party dependencies necessary for the proper functioning of Atostek ID. We update this list with each new release to reflect any changes

- Qt (6.5.3)
  - Qt6Core
  - Qt6Gui
  - Qt6Widgets
  - Qt6Network
  - Qt6PrintSupport
  - Qt6Xml
- Botan (2.19.4)
- OpenSSL (3.3.2)
  - libcrypto
  - libssl
- NSPR (4.25, for macOS 4.34.1) & NSS (3.51.1, for macOS 3.91)
  - freebl
  - nspr
  - nss
  - nssdbm
  - nssutil
  - plc
  - plds
  - smime
  - softokn
  - sqlite
- QPDF (11.9.1)
  - qpdf
  - libjpeg
  - libbz
- ZLIB (1.3.1)
  - zlib
  - libbz
- MINIZIP (13.1)
  - libminizip
  - libbz
- PCSC
  - winscard/pcsc-lite
- Other and compiler related
  - stdc++6
  - libgcc_s_seh
  - winpthread
  - eventprovider

6 Appendix

6.1 PKCS#11 – Atostek ID

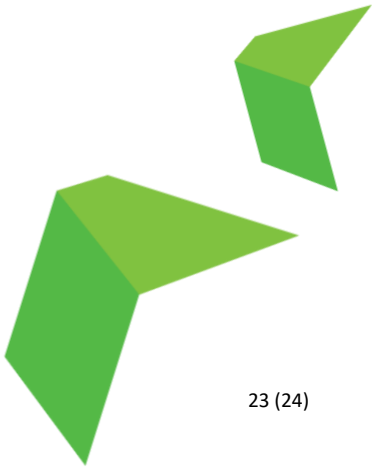
Note that some the functions of the PKCS#11 interface are not applicable to FINEID cards. The following functions are implemented in the most recent release:

- CancelFunction
- CloseAllSessions
- CloseSession
- Decrypt
- DecryptFinal
- DecryptInit
- DecryptUpdate
- DeriveKey
- Encrypt
- EncryptFinal
- EncryptInit
- EncryptUpdate
- Finalize
- FindObjects
- FindObjectsFinal
- FindObjectsInit
- GenerateKey
- GenerateKeyPair
- GetAttributeValue
- GetFunctionList
- GetFunctionStatus
- GetInfo
- GetInterface
- GetInterfaceList
- GetMechanismInfo
- GetMechanismList
- GetSessionsInfo
- GetSlotInfo
- GetSlotList
- GetTokenInfo
- InitPin
- Initialize
- InitToken
- Login
- Logout
- OpenSession
- SetAttributeValue
- SetPin
- Sign
- SignFinal
- SignInit
- SignUpdate
- Verify
- VerifyFinal
- VerifyInit
- VerifyUpdate
- WaitForSlotEvent

6.2 Minidriver – Atostek ID

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

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



6.3 Known deficiencies of the software

Below is a list of known issues with the software that have not been resolved yet. We aim to address these in future releases. Please note that the order of the list does not indicate the priority for fixing the issues. Fixes will be noted in the release notes of the release in which they are included. Also, this list does not cover any user suggestions for additional features or enhancements we have received.

- Atostek ID application
    - Dependency issues have been encountered with Linux installations. We are working to resolve these issues by ensuring all necessary dependencies are clearly listed for the installation process. In the meantime, users can manually resolve this problem by installing the required dependencies as outlined in the Atostek ID Linux Installation guide.
    - The custom PIN dialog provided by Atostek ID is not utilized on macOS 15 for mTLS authentication (suomi.fi), Adobe, and Apple Mail for encryption and signing activities, nor is it used for logging into the computer with a smart card. Instead, macOS 15 defaults to the system's built-in PIN dialog for these operations. For other versions of macOS, the Atostek ID custom PIN dialog is employed as usual.
    - Diagnostics dialog does not support changing cards without a restart
    - Trust Primo readers do not work with certain versions of macOS
- PKCS module
    - NFC readers are not yet supported.
    - The C_GetSlotList function causes problems when used together with the C_WaitForSlotEvent feature.
    - The module does not handle situations correctly when a card is removed from the reader during a read operation.
- Minidriver module
    - NFC readers not yet supported
    - Atostek ID PIN dialog raises LSA protection error in some systems. We are investigating this issue further. This appears to be caused by internet connection errors when the system tries to check the validity of the PIN library (CRL).